ultraviolet



WORLDBOOK

2026 EDITION

Current as of October 13, 2026

UltraViolet Cyber TIDE Team
tide@uvcyber.com

ABOUT THIS WORLDBOOK

NOTICE

Conditions, travel advisories, sanctions, and threat activity change quickly. This worldbook is provided for general awareness and does not constitute legal, security, or travel advice. Verify current conditions before making decisions. The worldbook is reviewed and reissued annually.

The Threat Intel Worldbook is built on the latest threat intelligence and open-source geopolitical intelligence, compiled and analyzed by the UltraViolet Cyber Threat Intelligence & Detection Engineering (TIDE) team.

Its purpose is to help security leaders, travel and risk teams, and the people they protect make informed decisions about operating, staffing, and traveling in each country. Each profile connects the geopolitical picture to the cyber picture: who is acting, what they are targeting, how that affects organizations, employees, and vendors, and what precautions to take.

Every country follows the same six sections: Country Overview, Geopolitical Landscape, Cyber Threats | Organizations, Cyber Threats | Individuals, State-Sponsored Cyber Threats, and Cyber Travel Considerations. Countries appear in alphabetical order, and names and recognition follow U.S. government practice.

How to read the ratings. Each profile shows two ratings side by side. The U.S. Department of State Risk Level is the government's travel advisory. The TIDE Cyber Risk Level is the TIDE team's own assessment of cyber risk to organizations, employees, and travelers. It weighs state surveillance and compelled access, internet controls, state-linked targeting, crime and device theft, conflict and instability, and the strength of local security capacity.

TIDE CYBER RISK LEVEL	GUIDANCE
Level 1: Exercise Normal Cyber Precautions	Standard cyber hygiene applies.
Level 2: Exercise Increased Cyber Precautions	Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.
Level 3: Heightened Cyber Precautions	Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.
Level 4: Maximum Cyber Precautions	Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Sources and method. Threat actor information comes from the TIDE team's ongoing tracking, and the counts describe actors that list a country among their targets, which measures actor interest and not incident volume. Geopolitical context comes from open-source reporting, government advisories, and conflict-monitoring organizations. Where public reporting is thin, the profile says so and describes regional patterns.

Important caveats. This worldbook reflects information available as of the date on the cover. Intelligence is assessed, not certain, and attribution, advisories, sanctions, and conditions on the ground can change quickly. It is provided for general awareness and is not legal, security, or travel advice. Verify current conditions and follow your organization's policies before making decisions.

QUICK REFERENCE

This table lists every profile in alphabetical order with its U.S. Department of State Risk Level and its TIDE Cyber Risk Level. The State Department rating reflects its Travel Advisory on the date shown in each profile, and the TIDE rating reflects the TIDE team's own assessment of cyber risk.

TIDE Cyber Risk Levels across this worldbook: Level 4 (26 profiles), Level 3 (29), Level 2 (63), and Level 1 (81).

COUNTRY	U.S. STATE DEPT.	TIDE CYBER RISK	PAGE
Afghanistan	Level 4	Level 4	10
Albania	Level 2	Level 2	14
Algeria	Level 2	Level 2	17
Andorra	Level 1	Level 1	20
Angola	Level 2	Level 2	23
Antigua and Barbuda	Level 1	Level 1	26
Argentina	Level 1	Level 2	29
Armenia	Level 2	Level 2	32
Australia	Level 1	Level 1	35
Austria	Level 1	Level 1	38
Azerbaijan	Level 3	Level 3	41
Bahamas	Level 2	Level 1	44
Bahrain	Level 3	Level 3	47
Bangladesh	Level 2	Level 2	51
Barbados	Level 1	Level 1	54
Belarus	Level 4	Level 4	57
Belgium	Level 2	Level 2	61
Belize	Level 2	Level 1	64
Benin	Level 2	Level 2	67
Bhutan	Level 1	Level 1	70
Bolivia	Level 2	Level 2	73
Bosnia and Herzegovina	Level 2	Level 2	76
Botswana	Level 2	Level 1	79
Brazil	Level 2	Level 2	82
Brunei	Level 1	Level 1	86
Bulgaria	Level 1	Level 1	89
Burkina Faso	Level 4	Level 4	92
Burma (Myanmar)	Level 4	Level 4	95

COUNTRY	U.S. STATE DEPT.	TIDE CYBER RISK	PAGE
Burundi	Level 3	Level 3	99
Cabo Verde	Level 1	Level 1	102
Cambodia	Level 2	Level 3	105
Cameroon	Level 2	Level 3	108
Canada	Level 1	Level 1	111
Central African Republic	Level 4	Level 4	114
Chad	Level 4	Level 4	117
Chile	Level 2	Level 2	120
China	Level 2	Level 4	123
Colombia	Level 3	Level 2	128
Comoros	Level 2	Level 1	131
Congo, Democratic Republic of the	Level 4	Level 4	133
Congo, Republic of the	Level 2	Level 2	136
Costa Rica	Level 2	Level 1	139
Cote d'Ivoire	Level 2	Level 2	142
Croatia	Level 1	Level 1	145
Cuba	Level 2	Level 3	148
Cyprus	Level 3	Level 2	151
Czechia	Level 1	Level 1	154
Denmark	Level 2	Level 1	157
Djibouti	Level 2	Level 2	160
Dominica	Level 1	Level 1	163
Dominican Republic	Level 2	Level 2	166
Ecuador	Level 2	Level 2	169
Egypt	Level 2	Level 3	172
El Salvador	Level 1	Level 2	175
Equatorial Guinea	Level 2	Level 3	178
Eritrea	Level 2	Level 4	181
Estonia	Level 1	Level 1	184
Eswatini	Level 2	Level 2	187
Ethiopia	Level 3	Level 3	190
Fiji	Level 1	Level 1	193
Finland	Level 1	Level 1	196
France	Level 2	Level 2	199

COUNTRY	U.S. STATE DEPT.	TIDE CYBER RISK	PAGE
Gabon	Level 2	Level 2	202
Gambia, The	Level 2	Level 1	205
Georgia	Level 1	Level 2	208
Germany	Level 2	Level 1	211
Ghana	Level 2	Level 2	214
Greece	Level 1	Level 1	217
Grenada	Level 2	Level 1	220
Guatemala	Level 3	Level 2	223
Guinea	Level 2	Level 2	226
Guinea-Bissau	Level 3	Level 3	229
Guyana	Level 3	Level 2	232
Haiti	Level 4	Level 4	235
Honduras	Level 3	Level 2	238
Hong Kong	Level 2	Level 3	241
Hungary	Level 1	Level 1	244
Iceland	Level 1	Level 1	247
India	Level 2	Level 2	250
Indonesia	Level 2	Level 2	254
Iran	Level 4	Level 4	257
Iraq	Level 4	Level 4	261
Ireland	Level 1	Level 1	264
Israel	Level 3	Level 3	267
Italy	Level 2	Level 1	270
Jamaica	Level 2	Level 2	273
Japan	Level 1	Level 1	276
Jordan	Level 3	Level 3	279
Kazakhstan	Level 1	Level 2	282
Kenya	Level 2	Level 2	285
Kiribati	Level 1	Level 1	288
Kosovo	Level 2	Level 2	291
Kuwait	Level 3	Level 3	294
Kyrgyz Republic, The	Level 1	Level 2	297
Laos	Level 2	Level 3	300
Latvia	Level 1	Level 1	303

COUNTRY	U.S. STATE DEPT.	TIDE CYBER RISK	PAGE
Lebanon	Level 4	Level 4	306
Lesotho	Level 2	Level 1	309
Liberia	Level 2	Level 2	312
Libya	Level 4	Level 4	315
Liechtenstein	Level 1	Level 1	318
Lithuania	Level 1	Level 1	321
Luxembourg	Level 1	Level 1	324
Macau	Level 2	Level 2	327
Madagascar	Level 2	Level 2	330
Malawi	Level 2	Level 1	333
Malaysia	Level 1	Level 1	336
Maldives	Level 2	Level 1	339
Mali	Level 4	Level 4	342
Malta	Level 1	Level 1	345
Marshall Islands	Level 1	Level 1	348
Mauritania	Level 3	Level 3	351
Mauritius	Level 2	Level 1	354
Mexico	Level 2	Level 2	357
Micronesia, Federated States of	Level 1	Level 1	360
Moldova	Level 2	Level 2	363
Monaco	Level 2	Level 1	366
Mongolia	Level 1	Level 1	369
Montenegro	Level 1	Level 1	372
Morocco	Level 2	Level 2	375
Mozambique	Level 2	Level 2	378
Namibia	Level 2	Level 1	381
Nauru	Level 1	Level 1	384
Nepal	Level 2	Level 2	387
Netherlands	Level 2	Level 1	390
New Zealand	Level 1	Level 1	393
Nicaragua	Level 3	Level 3	396
Niger	Level 4	Level 4	399
Nigeria	Level 3	Level 3	402
North Korea	Level 4	Level 4	405

COUNTRY	U.S. STATE DEPT.	TIDE CYBER RISK	PAGE
North Macedonia	Level 1	Level 1	409
Norway	Level 1	Level 1	412
Oman	Level 3	Level 3	415
Pakistan	Level 3	Level 3	418
Palau	Level 1	Level 1	421
Panama	Level 2	Level 2	424
Papua New Guinea	Level 3	Level 3	427
Paraguay	Level 1	Level 1	430
Peru	Level 2	Level 2	433
Philippines	Level 2	Level 2	436
Poland	Level 1	Level 1	439
Portugal	Level 1	Level 1	442
Qatar	Level 3	Level 3	445
Romania	Level 1	Level 1	448
Russia	Level 4	Level 4	451
Rwanda	Level 3	Level 3	456
Saint Kitts and Nevis	Level 1	Level 1	459
Saint Lucia	Level 1	Level 1	462
Saint Vincent and the Grenadines	Level 1	Level 1	465
Samoa	Level 1	Level 1	468
San Marino	Level 2	Level 1	471
Sao Tome and Principe	Level 2	Level 1	474
Saudi Arabia	Level 3	Level 4	477
Senegal	Level 1	Level 2	480
Serbia	Level 2	Level 2	483
Seychelles	Level 1	Level 1	486
Sierra Leone	Level 2	Level 2	489
Singapore	Level 1	Level 1	492
Slovakia	Level 1	Level 1	495
Slovenia	Level 1	Level 1	498
Solomon Islands	Level 2	Level 2	501
Somalia	Level 4	Level 4	504
South Africa	Level 2	Level 2	507
South Korea	Level 1	Level 1	510

COUNTRY	U.S. STATE DEPT.	TIDE CYBER RISK	PAGE
South Sudan	Level 4	Level 4	513
Spain	Level 2	Level 1	516
Sri Lanka	Level 2	Level 2	519
Sudan	Level 4	Level 4	522
Suriname	Level 1	Level 1	525
Sweden	Level 2	Level 1	528
Switzerland	Level 1	Level 1	531
Syria	Level 4	Level 4	534
Taiwan	Level 1	Level 2	537
Tajikistan	Level 2	Level 2	540
Tanzania	Level 3	Level 3	543
Thailand	Level 1	Level 2	546
Timor-Leste	Level 2	Level 1	549
Togo	Level 2	Level 2	552
Tonga	Level 1	Level 1	555
Trinidad and Tobago	Level 3	Level 3	558
Tunisia	Level 2	Level 2	561
Turkey	Level 2	Level 2	564
Turkmenistan	Level 1	Level 3	567
Tuvalu	Level 1	Level 1	570
Uganda	Level 4	Level 3	573
Ukraine	Level 4	Level 4	576
United Arab Emirates	Level 3	Level 3	579
United Kingdom	Level 2	Level 1	582
United States	N/A	Level 1	585
Uruguay	Level 2	Level 1	588
Uzbekistan	Level 1	Level 2	591
Vanuatu	Level 1	Level 1	594
Vatican City	Level 2	Level 1	597
Venezuela	Level 3	Level 3	600
Vietnam	Level 1	Level 2	603
West Bank and Gaza	Level 4	Level 4	606
Yemen	Level 4	Level 4	609
Zambia	Level 1	Level 2	612

COUNTRY	U.S. STATE DEPT.	TIDE CYBER RISK	PAGE
Zimbabwe	Level 2	Level 2	615

WORLDBOOK

AFGHANISTAN

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Kabul

GOVERNMENT
Islamic Emirate governed by Taliban de facto authorities (not recognized by the United States)

LANGUAGE
Pashto and Dari

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued February 20, 2026)

Risk indicators: Unrest, crime, health, kidnapping or hostage-taking, terrorism, wrongful detention, natural disaster

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Unrecognized Taliban authorities, device searches, communications blackouts, wrongful detention, and no U.S. consular presence.

Country Overview

Afghanistan sits at the crossroads of Central, South, and West Asia, and its history reflects centuries of passing empires and regional rivalry. The modern state traces to the Durrani Empire founded by Ahmad Shah Durrani in 1747. In the nineteenth century, Afghanistan served as a buffer between the British and Russian empires and fought three wars with Britain before gaining full control of its foreign affairs in 1919.

A monarchy ended in 1973, and a communist coup in 1978 was followed by the Soviet invasion in 1979 and a decade of war against Western- and Pakistan-backed mujahideen. Civil war and the rise of the Taliban in the 1990s led to Taliban rule from 1996 to 2001. A U.S.-led intervention followed the September 11 attacks and lasted twenty years. The Taliban returned to power in August 2021 as the Western-backed government collapsed and foreign forces withdrew.

Afghanistan is landlocked, mountainous, and young, with an uncertain population estimated between about 36 million and 49 million, since no census has been held since 1979, and one of the world's lowest per-capita incomes. The Taliban government is led by Supreme Leader Hibatullah Akhundzada and rules by decree under its interpretation of Islamic law. The United States does not recognize it as the government of Afghanistan.

Geopolitical Landscape

- **Conflict with Pakistan.** Pakistan and Afghanistan have been in open confrontation in 2026. Fighting began in late February, and Pakistan has conducted repeated airstrikes in Afghan provinces including Kandahar, Khost, Paktia, Kunar, and Helmand. Pakistan accuses the Taliban of sheltering the Tehrik-e-Taliban Pakistan (TTP), and Kabul denies it. Reporting in early October 2026 described the conflict as entering its third week of a new round, and Crisis Group listed Afghanistan as deteriorated in September and a conflict risk alert for October. Mediation by China, Turkey, Qatar, and Saudi Arabia has not produced a lasting ceasefire.
- **Recognition.** Russia formally recognized the Taliban government in July 2025. Most governments, including the United States, withhold recognition while maintaining varying levels of practical engagement.
- **Internal security.** Islamic State Khorasan Province (ISKP) remains active against the Taliban, minorities, and foreign targets. Anti-Taliban resistance groups operate at small scale, and Pakistan has been accused by the Taliban of supporting them.
- **Humanitarian conditions.** Restrictions on women's education and employment, aid cuts, returns of refugees from Iran and Pakistan, and recurring natural disasters continue to strain the country.
- **Sanctions and finance.** Afghan central bank assets remain frozen abroad, UN sanctions apply to senior Taliban figures, and the banking sector is largely cut off from international correspondent relationships.

Cyber Threats | Organizations

- **Limited commercial digital footprint.** Organizations operating in Afghanistan, mostly humanitarian, telecommunications, and development entities, work in an environment with little formal cyber regulation and no independent oversight of government access to data.
- **State control of connectivity.** Authorities have used internet restrictions as a policy tool, including fiber-optic bans in several northern provinces from mid-September 2025 and a nationwide communications blackout that began on September 29, 2025. Plan for sudden loss of connectivity, and avoid any dependency on a single carrier.
- **Legacy U.S.-era data.** Biometric and personnel databases built during the previous government, including identity and payroll systems, passed to the Taliban in 2021. Organizations that shared staff or beneficiary data with the former government should assume that data is in Taliban hands.
- **Espionage against telecommunications and government networks.** Regional state-linked actors have targeted Afghan government and telecommunications networks. This interest tracks with the strategic value of the country to neighbors.
- **Physical security drives cyber exposure.** Staff safety concerns mean that any leak of employee names, locations, or beneficiary lists can carry life-safety consequences, so data minimization carries more weight here than in most countries.
- **Employees based in country.** Staff face device inspection at checkpoints, loss of connectivity with little warning, and physical risk if employee names, locations, or contacts leak. Limit locally stored personal data and keep a non-internet check-in plan.
- **Vendor and supply chain risk.** Local telecom carriers, payroll processors, and contractors operate under Taliban oversight and can be compelled to disclose data. Legacy biometric and payroll systems passed to the Taliban in 2021. Screen vendors for sanctions exposure and minimize shared records.

The TIDE team tracks 18 threat actors that list Afghanistan among their targets. By attributed nexus, they break down as 6 unattributed or other, 4 China-nexus, 4 Iran-nexus, 1 Russia-nexus, 1 Pakistan-nexus, 1 India-nexus, and 1 cybercriminal. The most frequently targeted sectors are government (15), telecommunications (6), defense and defense industrial base (5), diplomatic and foreign affairs (4), and education and research (4). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Device inspection and surveillance.** Taliban checkpoints and security personnel inspect phones, and content related to the former government, foreign organizations, or women's rights can lead to detention. Individuals should assume devices are searched at checkpoints.
- **Social media exposure.** Past posts, photographs, and contacts tied to the previous government or to foreign forces create risk for Afghans. Account clean-up and deletion of contact lists protect people who stay in country.
- **Fraud and targeted extortion.** Scammers exploit visa, resettlement, and evacuation hopes. Messages offering paid places on programs, or asking for passport scans and payments, warrant extreme caution.
- **Mobile-first access.** Most users reach the internet by mobile. SIM registration and carrier controls limit anonymity.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Afghanistan. The Taliban government has limited known offensive cyber capability, and public reporting describes the country primarily as a target.

Cyber Travel Considerations

Official guidance

- The U.S. Department of State rates Afghanistan Level 4, Do Not Travel, and the United States has no embassy in Kabul and no ability to provide routine consular help. The advisory cites unrest, crime, health risks, kidnapping or hostage-taking, terrorism, and wrongful detention.
- Wrongful detention of foreigners, including U.S. citizens, has occurred. Business travel should proceed only with a documented security plan, an in-country partner, and executive sign-off.

TIDE Risk Level Rationale

- **Drivers.** Taliban authorities control telecommunications and have shut down the internet nationwide, security personnel inspect phones at checkpoints, and wrongful detention of foreigners has occurred. The fighting with Pakistan adds physical risk, and the United States has no consular presence to help.
- **What would change this rating.** Level 4 is the ceiling. The TIDE team would consider lowering the level only if connectivity restrictions end, device inspections stop, and the security situation with Pakistan stabilizes.

Public Wi-Fi

- Afghan authorities conduct device inspections at checkpoints and have implemented nationwide communications blackouts; avoid all public Wi-Fi, and assume compromised hotel networks. Use only a corporate VPN, with a plan to operate entirely offline if connectivity is cut.

Recommended corporate policy

- Apply a no device, no infrastructure policy: no company-issued devices, no company-linked accounts on personal devices, and no log-ins to company systems while in country.
- Issue clean loaner devices only when a business need is approved, with no persistent VPN or single sign-on, and reimage them on return.
- Block sign-ins from Afghanistan through geo-based conditional access and alert on every attempt.
- Remove contact lists, photographs, and messages that could endanger local colleagues before travel.

Connectivity and communications

- Expect shutdowns of internet and mobile service with little warning. Carry a communications plan that does not depend on local mobile data, and agree on check-in rules and escalation triggers with a named company contact.
- Treat all local networks and SIMs as monitored, and avoid public Wi-Fi and public charging.

Personal safety and legal exposure

- Check whether travel medical and evacuation coverage applies. Many policies exclude Level 4 destinations, and evacuation options are limited.
- Do not wear company apparel or discuss work in public. Prepare an approved cover answer.
- Retain counsel with experience in hostage and detention cases, and involve legal on sanctions and export-control issues.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

ALBANIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Tirana

GOVERNMENT
Parliamentary republic

LANGUAGE
Albanian

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 26, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Iran-linked destructive attacks on government in 2022, plus elevated fraud and phishing.

Country Overview

Albania occupies the western Balkans coast along the Adriatic and Ionian seas. Its people descend from ancient Illyrian tribes, and the territory passed through Roman, Byzantine, and Ottoman control. Albania declared independence from the Ottoman Empire in 1912 and was later briefly occupied by Italy and then Germany during the Second World War.

After the war, Enver Hoxha built one of the most isolated communist states in Europe, breaking with the Soviet Union and later China. The regime fell in 1991 and 1992, and the 1997 collapse of pyramid investment schemes triggered civil unrest and an international intervention. Albania joined NATO in 2009 and has been an EU candidate since 2014, with accession negotiations opened in 2022.

The country has about 2.3 million residents, a large diaspora in Italy, Greece, and the United States, and an economy reliant on tourism, remittances, and services. Prime Minister Edi Rama has led the government since 2013.

Geopolitical Landscape

- **EU accession.** Albania is among the leading candidates for EU membership and has aimed to complete negotiations by the end of the decade. Progress depends on judicial and anti-corruption reform.

- **Iran dispute.** Albania hosts the Mojahedin-e Khalq (MEK) opposition group. Iran-linked actors launched a destructive cyberattack on Albanian government systems in July 2022, and Albania cut diplomatic relations with Iran in September 2022. The two countries remain in a standoff.
- **Migration deal with Italy.** A 2023 agreement with Italy established processing centers in Albania for migrants intercepted at sea, and the arrangement has faced legal and logistical challenges.
- **Organized crime.** Albanian organized crime groups are active across Europe, and domestic corruption concerns persist despite vetting reforms in the judiciary.
- **Regional relations.** Albania maintains close ties with Kosovo and the United States, and balances relations with Greece and Serbia.

Cyber Threats | Organizations

- **Destructive state-linked attacks.** The July 2022 attack on Albanian government infrastructure used ransomware-style encryption and wiper behavior, disrupted public services, and led to a diplomatic rupture. Iran-linked actors, tracked by the TIDE team as Scarred Manticore and Homeland Justice, have targeted Albania. Albanian entities with Iran-related exposure should assume a continuing interest.
- **Government and telecommunications targeting.** The TIDE tracking data shows government, telecommunications, and defense as the leading targeted sectors.
- **Ransomware and fraud.** Small and medium enterprises with limited security staff face opportunistic ransomware and business email compromise, which mirrors patterns across the western Balkans.
- **Data exposure.** Several leaks of government and personal records have been reported, and organizations handling Albanian citizen data should plan for legal obligations under Albania's data protection law and EU alignment.
- **Employees based in country.** Employees with Iran-related business exposure or public profiles should expect targeted phishing and should use managed devices with phishing-resistant authentication. Everyday risk is fraud, card skimming, and public Wi-Fi.
- **Vendor and supply chain risk.** Small local IT firms and government-facing contractors often lack mature security, and Iran-linked actors have shown interest in Albanian government supply chains. Require security attestations and incident notification clauses.

The TIDE team tracks 3 threat actors that list Albania among their targets. By attributed nexus, they break down as 2 Iran-nexus, and 1 cybercriminal. The most frequently targeted sectors are government (3), telecommunications (2), defense and defense industrial base (1), banking and financial services (1), and education and research (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Fraud messages impersonating banks, couriers, and public agencies are common in Albanian-language channels.
- **Investment and romance scams.** Online investment schemes and romance fraud target both residents and diaspora.

- **Privacy of leaked records.** Past leaks of citizen records raise the risk of targeted phishing and identity fraud using genuine personal details.
- **Mobile and social platforms.** Smartphone use is high, and WhatsApp and social media serve as primary channels for scams.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Albania. Albania appears in TIDE tracking as a target of Iran-linked activity.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Albania Level 2, Exercise Increased Caution, for crime.

TIDE Risk Level Rationale

- **Drivers.** Iran-linked actors carried out a destructive attack on Albanian government systems in 2022, and fraud and phishing are common. State surveillance risk is low.
- **What would change this rating.** Raise to Level 3 if Iran-linked activity against Albanian organizations resumes at scale or travelers are targeted. Lower to Level 1 if the dispute with Iran eases and local security capacity improves.

Public Wi-Fi

- Iran-linked actors have deployed destructive malware against government systems; public networks expose credentials to interception. Restrict public Wi-Fi use strictly, and rely on a corporate VPN for any network access in hotels or at airports.

Device and account controls

- Company devices can travel under standard controls: full-disk encryption, a managed profile, phishing-resistant multi-factor authentication, and remote wipe.
- Use a corporate VPN.
- Carry only the devices and data the trip requires.

Local risks

- Street theft and card skimming occur in Tirana and coastal resort areas, so use bank-branch ATMs where possible and monitor card activity.
- Expect inconsistent mobile coverage in rural and mountain areas, and keep offline copies of key travel details.
- Employees with Iran-related business exposure should brief security before travel.

Return protocol

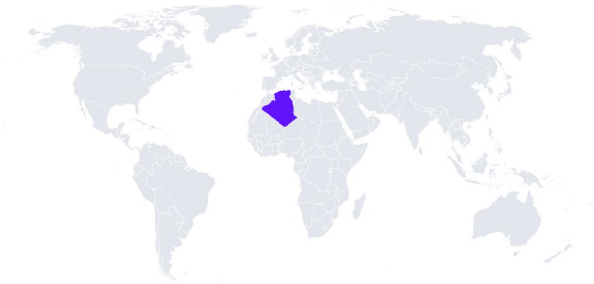
- Report any lost device immediately, revoke sessions, and review account activity after the trip.

WORLDBOOK

ALGERIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Algiers

GOVERNMENT
Presidential republic

LANGUAGE
Arabic and Tamazight (French widely used in business)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 25, 2026)

Risk indicators: Kidnapping or hostage-taking, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: State monitoring of communications, scheduled exam-period internet throttling, and espionage interest in the energy sector.

Country Overview

Algeria is Africa's largest country by area and sits on the Mediterranean coast of North Africa, with most of its territory in the Sahara. Berber peoples, Carthaginians, Romans, Arabs, and Ottomans all shaped its history. France conquered Algiers in 1830 and ruled Algeria as an integral part of France until a brutal war of independence from 1954 to 1962.

The National Liberation Front (FLN) governed as a one-party state after independence. A 1991 election that Islamists were poised to win was annulled, and a civil conflict in the 1990s killed an estimated 100,000 or more people. Abdelaziz Bouteflika served as president from 1999 until mass protests, known as the Hirak, forced him out in 2019. Abdelmadjid Tebboune has been president since December 2019.

Algeria has about 47.4 million people and one of the continent's largest hydrocarbon sectors, with natural gas exports to Europe through pipelines to Spain and Italy. The military plays a central role in politics.

Geopolitical Landscape

- **Rivalry with Morocco.** Algeria cut diplomatic relations with Morocco in 2021 and closed its airspace to Moroccan aircraft. The dispute centers on Western Sahara, where Algeria backs the Polisario Front and Morocco proposes autonomy under its sovereignty.
- **Tension with France.** Relations with France have been strained since 2024, when France shifted toward support for Morocco's autonomy plan for Western Sahara. Disputes over migration, detained individuals, and historical memory continue.
- **Sahel border tensions.** Algeria's relations with Mali deteriorated in 2025 after a drone incident, and instability along the southern border continues to concern Algiers.
- **Energy leverage.** Algeria has expanded gas supply to Europe since 2022 and balances ties with Russia, a major arms supplier, and with Western partners.
- **Domestic politics.** Tebboune won a second term in September 2024. Civic space remains restricted, and authorities have prosecuted journalists and activists.

Cyber Threats | Organizations

- **Energy sector targeting.** Hydrocarbon producers, pipeline operators, and their suppliers hold strategic data and operational technology, which attracts espionage and disruptive interest from regional and global actors.
- **Regional hacktivism.** Public reporting describes recurring hacktivist exchanges between Algerian and Moroccan groups, including website defacements and data leaks.
- **Government-controlled connectivity.** Authorities have throttled or cut internet access during national baccalaureate exams each year. Organizations should plan for scheduled degradation in June.
- **Ransomware and fraud.** Banks, telecommunications operators, and public institutions face criminal ransomware and phishing, and local security staffing is thin.
- **Data regulation.** Law 18-07 governs personal data protection, and the data protection authority is still maturing, so organizations should treat compliance expectations as evolving.
- **Employees based in country.** Staff should assume calls and messages can be intercepted and plan for degraded connectivity each June. Employees in the energy sector are higher-value targets for elicitation and phishing.
- **Vendor and supply chain risk.** Hydrocarbon contractors and telecom operators hold strategic data and are state-aligned or state-owned. Vendor access to production and pipeline systems warrants segmentation and monitoring.

The TIDE team does not currently track actors that list Algeria among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Monitoring.** Public discussion of the military, the presidency, or the Hirak can bring legal exposure, and authorities monitor social platforms.
- **Platform restrictions.** Authorities have periodically throttled social media, and VPN use is common.

- **Fraud.** Phishing and impersonation scams aimed at consumers, including fake delivery and banking messages, circulate in Arabic, French, and Algerian dialect.
- **Privacy of communications.** Individuals should assume that calls and text messages can be intercepted.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Algeria, and TIDE tracking does not currently list Algeria among the targets of tracked actors. This reflects limited public attribution rather than an absence of activity.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Algeria Level 2, with risk indicators for kidnapping or hostage-taking and terrorism, and advises against travel to specific areas near the borders and in the Sahara.

TIDE Risk Level Rationale

- **Drivers.** Authorities monitor communications and throttle the internet during June exams, and the energy sector draws espionage interest. Tensions with Morocco and Mali add hacktivist and state-linked activity.
- **What would change this rating.** Raise to Level 3 if shutdowns or VPN restrictions broaden or device inspections of visitors increase. Lower to Level 1 if monitoring and throttling ease.

Public Wi-Fi

- Algerian authorities monitor hotel and carrier networks; government monitoring is particularly heightened during June exam periods when internet is throttled. Use a corporate VPN for all public Wi-Fi access, and assume hotel networks record traffic.

Device and account controls

- Company devices can travel under standard controls with encryption, a managed profile, and remote wipe. Use phishing-resistant multi-factor authentication.
- Expect that hotel networks and local carriers are monitored, and use a corporate VPN. Be aware that VPN use can draw attention and that availability varies.
- Plan for degraded connectivity during June exam periods.

Local risks and practices

- Photography of government buildings, military sites, and energy infrastructure can lead to questioning.
- Carry printed copies of itineraries and invitation letters, since border officials may inspect electronic devices.
- Employees working in the energy sector should receive an elicitation briefing before travel.

Return protocol

- Reimage any device that showed signs of inspection, rotate credentials for accounts accessed in country, and debrief the traveler.

WORLDBOOK

ANDORRA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Andorra la Vella

GOVERNMENT
Parliamentary co-principality

LANGUAGE
Catalan

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 21, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable jurisdiction with low state-surveillance risk; main exposure is financial-sector fraud.

Country Overview

Andorra is a landlocked microstate of about 90,000 people in the eastern Pyrenees between France and Spain. According to tradition, Charlemagne granted the valleys to local rule, and a 1278 agreement, the Pareage, established joint sovereignty between the Count of Foix and the Bishop of Urgell.

Today the Bishop of Urgell and the President of France serve as co-princes, a unique arrangement dating from that agreement. A written constitution adopted in 1993 created a parliamentary democracy, and Andorra joined the United Nations the same year. It uses the euro under a monetary agreement with the EU but is not an EU member.

The economy rests on tourism, retail, ski resorts, and financial services. Andorra ended its traditional banking secrecy in recent years and has signed an association agreement with the EU.

Geopolitical Landscape

- **EU relationship.** Andorra concluded negotiations on an association agreement with the EU, which would give it access to parts of the single market, and ratification has proceeded slowly.
- **Financial transparency.** Andorra has adopted international tax transparency standards and strengthened anti-money laundering controls under pressure from the OECD and Moneyval.

- **Security.** Andorra has no standing army, and France and Spain provide defense under longstanding arrangements.
- **Low geopolitical profile.** Andorra has no active disputes and remains largely outside great-power competition.

Cyber Threats | Organizations

- **Financial sector.** Private banks and wealth managers handle high-value client data, which attracts fraud, business email compromise, and targeted phishing.
- **Tourism and retail.** Hotels, ski operators, and retailers face payment-card fraud and ransomware risks typical of seasonal businesses.
- **Small-state resourcing.** A small public sector and limited local security talent make third-party providers and cross-border services the main sources of exposure.
- **Regulatory context.** Andorra's personal data protection law aligns with the GDPR model, and the data protection agency enforces it.
- **Employees based in country.** Employees face the ordinary risks of tourist and resort areas: card fraud, phishing, and public Wi-Fi. Wealth-management staff face tailored social engineering.
- **Vendor and supply chain risk.** Small-state providers and cross-border French and Spanish vendors carry most of the exposure. Banks and wealth managers should verify subcontractor controls for client data.

The TIDE team does not currently track actors that list Andorra among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Phishing and card fraud.** Residents and visitors face consumer scams in Catalan, Spanish, and French, including bank and parcel impersonation.
- **Wealth-targeted social engineering.** Residents with high net worth face tailored fraud and extortion attempts.
- **Public Wi-Fi.** Ski resorts, hotels, and shopping areas offer public networks that attract credential theft.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Andorra, and TIDE tracking does not currently list Andorra among the targets of tracked actors.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Andorra Level 1, Exercise Normal Precautions.

TIDE Risk Level Rationale

- **Drivers.** Andorra is a stable, well-governed microstate with low state-surveillance risk. The main exposure is fraud against wealthy residents and visitors and third-party risk in the financial sector.
- **What would change this rating.** Raise to Level 2 if targeted campaigns against Andorran financial institutions emerge or a significant breach affects visitors.

Public Wi-Fi

- Financial sector networks in Andorra attract credential theft and business email compromise; ski resorts, hotels, and shopping areas present fraud risk. Use a corporate VPN when accessing public networks at resorts or shopping venues.

Device and account controls

- Standard business travel controls are appropriate: full-disk encryption, multi-factor authentication, a corporate VPN, and remote wipe.
- Avoid public USB charging stations, and bring personal chargers.

Local practices

- Travelers typically cross into Andorra from France or Spain, and customs checks at the borders can include random inspections. Carry only necessary devices and data.
- Watch for card skimming at fuel stations and busy retail areas.

WORLDBOOK

ANGOLA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Luanda

GOVERNMENT
Presidential republic

LANGUAGE
Portuguese

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued March 5, 2026)

Risk indicators: Crime, health, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Limited public reporting, growing connectivity, street crime, and strategic oil and mining data.

Country Overview

Angola lies on the southwestern coast of Africa. Bantu-speaking kingdoms, including Kongo and Ndongo, dominated the region before Portuguese traders arrived in the late fifteenth century. Angola became a center of the Atlantic slave trade and remained under Portuguese rule for about five centuries.

After a long independence struggle, Angola became independent in 1975. A civil war between the MPLA, backed by the Soviet Union and Cuba, and UNITA, backed by the United States and South Africa, lasted until 2002. The MPLA has governed since independence. President Joao Lourenco took office in 2017 after the 38-year presidency of Jose Eduardo dos Santos.

Angola has about 38.8 million people and is one of sub-Saharan Africa's largest oil producers. It left OPEC at the end of 2023. The economy is heavily dependent on hydrocarbons and diamonds, and Angola holds a large debt to China.

Geopolitical Landscape

- **Lobito Corridor.** Angola is the anchor of a U.S.- and EU-backed rail and port corridor linking the Atlantic coast to copper and cobalt regions in the Democratic Republic of the Congo and Zambia, and it competes with China-linked routes.

- **Great-power balance.** Angola holds significant debt to China, deepened ties with the United States and Europe under Lourenco, and mediates in regional conflicts, including between the DRC and Rwanda.
- **Domestic unrest.** Protests over fuel price increases in July 2025 turned deadly and highlighted pressure from the cost of living. Elections are scheduled for 2027.
- **Economic reform.** Angola is reducing fuel subsidies, diversifying away from oil, and managing debt service obligations.

Cyber Threats | Organizations

- **Oil, gas, and mining.** Extractive firms and their contractors hold geological, contract, and financial data of strategic value, and operational technology at terminals and processing sites warrants segmentation.
- **Financial sector.** Banks and mobile payment providers face fraud, account takeover, and insider-enabled theft as digital payments expand.
- **Public institutions.** Government systems rely on limited security staffing, and public reporting of incidents is sparse.
- **Third-party and vendor access.** Foreign contractors and joint ventures connect to local networks, so supply chain access is a key exposure.
- **Public reporting gap.** The TIDE team tracks only two actors that list Angola among their targets, which reflects sparse reporting. Treat Angola's actual exposure as comparable to other emerging economies with growing connectivity.
- **Employees based in country.** Employees face phone snatching in Luanda, SMS and WhatsApp phishing, and unreliable power and connectivity. Extractive-sector staff are targets for elicitation.
- **Vendor and supply chain risk.** Contractors and joint-venture partners connect to local networks, so third-party access to operational technology and contract data is the key exposure. Require segmentation, access logging, and sanctions and anti-corruption screening.

The TIDE team tracks 2 threat actors that list Angola among their targets. By attributed nexus, they break down as 1 unattributed or other, and 1 cybercriminal. The most frequently targeted sectors are government (2), civil society and activism (1), diplomatic and foreign affairs (1), banking and financial services (1), and education and research (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile and messaging scams.** Phishing by SMS and WhatsApp that impersonates banks, telecommunications operators, and government agencies is common across lusophone Africa.
- **Investment and job scams.** Fraudulent job offers and investment schemes target young and urban users.
- **SIM and account takeover.** SIM registration weaknesses can enable account takeover for mobile wallets.
- **Civic space.** Online criticism of the government carries some legal exposure, though enforcement varies.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Angola.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Angola Level 2, Exercise Increased Caution, citing crime and health risks.

TIDE Risk Level Rationale

- **Drivers.** Street crime and phone snatching are real risks, connectivity is unreliable, and oil and mining data attract targeting while local security capacity is thin. Public reporting is limited, which argues for caution.
- **What would change this rating.** Raise to Level 3 if unrest like the 2025 fuel protests brings internet restrictions or monitoring of dissent. Lower to Level 1 as security capacity and reporting improve.

Public Wi-Fi

- Angola's limited security capacity and reliance on foreign contractors mean hotel and carrier networks lack robust protection; phone snatching is common in Luanda and can facilitate account takeover if device access is gained. Conceal devices when using public networks, and always connect through a corporate VPN.

Device and account controls

- Company devices can travel under standard controls: encryption, managed profile, phishing-resistant multi-factor authentication, and remote wipe.
- Use a corporate VPN, avoid public Wi-Fi, and keep devices out of sight in vehicles and restaurants.

Local risks

- Street crime, including phone snatching and robbery, occurs in Luanda, so keep devices concealed and use hotel-arranged transport.
- Mobile data and electricity can be unreliable. Carry power banks and an offline plan for key contacts.
- Business travelers in oil and mining should receive an elicitation briefing and avoid discussing contracts in public.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and review account activity after travel.

WORLDBOOK

ANTIGUA AND BARBUDA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Saint John's

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 20, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low state-surveillance risk; exposure is tourism fraud and offshore-sector data.

Country Overview

Antigua and Barbuda is a twin-island nation in the eastern Caribbean. Indigenous Arawak and Carib peoples lived on the islands before Spain and then Britain colonized them. Britain established sugar plantations worked by enslaved Africans, and Antigua later served as a Royal Navy base at English Harbour.

The islands became independent from Britain in 1981 and remain a Commonwealth realm with the British monarch as head of state. Prime Minister Gaston Browne has led the government since 2014. The country has about 104,000 residents, and the economy depends on tourism and financial services.

Antigua and Barbuda operates a citizenship by investment program, which has drawn scrutiny from the United States, the EU, and international bodies over due diligence and money laundering risks.

Geopolitical Landscape

- **Citizenship by investment.** The program attracts foreign applicants who gain visa-free access to many countries. Western governments have pressed Caribbean states to tighten vetting, and reforms continue.
- **Climate vulnerability.** Hurricanes, including Irma in 2017 that devastated Barbuda, drive recovery spending and international advocacy on climate finance.

- **Regional integration.** Antigua and Barbuda is a member of CARICOM and the Organisation of Eastern Caribbean States, and has pursued reparations claims against former colonial powers.
- **Debt and resilience.** Public debt is high relative to the economy, and tourism recovery after the pandemic has supported growth.

Cyber Threats | Organizations

- **Tourism and hospitality.** Hotels and resorts handle payment cards and passport data, which attracts ransomware and card-skimming fraud.
- **Offshore and investment migration providers.** Agents, law firms, and program operators hold identity documents and financial records for thousands of applicants, a high-value target for fraud, extortion, and espionage.
- **Small-island resilience.** Limited local security staffing makes vendors and cloud providers the primary line of defense, and hurricane disruptions affect continuity planning.
- **Regional incidents.** Governments across the Caribbean have faced ransomware against public services, so Antigua and Barbuda should plan around that regional pattern.
- **Employees based in country.** Employees face tourist-area card skimming, rental scams, and hurricane-related disruption. Staff at citizenship-by-investment firms face tailored phishing.
- **Vendor and supply chain risk.** Hotels and program agents depend on small vendors and cloud providers. Investment-migration providers hold identity files and should be treated as high-value third parties.

The TIDE team does not currently track actors that list Antigua and Barbuda among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Tourist-targeted fraud.** Fake booking listings, rental scams, and card skimming target visitors.
- **Phishing in English.** Flow and Digicel each hold roughly half the mobile market; the Eastern Caribbean Central Bank recorded phishing attacks against commercial banks causing an estimated EC$765,000 or more in losses between January 2023 and March 2024, with business-email-compromise incidents more than doubling over the same period.
- **Identity exposure for program applicants.** People who hold or apply for citizenship through investment face targeted phishing using details from their applications.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Antigua and Barbuda, and TIDE tracking does not currently list the country among the targets of tracked actors.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Antigua and Barbuda Level 1, Exercise Normal Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low state-surveillance risk and ordinary tourist-area fraud. The citizenship-by-investment sector holds sensitive identity data, which matters for staff who work in it.
- **What would change this rating.** Raise to Level 2 if a major breach hits investment-migration providers or fraud against visitors rises.

Public Wi-Fi

- Citizenship-by-investment program agents and staff handle high-value identity data, and documented phishing and business-email-compromise losses against regional banks mean credential theft via public Wi-Fi can be weaponized against personnel or applicants. Use a corporate VPN for all public network access, and avoid public Wi-Fi in resort and cafe settings.

Device and account controls

- Standard business travel controls apply: encryption, multi-factor authentication, a corporate VPN, and remote wipe.
- Avoid public Wi-Fi in resorts and cafes, and verify booking links before paying.

Local practices

- Do not leave devices unattended on beaches or in rental vehicles.
- Hurricane season, June through November, can interrupt connectivity and travel, so confirm contingency plans.

WORLDBOOK

ARGENTINA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2



CAPITAL
Buenos Aires

GOVERNMENT
Federal presidential republic

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 10, 2026)

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Frequent phone snatching, active ransomware, and large leaked citizen datasets that fuel targeted fraud.

Country Overview

Argentina occupies most of the southern cone of South America and stretches from subtropical north to Antarctic south. Indigenous peoples lived across the territory before Spain founded Buenos Aires in the sixteenth century. Argentina declared independence in 1816, and waves of European immigration in the nineteenth and early twentieth centuries shaped its culture and cities.

The country was among the wealthiest in the world a century ago. Military coups, Peronist and anti-Peronist politics, and repeated economic crises defined the twentieth century. The last military dictatorship, from 1976 to 1983, killed or disappeared an estimated 30,000 people. Democracy returned in 1983, and a deep crisis in 2001 and 2002 included a record sovereign default.

Argentina has about 46 million people, a large agricultural and energy sector, and one of the world's largest shale and lithium resources. Javier Milei, a self-described libertarian, took office in December 2023.

Geopolitical Landscape

- **Economic reform.** Milei's government cut spending, devalued the peso, and reduced inflation sharply from triple-digit levels, at the cost of recession and poverty increases in the first phase. Libertarian reforms continue under a larger congressional bloc after the October 2025 midterm elections.

- **United States support.** The U.S. Treasury provided a currency swap line and financial support in October 2025, signaling strong political backing for Milei.
- **Falklands and Malvinas.** Argentina claims sovereignty over the Falkland Islands, which Britain administers, and the dispute remains unresolved.
- **China and the region.** Argentina maintains trade ties with China and Brazil, and has debated its alignment within Mercosur and with BRICS.
- **Iran and AMIA.** The 1994 AMIA bombing in Buenos Aires, attributed by Argentine prosecutors to Iran and Hezbollah, remains a focus of Argentine foreign policy.

Cyber Threats | Organizations

- **Ransomware and extortion.** Cybercriminal groups account for most of the activity directed at Argentine organizations in the TIDE tracking data. Healthcare, education, government, and financial services are leading sectors.
- **Public data exposure.** Leaked national identity and personal records are useful for fraud and targeted phishing, so employees should expect convincing impersonation attempts.
- **State-linked espionage.** The TIDE team tracks Chinese and Iranian state-linked actors, and a Russian-linked group, among the actors that list Argentina among their targets. Government, research, and critical infrastructure organizations attract that interest.
- **Financial fraud.** Digital wallets and instant transfers have expanded quickly, along with account takeover and social engineering.
- **Regulation.** Argentina's personal data protection law dates to 2000 and the EU treats it as adequate. Reform proposals have circulated for years.
- **Employees based in country.** Staff should expect phone snatching on streets and cafe tables, virtual-kidnapping calls built from leaked records, and phishing that uses genuine personal details.
- **Vendor and supply chain risk.** Argentine IT outsourcers and payment providers are common entry points for ransomware, and prior government data leaks raise identity-fraud risk. Include breach notification and subcontractor clauses in contracts.

The TIDE team tracks 20 threat actors that list Argentina among their targets. By attributed nexus, they break down as 14 cybercriminal, 2 China-nexus, 2 unattributed or other, 1 Russia-nexus, and 1 Iran-nexus. The most frequently targeted sectors are government (12), education and research (10), banking and financial services (10), healthcare and pharmaceuticals (9), and industrial and manufacturing (7). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and account takeover.** Impersonation of banks, digital wallets, and tax authorities is common.
- **Virtual kidnapping and extortion calls.** Scammers phone victims, claim to hold a relative, and demand quick payment.
- **Marketplace and rental scams.** Fake listings and payment-link fraud affect buyers and tourists.

- **Phone theft.** Street theft of phones, often by criminals on motorbikes in Buenos Aires, can lead to account takeover when devices are unlocked.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Argentina. Argentina appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Argentina Level 1, Exercise Normal Precautions.

TIDE Risk Level Rationale

- **Drivers.** Phone snatching in major cities is frequent, ransomware activity is high, and large leaked citizen datasets fuel targeted fraud and virtual-kidnapping calls. State surveillance of visitors is not a significant concern.
- **What would change this rating.** Lower to Level 1 if theft and fraud trends fall. Raise to Level 3 only if state-linked targeting of travelers or political violence emerges.

Public Wi-Fi

- Large leaked citizen datasets fuel targeted phishing and virtual-kidnapping calls built from personal details; open Wi-Fi combined with credential interception amplifies account takeover risk. Avoid public Wi-Fi entirely in Buenos Aires and other cities, and use a corporate VPN if public network access is unavoidable.

Device and account controls

- Company devices can travel under standard controls: encryption, managed profile, phishing-resistant multi-factor authentication, and remote wipe.
- Use a corporate VPN.
- Set a strong device passcode and disable lock-screen previews, since snatch theft is a real risk.

Local risks

- Phone snatching from pedestrians and cafe tables occurs in Buenos Aires and other cities. Keep devices out of sight and use them in secure spaces.
- Card skimming and exchange-rate scams exist. Use bank cards at reputable venues, and confirm the official rate for transactions.

Return protocol

- Report lost or stolen devices immediately, lock or wipe remotely, and revoke sessions and tokens.

WORLDBOOK

ARMENIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Yerevan

GOVERNMENT
Parliamentary republic

LANGUAGE
Armenian

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 5, 2025)

Risk indicators: Other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Russia-linked influence activity, regional espionage, and exposure from the Armenia-Azerbaijan peace process.

Country Overview

Armenia is a landlocked country in the South Caucasus with one of the world's oldest Christian traditions. The Kingdom of Armenia adopted Christianity as a state religion in the early fourth century. The territory later fell under Persian, Byzantine, Arab, Ottoman, and Russian rule.

The mass killings and deportations of Armenians in the Ottoman Empire beginning in 1915, which Armenia and many governments and historians recognize as genocide, shaped national identity. Armenia became a Soviet republic in 1920 and regained independence in 1991. War with Azerbaijan over Nagorno-Karabakh followed in the early 1990s.

Armenia has about 3.1 million residents and a large global diaspora. Nikol Pashinyan has led the government since the 2018 Velvet Revolution. The country belongs to the Russian-led Eurasian Economic Union and Collective Security Treaty Organization, though it has reduced participation in the latter.

Geopolitical Landscape

- **Peace with Azerbaijan.** Azerbaijan retook Nagorno-Karabakh in 2023, and more than 100,000 ethnic Armenians left. Armenia and Azerbaijan signed a joint declaration at the White House on August 8, 2025,

pledging to end the conflict. A final treaty depends on Armenia revising constitutional language that Azerbaijan says implies territorial claims, which requires a referendum.

- **TRIPP corridor.** The declaration granted the United States development rights over a transit route through southern Armenia linking Azerbaijan to its Nakhchivan exclave, called the Trump Route for International Peace and Prosperity. Reporting indicates construction could begin in late 2026.
- **June 2026 election.** Pashinyan's Civil Contract party won the June 7, 2026 parliamentary election with about 50 percent of the vote and a governing majority, defeating Russia-backed opposition forces amid reported Russian disinformation.
- **Orientation.** Armenia is deepening ties with the EU and Turkey while remaining in Russian-led structures. The EU and Armenia held a summit in Yerevan in May 2026.
- **Iran.** Iran borders Armenia and has voiced concern about any change to the southern border corridor.

Cyber Threats | Organizations

- **Election and influence operations.** Russian-linked disinformation targeted the 2026 election, and Armenian institutions should expect continued influence activity and phishing themed around politics and the peace process.
- **Government and diplomatic espionage.** The TIDE team tracks Turkey-nexus actors Marbled Dust and Bearfoot among those that target Armenia, and TIDE tracking shows government, telecommunications, and banking as leading sectors.
- **Regional conflict spillover.** Hacktivist and state-linked activity between Armenia and Azerbaijan has accompanied past hostilities, and cyber activity can rise around diplomatic milestones.
- **Technology sector and outsourcing.** Armenia hosts a sizable IT services sector, including relocated Russian firms, which creates software supply chain and personnel-vetting exposure.
- **Critical infrastructure.** Energy and transport links to Georgia, Iran, and potentially Turkey and Azerbaijan expand the attack surface as connectivity projects advance.
- **Employees based in country.** Employees in government, defense, civil society, or diplomatic roles face targeted phishing and spyware risk. Others face ordinary fraud and public Wi-Fi risk.
- **Vendor and supply chain risk.** Armenia's IT outsourcing sector includes relocated Russian firms and staff, which creates software supply chain and vetting exposure. Review developer access, ownership, and sanctions risk.

The TIDE team tracks 3 threat actors that list Armenia among their targets. By attributed nexus, they break down as 2 Turkey-nexus, and 1 cybercriminal. The most frequently targeted sectors are government (2), telecommunications (2), banking and financial services (1), civil society and activism (1), and education and research (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Targeted phishing of activists and journalists.** Political figures, civil society, and journalists face credential phishing, and Citizen Lab found widespread Pegasus infections within Armenian civil society.
- **Consumer fraud.** Bank and delivery impersonation scams circulate in Armenian and Russian.

- **Social media manipulation.** Disinformation campaigns around elections and peace talks aim to shape sentiment and erode trust.
- **Diaspora targeting.** Armenian diaspora organizations face phishing aligned with regional political events.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Armenia. Armenia appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Armenia Level 2, Exercise Increased Caution, and advises against travel near the border with Azerbaijan.

TIDE Risk Level Rationale

- **Drivers.** Russia-linked influence operations targeted the 2026 election, regional espionage is active, and the peace process with Azerbaijan raises interest in Armenian networks. Ordinary travelers face mainly fraud risk.
- **What would change this rating.** Raise to Level 3 if the peace process collapses or hostilities resume. Lower to Level 1 if a final treaty is signed and influence activity subsides.

Public Wi-Fi

- Russia-linked disinformation targeted the June 2026 election, and phishing around the peace process remains active; staff in government, defense, civil society, or diplomatic roles face elevated targeting via compromised networks. Use a corporate VPN for all public Wi-Fi access, particularly when traveling with government or political-related roles.

Device and account controls

- Company devices can travel under standard controls: encryption, managed profile, phishing-resistant multi-factor authentication, and remote wipe.
- Use a corporate VPN, particularly for travelers with government, defense, or political exposure.

Local risks

- Travelers with ties to diplomacy, defense, or the peace process should expect elevated phishing and elicitation attempts, and should receive a security briefing.
- Land border crossings with Azerbaijan and Turkey are limited, so confirm routes before travel.

Return protocol

- Report suspicious contacts or device behavior, rotate credentials after travel, and debrief high-profile travelers.

WORLDBOOK

AUSTRALIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Canberra

GOVERNMENT
Federal parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued August 18, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated, with border device-search powers and high-volume scam activity.

Country Overview

Aboriginal and Torres Strait Islander peoples have lived on the Australian continent for at least 60,000 years and maintain one of the world's oldest continuous cultures. British navigator James Cook claimed the east coast in 1770, and the First Fleet established a penal colony at Sydney in 1788. Six colonies federated into the Commonwealth of Australia in 1901.

Australia fought alongside Britain in both world wars and shifted its primary security alliance to the United States after 1942. Postwar immigration, the end of the White Australia policy, and trade growth with Asia transformed the country into one of the world's most multicultural economies.

Australia has about 27.8 million people, a large resource and agricultural economy, and the continent's only sovereign national government. It is a member of the Five Eyes intelligence alliance, the Quad, and AUKUS.

Geopolitical Landscape

- **AUKUS and defense.** Australia is acquiring nuclear-powered submarines under the AUKUS partnership with the United States and the United Kingdom, and is increasing defense spending in response to a changing Indo-Pacific balance.

- **Relations with China.** China is Australia's largest trading partner. Trade coercion between 2020 and 2023 eased after diplomatic stabilization, and security concerns about foreign interference, critical infrastructure, and Pacific influence persist.
- **Pacific engagement.** Australia competes with China for influence in Pacific island states through security, development, and infrastructure agreements.
- **Foreign interference laws.** Australia has enacted foreign interference and foreign influence transparency laws and has prosecuted espionage cases.
- **Regulatory leadership.** Australia introduced the Cyber Security Bill 2024 in October 2024 to codify ransomware reporting and smart-device security standards.

Cyber Threats | Organizations

- **Ransomware and data extortion.** Cybercriminal groups account for most of the actors in the TIDE tracking data that list Australia among their targets. Healthcare, government, and industrial and manufacturing organizations lead the targeted sectors. The 2022 breach of Medibank exposed data on 9.7 million current and former customers, and Australia sanctioned the Russian attacker responsible in January 2024.
- **State-linked espionage and pre-positioning.** China-nexus actors are the second-largest group in TIDE tracking that list Australia. The Australian Signals Directorate and partners have publicly warned about APT40, linked to China's Ministry of State Security, and about pre-positioning in critical infrastructure.
- **Third-party and supply chain exposure.** Customer data theft through third-party platforms has affected large Australian brands, including Qantas in 2025.
- **Critical infrastructure obligations.** The Security of Critical Infrastructure Act imposes risk management and reporting duties across energy, water, transport, finance, and health.
- **Mandatory ransom reporting.** Covered organizations must report ransom payments to the government, which affects incident response planning.
- **Employees based in country.** Employees face sophisticated scams, identity theft after large breaches, and border examination of devices. Remote regions have limited coverage.
- **Vendor and supply chain risk.** Third-party platforms were the source of major customer-data thefts in 2025, so SaaS and outsourced customer-service providers are the key exposure. Mandatory ransom-payment reporting and critical-infrastructure duties apply to covered entities.

The TIDE team tracks 109 threat actors that list Australia among their targets. By attributed nexus, they break down as 70 cybercriminal, 25 China-nexus, 5 Iran-nexus, 4 unattributed or other, 2 North Korea-nexus, 1 Russia-nexus, 1 Lebanon-nexus, and 1 hacktivist. The most frequently targeted sectors are healthcare and pharmaceuticals (63), government (58), industrial and manufacturing (52), technology (52), and banking and financial services (38). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Scams.** Australians lose large sums to investment, romance, and impersonation scams, and the government has funded a national anti-scam center. Bank impersonation and remote-access scams are common.

- **Identity theft after breaches.** Large breaches exposed identity document numbers and personal data for millions, and these data fuel phishing and fraud.
- **Account takeover and SIM swap.** Telecommunications and financial account takeover remain frequent.
- **Online safety.** Sextortion and image-based abuse have increased, and regulators have strengthened enforcement.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Australia. Australia appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Australia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Australia is stable and well-regulated, and the main traveler risks are sophisticated scams and legal border powers to examine devices. State-linked espionage targets organizations more than visitors.
- **What would change this rating.** Raise to Level 2 if state-linked targeting of travelers or large-scale device seizures at the border are reported.

Public Wi-Fi

- Australia's regulatory rigor is offset by high-volume ransomware activity and large citizen-data breaches that fuel identity theft and phishing; Australian Border Force can also inspect devices at the border. Use a corporate VPN for public networks, and consider traveling with minimal sensitive data to avoid border examination.

Device and account controls

- Standard business travel controls apply: encryption, phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe.
- Australian Border Force has legal powers to examine electronic devices and, in certain circumstances, to require passcodes. Travelers carrying sensitive data should limit what they bring and follow company guidance on border searches.

Local practices

- Verify that mobile roaming or a local eSIM covers remote areas, since coverage is limited outside cities and highways.
- Be alert to bank and tax impersonation scams after arrival.

Return protocol

- If a device left your control at the border, report it to security and have it checked before reconnecting to corporate resources.

WORLDBOOK

AUSTRIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Vienna

GOVERNMENT
Federal parliamentary republic

LANGUAGE
German

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued August 21, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable, but Vienna is a long-standing espionage hub for international organizations.

Country Overview

Austria lies in the heart of Central Europe and was once the center of the Habsburg Empire, which ruled large parts of the continent for centuries. Vienna served as the imperial capital, and the empire's multiethnic territories stretched from the Alps to the Carpathians.

Defeat in the First World War ended the monarchy and left a small republic. Germany annexed Austria in 1938. After the Second World War, four Allied powers occupied the country until the 1955 State Treaty restored independence on the condition of permanent neutrality, which is written into Austrian law.

Austria joined the EU in 1995 and the eurozone in 1999. It has about 9.2 million people and a prosperous export economy. Vienna hosts several UN offices, the OSCE, and OPEC.

Geopolitical Landscape

- **Neutrality and Ukraine.** Austria supports EU sanctions on Russia and aid to Ukraine while remaining militarily neutral and outside NATO.
- **Russian energy dependence.** Austria historically relied on Russian gas, and the end of Ukrainian transit at the start of 2025 and the termination of the main supply contract forced a shift to other sources.

- **Espionage hub.** Vienna has long been a center of espionage because of its international organizations. Austrian courts have handled cases of former officials accused of spying for Russia.
- **Domestic politics.** The far-right Freedom Party won the 2024 national election but was excluded from government. A three-party coalition formed in 2025.

Cyber Threats | Organizations

- **Ransomware and extortion.** Cybercriminal groups account for most actors in the TIDE tracking data that list Austria. Government, healthcare, and education lead the targeted sectors, and public entities, including municipalities and hospitals, have suffered disruption.
- **Pro-Russia hacktivism.** Distributed denial-of-service campaigns by pro-Russia hacktivist groups have hit Austrian government and media websites, especially around political decisions on Ukraine and elections.
- **Espionage around international organizations.** Diplomatic, nuclear-policy, and energy organizations in Vienna attract Russian, Chinese, and Iranian interest. The TIDE team tracks Callisto Group, Infy, Hafnium, and Neodymium among the actors that list Austria.
- **Industrial and supply chain exposure.** Austria's industrial base, including machinery and automotive suppliers, faces intellectual property theft and ransomware.
- **Regulation.** Austria is implementing the EU NIS2 Directive, which broadens security and incident reporting duties.
- **Employees based in country.** Employees in Vienna's diplomatic, energy, and international-organization community face elicitation and spear-phishing. Others face parcel and impersonation scams.
- **Vendor and supply chain risk.** Industrial suppliers and managed service providers are targets for ransomware and intellectual property theft. NIS2 obligations extend security expectations to suppliers.

The TIDE team tracks 19 threat actors that list Austria among their targets. By attributed nexus, they break down as 13 cybercriminal, 3 China-nexus, 1 Iran-nexus, 1 Turkey-nexus, and 1 Russia-nexus. The most frequently targeted sectors are government (13), healthcare and pharmaceuticals (13), education and research (11), industrial and manufacturing (11), and technology (8). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and parcel scams.** Messages impersonating postal services, banks, and tax authorities are common in German.
- **Fraud via messaging apps.** Scammers impersonate relatives using a new phone number to request urgent payments.
- **Online shopping and rental fraud.** Fake shops and fraudulent rental listings are widespread.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Austria. Austria appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Austria Level 1, Exercise Normal Precautions.

TIDE Risk Level Rationale

- **Drivers.** Conditions are stable with low surveillance risk. Vienna is an espionage hub for international organizations, which matters mainly for diplomatic, energy, and policy staff.
- **What would change this rating.** Raise to Level 2 for staff in those roles if Russia-linked targeting of Vienna-based organizations intensifies.

Public Wi-Fi

- Vienna remains a long-standing espionage hub targeting diplomatic, energy, and policy professionals; state-linked actors actively pursue credential theft through compromised networks. Use a corporate VPN strictly for public Wi-Fi access if your role involves diplomatic, energy, or international-organization work.

Device and account controls

- Standard business travel controls apply: encryption, phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe.

Local practices

- Pickpocketing is common at Vienna tourist sites, on public transport, and at Christmas markets, so keep phones and wallets secured.
- Travelers with diplomatic, energy, or international-organization roles in Vienna should expect elicitation attempts and should receive a security briefing.

Return protocol

- Report lost devices immediately and rotate credentials if a device left your control.

WORLDBOOK

AZERBAIJAN

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3

CAPITAL
Baku

GOVERNMENT
Presidential republic

LANGUAGE
Azerbaijani

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued April 28, 2026)

Risk indicators: Terrorism, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Documented spyware use, broad state access to data, regional espionage, and a U.S. Level 3 advisory.

Country Overview

Azerbaijan lies on the western shore of the Caspian Sea at the meeting point of Europe and Asia. Turkic and Persian influences shaped the region, and Russia absorbed the territory in the early nineteenth century. Azerbaijan briefly declared independence in 1918 as the first secular republic in the Muslim world, then became a Soviet republic in 1920.

Independence returned in 1991, followed by a war with Armenia over Nagorno-Karabakh that ended in a 1994 ceasefire. Heydar Aliyev built a dominant presidency, and his son Ilham Aliyev has led the country since 2003. Baku's oil and gas reserves, developed with Western investment, underpin the economy.

Azerbaijan has about 10.3 million people. It supplies natural gas to Europe through the Southern Gas Corridor, and it hosted the COP29 climate conference in 2024.

Geopolitical Landscape

- **Peace with Armenia.** Azerbaijan recaptured Nagorno-Karabakh in 2023. Aliyev and Armenian Prime Minister Pashinyan signed a joint declaration in Washington on August 8, 2025. Baku says a final treaty requires

Armenia to amend constitutional language it views as a territorial claim. Armenia's June 2026 election result kept Pashinyan in power and the process on track.

- **TRIPP corridor.** The U.S.-backed Trump Route for International Peace and Prosperity would link mainland Azerbaijan to its Nakhchivan exclave across southern Armenia, with construction expected from late 2026.
- **Relations with Russia.** Ties deteriorated sharply after the December 2024 crash of an Azerbaijan Airlines jet over Russian-controlled airspace and Russian law enforcement raids on Azerbaijani communities in 2025. Baku has hardened its stance toward Moscow.
- **Turkey and Israel.** Azerbaijan is a close partner of Turkey and supplies oil to Israel, which draws Iranian criticism.
- **Domestic politics.** Authorities have imprisoned journalists and activists, and international groups rate the country as not free.

Cyber Threats | Organizations

- **Energy sector.** Oil and gas producers, pipeline operators, and their contractors are strategic targets for espionage and disruption.
- **Espionage against government and defense.** The TIDE team tracks Confucius (India-nexus), Fox Kitten (Iran-nexus), and Turla (Russia-nexus) among the actors that list Azerbaijan. Government, defense, and diplomatic organizations are the leading sectors.
- **Regional tension.** Iran-linked and Russia-linked actors have reason to monitor Azerbaijani policy, and the Armenia-Azerbaijan peace process increases political interest in networks.
- **State access to data.** Authorities have broad ability to monitor and compel disclosure, so foreign organizations should treat locally hosted data as accessible to the state.
- **Ransomware and fraud.** Banks and telecommunications firms face financial crime and phishing.
- **Employees based in country.** Staff should assume communications are monitored and that political or Karabakh-related comments can bring legal exposure. Employees in energy, government, or media roles face spyware and phishing risk.
- **Vendor and supply chain risk.** Telecom operators and energy contractors are state-linked and can be compelled to share data. Vendor access to oil, gas, and pipeline systems requires strict segmentation, and vendors should be screened for sanctions and state ties.

The TIDE team tracks 4 threat actors that list Azerbaijan among their targets. By attributed nexus, they break down as 1 Russia-nexus, 1 Iran-nexus, 1 India-nexus, and 1 unattributed or other. The most frequently targeted sectors are government (4), defense and defense industrial base (3), diplomatic and foreign affairs (2), education and research (2), and technology (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Spyware and surveillance.** Citizen Lab and Amnesty International have documented spyware use against Azerbaijani journalists and activists. Individuals in these communities should apply hardened device settings.
- **Social media monitoring.** Online criticism of the government can lead to arrest. Authorities have blocked independent news sites.

- **Consumer fraud.** Phishing and fake-shop scams circulate in Azerbaijani and Russian.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Azerbaijan. Azerbaijan appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Azerbaijan Level 3, Reconsider Travel, citing terrorism and other risks, and advises against travel near the Armenian border and to Nagorno-Karabakh.

TIDE Risk Level Rationale

- **Drivers.** Spyware has been documented against journalists and activists, the state can access data held in country, and Azerbaijan is a target of Russia-, Iran-, and India-nexus espionage. The State Department rates the country Level 3.
- **What would change this rating.** Raise to Level 4 if detentions of foreigners or device inspections increase or relations with Russia or Iran deteriorate sharply. Lower to Level 2 if the Armenia peace treaty is signed and monitoring eases.

Public Wi-Fi

- Azerbaijan's state can access data held in country and use spyware against targets; hotel and carrier networks are monitored, and journalists, activists, and energy-sector staff face elevated phishing risk. Do not use public Wi-Fi without a corporate VPN, and assume all networks are observed by state authorities.

Recommended corporate policy

- Allow travel only for approved business needs. Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, and prefer a clean loaner laptop and phone for sensitive roles.
- Use a corporate VPN, and assume hotel and carrier networks are monitored.
- Avoid carrying sensitive documents, and limit data on devices to what the trip requires.

Local risks and practices

- Do not photograph government buildings, military sites, or energy infrastructure.
- Avoid commenting on politics, Karabakh, or the government on social media during the trip.
- Employees in the energy sector should receive an elicitation briefing.

Return protocol

- Report suspicious contacts, rotate credentials accessed during travel, and review device integrity before reconnecting to corporate systems.

WORLDBOOK

BAHAMAS

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Nassau

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 28, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low state-surveillance risk; exposure is tourism fraud and crime.

Country Overview

The Bahamas is an archipelago of about 700 islands and cays in the Atlantic Ocean southeast of Florida. The indigenous Lucayan people were the first Americans to meet Columbus in 1492 and were decimated within decades. British settlers arrived in the seventeenth century, and the islands later became a haven for pirates and a base for blockade runners during the American Civil War.

The Bahamas gained independence from Britain in 1973 and remains a Commonwealth realm. The country has about 400,000 residents. Tourism provides roughly half of economic output, and offshore financial services provide a second pillar.

Prime Minister Philip Davis has led the government since 2021.

Geopolitical Landscape

- **Climate and hurricanes.** Hurricane Dorian devastated Abaco and Grand Bahama in 2019, and storm risk shapes budgeting, insurance, and diplomacy on climate finance.
- **Financial sector compliance.** The Bahamas has worked to leave international money laundering watchlists and adopted stronger transparency rules following pressure from the Financial Action Task Force and OECD.

- **Crypto and FTX.** The collapse of FTX, headquartered in Nassau, in 2022 drew scrutiny of the country's digital asset regulation.
- **Migration and crime.** Irregular migration from Haiti and a rising homicide rate are central domestic issues.

Cyber Threats | Organizations

- **Tourism and hospitality.** Resorts and cruise operators hold payment and identity data, and they face ransomware, card fraud, and booking-system compromise.
- **Financial services.** Banks, trust companies, and digital asset firms handle high-value assets, which attracts phishing, account takeover, and extortion.
- **Public services.** Government and utilities depend on limited local security staffing, and island geography makes continuity planning important.
- **Regional pattern.** Caribbean governments have seen ransomware against public services, so Bahamian entities should plan around that pattern.
- **Employees based in country.** Employees face tourist-area theft, card skimming, and hurricane disruption. Financial-sector staff face phishing.
- **Vendor and supply chain risk.** Resorts and financial firms rely on small vendors and cloud services. Digital-asset and offshore providers hold high-value data.

The TIDE team does not currently track actors that list Bahamas among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Tourist-targeted fraud.** Fake accommodation listings, ticket scams, and card skimming target visitors.
- **Crime-linked device theft.** Opportunistic theft of phones and wallets occurs in tourist areas and on cruise excursions.
- **Phishing in English.** Bank and delivery impersonation scams are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to the Bahamas, and TIDE tracking does not currently list the country among the targets of tracked actors.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates the Bahamas Level 2, Exercise Increased Caution, for crime, and issues specific warnings about areas of Nassau and about water activities.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk with ordinary tourist-area crime and card fraud. Hurricane season can disrupt connectivity.

- **What would change this rating.** Raise to Level 2 if a significant breach affects the financial or digital-asset sector or theft against visitors rises.

Public Wi-Fi

- Tourism and financial sectors face card-skimming fraud and ransomware at resorts and payment terminals; public Wi-Fi at beaches and marinas attracts opportunistic credential theft. Use a corporate VPN for public network access, and verify booking links before entering payment information.

Device and account controls

- Standard business travel controls apply: encryption, multi-factor authentication, a corporate VPN, and remote wipe.
- Avoid public Wi-Fi at resorts, marinas, and airports, and verify booking links before paying.

Local practices

- Keep devices secured and out of sight on beaches, in rental cars, and on excursions.
- Hurricane season, June through November, can disrupt connectivity and travel.

WORLDBOOK

BAHRAIN

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Manama

GOVERNMENT
Constitutional monarchy

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 27, 2026)

Risk indicators: Terrorism, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: U.S.-Iran escalation affecting the Gulf, Iran-linked targeting, spyware use against dissidents, and a U.S. Level 3 advisory.

Country Overview

Bahrain is an island nation in the Persian Gulf between Saudi Arabia and Qatar. The ancient Dilmun civilization flourished there more than four thousand years ago, and the islands later passed under Portuguese, Persian, and Omani influence. The Al Khalifa family has ruled since 1783 and came under British protection in the nineteenth century.

Bahrain became independent in 1971. It was the first Gulf state to discover oil, in 1932, though reserves are now modest, and it developed into a regional banking hub. The population is about 1.6 million, with a Shia majority governed by a Sunni royal family, a division that underlies recurring political tension.

Protests in 2011 during the Arab Spring were suppressed with the help of Saudi and Emirati forces. King Hamad bin Isa Al Khalifa rules, and Crown Prince Salman bin Hamad serves as prime minister.

Geopolitical Landscape

- **Iran conflict spillover.** Crisis Group reports that Iran retaliated against U.S. sites in Bahrain, Jordan, Kuwait, and Iraq's Kurdistan region after U.S. strikes in early September 2026, following earlier hostilities in February 2026. The State Department rates Bahrain and neighboring Gulf states Level 3.
- **U.S. military hub.** Bahrain hosts the U.S. Fifth Fleet and Naval Forces Central Command, which makes the country a target for Iran-linked activity and an anchor of U.S. regional posture.
- **Abraham Accords.** Bahrain normalized relations with Israel in 2020, which drew domestic opposition and Iranian condemnation.
- **Saudi alignment.** Bahrain depends on financial support and security backing from Saudi Arabia and the UAE.
- **Domestic politics.** Opposition groups have been dissolved and leaders imprisoned, and authorities periodically revoke citizenship in security cases.

Cyber Threats | Organizations

- **Iran-linked targeting.** Bahrain's financial, energy, and government sectors are exposed to Iran-linked actors, particularly during regional escalations. Disruptive and espionage campaigns across the Gulf have targeted similar sectors.
- **Financial sector.** Banks and fintech firms, including digital-asset firms licensed in Bahrain, face phishing, business email compromise, and SWIFT-related fraud.
- **Critical infrastructure.** Oil refining, aluminum smelting, and port operations rely on industrial control systems that regional actors have probed.
- **Surveillance of dissidents.** Spyware, including Pegasus, has been used against Bahraini activists, according to Citizen Lab.
- **Regulation.** Bahrain's Personal Data Protection Law took effect in 2019, and the Central Bank issues cybersecurity rules for financial institutions.
- **Employees based in country.** Staff in government, defense, energy, and finance should expect Iran-linked phishing during escalations and should assume state monitoring. Commentary on the royal family, politics, or Israel carries legal risk.
- **Vendor and supply chain risk.** Gulf-wide managed service providers, telecoms, and financial platforms can be disrupted during regional conflict. Vendors serving the naval and energy sectors face elevated state-actor targeting.

The TIDE team tracks 1 threat actor that lists Bahrain among their targets. By attributed nexus, they break down as 1 unattributed or other. The most frequently targeted sectors are civil society and activism (1), diplomatic and foreign affairs (1), and government (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **State monitoring.** Authorities monitor social media and have prosecuted users for posts critical of the government, the royal family, or relations with Israel.
- **Spyware targeting.** Activists, lawyers, and journalists have been targets of commercial spyware.

- **Fraud.** Consumer phishing in Arabic and English impersonates banks, telecommunications providers, and government services.
- **VoIP restrictions.** Some voice-over-IP services face restrictions in the Gulf, so travelers should confirm which calling apps work.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Bahrain.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Bahrain Level 3, Reconsider Travel, citing terrorism and other risks, and updated the advisory on August 27, 2026. Conditions can change quickly because of the confrontation between Iran and the United States.

TIDE Risk Level Rationale

- **Drivers.** U.S.-Iran confrontation has reached Bahrain, with Iranian retaliation against U.S. sites in September 2026. Iran-linked targeting of Gulf finance and energy, documented spyware use against dissidents, and state monitoring raise the level.
- **What would change this rating.** Raise to Level 4 if hostilities escalate to attacks on Bahraini infrastructure or airspace closures. Lower to Level 2 if a durable U.S.-Iran de-escalation holds.

Public Wi-Fi

- U.S.-Iran confrontation escalated to Iranian retaliation against U.S. sites in Bahrain in September 2026, and Iran-linked actors target Gulf financial and energy sectors; hotel and carrier networks are monitored. Use a corporate VPN for all public Wi-Fi access, and assume networks are compromised during regional escalations.

Recommended corporate policy

- Approve travel only for defined business needs and brief travelers on the regional security situation.
- Use company-managed devices with encryption and phishing-resistant multi-factor authentication. Prefer loaner devices for travelers in government, defense, or energy roles.
- Use a corporate VPN and assume hotel and carrier networks are monitored.

Local practices

- Avoid commentary on the royal family, politics, or Israel on social media. Avoid demonstrations.
- Do not photograph government or military facilities, particularly around the naval base.
- Confirm evacuation and security-provider arrangements for the Gulf, since airspace closures have occurred during escalations.

Return protocol

- Rotate credentials for accounts accessed during travel, review device integrity, and debrief travelers with sensitive roles.

WORLDBOOK

BANGLADESH

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Dhaka

GOVERNMENT
Parliamentary republic

LANGUAGE
Bengali

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 30, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Past large-scale financial theft, South Asian espionage, unrest-related shutdowns, and mobile-money fraud.

Country Overview

Bangladesh occupies the delta of the Ganges, Brahmaputra, and Meghna rivers on the Bay of Bengal. The region was part of Bengal under Mughal and then British rule, and it became East Pakistan when British India partitioned in 1947. Language, economic, and political grievances against West Pakistan culminated in the 1971 Liberation War, which ended with Indian intervention and independence under Sheikh Mujibur Rahman.

Military coups and rivalry between the Awami League, led by Mujib's daughter Sheikh Hasina, and the Bangladesh Nationalist Party (BNP), founded by Ziaur Rahman, defined politics for decades. Hasina governed from 2009 until a student-led uprising forced her to flee to India on August 5, 2024. Nobel laureate Muhammad Yunus led an interim government afterward.

Bangladesh has about 170 million people in an area the size of Iowa and is a leading garment exporter. Its first post-uprising election was held on February 12, 2026.

Geopolitical Landscape

- **New government.** The BNP won the February 2026 election, with turnout near 60 percent, and Tarique Rahman was sworn in as prime minister on February 17, 2026. The Awami League was banned from contesting. Rahman's priorities include jobs, energy shortages, constitutional reform, and corruption.

- **India relations.** Ties have been strained since Hasina fled to India, where she remains despite extradition requests, after a Dhaka court sentenced her to death in 2025. Rahman chose China for his first state visit, and has described a relationship of mutual respect with India without promising a reset.
- **China, the United States, and Pakistan.** China is Bangladesh's largest trading partner, and the BNP government says it will balance relations with Washington and Beijing. Ties with Pakistan have warmed.
- **Rohingya.** Bangladesh hosts roughly one million Rohingya refugees from Myanmar in camps near Cox's Bazar, a long-term humanitarian and security challenge.
- **Domestic fragility.** Polarization between BNP and Awami League supporters, Islamist politics, and economic pressure remain risks.

Cyber Threats | Organizations

- **Financial sector.** The 2016 theft of 81 million dollars from Bangladesh Bank's account at the New York Fed, attributed by U.S. authorities to North Korea-linked Lazarus actors, remains a defining case. Banks, mobile financial services such as bKash, and payment switches remain high-value targets.
- **South Asian espionage.** The TIDE team tracks India-nexus actors Bitter, Donot Team, and Patchwork, and China-nexus actors, among those that list Bangladesh. Government, banking, and defense are the leading sectors.
- **Data exposure.** Large leaks of government and citizen data, including from national ID and government portals, have been reported in recent years.
- **Garment and manufacturing supply chain.** Exporters face business email compromise and ransomware, and invoice fraud affects buyers abroad.
- **Political cyber activity.** Elections and political transitions drew hacktivism, defacements, and disinformation.
- **Employees based in country.** Employees face SIM-swap and OTP fraud, phone snatching in traffic, and mobile-data shutdowns during unrest. Garment and finance staff face payment-fraud approaches.
- **Vendor and supply chain risk.** Garment suppliers and local IT vendors are common targets for business email compromise. Verify bank detail changes by phone, and require security standards from vendors that touch payments.

The TIDE team tracks 16 threat actors that list Bangladesh among their targets. By attributed nexus, they break down as 5 China-nexus, 4 India-nexus, 3 unattributed or other, 3 cybercriminal, and 1 Lebanon-nexus. The most frequently targeted sectors are government (12), banking and financial services (6), defense and defense industrial base (5), telecommunications (5), and diplomatic and foreign affairs (5). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile financial fraud.** Fraud through bKash and Nagad wallets, including social engineering for OTP codes, is common.
- **Social media manipulation.** Disinformation and online harassment, including targeting of minorities, spread through Facebook and messaging apps.
- **Internet restrictions.** Authorities have imposed mobile internet shutdowns during unrest, including in 2024.

- **Digital security law use.** Cyber laws have been used to prosecute speech, so individuals should be careful about posts on politics and religion.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Bangladesh. Bangladesh appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Bangladesh Level 2, Exercise Increased Caution, citing unrest, crime, kidnapping or hostage-taking, and terrorism, and advises against travel to the Chittagong Hill Tracts.

TIDE Risk Level Rationale

- **Drivers.** Mobile-money fraud, phone snatching, and shutdowns during unrest are the main risks, along with South Asian espionage against government and finance. The new government is stabilizing, but politics remain polarized.
- **What would change this rating.** Raise to Level 3 if unrest returns with internet shutdowns. Lower to Level 1 as fraud and theft risk decline.

Public Wi-Fi

- Bangladesh faces mobile-money fraud via SIM-swap and one-time password theft, and phone snatching in traffic can lead to account takeover; public networks amplify credential interception risk. Conceal devices in transit, use a corporate VPN when accessing public networks, and restrict mobile-money access when traveling.

Device and account controls

- Company devices can travel under standard controls: encryption, managed profile, phishing-resistant multi-factor authentication, and remote wipe.
- Use a corporate VPN, avoid public Wi-Fi, and keep devices concealed in traffic, where phone snatching occurs.
- Expect mobile and internet shutdowns during unrest and plan communications accordingly.

Local practices

- Avoid political gatherings and demonstrations, which can turn violent.
- Carry power banks, since outages are frequent.
- Business travelers in garment and finance sectors should expect payment-fraud approaches and verify bank details by phone.

Return protocol

- Rotate credentials accessed in country and report any device compromise.

WORLDBOOK

BARBADOS

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Bridgetown

GOVERNMENT
Parliamentary republic

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued April 10, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low state-surveillance risk; exposure is tourism and business-services fraud.

Country Overview

Barbados is a small island in the eastern Caribbean, east of the Windward Islands. English settlers arrived in 1627, and the island became one of Britain's earliest plantation societies, with a sugar economy built on enslaved African labor. Barbados remained British for more than three centuries.

Independence came in 1966, and the country removed the British monarch as head of state to become a republic on November 30, 2021, with Dame Sandra Mason as its first president. Prime Minister Mia Mottley has led the government since 2018, and her party won all seats in the 2022 election.

Barbados has about 260,000 people, strong social indicators, and an economy centered on tourism and international business services. The country is a leading voice on climate finance in the Caribbean.

Geopolitical Landscape

- **Climate finance diplomacy.** Mottley's Bridgetown Initiative calls for reform of global finance to support climate-vulnerable states.
- **Reparations.** Barbados is a leading advocate for reparations related to slavery, within CARICOM.
- **Debt restructuring.** A 2018 debt restructuring and subsequent reforms stabilized public finances.

- **Regional security.** Barbados participates in CARICOM security cooperation and has expressed concern over gang violence and arms flows in the region.

Cyber Threats | Organizations

- **Tourism and hospitality.** Hotels and attractions face payment-card and booking fraud.
- **International business sector.** Corporate service providers and financial firms hold client data that attracts phishing and extortion.
- **Small-state resourcing.** Vendors and cloud services carry most of the security burden, and hurricanes can disrupt continuity.
- **Regional pattern.** Caribbean public services have suffered ransomware in recent years.
- **Employees based in country.** Employees face tourist-area scams and hurricane disruption. Business-services staff face phishing.
- **Vendor and supply chain risk.** Small vendors and cloud providers carry most of the exposure. Corporate service providers hold client data and should be vetted.

The TIDE team tracks 2 threat actors that list Barbados among their targets. By attributed nexus, they break down as 1 China-nexus, and 1 cybercriminal. The most frequently targeted sectors are government (2), civil society and activism (1), diplomatic and foreign affairs (1), banking and financial services (1), and education and research (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Tourist-targeted scams.** Fake rental listings and taxi or tour overcharges affect visitors.
- **Phishing and government data breaches.** Flow and Digicel are the mobile operators; the Barbados Revenue Authority confirmed a data breach in October 2024 after a threat actor claimed to have obtained roughly 230GB from its vehicle-registration systems, and the Central Bank of Barbados separately warned in April 2025 of a fraudulent video impersonating its Governor to promote a fake investment scheme.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Barbados. TIDE tracking lists Barbados among the targets of two actors, including a China-nexus espionage campaign.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Barbados Level 1, Exercise Normal Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk and ordinary tourist fraud. Business-services staff face phishing, and hurricanes can disrupt operations.

- **What would change this rating.** Raise to Level 2 if ransomware affecting regional public services reaches Barbados.

Public Wi-Fi

- Government and revenue-authority systems have been targeted by credential-based intrusions, and video and messaging impersonation of officials is an active fraud vector; use a corporate VPN for public network access in business districts and resorts, and verify any investment offer attributed to a public official through an official channel before acting on it.

Device and account controls

- Standard business travel controls apply: encryption, multi-factor authentication, a corporate VPN, and remote wipe.
- Verify rental and booking links before paying.

Local practices

- Keep devices out of sight on beaches and in vehicles.
- Hurricane season, June through November, can interrupt connectivity and travel.

WORLDBOOK

BELARUS

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4

CAPITAL
Minsk

GOVERNMENT
Presidential republic (authoritarian)

LANGUAGE
Belarusian and Russian

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued December 29, 2025)

Risk indicators: Unrest, other

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Authoritarian state surveillance, arbitrary detention, sanctions, and a U.S. Level 4 advisory.

Country Overview

Belarus is a landlocked country in Eastern Europe bordered by Russia, Ukraine, Poland, Lithuania, and Latvia. Its territory was part of the Grand Duchy of Lithuania and later the Polish-Lithuanian Commonwealth before the Russian Empire absorbed it in the late eighteenth century. The Soviets established the Byelorussian Soviet Socialist Republic in 1919, and the republic suffered devastating losses in the Second World War.

Belarus became independent in 1991 when the Soviet Union dissolved. Alexander Lukashenko has been president since 1994, and constitutional changes have removed term limits. The 2020 election, which opposition and Western governments rejected as fraudulent, triggered mass protests and a harsh crackdown. Lukashenko won another term in January 2025 in a vote that Western governments did not recognize.

Belarus has about 9 million people. It forms a Union State with Russia, hosts Russian forces and nuclear weapons, and relies on Russian energy and markets.

Geopolitical Landscape

- **Alliance with Russia.** Belarus allowed Russia to use its territory to invade Ukraine in 2022 and hosts Russian military exercises, including the Zapad series. Belarus is subject to Western sanctions in coordination with those on Russia.
- **Hybrid pressure on neighbors.** Since 2021, Belarus has been accused of facilitating irregular migration to Poland, Lithuania, and Latvia, and of balloon incursions that closed airports and border crossings in Lithuania in 2025.
- **U.S. engagement.** Washington has traded sanctions relief for prisoner releases in three rounds: Belavia in September 2025 (52 prisoners), potash producers in December 2025 (123), and in March 2026 the removal of Belaruskali and the Belarusian Potash Company from the sanctions list plus relief for two state banks and the Finance Ministry (250). The talks have not changed Minsk's alignment with Moscow.
- **Political prisoners.** About 1,000 political prisoners remain in jail despite the releases, and authorities continue to prosecute opponents and journalists.
- **Opposition abroad.** Opposition leader Sviatlana Tsikhanouskaya operates from Lithuania, and exile groups, including the Cyber Partisans, continue activity against the government.

Cyber Threats | Organizations

- **Hacktivist operations against the state.** The Belarusian Cyber Partisans have breached government systems, railways, and police databases, and in July 2025 they claimed, with the group Silent Crow, an attack on Russia's Aeroflot.
- **State surveillance.** Authorities hold broad access to telecommunications and compel data from local firms. Foreign organizations should assume the state can observe data stored or transmitted in country.
- **Sanctions and technology constraints.** Western sanctions limit access to some technology and services, and Belarusian IT firms work with a mix of Western and Russian suppliers.
- **IT outsourcing sector.** The Hi-Tech Park sector historically served Western clients. Organizations with developers in Belarus should review access controls, legal exposure, and sanctions risk.
- **Targeting by Russia-linked actors.** The TIDE team tracks Turla and other Russia-nexus groups among the actors that list Belarus among their targets, together with China-nexus activity.
- **Employees based in country.** Staff face monitoring of devices and networks, checkpoint phone searches, prosecution for chat and channel membership, and risk of arbitrary detention. Remove all company access from personal devices.
- **Vendor and supply chain risk.** IT-outsourcing firms and telecoms operate under state control. Developers and contractors based in Belarus create sanctions, compelled-access, and code-integrity risk that warrants removal or strict isolation.

The TIDE team tracks 10 threat actors that list Belarus among their targets. By attributed nexus, they break down as 2 Russia-nexus, 2 Belarus-nexus, 2 hacktivist, 2 unattributed or other, 1 cybercriminal, and 1 China-nexus. The most frequently targeted sectors are government (8), diplomatic and foreign affairs (4), defense and defense industrial base (3), military (3), and industrial and manufacturing (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and prosecution.** Users have been prosecuted for comments, chat membership, and subscriptions to channels labeled extremist. Authorities designate independent media as extremist and criminalize their consumption.
- **Device searches.** Police inspect phones at checkpoints and during detentions.
- **Internet disruption.** Authorities cut or throttled internet access during the 2020 protests and after.
- **Phishing and fraud.** Consumer fraud impersonating banks and delivery services circulates in Russian.

State-Sponsored Cyber Threats

Belarus's state security services are linked to cyber activity aimed at neighbors and at dissidents. Attribution is less settled than for larger states, so the table notes where governments or vendors disagree.

GROUP	ALSO KNOWN AS	ATTRIBUTED SPONSOR	FOCUS	ACTIVE
Ghostwriter (UNC1151)	Operation Ghostwriter	Belarus military intelligence per Mandiant assessment; Germany has attributed related activity to Russia	Influence operations and credential theft	2016 to present
MoustachedBouncer	None widely used	Belarus state-aligned; TIDE links it to the State Security Committee (KGB)	Espionage against embassies and diplomats	2014 to present

Pro-Belarus groups' activity often overlaps with Russian operations, and the Belarusian Cyber Partisans are opposition hacktivists, not state actors.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Belarus Level 4, Do Not Travel, citing unrest and other risks, and the U.S. Embassy in Minsk suspended operations in 2022. Consular help is not available in country, and the advisory warns of arbitrary detention of U.S. citizens.

TIDE Risk Level Rationale

- **Drivers.** The state surveils communications, searches phones at checkpoints, and prosecutes people for chat and channel membership. Wrongful detention risk is acute, the U.S. Embassy is closed, and Belarus-based IT firms create sanctions and compelled-access risk.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require prisoner releases to continue, consular access to return, and an end to arbitrary detention of foreigners.

Public Wi-Fi

- Belarusian state surveillance monitors all telecommunications, police conduct device inspections at checkpoints, and VPN use can draw attention; public Wi-Fi with a VPN may itself trigger official interest. Do not access public Wi-Fi at all; remove all company access from personal devices before travel.

Recommended corporate policy: no device, no infrastructure

- Employees do not bring company-issued devices into Belarus.
- Employees remove all company-linked accounts and applications from personal devices before travel, including authenticator apps and password managers.
- Employees do not log in to company-linked accounts while in country.
- Block sign-ins from Belarus with geo-based conditional access, and alert on every attempt.
- If a business need is approved, issue a clean loaner device with minimal data and reimage it on return.

Communications and safety

- Assume communications and devices are monitored, and avoid public Wi-Fi and public charging.
- Do not wear company apparel or discuss work. Prepare an approved cover answer and treat unsolicited approaches with caution.
- Confirm that travel medical and evacuation coverage applies to Level 4 destinations and that any provider can operate in Belarus.
- Border crossings with Poland, Lithuania, and Latvia have faced closures, so confirm routes in advance.
- Involve counsel on sanctions and export controls.

Return protocol

- Treat any personal device that traveled as untrusted and wipe it before re-enrolling it. Rotate credentials for accounts it touched from a trusted network, and hold a debrief.

WORLDBOOK

BELGIUM

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Brussels

GOVERNMENT
Federal parliamentary constitutional monarchy

LANGUAGE
Dutch, French, and German

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 23, 2026)

Risk indicators: Terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: NATO and EU hub drawing persistent espionage, plus ransomware against public bodies.

Country Overview

Belgium sits in northwestern Europe between France, the Netherlands, Germany, and Luxembourg. The territory was long contested among European powers and was part of the Spanish and Austrian Netherlands. Belgium became independent from the Netherlands in 1830 after a revolution, and King Leopold I took the throne in 1831.

Belgium was occupied by Germany in both world wars. It colonized the Congo, first as Leopold II's personal possession and then as a state colony until 1960, a history that remains a subject of national reckoning. Belgium was a founding member of the European Coal and Steel Community and hosts NATO headquarters and the main EU institutions in Brussels.

Belgium has about 12 million people and a federal structure that divides power among Flemish, Walloon, and Brussels regions and three language communities. Prime Minister Bart De Wever took office in February 2025.

Geopolitical Landscape

- **EU and NATO host.** Brussels concentrates diplomats, lobbyists, and international officials, which creates persistent espionage interest.

- **Russia and Ukraine.** Belgium supports EU sanctions and holds a large share of immobilized Russian central bank assets at Euroclear, and has been cautious about plans to use them to finance Ukraine because of legal and financial risk.
- **Drones and hybrid threats.** Unidentified drones disrupted airports in Belgium in late 2025, and officials have discussed hybrid threats including sabotage and espionage.
- **Terrorism.** Belgium has experienced attacks, including the 2016 Brussels bombings, and maintains an elevated terrorism threat assessment.
- **Domestic politics.** Coalition negotiations are long and complex, and the government pursues budget consolidation and migration measures.

Cyber Threats | Organizations

- **State-linked espionage.** Chinese, Russian, and Iranian actors target EU institutions, NATO, and Belgian ministries. The TIDE team tracks 12 China-nexus actors and 2 Russia-nexus actors that list Belgium, including Cold River, Gallium, and Earth Minotaur.
- **Ransomware.** Cybercriminal groups are the largest group in TIDE tracking that list Belgium. Government, healthcare, and industrial and manufacturing organizations lead the sectors, and incidents have affected hospitals and local authorities.
- **Defense and logistics.** The Belgian Defence ministry suffered an intrusion through the Log4j vulnerability in December 2021, and the ports of Antwerp and Zeebrugge are critical logistics nodes.
- **Financial infrastructure.** Euroclear and SWIFT are headquartered in Belgium, which makes them high-value targets for espionage and disruption.
- **Regulation.** Belgium is implementing NIS2, and the Centre for Cybersecurity Belgium coordinates national response.
- **Employees based in country.** Employees at EU institutions, NATO, think tanks, and lobbying firms face targeted spear-phishing and fake-recruiter approaches. Others face parcel and bank impersonation.
- **Vendor and supply chain risk.** Euroclear, SWIFT, ports, and logistics suppliers are high-value nodes. Third parties serving EU and NATO customers are targeted as a path in, so require strong supplier assurance under NIS2.

The TIDE team tracks 39 threat actors that list Belgium among their targets. By attributed nexus, they break down as 17 cybercriminal, 12 China-nexus, 3 unattributed or other, 2 Russia-nexus, 2 Turkey-nexus, 2 Iran-nexus, and 1 Belarus-nexus. The most frequently targeted sectors are government (23), healthcare and pharmaceuticals (18), industrial and manufacturing (13), banking and financial services (10), and education and research (10). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and fraud.** Bank and parcel impersonation is common in Dutch, French, and English, and fraudulent calls claiming to be from a bank are widespread.
- **Targeting of officials and lobbyists.** Staff at EU institutions and think tanks face targeted spear-phishing and fake recruiter approaches.

- **Online marketplace fraud.** Fake listings and payment-link fraud affect buyers and sellers.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Belgium. Belgium appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Belgium Level 2, Exercise Increased Caution, for terrorism.

TIDE Risk Level Rationale

- **Drivers.** Brussels concentrates EU and NATO staff who draw persistent Chinese and Russian espionage and spear-phishing. Ordinary visitors face pickpocketing and impersonation scams, so the rating reflects role-based exposure.
- **What would change this rating.** Travelers outside EU, NATO, and policy roles face Level 1 conditions. Raise to Level 3 if sabotage or targeted device compromise at institutions increases.

Public Wi-Fi

- Brussels concentrates EU, NATO, and diplomatic staff who face persistent spear-phishing and device-targeting by Chinese and Russian actors; conference networks and hotels are monitored for espionage. Use a corporate VPN strictly for public Wi-Fi access if your role involves EU, NATO, or policy work, and avoid unknown charging points and USB devices.

Device and account controls

- Standard business travel controls apply: encryption, phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe.
- Travelers to EU institutions, NATO, or diplomatic events should expect elevated phishing and device-targeting risk, and should avoid unknown charging points, USB drives, and conference gifts.

Local practices

- Pickpocketing is common at Brussels train stations, on trams, and in tourist areas.
- Rail and airport strikes occur periodically, so confirm itineraries.

Return protocol

- If a device left your control during a conference, have it checked before reconnecting to corporate resources.

WORLDBOOK

BELIZE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Belmopan

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued March 12, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low state-surveillance risk; exposure is crime and tourism fraud.

Country Overview

Belize lies on the Caribbean coast of Central America between Mexico and Guatemala. The Maya civilization built major cities in the territory, and British settlers, known as Baymen, harvested logwood and mahogany from the seventeenth century. Britain formalized control as British Honduras in 1862.

Belize became independent in 1981, but a longstanding territorial claim by Guatemala delayed full security guarantees, and British troops remained for years. The claim is now before the International Court of Justice. The population is about 420,000, and it is the only Central American country with English as its official language.

Tourism, agriculture, and the Belize Barrier Reef, a UNESCO World Heritage site, anchor the economy. Prime Minister Johnny Briceno has led the government since 2020.

Geopolitical Landscape

- **Guatemala dispute.** The Guatemala-Belize territorial claim is before the International Court of Justice, and both countries have accepted its jurisdiction.
- **Debt and climate.** Belize restructured its debt in debt-for-nature swaps, and hurricane risk shapes fiscal planning.

- **Crime and gangs.** Gang violence in Belize City drives crime concerns, and authorities have used states of emergency in some areas.
- **Migration and transit.** Belize is on migration and narcotics routes through Central America.

Cyber Threats | Organizations

- **Tourism and hospitality.** Resorts and tour operators face payment fraud and ransomware.
- **Public institutions and utilities.** Limited local security staffing and reliance on vendors increase exposure.
- **Financial services and offshore sector.** Banks and corporate service providers hold client data attractive to fraud and extortion.
- **Regional pattern.** Central American and Caribbean governments have faced ransomware against ministries and utilities.
- **Employees based in country.** Employees face tourist-area theft and card fraud, limited coverage on the cayes, and hurricane disruption.
- **Vendor and supply chain risk.** Small vendors and offshore service providers hold client data with limited security staffing.

The TIDE team does not currently track actors that list Belize among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Tourist-targeted fraud.** Fake accommodation and tour listings, plus card skimming, target visitors.
- **Phishing in English and Spanish.** Digicel and state-owned Smart! (Belize Telemedia) provide mobile service; Belize's Police Information Technology and Cyber Unit investigates phishing and ATM fraud, and the Financial Intelligence Unit has warned of fraudulent emails falsely claiming to be from the FIU.
- **Device theft.** Opportunistic theft occurs in tourist areas and on public transport.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Belize, and TIDE tracking does not currently list Belize among the targets of tracked actors.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Belize Level 2, Exercise Increased Caution, for crime, and warns about areas of Belize City.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with crime and card fraud in tourist areas and limited connectivity on the cayes.

- **What would change this rating.** Raise to Level 2 if crime affecting visitors rises or a major breach hits local providers.

Public Wi-Fi

- Connectivity runs through the Strategic Evolution Underwater Link and the ARCOS-1 regional cable system; credit card skimming is documented in restaurants, bars, and hotels. Use a corporate VPN for public network access, keep devices concealed and secured, and verify booking and property-transfer details through official channels rather than links received by message.

Device and account controls

- Standard business travel controls apply: encryption, multi-factor authentication, a corporate VPN, and remote wipe.
- Keep devices out of sight and secured in vehicles, on boats, and at the beach.

Local practices

- Hurricane season, June through November, can interrupt travel and connectivity.
- Mobile coverage is limited on cayes and in remote areas, so carry offline copies of key details.

WORLDBOOK

BENIN

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Porto-Novo (seat of government in Cotonou)

GOVERNMENT
Presidential republic

LANGUAGE
French

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued January 7, 2026)

Risk indicators: Crime, kidnapping or hostage-taking, terrorism, unrest

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Regional fraud ecosystem, jihadist spillover in the north, and recent coup attempt.

Country Overview

Benin is a narrow West African country between Togo and Nigeria that extends from the Atlantic coast north to the Niger River. The Kingdom of Dahomey, a powerful state with a notable military tradition, dominated the south until French conquest in the 1890s. France ruled the territory as part of French West Africa and Benin became independent in 1960.

After independence, Benin experienced coups, and then a Marxist-Leninist government under Mathieu Kerekou from 1972 to 1990. A national conference in 1990 launched a peaceful transition to multiparty democracy, widely cited as a model for Africa.

Benin has about 13.6 million people and a cotton-dependent economy with a major port at Cotonou serving landlocked Sahel states. Patrice Talon has been president since 2016 and served the two terms permitted by the constitution.

Geopolitical Landscape

- **Transition of power.** Romuald Wadagni, Patrice Talon's chosen successor and finance minister, won the April 12, 2026 presidential election with about 94 percent of the vote and turnout near 59 percent. Talon is leaving after two terms. The governing coalition holds every seat in parliament after the main opposition party

missed the 20 percent threshold in the January 2026 elections, and observers note that sponsorship rules constrain opposition participation.

- **Coup attempt.** In December 2025, a group of soldiers announced on state television that they had seized power, and loyal forces, with support from Nigeria and regional partners, put down the attempt.
- **Jihadist spillover.** Armed groups linked to JNIM, operating from Burkina Faso and Niger, have attacked security forces in northern Benin, including a deadly attack on soldiers in April 2025.
- **Relations with Niger.** Benin and Niger have disputed border closures and the use of the Benin-Niger oil pipeline since the 2023 coup in Niger.
- **Regional alignment.** Benin remains in ECOWAS, while neighboring juntas in Burkina Faso, Mali, and Niger formed the Alliance of Sahel States.

Cyber Threats | Organizations

- **Port and logistics.** The Port of Cotonou, a gateway for regional trade, relies on digital customs and logistics systems that attract fraud and disruption.
- **Financial sector.** Banks and mobile money operators face account takeover, social engineering, and insider fraud. The TIDE team tracks one cybercriminal actor that lists Benin.
- **Public sector.** Limited local security capacity makes government systems susceptible to opportunistic attacks.
- **Business email compromise.** West African criminal groups run business email compromise and romance scams, often targeting foreign firms, and Benin is part of that regional ecosystem.
- **Employees based in country.** Staff face phone snatching on motorbike taxis, mobile-money fraud, and possible internet throttling around elections.
- **Vendor and supply chain risk.** Port of Cotonou logistics providers and mobile-money operators are key third parties for regional trade. West African business email compromise rings often target firms through compromised vendor mailboxes.

The TIDE team tracks 1 threat actor that lists Benin among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile money and messaging fraud.** Phishing and SIM-swap attacks target mobile money users.
- **Online scams.** Romance and advance-fee schemes use local and foreign victims.
- **Internet restrictions.** Authorities have throttled internet access around elections.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Benin.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Benin Level 2, with indicators for crime, kidnapping, terrorism, and unrest, and advises against travel to the northern border regions and national parks near Burkina Faso and Niger.

TIDE Risk Level Rationale

- **Drivers.** Mobile-money fraud and phone snatching are common, jihadist violence reaches the north, and a coup attempt in December 2025 shows political fragility. Internet throttling has occurred around elections.
- **What would change this rating.** Raise to Level 3 if instability or election-related shutdowns increase. Lower to Level 1 as the political transition stabilizes.

Public Wi-Fi

- West African criminal groups conduct business email compromise and mobile-money fraud via public networks; phone snatching on motorbike taxis is routine and can enable SIM-swap and account takeover. Conceal devices in public, use a corporate VPN for any public network access, and be cautious with mobile-money authentication.

Device and account controls

- Standard business travel controls apply: encryption, phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe.
- Keep devices concealed in traffic and on motorbike taxis, where snatching occurs.

Local practices

- Avoid the northern border areas, and avoid demonstrations.
- Mobile coverage and electricity are uneven, so carry power banks and offline details.

Return protocol

- Report lost devices immediately and rotate credentials for accounts accessed in country.

WORLDBOOK

BHUTAN

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Thimphu

GOVERNMENT
Parliamentary constitutional monarchy

LANGUAGE
Dzongkha

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued September 4, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low crime, but government and diplomatic targets draw China-nexus espionage.

Country Overview

Bhutan is a small Himalayan kingdom between India and China. Tibetan Buddhist leader Ngawang Namgyal unified the region in the seventeenth century, and Bhutan remained largely isolated. The Wangchuck dynasty has ruled since 1907, and Bhutan came under Indian influence through treaties after 1949.

Bhutan opened to the world slowly. Television and the internet arrived only in 1999. The fourth king introduced the philosophy of Gross National Happiness and voluntarily gave up absolute power, and the country held its first national elections in 2008 under a new constitution.

Bhutan has about 790,000 people, an economy built on hydropower exports to India and on tourism, and a policy of high-value, low-volume tourism. Prime Minister Tshering Tobgay has led the government since 2024.

Geopolitical Landscape

- **Between India and China.** Bhutan has no formal diplomatic relations with China and has held border talks for decades. The Doklam plateau, where Indian and Chinese forces faced off in 2017, remains a sensitivity.
- **India dependence.** India is Bhutan's largest trading partner and financier of hydropower, and the two countries have close security ties.

- **Gelephu Mindfulness City.** Bhutan is developing a special administrative region on its southern border to attract investment and to retain young Bhutanese who migrate abroad.
- **Emigration.** Large numbers of young Bhutanese have left for Australia and elsewhere, which affects the labor force.

Cyber Threats | Organizations

- **Government and diplomatic espionage.** The TIDE team tracks the China-nexus campaigns RedHotel and GhostNet among those that list Bhutan, with government and diplomatic organizations as the leading sectors.
- **National digital identity and e-government.** Bhutan's national digital identity system and e-government platforms hold sensitive citizen data and should be treated as strategic assets.
- **Hydropower infrastructure.** Hydropower plants are critical to the economy and to India's grid, and operational technology demands segmentation.
- **Digital assets.** Bhutan holds and mines cryptocurrency through state-linked entities, which creates theft and key-management risk.
- **Small-state resourcing.** Limited local security staffing increases reliance on international partners.
- **Employees based in country.** Most employees face ordinary travel risk. Staff in government, diplomatic, or hydropower roles may draw targeted phishing.
- **Vendor and supply chain risk.** Small government IT teams depend on international partners and a national digital identity platform. Hydropower and e-government vendors should be segmented from corporate systems.

The TIDE team tracks 2 threat actors that list Bhutan among their targets. By attributed nexus, they break down as 2 China-nexus. The most frequently targeted sectors are government (2), civil society and activism (1), diplomatic and foreign affairs (1), aerospace (1), and education and research (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and scams.** Consumer scams and fake-job schemes are rising as connectivity grows.
- **Fraud targeting emigrants.** Overseas Bhutanese face visa and employment scams.
- **Social media.** Facebook and messaging apps dominate, and misinformation can spread quickly in a small community.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Bhutan. Bhutan appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Bhutan Level 1, Exercise Normal Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low crime and light surveillance of visitors. Government and diplomatic staff may draw China-nexus targeting.
- **What would change this rating.** Raise to Level 2 for government-linked travelers if targeting increases.

Public Wi-Fi

- China-nexus campaigns target Bhutanese government and diplomatic staff; hydropower infrastructure supporting India's grid is also of strategic interest. Use a corporate VPN for public network access if your role involves government, diplomatic, or critical-infrastructure work.

Device and account controls

- Standard business travel controls apply: encryption, multi-factor authentication, a corporate VPN, and remote wipe.
- Travelers in diplomatic, defense, or government roles should expect elevated targeting.

Local practices

- Visitors must arrange travel through licensed operators, and a daily fee applies.
- Connectivity is limited in mountain and rural areas, so download documents and maps in advance.
- Altitude and weather can disrupt flights into Paro.

WORLDBOOK

BOLIVIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Sucre (constitutional) and La Paz (seat of government)

GOVERNMENT
Presidential republic (plurinational state)

LANGUAGE
Spanish and 36 recognized indigenous languages

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 18, 2026)

Risk indicators: Crime, unrest

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Street theft, express kidnappings, blockades that disrupt telecoms, and limited local security capacity.

Country Overview

Bolivia is a landlocked Andean country with highland, valley, and Amazonian lowland regions. The Tiwanaku culture and later the Inca Empire ruled the highlands before Spain conquered the territory in the sixteenth century and mined the silver of Potosi, once among the richest cities in the world. Simon Bolivar's lieutenant Antonio Jose de Sucre led the forces that secured independence in 1825.

Bolivia lost its Pacific coastline to Chile in the War of the Pacific (1879 to 1884) and later lost territory to Brazil and Paraguay. Frequent coups marked the twentieth century. In 2006, Evo Morales became the first indigenous president, governed until 2019, and nationalized hydrocarbons. A 2019 election dispute forced him from office, and his party's Luis Arce won in 2020.

Bolivia has about 11.4 million people, with large reserves of lithium and natural gas. Rodrigo Paz won the October 2025 runoff and took office in November 2025, ending two decades of rule by the Movement for Socialism (MAS) party.

Geopolitical Landscape

- **Economic crisis.** Fuel and dollar shortages, falling gas output, and inflation have strained the economy, and the new government is pursuing stabilization measures that have prompted protests and blockades.

- **Political realignment.** Paz's government has reoriented foreign policy toward the United States and regional partners after years of alignment with Russia, China, and Venezuela.
- **Morales and the MAS.** Evo Morales faces legal proceedings and an arrest warrant and remains a mobilizing figure among supporters in the Chapare region, which makes unrest likely around contested policy.
- **Lithium.** Bolivia holds some of the world's largest lithium resources, and contracts with Russian and Chinese firms have drawn scrutiny.
- **Chile access and border.** Bolivia's maritime claim against Chile ended with an International Court of Justice ruling in 2018, and the border region is a route for smuggling and migration.

Cyber Threats | Organizations

- **Government and critical sector exposure.** Public agencies and state firms, including those in hydrocarbons and mining, have limited security capacity. The TIDE team tracks a Russia-nexus actor, Turla, among those that list Bolivia, with defense and diplomatic organizations as the leading sectors.
- **Financial sector.** Banks and cooperatives face phishing, account takeover, and card fraud as digital payments expand.
- **Blockades and infrastructure disruption.** Roadblocks and protests disrupt logistics, and telecommunications can degrade during unrest.
- **Public reporting gap.** Public incident reporting is limited, so organizations should rely on peer threat intelligence and regional patterns for the Andean region.
- **Employees based in country.** Employees face phone theft and virtual-kidnapping calls, along with road blockades that can strand staff for days and degrade connectivity.
- **Vendor and supply chain risk.** State firms and mining contractors have limited security maturity. Vendors in hydrocarbons and lithium may have ties to Russian or Chinese firms, so screen for ownership and access.

The TIDE team tracks 1 threat actor that lists Bolivia among their targets. By attributed nexus, they break down as 1 Russia-nexus. The most frequently targeted sectors are defense and defense industrial base (1), diplomatic and foreign affairs (1), education and research (1), government (1), and technology (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile and messaging scams.** WhatsApp and SMS scams impersonating banks and utilities are widespread.
- **Virtual kidnapping and extortion calls.** Callers claim to hold a relative to extract payments, a pattern common across Latin America.
- **Phone theft.** Street theft in La Paz, Santa Cruz, and Cochabamba can lead to account takeover when devices are unlocked.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Bolivia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Bolivia Level 2, Exercise Increased Caution, citing crime and unrest, and advises caution during protests and road blockades.

TIDE Risk Level Rationale

- **Drivers.** Express kidnapping, phone theft, and virtual-kidnapping calls are the main risks, and road blockades can strand travelers and degrade connectivity. Local security capacity is limited.
- **What would change this rating.** Raise to Level 3 if unrest and blockades intensify around economic reforms. Lower to Level 1 as crime and disruption ease.

Public Wi-Fi

- Public Wi-Fi networks pose elevated risk in Bolivia due to widespread phone theft and virtual-kidnapping calls that exploit unlocked devices, compounded by network degradation during blockades and protests. Use a corporate VPN if public networks must be accessed.

Device and account controls

- Company devices can travel under standard controls: encryption, managed profile, phishing-resistant multi-factor authentication, and remote wipe.
- Use a corporate VPN, and keep devices concealed in public.

Local risks

- Express kidnappings and robberies, sometimes involving fake taxis, have been reported in major cities, so use hotel-arranged or app-based transport.
- Blockades can strand travelers for days, so keep flexible itineraries and offline communication plans.
- Altitude in La Paz (about 3,600 meters) strains devices as well as people, and cold affects battery performance.

Return protocol

- Report lost or stolen devices immediately and rotate credentials for accounts accessed during travel.

WORLDBOOK

BOSNIA AND HERZEGOVINA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Sarajevo

GOVERNMENT
Federal parliamentary republic with international oversight (Office of the High Representative)

LANGUAGE
Bosnian, Croatian, and Serbian

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 27, 2026)

Risk indicators: Crime, terrorism, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Election-period tension, Russia-linked influence activity, and thin local security capacity.

Country Overview

Bosnia and Herzegovina lies in the western Balkans and sits where Ottoman, Habsburg, and Orthodox, Catholic, and Muslim influences meet. Ottoman rule from the fifteenth century brought Islam to many residents, and Austria-Hungary annexed the territory in 1908. The 1914 assassination of Archduke Franz Ferdinand in Sarajevo triggered the First World War.

Bosnia became part of Yugoslavia and declared independence in 1992, which led to a war with Serbian and Croatian nationalist forces that killed about 100,000 people and included the 1995 Srebrenica genocide. The 1995 Dayton Peace Agreement ended the war and created a state of two entities, the Federation of Bosnia and Herzegovina and Republika Srpska, plus the Brcko District.

The country has about 3.2 million people and a complex power-sharing system among Bosniaks, Serbs, and Croats. An international High Representative retains powers to impose laws, and an EU-led force, EUFOR Althea, maintains security. Bosnia became an EU candidate in 2022.

Geopolitical Landscape

- **Republika Srpska crisis.** Milorad Dodik, the Republika Srpska leader, was convicted in 2025 for defying the High Representative and was stripped of his mandate. Early entity elections in November 2025, repeated at some polling stations in February 2026, were won by Sinisa Karan of Dodik's SNSD. The United States lifted its sanctions on Dodik in October 2025. Secessionist rhetoric remains a security concern.
- **EU path.** Bosnia opened EU accession negotiations in principle in 2024, but progress depends on reforms that the power-sharing structure complicates.
- **Russian influence.** Russia supports Serb nationalist leaders and opposes NATO enlargement, and Russia-linked influence operations target the country.
- **October 2026 elections.** Bosnia held general elections on October 4, 2026, with turnout near 42 percent. Preliminary results show Zeljka Cvijanovic of Dodik's SNSD leading the Serb seat on the presidency with about 55 percent, incumbent Denis Becirovic leading the Bosniak seat, and Darijana Filipovic of the HDZ leading the Croat seat. Dodik was not on the ballot. Official results are due by November 20, and government formation typically takes months.
- **Corruption and migration.** Governance weaknesses and migrant transit routes remain domestic priorities.

Cyber Threats | Organizations

- **Government and critical infrastructure.** Public bodies and utilities have limited security resources. The TIDE team tracks the Russia-nexus Cadet Blizzard and a China-nexus group among the actors that list Bosnia.
- **Election-period activity.** Phishing, disinformation, and denial-of-service attacks tend to cluster around elections and political crises.
- **Ransomware.** Local authorities and firms have faced ransomware, and few local firms maintain mature incident response.
- **Banking sector.** Foreign-owned banks dominate, and they face fraud and phishing common across the Balkans.
- **Employees based in country.** Employees face political disinformation, phishing, and landmine and rally risks. Government-adjacent staff should expect targeted phishing during post-election formation.
- **Vendor and supply chain risk.** Public bodies, utilities, and small IT vendors lack mature security. Foreign-owned banks dominate the financial sector and extend group-level controls to local suppliers.

The TIDE team tracks 2 threat actors that list Bosnia and Herzegovina among their targets. By attributed nexus, they break down as 1 Russia-nexus, and 1 China-nexus. The most frequently targeted sectors are government (2), critical infrastructure (general) (1), education and research (1), energy (1), and military (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, couriers, and public agencies circulate in local languages.
- **Disinformation.** Ethnic and political narratives spread widely on social media and messaging apps.

- **Online fraud.** Fake shops and fraudulent listings affect residents and diaspora.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Bosnia and Herzegovina. Bosnia appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Bosnia and Herzegovina Level 2, Exercise Increased Caution, and warns about unmarked landmines outside populated areas.

TIDE Risk Level Rationale

- **Drivers.** Disinformation and phishing cluster around elections and government formation, and Russia-linked influence activity is present. Public bodies and small vendors have limited security.
- **What would change this rating.** Raise to Level 3 if the Republika Srpska dispute escalates into an institutional crisis. Lower to Level 1 as government formation concludes calmly.

Public Wi-Fi

- Election-period tension and Russia-linked influence campaigns increase phishing risk over public networks, particularly through messages impersonating banks and government services. Connect through a corporate VPN to protect credentials during election-related activity.

Device and account controls

- Standard business travel controls apply: encryption, phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe.

Local practices

- Stay on marked paths when hiking, since landmines remain from the 1990s war.
- Avoid political rallies. Official election results are due by November 20, so expect political tension while governments form.
- Be alert to taxi overcharging and card skimming.

WORLDBOOK

BOTSWANA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Gaborone

GOVERNMENT
Parliamentary republic

LANGUAGE
English and Setswana

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued June 17, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable democracy; mining and diplomatic data attract limited targeting.

Country Overview

Botswana is a landlocked country in southern Africa dominated by the Kalahari Desert and the Okavango Delta. The Tswana peoples settled the region, and the British declared the Bechuanaland Protectorate in 1885, in part to prevent expansion by Boer settlers and Germany.

Botswana became independent in 1966 as one of Africa's poorest countries. The discovery of diamonds shortly afterward, prudent management, and stable democratic institutions produced one of the continent's fastest-growing economies. The Botswana Democratic Party governed for 58 years until Duma Boko's Umbrella for Democratic Change won the October 2024 election.

Botswana has about 2.4 million people and is a leading diamond producer through Debswana, a joint venture with De Beers. The economy has struggled as global diamond demand has fallen.

Geopolitical Landscape

- **Diamond downturn.** Falling demand and competition from lab-grown stones cut government revenue, and the government declared a public health emergency in 2025 over medicine shortages tied to the fiscal squeeze.

- **Political change.** Boko's government is pursuing economic diversification and a larger state stake in the diamond sector.
- **Regional position.** Botswana is a stable democracy with generally cordial relations with South Africa, Zimbabwe, and Namibia, and has been vocal on wildlife conservation and elephant management.
- **U.S. and China ties.** Botswana balances engagement with the United States, with which it has long security cooperation, and with China, a growing investor.

Cyber Threats | Organizations

- **Mining and diamonds.** Producers, traders, and logistics firms hold high-value commercial and operational data, which attracts espionage and fraud.
- **Government and diplomatic targeting.** The TIDE team tracks Turla (Russia-nexus) among the actors that list Botswana, with defense and diplomatic sectors as the leading targets.
- **Financial sector.** Banks and mobile money providers face phishing and account takeover.
- **Public reporting gap.** Public incident reporting is limited, and organizations should plan around patterns common to southern African governments and mining firms.
- **Employees based in country.** Employees face vehicle smash-and-grab theft and SMS phishing. Mining and diamond-trade staff should expect elicitation.
- **Vendor and supply chain risk.** Diamond traders, logistics firms, and mining contractors hold high-value commercial data. Require segmentation and access logging for vendor connections.

The TIDE team tracks 1 threat actor that lists Botswana among their targets. By attributed nexus, they break down as 1 Russia-nexus. The most frequently targeted sectors are defense and defense industrial base (1), diplomatic and foreign affairs (1), education and research (1), government (1), and technology (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile and messaging scams.** SMS and WhatsApp phishing impersonating banks and mobile operators is common.
- **Investment and job fraud.** Scams tied to investment schemes and fake job offers target urban users.
- **SIM and mobile money fraud.** SIM swap and fraudulent transfers affect wallet users.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Botswana.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Botswana Level 2, Exercise Increased Caution, for crime.

TIDE Risk Level Rationale

- **Drivers.** Botswana is a stable democracy with low surveillance risk. Vehicle break-ins and SMS phishing are the main traveler risks, and mining staff may face elicitation.
- **What would change this rating.** Raise to Level 2 for mining and diamond staff if targeting or fraud against the sector increases.

Public Wi-Fi

- SMS phishing impersonating mobile money providers and banks is endemic on public networks, with particular targeting of users in mining and diamond-trade sectors. Route all public network access through a corporate VPN to prevent credential capture.

Device and account controls

- Standard business travel controls apply: encryption, multi-factor authentication, a corporate VPN, and remote wipe.

Local practices

- Smash-and-grab theft from vehicles occurs in Gaborone and Francistown, so keep devices out of sight.
- Mobile coverage is limited in safari and desert areas, so download maps and documents before leaving cities.
- Travelers in mining and diamond trading should receive an elicitation briefing.

WORLDBOOK

BRAZIL

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Brasilia

GOVERNMENT
Federal presidential republic

LANGUAGE
Portuguese

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 31, 2026)

Risk indicators: Crime, kidnapping or hostage-taking. Level 4 applies to international land borders, informal housing developments, and certain areas around Brasilia.

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Pervasive payment fraud, device theft, ransomware, and election-period activity.

Country Overview

Indigenous peoples inhabited the territory for millennia before the Portuguese expedition of Pedro Alvares Cabral arrived in 1500. Brazil became a Portuguese colony built on sugar, gold, and enslaved labor, and it was the last country in the Americas to abolish slavery, in 1888. The Portuguese court relocated to Rio de Janeiro in 1808 to escape Napoleon's army, and Pedro I declared independence on September 7, 1822.

Brazil remained a monarchy until a republic was proclaimed in 1889. Getulio Vargas dominated national politics from 1930 to 1945 and again from 1951 to 1954. A military regime ruled from 1964 to 1985, and the 1988 constitution established the current democratic order. Luiz Inacio Lula da Silva served as president from 2003 to 2010 and returned to office in 2023. Jair Bolsonaro governed from 2019 to 2022.

Brazil is the largest country in South America, has a population above 200 million, and holds the largest economy in Latin America. Brasilia, founded in 1960, serves as the capital. Brazil is a founding member of the BRICS grouping and hosted the COP30 climate conference in Belem in November 2025.

Geopolitical Landscape

- **Presidential runoff.** Brazil voted on October 4, 2026. Senator Flavio Bolsonaro of the PL party led the first round with about 47 percent, ahead of President Lula at about 45 percent. Neither cleared the 50 percent threshold, so the two face a runoff on October 25, 2026. The right also made strong gains in Congress and state governorships, and the PL became the largest party in both chambers.
- **Bolsonaro conviction.** Jair Bolsonaro is serving a 27-year sentence, under house arrest, for plotting to overturn the 2022 election.
- **U.S. trade measures.** A 25 percent U.S. tariff under Section 301 of the Trade Act took effect on Brazilian goods on July 22, 2026, following a USTR investigation into Brazilian digital trade and electronic payment rules, anti-corruption enforcement, intellectual property, ethanol market access, preferential tariffs, and deforestation. The measure exempts many products, including beef, orange juice, aircraft and parts, and energy products, along with goods already subject to Section 232 tariffs. Earlier IEEPA-based tariffs on Brazil were invalidated by the U.S. Supreme Court in February 2026.
- **Sanctions.** The U.S. sanctioned Supreme Court Justice Alexandre de Moraes under the Global Magnitsky Act in July 2025 and removed the designation in December 2025, according to Brazilian press reporting. Brazilian officials have said further measures remain possible.
- **U.S. role in the election.** President Lula has accused the Trump administration of trying to influence the election, and the U.S. State Department has denied it. President Trump said he is watching the race closely and did not endorse a candidate.
- **Organized crime.** Gang activity and organized crime are widespread and often tied to the drug trade, according to the U.S. State Department. Groups such as the PCC and Comando Vermelho operate across states and prisons.

Cyber Threats | Organizations

- **Payment infrastructure and third-party providers.** On June 30, 2025, attackers compromised C&M Software, a provider that connects smaller financial institutions to the Central Bank and the Pix instant payment system, and issued fraudulent transfers in a single night. Police initially reported more than 540 million reais (about 100 million U.S. dollars) diverted at one institution, and other reports put the total near 800 million reais. Investigators arrested an IT employee accused of selling his credentials. The Central Bank disconnected C&M, which interrupted Pix access for several institutions.
- **Banking trojans.** Brazilian financial institutions face persistent banking malware. Kaspersky reported in March 2026 that the GoPix trojan, active for more than three years, had produced about 90,000 infection attempts. GoPix uses malicious Google Ads, runs in memory to limit forensic traces, and manipulates Pix transactions and boleto payment slips.
- **Ransomware and extortion.** Cybercriminal groups account for most of the activity directed at Brazilian organizations in the TIDE tracking data. Healthcare, government, and industrial and manufacturing organizations lead the targeted sectors.
- **State-linked espionage.** China-nexus actors and North Korea-nexus actors, including Andariel and Bronze Starlight, appear among actors that list Brazil, which reflects interest in government, technology, and finance.

- **Election-period activity (assessment).** Election periods draw phishing, denial-of-service activity, and disinformation themed around candidates and voting. The October 25 runoff warrants heightened monitoring for organizations with Brazilian operations.
- **Regulatory context.** Brazil's data protection law, the LGPD, is enforced by the national data protection authority and applies to organizations handling the personal data of people in Brazil.
- **Employees based in country.** Employees face phone snatching, Pix and boleto fraud, drink-spiking robberies tied to dating apps, and election-themed phishing around the October 25 runoff.
- **Vendor and supply chain risk.** The C&M Software incident showed that third-party payment providers can expose many institutions at once. Verify security controls for payment, fintech, and outsourcing vendors, and monitor for insider-recruited access.

The TIDE team tracks 70 threat actors that list Brazil among their targets. By attributed nexus, they break down as 49 cybercriminal, 12 China-nexus, 5 unattributed or other, 3 North Korea-nexus, and 1 Iran-nexus. The most frequently targeted sectors are healthcare and pharmaceuticals (45), government (39), industrial and manufacturing (36), technology (32), and banking and financial services (28). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Payment fraud.** Pix is used by about three quarters of Brazil's population, which makes it the primary target for consumer fraud. Malware such as PixPirate and GoPix monitors or manipulates Pix and boleto payments on infected devices.
- **Malvertising.** GoPix reaches victims through malicious ads that lead to fake landing pages, so searching for a service and clicking a sponsored result carries risk.
- **Targeting through dating apps.** Criminals target foreigners through dating apps and bars, then drug and rob them, according to the U.S. State Department, especially in Rio de Janeiro. These incidents often end with a stolen phone and unlocked accounts.
- **Device theft.** Street theft of phones is common in major cities, and a stolen unlocked phone can give a thief access to banking, email, and messaging.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Brazil. Brazil appears in TIDE tracking as a target. The single tracked entry linked to Brazil, Poseidon Group, is classified as cybercriminal and was last reported active in 2016.

Cyber Travel Considerations

Official guidance

Brazil sits at a Level 2 advisory, driven by violent crime and kidnapping rather than state surveillance. Company devices can travel under standard controls, and the main cyber risks come from theft, fraud, and unsafe networks.

TIDE Risk Level Rationale

- **Drivers.** Phone theft, Pix and boleto fraud, and drink-spiking robberies tied to dating apps are frequent, and ransomware is active. The October 25 runoff adds election-themed phishing and disinformation.
- **What would change this rating.** Raise to Level 3 if post-runoff unrest or large-scale attacks on payment infrastructure occur. Lower to Level 1 only if theft and fraud fall markedly.

Public Wi-Fi

- Public Wi-Fi networks are preferred vectors for malware distribution and banking trojans that manipulate Pix payments; the June 2025 C&M Software compromise demonstrated the risk from compromised third-party access points. If public networks are unavoidable, connect through a corporate VPN first.

Device and account controls

- Use company-managed devices with full-disk encryption, a strong lock screen, and remote wipe enabled before departure.
- Use phishing-resistant multi-factor authentication, such as hardware security keys, and avoid SMS codes where an alternative exists.
- Carry only the devices and data the trip requires. Leave unneeded laptops, spare phones, and external drives at home.
- Use a corporate VPN, and avoid public USB charging stations. Travelers bring their own chargers.
- Do not use a phone openly in crowded areas, on public buses, or near street edges where snatch theft occurs.

Payments and fraud

- Verify the recipient before approving any Pix payment, and do not scan QR codes from unsolicited sources.
- Type a service's address directly instead of clicking sponsored search results, especially for banking and payment apps.

Physical safety and incident response

- Avoid meeting strangers from dating apps in unfamiliar venues, and watch drinks in bars, especially in Rio de Janeiro.
- Avoid international land border areas, informal housing developments, and the Brasilia satellite cities flagged at Level 4.
- Give travelers a stolen-device procedure: report the loss to the security team immediately, lock or wipe the device remotely, and revoke sessions and tokens.
- Check the current State Department advisory at approval time and again before departure. Citizens of the United States can enroll in the Smart Traveler Enrollment Program (STEP), Canadians can use Registration of Canadians Abroad, and British travelers can use travel advice alerts.
- Expect heightened political activity around the October 25 runoff. Avoid demonstrations and monitor local guidance.

WORLDBOOK

BRUNEI

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Bandar Seri Begawan

GOVERNMENT
Absolute monarchy (Sultanate)

LANGUAGE
Malay

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 14, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and low crime; energy and government sectors draw regional espionage.

Country Overview

Brunei is a small Islamic sultanate on the northern coast of Borneo, split into two parts by Malaysia's Sarawak state. The Sultanate of Brunei rose to prominence in the fifteenth and sixteenth centuries and once controlled much of Borneo and parts of the Philippines. Territorial losses to European and local powers shrank it to its present size.

Brunei became a British protectorate in 1888 and gained full independence on January 1, 1984. Sultan Hassanal Bolkiah, who has ruled since 1967, serves as head of state and government and holds ministerial roles. Oil and gas, discovered in the 1920s, finance a generous welfare state with no personal income tax.

Brunei has about 460,000 people. Its Sharia-based penal code, phased in from 2014, drew international criticism, particularly over penalties introduced in 2019. The economy is heavily dependent on hydrocarbons.

Geopolitical Landscape

- **South China Sea.** Brunei claims part of the South China Sea within its exclusive economic zone and overlaps with China's nine-dash line, while avoiding public confrontation and favoring negotiation.
- **ASEAN and diversification.** Brunei is an ASEAN member and pursues economic diversification under Wawasan 2035, which includes downstream energy and halal industries.

- **Succession.** The sultan, born in 1946, has the crown prince, Al-Muhtadee Billah, as heir, and succession planning is a long-term stability factor.
- **Chinese investment.** The Hengyi refinery on Muara Besar island is a major Chinese-funded project and a pillar of Brunei's diversification.

Cyber Threats | Organizations

- **Energy sector.** Brunei Shell Petroleum and Brunei LNG operate critical infrastructure that regional actors may target for espionage or disruption.
- **Government and military targeting.** The TIDE team tracks the China-nexus Dark Pink and GhostNet and the India-nexus Confucius among the actors that list Brunei, with government and military organizations the leading sectors.
- **Financial sector.** Banks and Islamic finance institutions face phishing and business email compromise.
- **Government cybersecurity.** Brunei's national CERT, BruCERT, coordinates incident response and promotes awareness.
- **Employees based in country.** Most employees face ordinary risk. Staff in energy, government, or defense roles may draw targeted phishing, and border officials can inspect devices.
- **Vendor and supply chain risk.** Energy operators depend on a small set of contractors. Vendors serving government and military customers face elevated targeting.

The TIDE team tracks 3 threat actors that list Brunei among their targets. By attributed nexus, they break down as 2 China-nexus, and 1 India-nexus. The most frequently targeted sectors are government (3), military (2), civil society and activism (1), diplomatic and foreign affairs (1), and defense and defense industrial base (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Scams and phishing.** Bank and delivery impersonation scams circulate in Malay and English.
- **Content and speech limits.** Online criticism of the monarchy or religion can lead to prosecution.
- **Investment fraud.** Online investment and cryptocurrency scams target residents.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Brunei. Brunei appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Brunei Level 1, Exercise Normal Precautions.

TIDE Risk Level Rationale

- **Drivers.** Brunei is a stable, low-crime country with limited surveillance of visitors. Energy, government, and defense staff may draw regional espionage interest.
- **What would change this rating.** Raise to Level 2 for those roles if South China Sea tension increases targeting of Brunei.

Public Wi-Fi

- Regional espionage targeting energy infrastructure and government sectors occurs over public networks, and border officials routinely inspect devices for compromise. Use a corporate VPN to encrypt traffic and avoid device inspection risks when accessing public networks.

Device and account controls

- Standard business travel controls apply: encryption, phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe.
- Travelers in government, defense, and energy roles should expect elevated targeting and should receive a security briefing.

Local practices

- Observe local laws and customs, including alcohol restrictions and public conduct rules, and avoid commentary about the monarchy or religion.
- Carry only the data you need, since border officials may inspect devices.

WORLDBOOK

BULGARIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Sofia

GOVERNMENT
Parliamentary republic

LANGUAGE
Bulgarian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued October 9, 2025)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: EU member with fraud-hosting ecosystem and Russia-linked hacktivism.

Country Overview

Bulgaria lies in southeastern Europe on the Black Sea. Thracians, Romans, and Byzantines ruled the region before Bulgar and Slavic peoples founded the First Bulgarian Empire in 681. The Cyrillic script was developed in Bulgarian lands in the ninth and tenth centuries. Ottoman rule lasted nearly five centuries until Russian forces helped establish an autonomous Bulgaria in 1878.

Bulgaria declared full independence in 1908 and fought in both world wars on the losing side in the first and aligned with Germany in the second. A Soviet-aligned communist government ruled from 1946 until 1989, when Todor Zhivkov was removed. Bulgaria joined NATO in 2004 and the EU in 2007.

Bulgaria has about 6.4 million people, a shrinking population, and a low-wage but growing economy. The country adopted the euro on January 1, 2026.

Geopolitical Landscape

- **Eurozone entry.** Bulgaria joined the eurozone on January 1, 2026, after years of delay linked to inflation criteria, and it also aims to join the Schengen area fully, which it did for air and sea borders in 2024 and land borders in 2025.
- **New single-party government.** Large anti-corruption protests brought down the previous government in December 2025. Former president Rumen Radev resigned in January 2026, and his Progressive Bulgaria

party won an outright majority (131 of 240 seats) on April 19, 2026, the first for a single party since 1997 and Bulgaria's eighth general election since 2021. Parliament approved Radev as prime minister on May 8, 2026. He has criticized aspects of EU and Russia policy but says Bulgaria's EU and NATO path is settled.

- **Russia ties and energy.** Bulgaria has historic cultural and energy ties to Russia, and public opinion on Ukraine is divided. Russian gas deliveries stopped in 2022 after Bulgaria refused to pay in rubles, and the prior government committed to ending Russian gas transit by autumn 2027. U.S. sanctions on Lukoil in 2025 affect the Burgas refinery, which Lukoil owns.
- **Black Sea security.** Bulgaria hosts NATO forces and is a littoral state in a region affected by the war in Ukraine.
- **Corruption and organized crime.** Corruption concerns have delayed some EU funds, and organized crime influence remains a rule-of-law issue.

Cyber Threats | Organizations

- **Cybercrime hosting and fraud.** Bulgaria is a significant base for call-center and investment fraud operations that target victims abroad, and it hosts a large IT outsourcing sector.
- **State-linked espionage.** The TIDE team tracks the Russia-nexus Callisto Group and the China-nexus Stately Taurus among the actors that list Bulgaria. Banking, government, and civil society organizations lead the sectors.
- **Energy and critical infrastructure.** Energy operators, including Kozloduy nuclear plant and the gas network, are critical and have drawn attention from Russia-linked actors.
- **Ransomware and DDoS.** Municipalities and companies have suffered ransomware, and pro-Russia hacktivist groups have used denial-of-service against Bulgarian government sites.
- **Regulation.** Bulgaria is implementing NIS2 and applies the GDPR.
- **Employees based in country.** Employees face ATM skimming, taxi overcharging, and pickpocketing. Energy and government staff may draw Russia-linked phishing.
- **Vendor and supply chain risk.** Bulgaria's large IT outsourcing and call-center sector is a third-party risk for foreign firms. Review subcontractor vetting and access, and monitor for fraud operations.

The TIDE team tracks 6 threat actors that list Bulgaria among their targets. By attributed nexus, they break down as 3 cybercriminal, 1 Russia-nexus, 1 unattributed or other, and 1 China-nexus. The most frequently targeted sectors are banking and financial services (3), government (3), civil society and activism (2), hospitality and travel (1), and retail and e-commerce (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and card fraud.** Parcel, bank, and tax impersonation is common.
- **Resort and rental scams.** Fake rental listings and ATM or card skimming occur at Black Sea resorts.
- **Disinformation.** Narratives about the war and the euro spread through social media.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Bulgaria. Bulgaria appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Bulgaria Level 1, Exercise Normal Precautions.

TIDE Risk Level Rationale

- **Drivers.** Bulgaria is an EU member with ordinary travel risks such as ATM skimming and pickpocketing, and a large fraud and call-center ecosystem that matters for vendors. Russia-linked hacktivism targets public sites.
- **What would change this rating.** Raise to Level 2 if Russia-linked targeting of energy or government networks rises under the new government.

Public Wi-Fi

- Bulgaria's role in the regional fraud-hosting ecosystem and Russia-linked influence operations mean public networks carry elevated risk of malware injection and account compromise. Protect connections with a corporate VPN before accessing public Wi-Fi.

Device and account controls

- Standard business travel controls apply: encryption, phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe.

Local practices

- Use bank ATMs and avoid standalone machines, since skimming occurs.
- Pickpocketing occurs on Sofia public transport and at resorts.
- Use licensed or app-based taxis to avoid overcharging.

WORLDBOOK

BURKINA FASO

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4

CAPITAL
Ouagadougou

GOVERNMENT
Military-led transitional government

LANGUAGE
French

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued May 4, 2026)

Risk indicators: Crime, kidnapping or hostage-taking, terrorism, health

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Insurgency across much of the country, state internet suspensions, junta repression, and a U.S. Level 4 advisory.

Country Overview

Burkina Faso is a landlocked Sahel country in West Africa. The Mossi kingdoms ruled the central plateau for centuries before French conquest in the 1890s. France administered the territory as Upper Volta, and the country became independent in 1960.

Military coups dominated its early history. In 1983, Thomas Sankara took power and renamed the country Burkina Faso, meaning land of upright people, before being assassinated in 1987 in a coup led by Blaise Compaore, who ruled until a popular uprising ended his 27-year presidency in 2014. Two coups in 2022 brought Captain Ibrahim Traore to power.

Burkina Faso has about 24.7 million people and is among the world's poorest countries. Gold is its main export. Armed groups linked to al-Qaeda and the Islamic State have fought the state since 2015 and control or contest large parts of the country.

Geopolitical Landscape

- **Jihadist insurgency.** JNIM, an al-Qaeda affiliate, and Islamic State Sahel Province operate across much of the country, and Crisis Group lists Mali and Burkina Faso among the most serious conflicts to watch. Attacks on civilians and security forces occur frequently, and large areas lie outside government control.
- **Alliance of Sahel States.** Burkina Faso formed the Alliance of Sahel States with Mali and Niger in 2023 and left ECOWAS in January 2025. The three juntas have turned away from France and toward Russia and other partners.
- **Russian security partnership.** Russian paramilitary personnel, later organized under the Africa Corps, have been reported in the Sahel to support the juntas.
- **Political repression.** Authorities have conscripted critics, suspended media outlets, and delayed a return to civilian rule.
- **Humanitarian crisis.** Millions are displaced or in need, and some towns are under blockade.

Cyber Threats | Organizations

- **Limited commercial digital footprint.** Mining firms, telecommunications operators, and NGOs form most of the digital footprint of foreign organizations. Gold mining operators hold valuable production and shipping data.
- **State control of connectivity.** Authorities have suspended internet access, social media, and foreign media. Plan for unannounced outages and loss of foreign news channels.
- **Financial sector.** Banks and mobile money providers face fraud and account takeover. The TIDE team tracks one cybercriminal actor that lists Burkina Faso.
- **Insecurity and staff data.** Leaks of staff or contractor data can create physical risk in an insurgent environment, so minimize and protect location data.
- **Employees based in country.** Staff face internet and mobile suspensions, monitoring, and physical risk if employee or beneficiary location data leaks. Remove company access from personal devices and minimize stored data.
- **Vendor and supply chain risk.** Mining contractors, telecoms, and NGOs operate in an insecure environment with little local incident response. Vendor staff lists and site data create physical-safety risk if exposed.

The TIDE team tracks 1 threat actor that lists Burkina Faso among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile money and phishing fraud.** SMS and WhatsApp scams target mobile money users.
- **Surveillance and speech.** Journalists and critics have been abducted or conscripted, and authorities monitor social media.
- **Disinformation.** Information operations, including pro-junta and pro-Russia narratives, circulate widely on social media.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Burkina Faso.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Burkina Faso Level 4, Do Not Travel, citing crime, kidnapping or hostage-taking, terrorism, and health risks. U.S. government ability to assist is very limited.

TIDE Risk Level Rationale

- **Drivers.** Insurgents operate across much of the country, authorities suspend internet and mobile service, and the junta represses critics. Leaks of staff or location data can create physical risk.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable security improvement and an end to communications suspensions.

Public Wi-Fi

- State-ordered internet suspensions and limited network security capacity mean public Wi-Fi offers minimal protection and may be subject to network monitoring. Connect through a corporate VPN before using public networks in Ouagadougou or other major centers.

Recommended corporate policy

- Allow travel only with a documented security plan, an in-country security provider, and executive approval.
- Use a no device, no infrastructure approach: no company devices, no company-linked accounts on personal devices, and no log-ins to company systems in country. If a business need is approved, issue a clean loaner device with minimal data and reimage it on return.
- Block sign-ins from Burkina Faso with geo-based conditional access, and alert on every attempt.

Communications and safety

- Expect internet and mobile disruptions. Carry a satellite or alternate communication option and agree on check-in rules.
- Do not wear company apparel or discuss work in public. Prepare an approved cover answer.
- Confirm that travel medical and evacuation coverage applies to Level 4 destinations and that the provider can operate in country.

Return protocol

- Treat any device that traveled as untrusted, wipe it, rotate credentials for accounts it touched from a trusted network, and hold a debrief.

WORLDBOOK

BURMA (MYANMAR)

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Naypyidaw

GOVERNMENT
Military-backed government (presidential system)

LANGUAGE
Burmese

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued May 8, 2026)

Risk indicators: Unrest, crime, health, other

Note: The U.S. government uses the name Burma. Many governments and the United Nations use Myanmar.

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Military-backed government, VPN criminalization, shutdowns, scam compounds, and a U.S. Level 4 advisory.

Country Overview

Burma, officially Myanmar, lies on the Bay of Bengal and the Andaman Sea between India, China, and Thailand. The Pagan kingdom unified much of the Irrawaddy valley in the eleventh century, and later dynasties ruled until Britain conquered the country in three wars between 1824 and 1885 and administered it as part of British India.

Burma gained independence in 1948. Aung San, who negotiated independence, was assassinated in 1947. Ethnic insurgencies began almost immediately. General Ne Win took power in 1962 and imposed military rule and isolation. Mass protests in 1988 and a landslide win by Aung San Suu Kyi's National League for Democracy in 1990 did not lead to civilian rule, but a gradual opening from 2011 led to the NLD's government in 2016.

The military overthrew the elected government on February 1, 2021, and arrested Aung San Suu Kyi, and a civil war followed. The country has about 51.4 million people, many ethnic groups, and one of the world's largest drug and scam economies.

Geopolitical Landscape

- **Civil war.** Resistance forces, including the People's Defense Forces and long-standing ethnic armed organizations, fight the military across much of the country, and the junta fully controls only a fraction of territory. In late March 2026, anti-junta groups announced a combined front.
- **Managed election and new government.** The military held a three-phase election from December 2025 to January 2026 that critics and Western governments called a sham, with no voting in large areas and many parties barred. Parliament elected Min Aung Hlaing president on April 3, 2026, and he took office on April 10 after stepping down as commander-in-chief. ASEAN has not recognized the outcome, and only a few countries have.
- **Peace talks.** Min Aung Hlaing offered talks to armed groups within 100 days in April 2026, and the KNU and another key group rejected the offer.
- **Aung San Suu Kyi.** She remains imprisoned on a 27-year sentence that the government reduced by one-sixth in April 2026.
- **Major power support.** China, Russia, and India deal with the junta, and China congratulated the new president.
- **Scam compounds and sanctions.** Cyber scam compounds in border areas such as Myawaddy have drawn raids, international sanctions on operators, and pressure from Thailand, China, and the United States.

Cyber Threats | Organizations

- **Scam compound ecosystem.** Criminal syndicates, many linked to Chinese organized crime, run large scam compounds that use trafficked and coerced workers for investment, romance, and crypto fraud against victims worldwide. Compounds have used satellite internet and cross-border infrastructure.
- **State control and surveillance.** The junta has imposed internet shutdowns, platform blocks, and a cybersecurity law that criminalizes VPN use without authorization. Telecom operators are required to install interception capability.
- **Targeting of government and civil society.** The TIDE team tracks 11 China-nexus actors among those that list Burma, including Evasive Panda, Bookworm, and Lotus Blossom. Government, telecommunications, and civil society are the leading sectors.
- **Resistance and hacktivist activity.** Pro-democracy hacktivists have leaked junta data and defaced websites, which adds risk for organizations seen as aligned with the military.
- **Sanctions exposure.** U.S. and other sanctions on junta-linked firms and individuals create compliance risk for any foreign business in the country.
- **Employees based in country.** Staff face phone searches, arrest for VPN use or posts, shutdowns, and trafficking-linked job scams. Remove company access from personal devices and avoid border scam areas.
- **Vendor and supply chain risk.** Telecom operators must install interception capability, and local vendors may be sanctioned or military-linked. Scam compounds create insider and money-laundering risk for payment providers. Screen all vendors for sanctions.

The TIDE team tracks 12 threat actors that list Burma among their targets. By attributed nexus, they break down as 11 China-nexus, and 1 India-nexus. The most frequently targeted sectors are government (11),

telecommunications (5), civil society and activism (3), diplomatic and foreign affairs (3), and religious organizations (3). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Surveillance and arrest.** Users have been arrested for social media posts and for owning or using VPN apps. Soldiers and police search phones at checkpoints.
- **Connectivity disruption.** Internet and mobile service has been cut for long periods in conflict regions.
- **Scams and trafficking recruitment.** Fake job offers lure people from across Asia and beyond to scam compounds, where they may be held against their will.
- **Phishing and data theft.** Digital payment fraud and account takeover are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Burma. Burma appears in TIDE tracking as a target, primarily of China-nexus espionage.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Burma Level 4, Do Not Travel, citing unrest, crime, health risks, and other threats. The U.S. government has very limited ability to assist citizens.

TIDE Risk Level Rationale

- **Drivers.** The military-backed government criminalizes VPN use, searches phones, and imposes shutdowns, and civil war covers much of the country. Scam compounds and trafficking-linked job offers add risk.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require an end to VPN criminalization and device searches and a durable ceasefire.

Public Wi-Fi

- VPN use is criminalized by the military government and internet shutdowns are frequent; public Wi-Fi itself may be monitored or blocked entirely. Do not use public Wi-Fi at all, and rely on the approved devices and connectivity plan.

Recommended corporate policy: no device, no infrastructure

- Employees do not bring company-issued devices into Burma.
- Employees remove all company-linked accounts and applications from personal devices before travel.
- Employees do not log in to company-linked accounts while in country.
- Block sign-ins from Burma with geo-based conditional access and alert on every attempt.
- Approve exceptions only with a documented security plan, and issue clean loaner devices with minimal data.

Communications and safety

- Avoid VPN use, which is criminalized, and assume phones and networks are monitored.

- Expect shutdowns and conflict disruption.
- Avoid border areas known for scam compounds and treat any job offer from the region with extreme caution.
- Involve counsel on sanctions and export-control exposure.

Return protocol

- Treat any device that traveled as untrusted, wipe it, rotate credentials from a trusted network, and hold a debrief.

WORLDBOOK

BURUNDI

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3

CAPITAL
Gitega (political) and Bujumbura (economic)

GOVERNMENT
Presidential republic

LANGUAGE
Kirundi, French, and English

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued April 29, 2025)

Risk indicators: Unrest, crime, health

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: State monitoring, fuel and currency crisis, tension with Rwanda, and a U.S. Level 3 advisory.

Country Overview

Burundi is a small, densely populated landlocked country in the African Great Lakes region. A Tutsi-led monarchy ruled the area for centuries before German and then Belgian colonization. Burundi became independent in 1962.

Ethnic violence between Hutu and Tutsi communities shaped the country's politics. A 1993 coup and assassination of the first Hutu president triggered a civil war that lasted until 2005 and killed an estimated 300,000 people. President Pierre Nkurunziza's 2015 decision to seek a third term sparked a failed coup and violent crackdown.

Burundi has about 12.3 million people and is among the world's poorest countries. Evariste Ndayishimiye, from the ruling CNDD-FDD, has been president since 2020, and the party won the June 2025 parliamentary elections.

Geopolitical Landscape

- **Tension with Rwanda.** Relations are hostile. Burundi closed the border in 2024, accusing Rwanda of backing the Red Tabara rebel group. Crisis Group reported that Burundian and Rwandan forces reportedly exchanged

fire along the border in late August and early September 2026 without casualties, as both sides reinforced their positions.

- **Role in eastern DRC.** Burundi sent troops to eastern Congo to fight alongside Congolese forces against the Rwanda-backed M23 rebels, which links its security to the regional war.
- **Economic crisis.** Shortages of fuel and foreign currency, and a stagnant economy, strain households and the government.
- **Political space.** The CNDD-FDD dominates institutions, opposition parties are constrained, and human rights groups report abuses by security forces and the youth league.

Cyber Threats | Organizations

- **Limited commercial footprint.** The TIDE team tracks no actors that list Burundi, which reflects sparse reporting. Foreign organizations, mostly NGOs, banks, and telecommunications operators, face the typical exposure of fragile states: phishing, fraud, and weak local security.
- **State access to data.** Security services have broad powers to monitor communications, and foreign organizations should assume locally hosted data is accessible to the state.
- **Financial sector.** Mobile money and banking fraud affect operators and customers.
- **Regional spillover.** Escalation with Rwanda could increase hacktivist and state-linked activity.
- **Employees based in country.** Staff should assume communications are monitored, expect power and connectivity problems, and avoid political activity and photography of sensitive sites.
- **Vendor and supply chain risk.** NGOs, banks, and telecom operators rely on weak local security. Vendors with access to systems should be limited, segmented, and monitored.

The TIDE team does not currently track actors that list Burundi among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Surveillance.** Authorities monitor opposition figures, activists, and journalists, and critics have faced arrest.
- **Mobile money and phone scams.** Fraud targets users of mobile wallets.
- **Internet restrictions.** Authorities have blocked social media at sensitive moments, including in 2015 and around elections.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Burundi.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Burundi Level 3, Reconsider Travel, citing unrest, crime, and health risks, and advises against travel to the border areas with the Democratic Republic of the Congo and parts of the countryside.

TIDE Risk Level Rationale

- **Drivers.** State monitoring, a fuel and currency crisis that disrupts power and connectivity, and tension with Rwanda, including exchanges of fire along the border in late summer 2026, drive the rating.
- **What would change this rating.** Raise to Level 4 if fighting with Rwanda escalates or detentions of foreigners occur. Lower to Level 2 if the border situation and economy stabilize.

Public Wi-Fi

- State monitoring capabilities and fragile security infrastructure elevate the risk of eavesdropping and credential theft over public networks during periods of political tension. Use a corporate VPN to encrypt traffic on any public Wi-Fi connection.

Recommended corporate policy

- Allow travel only for approved business needs and brief travelers on security conditions.
- Use company-managed devices with encryption and phishing-resistant multi-factor authentication, and prefer clean loaner devices for travelers with sensitive roles.
- Use a corporate VPN, avoid public Wi-Fi, and assume local networks and SIMs are monitored.

Local practices

- Avoid political gatherings and demonstrations, and avoid photographing government or military sites.
- Expect fuel shortages and unreliable power, and carry power banks and offline plans.
- Check conditions near the Rwanda border and the DRC border before any road travel.

Return protocol

- Report lost devices immediately, rotate credentials accessed in country, and debrief the traveler.

WORLDBOOK

CABO VERDE

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Praia

GOVERNMENT
Semi-presidential republic

LANGUAGE
Portuguese (Cabo Verdean Creole widely spoken)

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued December 18, 2025)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable democracy with low state-surveillance risk; exposure is tourism fraud.

Country Overview

Cabo Verde is an archipelago of ten volcanic islands about 600 kilometers off the coast of Senegal. Portuguese navigators found the islands uninhabited in the 1460s, and the territory became a hub of the Atlantic slave trade and later a coaling station for ships. Independence from Portugal came in 1975 after a joint struggle with Guinea-Bissau, and a one-party system gave way to multiparty democracy in 1991.

The country has about 490,000 residents and a larger diaspora in the United States, Portugal, and the Netherlands. Tourism and remittances drive the economy, and Cabo Verde has a record of stable elections and peaceful transfers of power.

Geopolitical Landscape

- **Stable democracy.** Cabo Verde is regularly ranked among Africa's most democratic and best-governed states, and it has strong ties with Portugal, the EU, and the United States.
- **Maritime and drug-trafficking exposure.** The islands sit on air and sea routes between West Africa, Latin America, and Europe, and authorities have worked with international partners against narcotics transit.
- **Climate and island vulnerability.** Drought, water scarcity, and limited arable land shape policy, and the economy depends heavily on tourism.

Cyber Threats | Organizations

- **Tourism and hospitality.** Hotels, airlines, and tour operators hold payment and passport data and face ransomware and card fraud.
- **Financial and telecom sectors.** Banks and telecommunications firms are small and rely on foreign parent companies and vendors, so third-party exposure drives risk.
- **Public sector.** Government has digitized services quickly, and security staffing is limited.
- **Employees based in country.** Employees face tourist-area theft, card skimming, and fake rental listings.
- **Vendor and supply chain risk.** Hotels and banks depend on foreign parent companies and small vendors. Verify subcontractor controls.

The TIDE team does not currently track actors that list Cabo Verde among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Phishing and scams.** Bank and delivery impersonation circulates in Portuguese, and fake rental and tour listings target visitors.
- **Card skimming.** Skimming and payment fraud occur in tourist zones.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Cabo Verde.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Cabo Verde Level 1, Exercise Normal Precautions, citing crime. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A stable democracy with low surveillance risk and ordinary tourist-area theft and card fraud.
- **What would change this rating.** Raise to Level 2 if fraud or theft against visitors rises sharply.

Public Wi-Fi

- Tourism-targeted fraud schemes operate over public networks in hotels and hospitality venues, compromising travelers' payment methods and accounts. Connect through a corporate VPN before using public Wi-Fi to prevent phishing and card fraud.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Keep devices out of sight on beaches and in rental vehicles, and avoid public Wi-Fi at resorts.
- Inter-island flights and ferries can be delayed, so confirm itineraries and keep offline copies of key details.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

CAMBODIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 3

CAPITAL
Phnom Penh

GOVERNMENT
Constitutional monarchy with a dominant-party government

LANGUAGE
Khmer

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 15, 2026)

Risk indicators: Crime, unrest, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Scam compound ecosystem, state surveillance, China-linked espionage, and border conflict with Thailand.

Country Overview

Cambodia sits in mainland Southeast Asia and was the heart of the Khmer Empire, which built Angkor between the ninth and fifteenth centuries. France ruled the territory as a protectorate from 1863 and Cambodia gained independence in 1953 under King Norodom Sihanouk.

The Vietnam War spilled into Cambodia, and the Khmer Rouge seized power in 1975 and ruled until 1979, killing roughly 1.5 to 2 million people. Vietnam's invasion ended the regime, and a UN-run transition followed in 1991 to 1993. Hun Sen led the government for nearly four decades until his son, Hun Manet, became prime minister in August 2023, with Hun Sen remaining a dominant political figure.

Cambodia has about 17.8 million people, a garment and tourism economy, and a close partnership with China.

Geopolitical Landscape

- **Conflict with Thailand.** A long-running border dispute erupted into deadly fighting in July 2025 and again in December 2025, killing dozens and displacing hundreds of thousands of people. A U.S.-brokered ceasefire in December ended the second round, but Prime Minister Hun Manet calls it fragile and says Thai forces occupy Cambodian territory.

- **China ties.** China is Cambodia's largest investor and creditor and has supported development of the Ream naval base, which has drawn U.S. concern.
- **Scam compounds and sanctions.** Cambodia hosts large online scam operations that use trafficked workers. In October 2025 the United States and United Kingdom sanctioned the Prince Group network over scam and money laundering activity. The government says it is deporting compound workers and has advanced a new anti-scam law.
- **Political space.** The ruling Cambodian People's Party faces little organized opposition, and independent media and activists face pressure.

Cyber Threats | Organizations

- **Scam compound ecosystem.** Criminal syndicates run industrial-scale investment, romance, and crypto fraud from compounds in Phnom Penh, Sihanoukville, and border towns, creating insider-threat, money laundering, and data-theft risks for financial institutions and telecoms.
- **State-linked espionage.** Government, defense, and civil society organizations draw Chinese and other regional espionage interest, and Cambodian networks have been used as infrastructure in other operations.
- **Financial sector.** Banks and the Bakong payment system face fraud and money laundering exposure tied to scam proceeds.
- **Data access.** Authorities have broad surveillance powers, and a national internet gateway plan raised concerns about control of traffic.
- **Employees based in country.** Staff face trafficking-linked job scams, motorbike phone snatching, and monitoring of communications. Online criticism of the government can lead to arrest.
- **Vendor and supply chain risk.** Banks, payment providers, and telecoms face money-laundering and insider risk tied to scam proceeds. Local vendors may be linked to sanctioned networks, so screen ownership and sanctions exposure.

The TIDE team tracks 14 threat actors that list Cambodia among their targets. By attributed nexus, they break down as 13 China-nexus, and 1 Vietnam-nexus. The most frequently targeted sectors are government (10), telecommunications (6), aerospace (4), defense and defense industrial base (3), and education and research (3). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Scam recruitment.** Fake job offers lure people to compounds where they may be held and forced to commit fraud.
- **Online fraud.** Investment, romance, and loan-app scams target residents and foreigners.
- **Speech and monitoring.** Online criticism of the government can lead to arrest.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Cambodia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Cambodia Level 2, Exercise Increased Caution, citing crime, unrest, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Scam compounds create insider, trafficking, and money-laundering risk, the state monitors communications, and China-linked espionage and a fragile ceasefire with Thailand add exposure.
- **What would change this rating.** Raise to Level 4 if fighting with Thailand resumes or detention risk for foreigners increases. Lower to Level 2 if compound crackdowns succeed and the border stabilizes.

Public Wi-Fi

- Organized cybercrime compounds and state surveillance infrastructure actively monitor public networks; scammers harvest credentials over Wi-Fi with minimal local law enforcement response. Access public networks only through a corporate VPN.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Treat unsolicited job offers in the region with extreme caution, and avoid border areas with Thailand.
- Snatch theft from motorbikes occurs in Phnom Penh and Siem Reap, so keep phones secured.

Return protocol

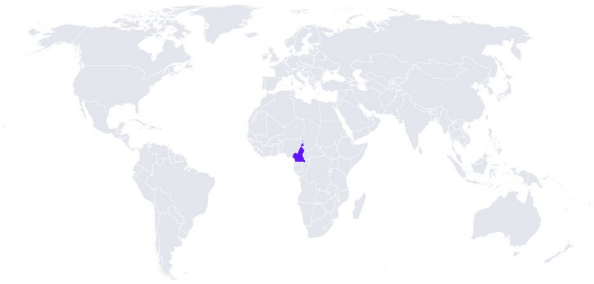
- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

CAMEROON

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 3



CAPITAL
Yaounde

GOVERNMENT
Presidential republic

LANGUAGE
French and English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 15, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, other, health

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Internet shutdowns, conflict in several regions, contested politics, and a regional cybercrime ecosystem.

Country Overview

Cameroon lies where West and Central Africa meet and is often called Africa in miniature for its geographic and ethnic diversity. Germany colonized the territory in 1884. After the First World War, Britain and France divided it under League of Nations mandates, and French Cameroun became independent in 1960 while part of British Cameroons joined it in 1961.

Cameroon has had only two presidents since independence. Paul Biya has led since 1982 and won an eighth term in October 2025 at age 92 in a disputed vote that triggered protests and deadly repression. The country has about 29.4 million people and exports oil, cocoa, and timber.

Geopolitical Landscape

- **Post-election tension.** The October 2025 result was contested by opposition candidate Issa Tchiroma Bakary, and demonstrations were met with force. Questions about succession shape politics.
- **Anglophone crisis.** A separatist conflict in the English-speaking Northwest and Southwest regions has killed thousands and displaced hundreds of thousands since 2017.

- **Boko Haram and ISWAP.** Jihadist groups attack civilians and soldiers in the Far North and around Lake Chad, and Crisis Group reported rising violence in Logone-et-Chari in September 2026.
- **Regional spillover.** Refugees from the Central African Republic and Nigeria strain eastern and northern areas.

Cyber Threats | Organizations

- **Oil, ports, and logistics.** The Douala port and the Chad-Cameroon pipeline are regional chokepoints that rely on digital systems and foreign contractors.
- **Financial and mobile money fraud.** Banks, microfinance, and mobile money operators face account takeover and social engineering.
- **Internet controls.** Authorities have imposed regional internet shutdowns, notably in Anglophone areas in 2017 and 2018, and can throttle access around contested events.
- **Cybercrime ecosystem.** Cameroon-based fraud rings run romance and advance-fee scams, which also drive local law enforcement focus.
- **Employees based in country.** Staff face possible shutdowns in conflict regions, mobile-money fraud, and monitoring of opposition and media contacts.
- **Vendor and supply chain risk.** Mobile-money operators and local IT firms face account-takeover and fraud rings. Port and pipeline contractors in Douala and the Chad-Cameroon corridor warrant segmentation.

The TIDE team tracks 1 threat actor that lists Cameroon among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile money fraud.** SIM-swap and OTP scams affect wallet users.
- **Surveillance and speech.** Journalists and opposition figures face prosecution, and authorities monitor social platforms.
- **Phishing.** Impersonation scams circulate in French and English.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Cameroon.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Cameroon Level 2, Exercise Increased Caution, citing unrest, crime, kidnapping or hostage-taking, terrorism, other, health. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Internet shutdowns have occurred in conflict regions, the aftermath of the October 2025 election showed forceful repression of protest, and mobile-money fraud rings are active.
- **What would change this rating.** Raise to Level 4 if unrest spreads or shutdowns become national. Lower to Level 2 if the political situation settles.

Public Wi-Fi

- Government-ordered internet shutdowns and regional cybercrime operations targeting public access points create an unstable threat environment over Wi-Fi. If public networks are available, route all access through a corporate VPN to avoid compromise.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid the Northwest, Southwest, Far North, and border areas flagged in the advisory.
- Expect possible internet disruption around elections and unrest, and keep offline communication plans.

Return protocol

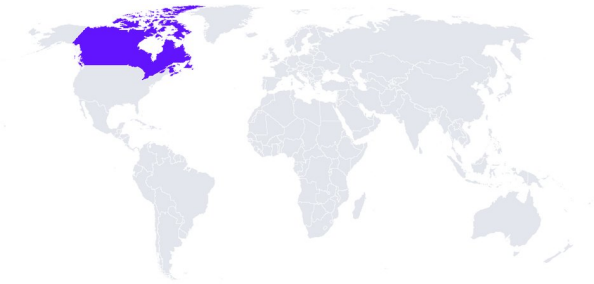
- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

CANADA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Ottawa

GOVERNMENT
Federal parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English and French

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued June 5, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated, with border device-inspection powers and sophisticated state and criminal threats.

Country Overview

First Nations, Inuit, and Metis peoples have lived in what is now Canada for thousands of years. French settlement began in the early seventeenth century, Britain took control of New France in 1763, and the British North America Act created the Dominion of Canada in 1867 through confederation of four provinces.

Canada gained legislative independence from Britain through the Statute of Westminster in 1931 and patriated its constitution in 1982. It is the world's second-largest country by area, has about 41 million people, and is a major energy, mining, and agricultural exporter. Mark Carney became prime minister in March 2025 and won an election the following month.

Geopolitical Landscape

- **Relations with the United States.** The United States is Canada's largest trading partner and security ally. U.S. tariffs and political pressure since 2025 strained relations, and the review of the Canada-United States-Mexico Agreement (CUSMA) is a focus in 2026.
- **Trade diversification.** Ottawa is seeking new markets and defense partners in Europe and Asia and is raising defense spending.

- **Arctic and sovereignty.** Climate change opens the Arctic and sharpens questions about sovereignty and northern security.
- **Foreign interference.** A public inquiry examined interference by China, India, and others in Canadian politics, and relations with India and China have been tense in recent years.
- **Five Eyes.** Canada is a core member of the Five Eyes alliance with the United States, United Kingdom, Australia, and New Zealand.

Cyber Threats | Organizations

- **Ransomware and extortion.** Cybercriminal groups account for most actors that target Canada. Healthcare, government, education, and industrial organizations are frequent victims.
- **State-sponsored threats.** The Canadian Centre for Cyber Security assesses that China is the most sophisticated state cyber threat, followed by Russia, Iran, and North Korea, and warns of pre-positioning in critical infrastructure.
- **Hacktivist attacks on industrial systems.** Canadian authorities warned in 2025 that hacktivists were tampering with internet-exposed industrial control systems at water, energy, and agriculture sites.
- **Telecommunications.** Telecom operators were identified among targets of Chinese actors in the Salt Typhoon campaign, according to Canadian and allied advisories.
- **Regulation.** Canada's critical cyber systems legislation and federal and provincial privacy laws shape compliance duties.
- **Employees based in country.** Employees face phishing and identity fraud, and border officers can examine devices. Staff in critical-infrastructure roles may draw state-linked interest.
- **Vendor and supply chain risk.** Telecom, cloud, and industrial-control suppliers are targets for state actors and hacktivists, so apply supplier assurance and monitor exposed control systems.

The TIDE team tracks 146 threat actors that list Canada among their targets. By attributed nexus, they break down as 102 cybercriminal, 22 China-nexus, 6 Iran-nexus, 5 Russia-nexus, 5 unattributed or other, 4 North Korea-nexus, 1 Lebanon-nexus, and 1 hacktivist. The most frequently targeted sectors are healthcare and pharmaceuticals (91), industrial and manufacturing (74), technology (71), government (70), and banking and financial services (56). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Fraud and phishing.** Bank, tax, and delivery impersonation and investment scams are common, and the Canadian Anti-Fraud Centre reports large annual losses.
- **Identity theft after breaches.** Large retail, health, and telecom breaches have exposed personal data.
- **Account takeover and SIM swap.** Mobile and financial account takeover remains frequent.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Canada. Canada appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Canada Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Canada is stable and well-regulated. Travelers face phishing and identity fraud, and border officers may examine devices, while state-linked and hacktivist threats target organizations more than visitors.
- **What would change this rating.** Raise to Level 2 if state-linked targeting of travelers or critical-infrastructure incidents begin to affect visitors.

Public Wi-Fi

- Sophisticated state-sponsored espionage targeting government, technology, and research sectors occurs over public networks, and border authorities possess device-inspection powers. Use a corporate VPN and maintain clean device state when accessing public Wi-Fi.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Canada Border Services Agency officers can examine electronic devices at the border, so travelers carrying sensitive data should limit what they bring.
- Rural and northern areas have limited coverage, so download maps and documents in advance.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

CENTRAL AFRICAN REPUBLIC

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Bangui

GOVERNMENT
Presidential republic

LANGUAGE
French and Sango

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued January 15, 2026)

Risk indicators: Unrest, crime, health, kidnapping or hostage-taking, other, terrorism

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Fragmented control, Russia-aligned influence operations, minimal infrastructure, and a U.S. Level 4 advisory.

Country Overview

The Central African Republic is a landlocked country in the heart of Africa. French colonizers administered it as Ubangi-Shari, and it became independent in 1960. Its history includes coups, the rule of Jean-Bedel Bokassa, who crowned himself emperor in 1977, and recurring rebellions.

A civil war began in 2012 when the mostly Muslim Seleka coalition seized power, followed by Christian anti-balaka militias, and conflict has since fragmented the country among armed groups. Faustin-Archange Touadera, president since 2016, won a third, seven-year term in December 2025 with 77.9 percent in a vote the opposition boycotted and rejected, and was sworn in on March 30, 2026. The country has about 6.5 million people and is one of the world's poorest despite diamonds, gold, and timber.

Geopolitical Landscape

- **Fragmented control.** Armed groups control much of the territory outside Bangui and profit from mining and trade routes.

- **Russian security partnership.** Russian paramilitary forces, first the Wagner Group and later the Africa Corps, protect the government and mining interests and have been accused of abuses.
- **UN presence.** The MINUSCA peacekeeping mission supports the state, and its mandate and funding face pressure.
- **Sudan spillover.** The war in Sudan sends refugees and fighters into the northeast.

Cyber Threats | Organizations

- **Minimal formal digital footprint.** Mining firms, NGOs, and mobile operators make up most foreign exposure, with limited local security capacity and unreliable power and connectivity.
- **Influence operations.** Russia-linked information campaigns have operated in the country in support of the government.
- **Staff safety.** Leaks of staff or beneficiary locations can create physical risk, so data minimization matters.
- **Employees based in country.** Staff face unreliable power and connectivity, monitoring by authorities and armed groups, and physical risk if location data leaks.
- **Vendor and supply chain risk.** Mining firms, NGOs, and mobile operators work with minimal local security capacity. Minimize data shared with vendors and protect staff location data.

The TIDE team does not currently track actors that list Central African Republic among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile-first fraud.** TELECEL, Orange, MOOV, and AZUR provide mobile service, mostly limited to urban centers; SMS and mobile money scams affect users.
- **Surveillance and disinformation.** Authorities and armed groups can monitor communications, and journalists face intimidation; the Wagner Group, rebranded Africa Corps after its founder's death in 2023, has run documented disinformation campaigns using fabricated social media accounts and recruited local journalists to spread propaganda.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Central African Republic.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Central African Republic Level 4, Do Not Travel, citing unrest, crime, health, kidnapping or hostage-taking, other, terrorism. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. Embassy in Bangui has very limited ability to assist.

TIDE Risk Level Rationale

- **Drivers.** Armed groups control much of the territory, infrastructure is minimal, Russia-aligned influence operations are active, and the United States has very limited ability to assist.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require durable security gains outside Bangui.

Public Wi-Fi

- Minimal local security infrastructure and the documented Russia-aligned Wagner Group/Africa Corps information operations mean public networks offer little protection from eavesdropping or account compromise, and connectivity is concentrated in Bangui and a few urban centers. Protect connections with a corporate VPN before using public Wi-Fi.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

CHAD

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
N'Djamena

GOVERNMENT
Presidential republic (transitional authoritarian)

LANGUAGE
French and Arabic

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued April 28, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, other, health

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Authoritarian transition, internet blocks around unrest, Sudan-war spillover, and a U.S. Level 4 advisory.

Country Overview

Chad is a landlocked country at the crossroads of North and Central Africa, stretching from the Sahara to the savanna. The Kanem-Bornu empire and other states ruled parts of the region before French colonization. Chad became independent in 1960 and has experienced coups, rebellions, and a war with Libya in the 1980s.

Idriss Deby took power in 1990 and ruled until he was killed in April 2021 fighting rebels. His son, Mahamat Idriss Deby, led a military transition and won a disputed election in May 2024. Opposition leader Succes Masra was sentenced to 20 years in prison in 2025. Chad has about 20 million people, mostly dependent on agriculture, livestock, and oil.

Geopolitical Landscape

- **Sudan war.** More than a million Sudanese refugees have entered eastern Chad, and the government is accused by critics of allowing weapons transit to the Rapid Support Forces, which it denies.
- **Break with France.** France withdrew its troops in early 2025 after Chad ended a defense agreement, and N'Djamena has diversified partners to include the UAE, Turkey, and Russia.

- **Boko Haram and instability.** Insurgents operate around Lake Chad, and rebels and communal conflicts persist.
- **Political repression.** Authorities restrict opposition and civic space.

Cyber Threats | Organizations

- **Oil and infrastructure.** Oil operators and the pipeline to Cameroon are strategic and hold sensitive commercial data.
- **State control of connectivity.** Authorities have blocked internet and social media around elections and unrest.
- **Limited local security capacity.** Telecom, banks, and NGOs face phishing and fraud with little local incident response.
- **Employees based in country.** Staff face internet and social media blocks, monitoring of opposition contacts, and physical risk from instability.
- **Vendor and supply chain risk.** Oil and pipeline contractors and local telecoms have limited incident response. Vendor access should be segmented and carefully limited.

The TIDE team does not currently track actors that list Chad among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Surveillance and shutdowns.** Opposition figures and journalists face monitoring, and internet disruptions occur at sensitive moments.
- **Mobile fraud.** SMS and mobile money scams are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Chad.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Chad Level 4, Do Not Travel, citing unrest, crime, kidnapping or hostage-taking, terrorism, other, health. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. U.S. government ability to assist is very limited, and the advisory warns of terrorism, kidnapping, and unrest.

TIDE Risk Level Rationale

- **Drivers.** An authoritarian transition with internet blocks around unrest, spillover from the Sudan war, and very limited ability for the United States to assist.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require an end to communications blocks and improved security.

Public Wi-Fi

- Government-ordered internet blocks during political transitions and the Sudan-war spillover create chaotic and monitored network conditions over public Wi-Fi. When public networks are available, use a corporate VPN to encrypt traffic and avoid surveillance.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

CHILE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Santiago

GOVERNMENT
Presidential republic

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 19, 2026)

Risk indicators: Unrest, crime, health

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Frequent phone theft, ransomware, and espionage interest in mining and research.

Country Overview

Chile is a long, narrow country between the Andes and the Pacific that spans desert in the north to glaciers in the south. The Mapuche resisted Spanish rule for centuries after Spain's arrival in the sixteenth century, and Chile declared independence in 1818. It won the War of the Pacific (1879 to 1884) against Peru and Bolivia, gaining its northern mining regions.

A 1973 coup brought General Augusto Pinochet to power, and his dictatorship killed or disappeared thousands before a 1988 plebiscite began the return to democracy in 1990. Chile has about 20.2 million people and is the world's largest copper producer and a leading lithium producer. Jose Antonio Kast, a conservative, took office in March 2026.

Geopolitical Landscape

- **Political shift.** Kast's government has prioritized security, migration control, and economic growth after years of divisive debate over a rewritten constitution that voters rejected twice.
- **Copper and lithium.** Chile's mining sector is central to global supply chains, and Santiago balances China, its largest trade partner, with the United States.

- **Security concerns.** Organized crime, including Venezuelan and Colombian networks, and violence in the Araucania region have grown as political issues.
- **Territorial claims.** Chile claims part of Antarctica and maintains a maritime agenda with Argentina and Bolivia.

Cyber Threats | Organizations

- **Mining sector.** Copper and lithium producers hold valuable operational and geological data and are targets for espionage and ransomware.
- **Financial sector.** Banks in Chile are targets of ransomware and destructive malware, so financial-sector vendors should expect elevated scrutiny.
- **Ransomware and data leaks.** Public and private organizations have suffered ransomware and leaks, and a 2024 data protection law update strengthens duties.
- **State-linked interest.** China-nexus and other espionage groups target government, mining, and research organizations in Latin America.
- **Employees based in country.** Employees face street phone theft, virtual-kidnapping calls, and protest-related disruption in Santiago.
- **Vendor and supply chain risk.** Mining suppliers and outsourcers hold valuable operational data. Past bank incidents show that third-party and masked destructive attacks can occur.

The TIDE team tracks 14 threat actors that list Chile among their targets. By attributed nexus, they break down as 10 cybercriminal, 2 unattributed or other, 1 Russia-nexus, and 1 Iran-nexus. The most frequently targeted sectors are healthcare and pharmaceuticals (10), government (9), industrial and manufacturing (9), education and research (7), and technology (6). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and account takeover.** Bank and delivery impersonation scams are common in Spanish.
- **Phone theft.** Street theft of phones is common in Santiago and Valparaiso.
- **Virtual kidnapping and extortion calls.** Callers claim to hold relatives and demand payment.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Chile.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Chile Level 2, Exercise Increased Caution, citing unrest, crime, health. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Street phone theft and virtual-kidnapping calls are the main traveler risks, protests periodically disrupt Santiago, and mining and research draw espionage.
- **What would change this rating.** Lower to Level 1 if theft trends fall. Raise to Level 3 if unrest becomes sustained.

Public Wi-Fi

- Ransomware groups actively target public networks for initial access, and phone theft is frequent; compromised devices accessed over public Wi-Fi expose corporate systems. Use a corporate VPN and keep devices physically secured when on public networks.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Keep phones out of sight on streets and metro platforms, and set strong passcodes.
- Protests and strikes disrupt Santiago periodically, so avoid demonstrations.

Return protocol

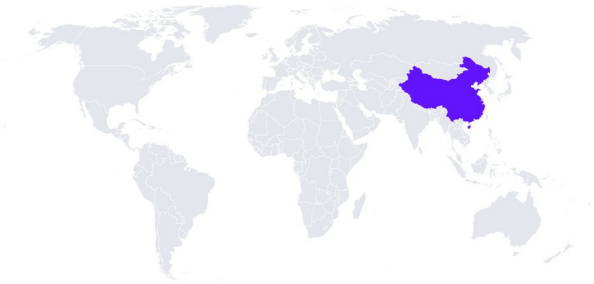
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

CHINA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 4



CAPITAL
Beijing

GOVERNMENT
One-party socialist state led by the Chinese Communist Party

LANGUAGE
Mandarin Chinese

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 4, 2026)

Risk indicators: Other (arbitrary enforcement of local laws, including exit bans)

Note: U.S. recognition: the United States recognizes the People's Republic of China. Taiwan, Hong Kong, and Macau have their own profiles.

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Compelled access under state security laws, pervasive monitoring, device inspection, blocked services, exit bans, and heavy state-linked targeting.

Country Overview

China is the world's most populous country after India, with about 1.4 billion people, and traces a continuous civilization back more than three thousand years through dynasties from the Shang and Zhou to the Qin, Han, Tang, Song, Ming, and Qing. The last imperial dynasty fell in 1912, and the Republic of China that followed gave way to warlordism, Japanese invasion, and a civil war between Nationalists and Communists.

The Communists under Mao Zedong won the civil war and proclaimed the People's Republic in 1949, and the Nationalists retreated to Taiwan. Mao's campaigns, including the Great Leap Forward and the Cultural Revolution, caused immense loss of life. Deng Xiaoping's reforms from 1978 opened the economy and drove decades of rapid growth. Xi Jinping has led the Party since 2012 and removed presidential term limits in 2018.

China is the world's second-largest economy, a leading manufacturer, a permanent member of the UN Security Council, and a nuclear power.

Geopolitical Landscape

- **U.S.-China trade truce.** Presidents Trump and Xi met in Busan in October 2025, in Beijing in May 2026, and in Washington in September 2026. A truce that holds U.S. tariffs on Chinese goods near 47 percent and suspends Chinese rare-earth export controls was extended in September 2026 to January 10, 2027, with further meetings planned for November and December. A U.S. arms package for Taiwan remains frozen.
- **Taiwan.** Beijing claims Taiwan and has not renounced force. The United States maintains unofficial relations with Taiwan and opposes unilateral change to the status quo. PLA exercises around the island recur.
- **South China Sea.** China's claims overlap with those of the Philippines, Vietnam, Malaysia, and others, and clashes with the Philippines at sea occur periodically.
- **Technology controls.** Export controls on advanced semiconductors, sanctions, and investment screening define the technology rivalry.
- **Russia partnership.** China backs Russia economically and diplomatically while avoiding direct military aid, and it is a leading buyer of Russian energy.
- **Xinjiang, Tibet, and Hong Kong.** Human rights concerns and Western sanctions over Xinjiang, Tibet, and Hong Kong remain a source of friction.

Cyber Threats | Organizations

- **Compelled access and data law.** The Cybersecurity Law, Data Security Law, Personal Information Protection Law, and national intelligence law require organizations to store certain data in country, pass security reviews for cross-border transfers, and cooperate with state security. Foreign organizations should assume state access to data stored or transmitted in China.
- **The Great Firewall and connectivity.** Foreign platforms including Google services, Meta platforms, and many news sites are blocked, and VPN use is restricted. Unapproved cross-border tunnels can violate regulations.
- **Intellectual property theft.** Manufacturing, technology, pharmaceutical, and research organizations with Chinese operations face espionage by state-linked groups and insider-enabled theft.
- **Domestic ransomware and fraud.** Chinese enterprises face ransomware and data theft. Taiwan- and U.S.-linked operations have been alleged by Chinese authorities.
- **Supply chain and testing regimes.** Mandatory product certification and source-code or security review requirements create exposure for foreign technology vendors.
- **Employees based in country.** Staff should assume communications, devices, and WeChat activity are monitored and that devices can be inspected. Employees with intellectual property or export-controlled access are priority targets, and exit-ban risk exists in disputes.
- **Vendor and supply chain risk.** Vendors, hosting providers, and software suppliers in China must comply with state data and security-review laws, and compromised updates and contractors are a recognized pathway for IP theft. Segment or remove China-based vendor access, and review hardware and software provenance.

The TIDE team tracks 42 threat actors that list China among their targets. By attributed nexus, they break down as 14 China-nexus, 14 cybercriminal, 3 North Korea-nexus, 3 India-nexus, 3 unattributed or other, 2 Iran-nexus, 1 Russia-nexus, 1 Vietnam-nexus, and 1 Lebanon-nexus. The most frequently targeted sectors are government

(21), technology (14), banking and financial services (10), healthcare and pharmaceuticals (10), and education and research (9). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Pervasive monitoring.** Real-name registration, platform monitoring, and a large camera network mean limited anonymity. WeChat messages are monitored.
- **Device inspection.** Police can inspect phones, and visitors have reported checks of messages, photos, and apps, particularly in Xinjiang and at borders.
- **Scams.** Telecom and online fraud, including fake investment platforms and impersonation of officials, are common.
- **Exit bans.** Authorities can bar foreigners from leaving China in civil and criminal matters, including business disputes.

State-Sponsored Cyber Threats

Chinese state cyber operations are conducted by or on behalf of the Ministry of State Security (MSS), the People's Liberation Army (PLA), and contractors that support them. The groups below carry public government or vendor attribution.

GROUP	ALSO KNOWN AS	ATTRIBUTED SPONSOR	FOCUS	ACTIVE
APT1	Comment Crew, Comment Panda, PLA Unit 61398	PLA Unit 61398 (Second Bureau, Third Department)	Espionage	2006 to 2018
APT3	Gothic Panda, Buckeye, UPS Team	MSS-affiliated contractor Boyusec (Guangzhou)	Espionage	2007 to 2017
APT10	Stone Panda, menuPass, Cicada, Potassium	MSS, Tianjin State Security Bureau	Espionage	2009 to 2024
APT31	Judgment Panda, Zirconium, Violet Typhoon	MSS-affiliated contractor (Wuhan Xiaoruizhi)	Espionage	2016 to 2026
APT40	Leviathan, TEMP.Periscope, Bronze Mohawk	MSS, Hainan State Security Department	Espionage	2009 to 2026
APT41	Wicked Panda, Winnti, Brass Typhoon	MSS-affiliated contractor (Chengdu 404)	Espionage and financial	2012 to 2026
Volt Typhoon	Bronze Silhouette, Vanguard Panda, Voltzite	PRC state-sponsored per U.S. and allied government advisories	Pre-positioning in critical infrastructure	2021 to 2026
Salt Typhoon	GhostEmperor, FamousSparrow, Earth Estries	MSS-affiliated contractor (Sichuan Juxinhe)	Telecommunications espionage	2020 to 2026
Flax Typhoon	Ethereal Panda, Storm-0919, Red Juliet		Espionage and botnet operations	2021 to 2026

GROUP	ALSO KNOWN AS	ATTRIBUTED SPONSOR	FOCUS	ACTIVE
		PRC-linked; U.S. government tied it to Integrity Technology Group		
Hafnium	Silk Typhoon, Murky Panda	MSS	Espionage	2021 to 2025
Mustang Panda	Bronze President, RedDelta, Stately Taurus	China-nexus (no agency publicly named)	Espionage	2012 to 2026
APT27	Emissary Panda, LuckyMouse, Iron Tiger	China-nexus (no agency publicly named)	Espionage	2010 to 2025
Naikon	Lotus Panda, APT30	PLA Unit 78020	Espionage	2010 to 2024

Many other China-nexus clusters are active across espionage, pre-positioning, and cybercrime, and vendors track them under differing names. Attribution to specific agencies is public only for some groups. This list excludes U.S. agencies by design.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates China Level 2, Exercise Increased Caution, with an indicator for arbitrary enforcement of local laws, including exit bans, and for risks to U.S. citizens of detention in connection with business or other disputes.

TIDE Risk Level Rationale

- **Drivers.** State security laws compel access to data. Communications and WeChat are monitored, devices can be inspected, foreign services are blocked, and exit bans have been used in disputes. State-linked groups heavily target travelers with sensitive access.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require clear limits on compelled access and device inspection, which is unlikely in the near term. The U.S.-China trade truce does not change the cyber assessment.

Public Wi-Fi

- Compelled access under state security laws and pervasive monitoring of all internet traffic mean public Wi-Fi is monitored and subject to account hijacking, credential harvesting, and malware injection, with device inspection at borders. Do not use public Wi-Fi; rely on approved devices and connectivity plans.

Recommended corporate policy: no device, no infrastructure

- Employees do not bring company-issued devices into China, remove all company-linked accounts and applications (Teams, Outlook, Slack, authenticator apps, password managers, and similar) from personal devices before travel, and do not log in to company-linked accounts while in country for any reason.

- Require advance travel reporting. Block sign-ins from China with geo-based conditional access and alert on every blocked attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- For genuine business needs, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Hardware security keys stay home. Executives, privileged administrators, and staff with intellectual property or export-controlled access warrant stricter rules.

Connectivity and communications

- Avoid hotel, public, and cafe Wi-Fi and public USB charging. Travelers bring their own chargers.
- Expect blocked Western apps and services, and assume communications are monitored. WeChat and Alipay are central to daily payments and messaging.
- Keep devices on your person rather than in hotel rooms or safes, and treat rooms, vehicles, and restaurants as non-private.

Payments and logistics

- Foreign cards are accepted at limited venues. Set up mobile payment options before arrival through a travel provider, and carry some cash.
- Confirm that travel medical coverage and evacuation arrangements work in your destination.

Personal safety and legal exposure

- Do not discuss sensitive business or political topics in public, and prepare an approved cover answer about employment.
- Be aware of exit-ban and detention risk, especially in commercial disputes, and identify counsel in advance. Involve counsel on export controls, including encryption on devices.
- Treat unsolicited approaches with caution, including contacts through LinkedIn and social media before and after the trip. Citizens of the United States can enroll in STEP.

Return protocol

- Treat any personal device that traveled as untrusted and wipe it before re-enrolling it for company access. Rotate passwords and revoke sessions for personal accounts used on the device, from a trusted network and device, starting with personal email.
- Hold a debrief to capture suspicious contacts or device behavior, and apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

COLOMBIA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 2



CAPITAL
Bogota

GOVERNMENT
Presidential republic

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued March 31, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, natural disaster

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Active ransomware, virtual kidnapping, phone theft, and armed-group risk to infrastructure.

Country Overview

Colombia sits at the northwestern corner of South America with coasts on both the Caribbean and the Pacific. Indigenous civilizations including the Muisca and Tairona lived there before Spain's conquest in the sixteenth century. Simon Bolivar's forces secured independence from Spain in 1819, and the territory later separated from Gran Colombia.

Liberal-Conservative violence in the twentieth century, including the decade called La Violencia, gave way to a conflict from the 1960s among left-wing guerrillas such as the FARC, right-wing paramilitaries, and the state, intertwined with the cocaine trade. A 2016 peace accord with the FARC ended the largest insurgency, though other armed groups remain.

Colombia has about 53.4 million people and a diversified economy built on oil, coal, coffee, and flowers.

Geopolitical Landscape

- **New government.** Abelardo de la Espriella, an outsider on the right, won the June 21, 2026 runoff with about 49.7 percent over leftist Ivan Cepeda and was sworn in on August 7, 2026, in Cali. His platform emphasizes a tough approach to crime inspired by El Salvador's model. The United States announced 1 billion dollars in security assistance on August 8.

- **Relations with Washington.** Relations were strained under outgoing President Gustavo Petro, and President Trump endorsed de la Espriella. The new government is expected to align more closely with the United States on security and drugs.
- **Armed groups.** The ELN, FARC dissident factions, and the Clan del Golfo control territory and drug routes, and violence has risen in areas such as Catatumbo and Cauca. Political violence included the 2025 assassination attempt on Senator Miguel Uribe.
- **Venezuela border.** Migration and armed-group activity shape the long border with Venezuela.

Cyber Threats | Organizations

- **Ransomware and extortion.** Colombian organizations in health, government, and finance have been repeatedly hit by ransomware.
- **Banking fraud.** Banks face account takeover, SIM swap, and social engineering.
- **Election and political activity.** Disinformation and AI-generated content played a visible role in the 2026 campaign, and political figures are targeted by phishing and doxxing.
- **Energy and critical infrastructure.** Pipelines and power assets face sabotage by armed groups and cyber risk.
- **Employees based in country.** Employees face virtual-kidnapping calls using breached data, phone snatching, and dating-app robberies. Political events can bring doxxing and disinformation.
- **Vendor and supply chain risk.** The 2023 IFX Networks incident showed that one supplier can disrupt many organizations. Verify resilience and breach terms for IT, health, and payment vendors.

The TIDE team tracks 16 threat actors that list Colombia among their targets. By attributed nexus, they break down as 12 cybercriminal, 2 unattributed or other, 1 China-nexus, and 1 Russia-nexus. The most frequently targeted sectors are government (11), healthcare and pharmaceuticals (10), industrial and manufacturing (9), education and research (8), and technology (6). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and account takeover.** Bank, tax, and delivery impersonation is common.
- **Virtual kidnapping and extortion.** Callers claim to hold a relative and demand payment, often using data from breaches.
- **Dating-app crimes.** Criminals target foreigners through dating apps, then drug and rob them, according to U.S. advisories.
- **Phone theft.** Snatch theft in Bogota and Medellin is common, often by thieves on motorbikes.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Colombia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Colombia Level 3, Reconsider Travel, citing unrest, crime, kidnapping or hostage-taking, terrorism, natural disaster. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Virtual kidnapping using breached data, phone snatching, and dating-app robberies are frequent, ransomware is active, and armed groups threaten infrastructure in some regions. The State Department rates the country Level 3 for crime, kidnapping, terrorism, and unrest.
- **What would change this rating.** Raise to Level 3 if armed-group violence reaches major cities or targeted cyber campaigns against business travelers emerge. Lower only on sustained declines in crime and fraud.

Public Wi-Fi

- Active ransomware campaigns and virtual kidnapping scams exploit device access over unsecured public networks, and armed-group targeting of infrastructure adds instability. Use a corporate VPN before accessing public Wi-Fi to prevent compromise.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Use hotel-arranged or app-based transport, and avoid hailing street taxis.
- Avoid areas flagged in the advisory, including parts of Cauca, Catatumbo, and border regions, and avoid demonstrations.
- Do not accept drinks from strangers, and meet dating-app contacts in public, known venues.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

COMOROS

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Moroni

GOVERNMENT
Federal presidential republic

LANGUAGE
Comorian, Arabic, and French

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued January 12, 2026)

Risk indicators: Unrest, crime, health

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Limited digital footprint and low state-surveillance risk; exposure is fraud.

Country Overview

Comoros is an archipelago of volcanic islands in the Indian Ocean between Mozambique and Madagascar. Arab traders, Shirazi settlers from Persia, and later French colonizers shaped the islands. Three of the four main islands voted for independence from France in 1975, and Mayotte voted to stay French, a status Comoros contests.

Comoros has experienced about twenty coups and coup attempts since independence. Azali Assoumani has led the country since 2016, following an earlier stint after a 1999 coup, and was reelected in 2024 in a vote the opposition disputed. The country has about 940,000 people and depends on vanilla, cloves, and remittances.

Geopolitical Landscape

- **Mayotte dispute.** Comoros claims Mayotte, a French department, and migration from Anjouan to Mayotte is a source of tension with France.
- **Political concentration of power.** Azali's government has been accused of limiting opposition and arranging succession toward his son.
- **Climate and cyclones.** Cyclones and volcanic risk affect infrastructure.

Cyber Threats | Organizations

- **Limited digital footprint.** The small financial and telecom sectors rely on foreign vendors and have limited local security capacity.
- **Offshore and remittance flows.** Money transfer operators and banks face fraud and abuse.
- **Employees based in country.** Employees face mobile and messaging fraud and limited connectivity.
- **Vendor and supply chain risk.** Small financial and telecom sectors rely on foreign vendors with limited local security capacity.

The TIDE team does not currently track actors that list Comoros among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile and messaging scams.** SMS and WhatsApp fraud targets mobile money and remittance users.
- **Speech limits.** Online criticism of the government can lead to detention.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Comoros.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Comoros Level 2, Exercise Increased Caution, citing unrest, crime, health. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Limited digital footprint and low surveillance risk, with mobile fraud as the main exposure.
- **What would change this rating.** Raise to Level 2 if political unrest brings connectivity restrictions.

Public Wi-Fi

- Limited local security oversight and fraud targeting travelers on nascent public networks mean Wi-Fi offers minimal protection against phishing and payment fraud. Connect through a corporate VPN before using public networks.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Return protocol

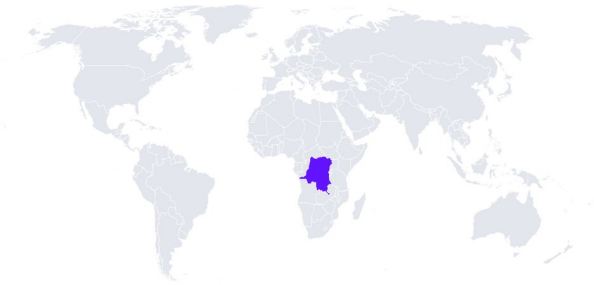
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

CONGO, DEMOCRATIC REPUBLIC OF THE

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Kinshasa

GOVERNMENT
Semi-presidential republic

LANGUAGE
French (with Lingala, Swahili, Kikongo, and Tshiluba)

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued July 15, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, health

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Armed conflict in the east, state internet restrictions, thin security capacity, and a U.S. Level 4 advisory.

Country Overview

The Democratic Republic of the Congo is the second-largest country in Africa and holds the Congo River basin, one of the world's great rainforests, and vast mineral wealth. The Kongo, Luba, and Lunda kingdoms flourished before Belgium's King Leopold II seized the territory as a personal possession in the 1880s, an era of forced labor and mass death. Belgium ruled the colony from 1908 until independence in 1960.

Prime Minister Patrice Lumumba was assassinated in 1961, and Mobutu Sese Seko ruled from 1965 to 1997 as Zaire. Rwandan and Ugandan-backed rebels overthrew Mobutu, and the Second Congo War (1998 to 2003) drew in several African armies and caused millions of deaths. Felix Tshisekedi has been president since 2019.

The country has about 116 million people and holds major reserves of cobalt, copper, and coltan that supply global batteries and electronics.

Geopolitical Landscape

- **M23 and eastern Congo.** The Rwanda-backed M23 rebels seized Goma and Bukavu in early 2025 and still hold large areas of the Kivus. The United States brokered a Washington peace agreement between Congo and Rwanda in June 2025 and the Washington Accords in December 2025, and Qatar mediates talks between Kinshasa and M23. A Doha framework and an August 2026 roadmap have not ended fighting, and Crisis Group reported continued clashes in September 2026.
- **Domestic politics.** Tshisekedi's push for constitutional reform and tight control of a national dialogue process have raised tensions.
- **Minerals diplomacy.** Washington and Kinshasa are pursuing a minerals-for-security arrangement, while China holds major mining interests.
- **Other armed groups.** More than 100 armed groups operate in the east, including ADF, an Islamic State affiliate.

Cyber Threats | Organizations

- **Mining sector.** Cobalt and copper producers, traders, and logistics firms hold high-value commercial and ESG data and face espionage, fraud, and supply chain targeting.
- **State control of connectivity.** Authorities have restricted internet and social media around elections and unrest.
- **Limited local capacity.** Telecoms, banks, and NGOs face phishing and fraud with little incident response capacity.
- **Conflict-linked information operations.** Parties to the conflict run influence campaigns on social media.
- **Employees based in country.** Staff face internet restrictions around unrest, monitoring, mobile-money fraud, and physical risk. Remove company access from personal devices.
- **Vendor and supply chain risk.** Mining, trading, and logistics vendors hold high-value data and face espionage and fraud. Telecoms and local IT firms have limited incident response, so isolate vendor access.

The TIDE team does not currently track actors that list the Democratic Republic of the Congo among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile money fraud.** SIM-swap and OTP scams affect wallet users.
- **Surveillance.** Journalists and activists face monitoring and arrest.
- **Disinformation.** False content about the war spreads quickly through WhatsApp and Facebook.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to the Democratic Republic of the Congo.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates the Democratic Republic of the Congo Level 4, Do Not Travel, citing unrest, crime, kidnapping or hostage-taking, terrorism, health. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. U.S. government ability to assist is very limited, and the advisory warns of armed conflict, terrorism, and kidnapping in the east.

TIDE Risk Level Rationale

- **Drivers.** Armed conflict in the east, state internet restrictions around unrest, thin security capacity, and high-value mining data drive the rating.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable peace agreement and a sustained end to restrictions.

Public Wi-Fi

- Government-imposed internet restrictions and minimal security oversight amid armed conflict create unpredictable conditions over public Wi-Fi; networks may be monitored or compromised. Use a corporate VPN to protect credentials when public networks must be accessed.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

CONGO, REPUBLIC OF THE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Brazzaville

GOVERNMENT
Presidential republic

LANGUAGE
French

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued October 2, 2024)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Limited reporting, election-period connectivity controls, and oil-sector exposure.

Country Overview

The Republic of the Congo lies on the west bank of the Congo River opposite Kinshasa. The Kingdom of Kongo and the Teke kingdom held sway before France colonized the area, which became part of French Equatorial Africa. Independence came in 1960.

A Marxist-Leninist one-party state ruled from 1969 to 1991, and civil wars in the 1990s brought Denis Sassou Nguesso back to power in 1997. He has held office for all but five years since 1979. The country has about 6.1 million people and relies on oil, which accounts for most exports.

Geopolitical Landscape

- **Long-serving leadership.** Sassou Nguesso's government dominates politics, and critics cite weak accountability.
- **Oil dependence and debt.** Falling output and high debt service strain public finances.
- **Regional role.** Brazzaville borders the DRC and plays a mediation role in Central African affairs.

Cyber Threats | Organizations

- **Oil and port sector.** Oil operators and the Pointe-Noire port hold sensitive commercial data.
- **Limited local capacity.** Banks, telecoms, and public bodies face fraud and phishing with little local incident response.
- **Connectivity controls.** Authorities have cut internet access around elections.
- **Employees based in country.** Staff face mobile-money fraud and possible internet cuts around elections.
- **Vendor and supply chain risk.** Oil operators and port logistics providers hold sensitive commercial data. Vendors have limited incident response.

The TIDE team does not currently track actors that list the Republic of the Congo among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile money and SMS fraud.** Fraud affects mobile wallets offered by the country's mobile operators.
- **Surveillance and speech.** Opposition figures and journalists face monitoring, and the government has twice ordered nationwide internet shutdowns during election periods, most recently in March 2026, following a similar shutdown around the March 2021 election.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to the Republic of the Congo.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates the Republic of the Congo Level 2, Exercise Increased Caution, citing crime. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Limited reporting, election-period connectivity controls, and sensitive oil-sector data warrant increased precautions.
- **What would change this rating.** Raise to Level 3 if shutdowns or unrest occur. Lower to Level 1 as reporting and security capacity improve.

Public Wi-Fi

- Election-period connectivity controls are a documented pattern, with internet shutdowns recorded around both the 2021 and 2026 elections; combined with mobile-money fraud targeting, connect through a corporate VPN before using hotel or airport networks, and expect possible disruption during politically sensitive periods.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

COSTA RICA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
San Jose

GOVERNMENT
Presidential republic

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued April 2, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable democracy, but the 2022 ransomware national emergency shows real exposure.

Country Overview

Costa Rica lies between Nicaragua and Panama with coasts on the Caribbean and Pacific. Spain's colonial presence there was thin and poor, which shaped an egalitarian society. Costa Rica joined independent Central America in 1821 and developed coffee and banana economies.

After a brief civil war in 1948, the country abolished its army in 1949 and built a durable democracy and strong social programs. It has about 5.2 million people and an economy based on tourism, medical devices, and agriculture, and it is known for conservation and ecotourism.

Geopolitical Landscape

- **Security and crime.** Homicide rates have risen as drug trafficking groups use Costa Rican ports and territory, and security is the leading political issue.
- **U.S. ties.** Costa Rica is closely aligned with the United States on security and trade, and President Laura Fernandez, successor to Rodrigo Chaves, took office on May 8, 2026 promising a tough approach to crime.
- **Nicaragua tension.** Relations with Nicaragua are strained by migration and the dispute over the San Juan river area.

- **Chinese investment.** Costa Rica was the first Central American country to recognize the People's Republic in 2007 and has debated 5G and infrastructure partners.

Cyber Threats | Organizations

- **National ransomware emergency.** In April 2022 Russian-speaking attackers hit Costa Rica's Finance Ministry with ransomware, which crippled tax collection and export systems, and the new president declared a national emergency. Attackers also encrypted servers at the Ministry of Public Works in January 2023.
- **Public sector and utilities.** Public bodies have limited security capacity and have continued to see ransomware and extortion.
- **Tourism and medical devices.** Hotels and medical device manufacturers hold payment and intellectual property data.
- **Financial sector.** Banks face fraud and phishing.
- **Employees based in country.** Employees face opportunistic theft at beaches, buses, and rental cars, plus SMS and WhatsApp scams.
- **Vendor and supply chain risk.** Public bodies and utilities remain exposed to ransomware, and medical-device and tourism suppliers hold payment and IP data. Review supplier incident readiness.

The TIDE team tracks 4 threat actors that list Costa Rica among their targets. By attributed nexus, they break down as 2 cybercriminal, 1 China-nexus, and 1 unattributed or other. The most frequently targeted sectors are government (3), banking and financial services (2), diplomatic and foreign affairs (1), energy (1), and education and research (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Tourist-targeted fraud.** Fake rental and tour listings and card skimming target visitors.
- **Phone theft.** Opportunistic theft occurs at beaches, buses, and tourist sites.
- **SMS and WhatsApp scams.** Impersonation of banks and agencies is common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Costa Rica.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Costa Rica Level 2, Exercise Increased Caution, citing crime. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Costa Rica is a stable democracy, and opportunistic theft and scams are the main traveler risks, though the 2022 ransomware emergency shows public-sector exposure.

- **What would change this rating.** Raise to Level 2 if crime against visitors rises or a new nationwide cyber incident occurs.

Public Wi-Fi

- While Costa Rica suffered ransomware attacks on government systems in 2022, resort and tourist-area fraud remains the primary visitor risk; use a corporate VPN if connecting to hotel or public networks.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Keep devices out of sight at beaches and in rental cars, which are frequent theft targets.
- Use licensed or app-based transport and avoid isolated areas at night.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

COTE D'IVOIRE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Yamoussoukro (political) and Abidjan (economic)

GOVERNMENT
Presidential republic

LANGUAGE
French

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued February 18, 2026)

Risk indicators: Unrest, crime, health, terrorism, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Large cybercrime ecosystem, mobile-money fraud, and election-period tension.

Country Overview

Cote d'Ivoire is a West African country on the Gulf of Guinea and the world's largest cocoa producer. The kingdoms of Gyaman and Kong flourished before French conquest in the late nineteenth century. Independence came in 1960 under Felix Houphouet-Boigny, who led for 33 years and built a stable, prosperous state known as an African success story.

Succession struggles led to coups, a civil war from 2002 and a postelection crisis in 2010 and 2011 that killed about 3,000 people. Alassane Ouattara has been president since 2011 and won a fourth term in October 2025. The country has about 31 million people.

Geopolitical Landscape

- **Fourth term.** Ouattara's reelection in October 2025 followed the exclusion of major opposition candidates, and political tension remains.
- **Sahel spillover.** Jihadist violence from Burkina Faso and Mali reaches northern border areas, and Abidjan has strengthened border security.
- **Economic growth.** The economy has grown rapidly on cocoa, cashews, oil, and infrastructure, and Abidjan is a regional financial hub.

- **French ties.** France transferred its military bases to Ivorian control in 2025.

Cyber Threats | Organizations

- **Financial hub.** Abidjan hosts regional banks, the West African stock exchange, and mobile money firms such as Orange Money and Wave, which face fraud and account takeover.
- **Cybercrime ecosystem.** Ivorian fraud networks, known locally as brouteurs, run romance and advance-fee scams and sextortion against victims abroad, and the national agency PLCC works with international law enforcement.
- **Cocoa and agriculture.** Commodity traders and processors hold valuable pricing and logistics data.
- **Public sector.** E-government expansion outpaces security capacity.
- **Employees based in country.** Staff face SIM-swap fraud, phone snatching in traffic, and political tension around contested events.
- **Vendor and supply chain risk.** Abidjan's regional financial and mobile-money providers are central third parties, and fraud rings use compromised vendor mailboxes. Require strong authentication and monitoring for vendor payments.

The TIDE team tracks 1 threat actor that lists Cote d'Ivoire among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile money fraud.** SIM-swap and OTP scams are widespread.
- **Sextortion and romance scams.** Criminal networks target victims inside and outside the country.
- **Election-period monitoring.** Authorities monitor social media, and critics have been prosecuted.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Cote d'Ivoire.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Cote d'Ivoire Level 2, Exercise Increased Caution, citing unrest, crime, health, terrorism, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A large cybercrime ecosystem, mobile-money fraud, snatch theft in traffic, and political tension around contested elections drive the rating.
- **What would change this rating.** Raise to Level 3 if post-election unrest or shutdowns occur. Lower to Level 1 as fraud and tension recede.

Public Wi-Fi

- A large cybercrime ecosystem and mobile-money fraud networks operating in Abidjan make SIM-swap and account takeover attacks common; ensure a corporate VPN protects all public network connections.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, and expect political tension around contested events.
- Keep devices concealed in traffic, where snatch theft occurs.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

CROATIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Zagreb

GOVERNMENT
Parliamentary republic

LANGUAGE
Croatian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 18, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: EU member with stable conditions; exposure is ransomware, tourism fraud, and hacktivism.

Country Overview

Croatia lies on the Adriatic coast at the meeting point of Central Europe and the Balkans. A medieval kingdom of Croatia was established in the tenth century and later joined the Hungarian crown, while Dalmatia and Dubrovnik developed under Venice and as an independent republic. Croatia was then part of the Habsburg Empire before joining Yugoslavia after the First World War.

Croatia declared independence in 1991, and the Croatian War of Independence lasted until 1995. It joined NATO in 2009, the EU in 2013, the eurozone and Schengen area in January 2023. The country has about 3.9 million people and an economy driven by tourism, with strong shipbuilding and energy sectors.

Geopolitical Landscape

- **EU and NATO anchor.** Croatia is aligned with the EU and NATO and supports Ukraine. Prime Minister Andrej Plenkovic has led the government since 2016.
- **Regional relations.** Croatia manages border and minority issues with Serbia and Bosnia and Herzegovina and maritime issues with Slovenia.
- **LNG hub.** The Krk LNG terminal is an important route for gas diversification in Central and Eastern Europe.
- **Migration route.** Croatia sits on Balkan migration routes into the Schengen area.

Cyber Threats | Organizations

- **Public sector and healthcare.** Government and healthcare organizations have suffered ransomware, including a June 2024 ransomware attack on the Clinical Hospital Centre Zagreb that LockBit claimed and denial-of-service attacks by the pro-Russia group NoName057(16) on the finance ministry, tax service, and stock exchange.
- **Tourism.** Hotels and booking platforms face fraud and card theft.
- **Pro-Russia hacktivism.** DDoS campaigns have targeted Croatian government and media sites.
- **Regulation.** Croatia is implementing NIS2.
- **Employees based in country.** Employees face pickpocketing in tourist areas and fake rental listings.
- **Vendor and supply chain risk.** Hospitals, insurers, and service providers have suffered ransomware, so check supplier recovery capability.

The TIDE team tracks 1 threat actor that lists Croatia among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are government (1), healthcare and pharmaceuticals (1), industrial and manufacturing (1), and technology (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and parcel scams.** Bank, courier, and tax impersonation is common.
- **Rental and booking fraud.** Fake accommodation listings affect visitors on the coast.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Croatia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Croatia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Croatia is an EU member with ordinary tourist-area risks, and ransomware and hacktivism affect public bodies.
- **What would change this rating.** Raise to Level 2 if attacks on health or transport systems disrupt visitors.

Public Wi-Fi

- Hotels and tourism-sector providers face card theft and ransomware from cybercriminals and pro-Russia groups; connect through a corporate VPN to protect credentials and payment data on public networks.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Pickpocketing occurs in Dubrovnik, Split, and other busy areas.
- Summer coastal congestion and ferry delays are common, so confirm itineraries.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

CUBA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 3

CAPITAL
Havana

GOVERNMENT
One-party socialist republic (Communist Party)

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 7, 2025)

Risk indicators: Crime, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: State control of telecoms, pervasive monitoring, sanctions exposure, and unreliable power and internet.

Country Overview

Cuba is the largest island in the Caribbean. Spain colonized it in the early sixteenth century and held it until the Spanish-American War in 1898, after which the United States exerted heavy influence. A 1959 revolution led by Fidel Castro overthrew Fulgencio Batista and established a communist state allied with the Soviet Union.

The 1962 missile crisis brought the world close to nuclear war. After the Soviet collapse, Cuba entered a deep crisis, and the United States has maintained an embargo since the early 1960s. Raul Castro succeeded Fidel in 2008, and Miguel Diaz-Canel became president in 2018. The island has about 9.4 million people and has lost a large share of its population to emigration in recent years.

Geopolitical Landscape

- **2026 fuel and power crisis.** After the United States captured Venezuela's president in January 2026, Venezuelan oil shipments to Cuba stopped and President Trump threatened tariffs on any country supplying oil to the island. Cuba reported no oil imports for more than 90 days by mid-March, an island-wide grid collapse on March 16, and in May said it had exhausted its fuel oil and diesel, with blackouts of 20 hours a

day in parts of Havana and protests in the capital. Cuba confirmed in March that it was in talks with the United States, and a U.S. intelligence chief met Cuban officials in Havana in May.

- **U.S. embargo and sanctions.** The embargo, a restricted-entity list, and visa and remittance rules shape economic life and are tightened or loosened with each U.S. administration. Cuba's government blames sanctions for shortages.
- **Economic crisis.** Chronic blackouts, fuel and food shortages, inflation, and mass emigration have strained the system, and protests have flared periodically since July 2021.
- **Partners.** Cuba relies on Russia, China, and Venezuela for trade, energy, and support, and has provided medical missions abroad that Washington criticizes.
- **Political control.** The Communist Party monopolizes politics, and authorities imprison dissidents and restrict independent media.

Cyber Threats | Organizations

- **Grid and fuel collapse.** Repeated island-wide blackouts and fuel shortages disrupt connectivity, data center and telecom operations, and travel, so operations depend on generators and solar power.
- **State control of telecommunications.** ETECSA, the state telecom monopoly, controls the network and has cut or throttled internet access during protests.
- **Sanctions exposure.** U.S. sanctions create compliance risk for any organization with Cuban business ties, and data in country should be treated as accessible to the state.
- **Foreign intelligence interest.** Russia and China are reported to have intelligence facilities or partnerships on the island, and Cuba's own services conduct surveillance of foreigners.
- **Limited local security maturity.** Aging infrastructure and electricity outages degrade availability for any operation.
- **Employees based in country.** Staff should assume communications and Wi-Fi are monitored and plan for blackouts and unreliable connectivity. Foreign-intelligence interest in visitors is high.
- **Vendor and supply chain risk.** The state telecom monopoly and state-run vendors control the network, so locally hosted data is state-accessible. U.S. sanctions create compliance risk for any vendor relationship.

The TIDE team tracks 2 threat actors that list Cuba among their targets. By attributed nexus, they break down as 1 unattributed or other, and 1 cybercriminal. The most frequently targeted sectors are government (2), energy (1), military (1), telecommunications (1), and technology (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Surveillance and speech.** State monitoring is pervasive, and online criticism has led to prosecution.
- **Connectivity.** Internet access is expensive and unreliable, and public Wi-Fi hotspots are monitored.
- **Scams.** Tourist scams and fake booking schemes target visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Cuba.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Cuba Level 2, Exercise Increased Caution, citing crime, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** The state telecom monopoly controls the network, monitoring is pervasive, blackouts degrade connectivity, and U.S. sanctions add compliance risk for vendors.
- **What would change this rating.** Raise to Level 4 if detention risk for foreigners rises or the state restricts internet access broadly. Lower to Level 2 if monitoring and sanctions exposure ease.

Public Wi-Fi

- The state telecom monopoly monitors all connectivity and has throttled internet during protests; assume hotel and public networks are monitored and do not use public Wi-Fi without exceptional authorization and a corporate VPN.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Assume communications and devices are monitored, avoid public Wi-Fi, and consider clean loaner devices for sensitive roles.
- Involve counsel on U.S. sanctions and travel rules, since U.S. travel categories and spending limits apply.
- Expect blackouts and unreliable internet, and carry cash, since U.S.-issued cards do not work.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

CYPRUS

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 2

CAPITAL
Nicosia

GOVERNMENT
Presidential republic

LANGUAGE
Greek and Turkish

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued March 3, 2026)

Risk indicators: Other

Note: The island is divided. The United States recognizes only the Republic of Cyprus, which controls the south. The northern third is administered by a self-declared Turkish Cypriot entity recognized only by Turkey.

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Regional conflict proximity, hacktivism, and financial-sector exposure.

Country Overview

Cyprus lies in the eastern Mediterranean and has been fought over by Egyptians, Greeks, Romans, Byzantines, Venetians, Ottomans, and Britain, which took control in 1878 and annexed it in 1914. Independence came in 1960 with a power-sharing constitution between Greek and Turkish Cypriots.

Communal violence and a 1974 coup backed by Greece's junta prompted a Turkish invasion that split the island. The Republic of Cyprus joined the EU in 2004, and the north remained outside EU law. The Republic of Cyprus has about 980,000 people in the government-controlled south, and the economy rests on tourism, shipping, and financial and business services. Cyprus held the rotating EU Council presidency in the first half of 2026.

Geopolitical Landscape

- **Division and talks.** UN-facilitated talks on reunification have repeatedly stalled, and a UN buffer zone runs across the island.
- **Iran war spillover.** An Iranian-made Shahed-type drone struck a hangar at the British base at RAF Akrotiri on March 1 and 2, 2026, the first strike on an EU member state in the war, and more drones were intercepted on

March 1 and 4. Cyprus's foreign minister said the drone was launched from Lebanon. The State Department raised its advisory to Level 3 on March 3 and allowed non-essential U.S. government staff to leave, airlines suspended flights, and Greece, France, and others sent air defenses and aircraft.

- **Eastern Mediterranean gas.** Disputes over offshore gas rights involve Turkey, Greece, Cyprus, and Israel.
- **Russian money and sanctions.** Cyprus's financial sector has faced scrutiny over Russian deposits, and the country has tightened sanctions enforcement.

Cyber Threats | Organizations

- **Financial and shipping sectors.** Banks, corporate service providers, and maritime firms hold high-value data and face phishing, business email compromise, and extortion.
- **State-linked targeting.** Government, defense, and energy organizations attract interest from regional actors, and Cyprus has experienced attacks tied to regional tensions.
- **Hacktivism.** Turkish and pro-Russia groups have launched DDoS attacks at Cypriot sites around political events.
- **Regulation.** Cyprus is implementing NIS2 and applies the GDPR.
- **Employees based in country.** Employees face phishing, travel disruption during regional escalations, and elevated scrutiny at the buffer zone.
- **Vendor and supply chain risk.** Corporate service providers, shipping firms, and banks hold high-value data and are exposed to business email compromise, so verify subcontractor controls.

The TIDE team tracks 7 threat actors that list Cyprus among their targets. By attributed nexus, they break down as 2 China-nexus, 2 cybercriminal, 2 Turkey-nexus, and 1 hacktivist. The most frequently targeted sectors are government (5), civil society and activism (3), telecommunications (3), banking and financial services (2), and cryptocurrency and digital assets (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and parcel scams.** Bank and courier impersonation messages circulate in Greek, English, and Russian.
- **Rental and booking fraud.** Fake listings target visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Cyprus.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Cyprus Level 3, Reconsider Travel, citing other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Cyprus sits close to regional conflict and faces hacktivism and financial-sector exposure. The State Department rated it Level 3 in an advisory issued in early March 2026.
- **What would change this rating.** Raise to Level 3 if Gulf hostilities spread to the eastern Mediterranean. Lower to Level 1 if regional tension subsides.

Public Wi-Fi

- Regional conflict and hacktivism targeting government and financial institutions create elevated phishing and account-takeover risk; use a corporate VPN before connecting to airport or hotel networks.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Review the current advisory and regional security updates before approving travel, since the situation can change quickly.
- Crossing the buffer zone requires documents, and some checkpoints inspect bags and electronics.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

CZECHIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Prague

GOVERNMENT
Parliamentary republic

LANGUAGE
Czech

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued January 8, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: EU and NATO member with known Chinese and Russian targeting of government and defense.

Country Overview

Czechia, also known as the Czech Republic, was historically the Kingdom of Bohemia, which became part of the Habsburg Empire in the sixteenth century. Czechoslovakia was founded in 1918 and was the interwar region's only durable democracy until Germany dismembered it in 1938 and 1939. A communist coup in 1948 placed the country in the Soviet bloc, and Soviet-led forces crushed the Prague Spring in 1968.

The Velvet Revolution of 1989 ended communist rule, and Czechoslovakia split peacefully in 1993. Czechia joined NATO in 1999 and the EU in 2004. The country has about 10.9 million people and a strong industrial economy centered on automobiles and machinery. Andrej Babis became prime minister in December 2025 after his ANO party won the October 2025 election.

Geopolitical Landscape

- **Government change.** Babis leads a government that has questioned some EU policies and aid to Ukraine, which has drawn attention from partners.
- **Russia and sabotage.** Czechia has attributed sabotage and espionage to Russian services, including the 2014 Vrbetice ammunition depot explosions, and has expelled diplomats.
- **China.** In 2025 the Czech government attributed a cyber espionage campaign against its foreign ministry to China's APT31, and relations with Beijing are cautious while ties with Taiwan have grown.

- **Energy.** Czechia ended reliance on Russian gas and oil and is expanding nuclear power.

Cyber Threats | Organizations

- **State-linked espionage.** Chinese and Russian actors target government and defense organizations, and Czech authorities attributed the APT31 campaign to China.
- **Ransomware.** Hospitals, municipalities, and manufacturers have been hit by ransomware.
- **Pro-Russia hacktivism.** DDoS campaigns target government, transport, and financial websites around political decisions.
- **Industrial base.** Automotive and machinery suppliers face intellectual property theft and ransomware.
- **Regulation.** Czechia implemented a new cybersecurity act under NIS2, led by the national cyber and information security agency NUKIB, which has also warned about Chinese technology risks.
- **Employees based in country.** Employees in government, defense, and policy roles may draw targeted phishing, and tourist areas carry pickpocket risk.
- **Vendor and supply chain risk.** Industrial and automotive suppliers face ransomware and IP theft, and the national cyber agency has warned about Chinese technology risk. Review hardware and software supplier provenance.

The TIDE team tracks 20 threat actors that list Czechia among their targets. By attributed nexus, they break down as 7 cybercriminal, 6 China-nexus, 3 Russia-nexus, 2 North Korea-nexus, 1 unattributed or other, and 1 hacktivist. The most frequently targeted sectors are government (15), banking and financial services (7), defense and defense industrial base (6), healthcare and pharmaceuticals (6), and critical infrastructure (general) (5). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and parcel scams.** Bank and courier impersonation is common.
- **Marketplace fraud.** Fake listings and payment links affect buyers and sellers.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Czechia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Czechia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Czechia is an EU and NATO member with ordinary travel risks. Chinese and Russian actors target government and defense, which matters mainly for staff in those roles.
- **What would change this rating.** Raise to Level 2 for government and defense staff if targeting increases.

Public Wi-Fi

- Chinese and Russian threat actors actively target government and defense sectors; staff in those roles should use a corporate VPN even on commercial hotel networks to avoid surveillance.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Pickpocketing is common in central Prague, on trams, and at tourist sites.
- Use licensed taxis or ride-hailing apps to avoid overcharging.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

DENMARK

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Copenhagen

GOVERNMENT
Parliamentary constitutional monarchy

LANGUAGE
Danish

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 17, 2024)

Risk indicators: Terrorism

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; exposure is ransomware, hacktivism, and espionage in shipping and Arctic sectors.

Country Overview

Denmark is a Nordic country made up of the Jutland peninsula and more than 400 islands, and it also includes two self-governing territories, the Faroe Islands and Greenland. Viking-age kings unified the realm in the tenth century, and Denmark later led the Kalmar Union that joined the Nordic kingdoms. It lost Norway in 1814 and Schleswig-Holstein in 1864.

Denmark was occupied by Germany from 1940 to 1945. It joined NATO in 1949 and the European Community in 1973 but keeps opt-outs from some EU policies, including the euro. The country has about 6 million people, a high-income economy, and global firms in shipping, pharmaceuticals, and wind energy. Mette Frederiksen has led the government since 2019.

Geopolitical Landscape

- **Greenland.** U.S. interest in acquiring Greenland has strained relations with Copenhagen since 2025. Denmark and Greenland reject any transfer and have expanded Arctic defense spending.
- **Russia and the Baltic.** Denmark controls the straits at the Baltic entrance, supports Ukraine strongly, and has faced drone sightings and suspected sabotage around critical sites.

- **Terrorism and extremism.** The State Department cites terrorism risk, and Denmark has experienced attacks and plots, including the 2015 Copenhagen shootings.
- **EU and NATO anchor.** Denmark joined the EU defense policy framework after a 2022 referendum ended its defense opt-out.

Cyber Threats | Organizations

- **Ransomware and extortion.** Cybercriminal groups drive most activity. Danish critical infrastructure suffered a coordinated attack on energy companies in 2023, and shipping and pharmaceutical firms are frequent victims.
- **State-linked espionage.** Russia- and China-linked actors target government, defense, shipping, and Arctic interests, and the Centre for Cyber Security warns of pre-positioning.
- **Hacktivist DDoS.** Pro-Russia groups have attacked Danish government, transport, and media sites.
- **Regulation.** Denmark applies NIS2 and the GDPR.
- **Employees based in country.** Employees face MitID and bank impersonation scams and bicycle and pickpocket theft in Copenhagen. Staff in shipping, defense, or Arctic roles may draw targeted phishing.
- **Vendor and supply chain risk.** Shipping, energy, and pharmaceutical suppliers are common third-party entry points. NIS2 extends security duties to suppliers, so request attestations and incident notification terms.

The TIDE team tracks 15 threat actors that list Denmark among their targets. By attributed nexus, they break down as 9 cybercriminal, 2 Iran-nexus, 2 hacktivist, 1 Russia-nexus, and 1 China-nexus. The most frequently targeted sectors are government (8), healthcare and pharmaceuticals (8), technology (7), industrial and manufacturing (7), and banking and financial services (6). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, MitID, and postal services are common.
- **Marketplace fraud.** Fake listings and payment-link fraud affect buyers.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Denmark.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Denmark Level 2, Exercise Increased Caution, citing terrorism. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Denmark is stable and well-regulated, and exposure comes from ransomware, hacktivism, and espionage in shipping and Arctic sectors rather than from risks to ordinary visitors.

- **What would change this rating.** Raise to Level 2 if Russia-linked sabotage or cyber activity against Danish infrastructure escalates.

Public Wi-Fi

- Ransomware and Russia-linked DDoS campaigns targeting shipping and critical infrastructure mean that travelers from those sectors face elevated network surveillance risk; use a corporate VPN on all public networks.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Pickpocketing occurs at Copenhagen transit hubs and tourist areas, so secure phones and wallets.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

DJIBOUTI

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Djibouti

GOVERNMENT
Presidential republic

LANGUAGE
French and Arabic

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued March 6, 2025)

Risk indicators: Terrorism, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Strategic chokepoint with competing foreign bases, state-controlled telecoms, and limited local capacity.

Country Overview

Djibouti is a small country at the southern entrance to the Red Sea on the Bab el-Mandeb strait. France established French Somaliland in the nineteenth century, and the territory became independent as Djibouti in 1977. Ismail Omar Guelleh has led the country since 1999.

Djibouti has about 1.1 million people and no natural resources of note, but its location makes it a global logistics and military hub. It hosts the only permanent U.S. military base in Africa, Camp Lemonnier, and bases of France, Japan, Italy, and China, and it is the main port for landlocked Ethiopia.

Geopolitical Landscape

- **Military hub.** Competing foreign bases make Djibouti a strategic chokepoint. China's naval base there, opened in 2017, is its first overseas base.
- **Red Sea shipping.** Houthi attacks on shipping since late 2023 have disrupted Red Sea traffic and raised regional risk.
- **Ethiopia dependence.** Port and rail links to Ethiopia drive the economy, and renewed Ethiopia-Eritrea tension is a concern.

- **Political control.** Power is concentrated in a long-serving presidency, and opposition space is limited.

Cyber Threats | Organizations

- **Ports and logistics.** Port operators and shipping firms hold high-value cargo and customs data and are exposed to espionage and fraud.
- **Foreign intelligence interest.** The density of foreign bases attracts intelligence collection against telecommunications and visitors.
- **Telecom concentration.** A state-controlled telecom operator and the landing of subsea cables make Djibouti a key regional internet node.
- **Limited local security capacity.** Banks and public bodies face phishing and fraud with thin response capacity.
- **Employees based in country.** Staff should assume communications are observable, expect elicitation from competing foreign interests, and plan for heat and power disruptions.
- **Vendor and supply chain risk.** Port, logistics, and telecom vendors sit at a strategic chokepoint where state-linked and foreign actors have interest. Limit vendor access and monitor remote connections.

The TIDE team tracks 2 threat actors that list Djibouti among their targets. By attributed nexus, they break down as 1 India-nexus, and 1 unattributed or other. The most frequently targeted sectors are banking and financial services (2), government (2), critical infrastructure (general) (1), defense and defense industrial base (1), and education and research (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring.** The state-run monopoly Djibouti Telecom gives authorities direct control of all fixed, mobile, and internet services, enabling surveillance of communications.
- **Mobile fraud.** SMS and mobile money scams affect users.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Djibouti.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Djibouti Level 2, Exercise Increased Caution, citing terrorism, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A strategic chokepoint with competing foreign bases, a state-controlled telecom operator, and heavy intelligence interest in visitors.
- **What would change this rating.** Raise to Level 3 if Red Sea or Ethiopia-Eritrea hostilities reach Djibouti.

Public Wi-Fi

- As a strategic chokepoint where ten international submarine cables land and competing foreign military bases operate in close proximity, including the United States' Camp Lemonnier and a Chinese base a few miles away, Djibouti's single state-controlled telecom operator creates an unusually concentrated intelligence collection opportunity; connect through a corporate VPN before accessing any public network.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Photography of port and military sites is restricted.
- Expect high heat and occasional connectivity disruption.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

DOMINICA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Roseau

GOVERNMENT
Parliamentary republic

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 20, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low state-surveillance risk; exposure is tourism fraud and hurricane disruption.

Country Overview

Dominica is a mountainous Caribbean island between Guadeloupe and Martinique, known as the Nature Isle. The Kalinago people were its original inhabitants, and France and Britain contested it before Britain took control in the late eighteenth century. It became independent in 1978 and is a republic within the Commonwealth.

Dominica has about 65,000 people and depends on agriculture, tourism, and a citizenship-by-investment program. Hurricane Maria devastated the island in 2017. Prime Minister Roosevelt Skerrit has led the government since 2004.

Geopolitical Landscape

- **Citizenship by investment.** The program funds public spending and draws scrutiny from the United States and EU over vetting.
- **Climate resilience.** Dominica aims to become the first climate-resilient nation after Hurricane Maria.
- **Small-state debt.** Public debt and storm recovery shape budgets.

Cyber Threats | Organizations

- **Tourism and small business.** Hotels and local firms face payment fraud and ransomware.

- **Investment migration providers.** Agents hold identity documents and financial records.
- **Limited security capacity.** Government depends on vendors and regional partners.
- **Employees based in country.** Employees face tourist-area scams and hurricane disruption, and staff at investment-migration firms face tailored phishing.
- **Vendor and supply chain risk.** Small local vendors and regional cloud providers carry most exposure. Investment-migration agents hold identity files and warrant vetting.

The TIDE team does not currently track actors that list Dominica among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Tourist-targeted scams.** Fake rental and tour listings and card skimming target visitors.
- **Phishing in English.** Digicel and Flow (Cable & Wireless) are the mobile operators; bank and delivery impersonation is common, and a 2025 Eastern Caribbean Central Bank advisory warned regionally of AI-assisted fraud and fake crypto schemes spreading over WhatsApp and Telegram.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Dominica.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Dominica Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk and ordinary tourist fraud, with hurricane disruption and sensitive identity data held by investment-migration firms.
- **What would change this rating.** Raise to Level 2 if a major breach hits those providers.

Public Wi-Fi

- Dominica connects via the Eastern Caribbean Fibre System, upgraded in 2015 to 3.4 Tbps capacity, with the Southern Caribbean Fiber system providing some redundancy; secure connections through a corporate VPN if using hotel or cafe networks during your stay.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Hurricane season, June through November, can interrupt travel and connectivity, and Dominica remains vulnerable to major storms, as Hurricane Maria demonstrated in 2017, so confirm evacuation and connectivity contingency plans before traveling.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

DOMINICAN REPUBLIC

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Santo Domingo

GOVERNMENT
Presidential republic

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued June 12, 2025)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Phone snatching, resort fraud, public-sector ransomware, and an active outsourcing sector.

Country Overview

The Dominican Republic shares the island of Hispaniola with Haiti. Christopher Columbus landed there in 1492, and Santo Domingo became the first permanent European settlement in the Americas. The country declared independence from Haiti in 1844 and endured a U.S. occupation from 1916 to 1924 and the Trujillo dictatorship from 1930 to 1961.

The Dominican Republic has about 10.8 million people and one of Latin America's faster-growing economies, based on tourism, remittances, and free-trade-zone manufacturing. Luis Abinader has been president since 2020 and was reelected in 2024.

Geopolitical Landscape

- **Haiti crisis.** Haitian gang violence and state collapse drive migration and border tension, and Santo Domingo has fortified the border and stepped up deportations.
- **U.S. alignment.** Santo Domingo cooperates closely with Washington on security and migration.
- **Tourism dependence.** Millions of visitors each year make the sector central to the economy.

- **Crime.** Violent crime and drug trafficking concern authorities, though tourist areas are generally better protected.

Cyber Threats | Organizations

- **Government ransomware.** A 2022 ransomware attack on the Dominican Agrarian Institute showed public-sector exposure.
- **Tourism and hospitality.** Resorts and booking platforms hold payment and passport data and face fraud.
- **Financial sector.** Banks face account takeover and card fraud.
- **Call-center and BPO sector.** Outsourcers handle foreign customer data and are potential third-party risks.
- **Employees based in country.** Employees face phone snatching from motorbikes, resort card skimming, and Spanish-language bank phishing.
- **Vendor and supply chain risk.** Call-center and outsourcing providers handle customer data and are common third-party exposures. Require access controls, monitoring, and breach notification terms.

The TIDE team tracks 1 threat actor that lists Dominican Republic among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are education and research (1), government (1), healthcare and pharmaceuticals (1), and industrial and manufacturing (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Tourist scams.** Fake rental listings and card skimming target visitors.
- **Phishing and SIM swap.** Bank and carrier impersonation is common in Spanish.
- **Phone theft.** Motorbike snatch theft occurs in Santo Domingo.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Dominican Republic.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Dominican Republic Level 2, Exercise Increased Caution, citing crime. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Phone snatching from motorbikes, resort card skimming, and Spanish-language bank phishing, plus third-party exposure in the outsourcing sector.
- **What would change this rating.** Raise to Level 3 if Haitian instability spills over. Lower to Level 1 as theft and fraud fall.

Public Wi-Fi

- Resort card skimming and phone snatching from motorbikes are documented threats to travelers; use a corporate VPN on hotel networks and keep devices out of sight in public spaces.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Keep phones out of sight on streets, and use resort or app-based transport.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

ECUADOR

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Quito

GOVERNMENT
Presidential republic

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 18, 2026)

Risk indicators: Crime, terrorism, unrest, kidnapping or hostage-taking

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Gang extortion using leaked data, express kidnapping, phone theft, and states of emergency.

Country Overview

Ecuador straddles the equator on South America's Pacific coast and includes the Andes, the Amazon basin, and the Galapagos Islands. The Inca Empire absorbed the highlands before Spain conquered the region in the sixteenth century. Ecuador became independent in 1822 and left Gran Colombia in 1830.

The country has about 18 million people and depends on oil, bananas, shrimp, and remittances. Political instability, the dollarized economy, and the rise of transnational gangs have defined recent years. Daniel Noboa has been president since 2023 and was reelected in 2025.

Geopolitical Landscape

- **Internal armed conflict.** Noboa declared an internal armed conflict against drug gangs in January 2024 after prison breaks and attacks. Violence, kidnapping, and extortion have risen, and states of emergency recur.
- **U.S. security cooperation.** Ecuador deepened security ties with Washington, though voters rejected hosting foreign military bases in a November 2025 referendum.
- **Energy and economy.** Droughts and oil-sector shocks have caused power cuts and fiscal strain.
- **Peru and Colombia borders.** Border regions are used for trafficking and armed-group activity.

Cyber Threats | Organizations

- **Ransomware and financial fraud.** Banks and public bodies have been hit by ransomware and breaches.
- **Extortion and doxxing.** Gangs use stolen personal data to threaten businesses and staff.
- **Oil and critical infrastructure.** Energy firms hold operational data and face espionage and ransomware.
- **Regulation.** A 2021 data protection law created new duties for organizations.
- **Employees based in country.** Employees face extortion calls built from leaked personal data, phone theft, and express kidnapping risk in major cities. Business owners and managers are priority extortion targets.
- **Vendor and supply chain risk.** Logistics, security, and payment vendors can leak staff and route information to gangs. Limit shared personal data, vet vendor employees, and monitor for insider-enabled extortion.

The TIDE team tracks 4 threat actors that list Ecuador among their targets. By attributed nexus, they break down as 3 unattributed or other, and 1 China-nexus. The most frequently targeted sectors are government (3), banking and financial services (2), energy (2), healthcare and pharmaceuticals (1), and insurance (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Virtual kidnapping and extortion.** Callers claim to hold relatives and demand payments, often using leaked data.
- **Phone theft and express kidnapping.** Street theft and fake-taxi robberies occur in Quito and Guayaquil.
- **Phishing.** Bank impersonation is common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Ecuador.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Ecuador Level 2, Exercise Increased Caution, citing crime, terrorism, unrest, kidnapping or hostage-taking. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Gangs use leaked personal data for extortion and virtual kidnapping, express kidnapping and phone theft occur in major cities, and states of emergency recur.
- **What would change this rating.** Raise to Level 3 if violence or extortion against business travelers increases. Lower if the security situation improves.

Public Wi-Fi

- Gangs use leaked personal data for extortion calls and virtual kidnapping targeting business travelers; connect through a corporate VPN to prevent device compromise that could expose you to data theft and targeting.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Use hotel-arranged or app-based transport, and avoid hailing street taxis.
- Avoid areas under states of emergency and border regions flagged in the advisory.

Return protocol

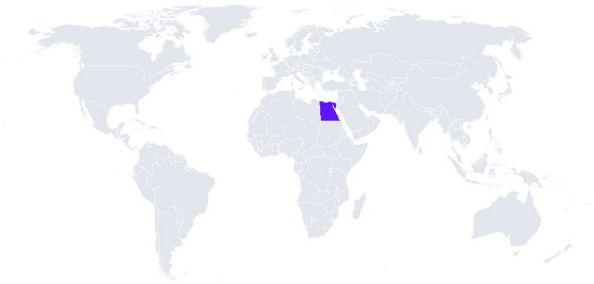
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

EGYPT

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 3



CAPITAL
Cairo

GOVERNMENT
Presidential republic

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 15, 2025)

Risk indicators: Terrorism, other, crime, health

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Pervasive state monitoring, VPN blocking, documented spyware use, and reported device inspections.

Country Overview

Egypt has one of the world's oldest continuous civilizations, built along the Nile for more than five thousand years. Pharaonic dynasties, then Greek, Roman, Arab, and Ottoman rule shaped the country. Britain controlled Egypt from 1882, and a 1952 coup by army officers ended the monarchy and brought Gamal Abdel Nasser to power.

Egypt signed a peace treaty with Israel in 1979. The 2011 uprising ended Hosni Mubarak's rule, Mohamed Morsi of the Muslim Brotherhood won a 2012 election and was removed by the army in 2013, and Abdel Fattah el-Sisi has been president since 2014. Egypt has about 109 million people and operates the Suez Canal.

Geopolitical Landscape

- **Gaza.** Egypt borders Gaza, mediated the October 2025 ceasefire process, and opposes displacement of Palestinians into Sinai.
- **Suez Canal revenue.** Red Sea attacks cut canal traffic and revenue, adding to an economic crisis marked by debt, inflation, and currency devaluations backed by Gulf and IMF support.

- **Sudan and Libya.** Egypt hosts millions of Sudanese refugees and is concerned about instability on its western and southern borders.
- **Nile dam.** The dispute with Ethiopia over the Grand Ethiopian Renaissance Dam remains unresolved.
- **Political control.** Authorities restrict opposition and media, and thousands of political prisoners are reported.

Cyber Threats | Organizations

- **Pervasive state monitoring.** Security services monitor communications and have blocked hundreds of websites and many VPN services.
- **Spyware.** Authorities monitor communications and online activity.
- **Energy, banking, and Suez logistics.** Strategic sectors draw espionage and disruption interest from regional actors.
- **Ransomware and fraud.** Banks, telecoms, and manufacturers face phishing and ransomware.
- **Employees based in country.** Staff should assume calls, messages, and hotel networks are monitored, expect VPN blocking, and avoid political content and photography of government sites. Device inspection by police has been reported.
- **Vendor and supply chain risk.** Telecom carriers and many large vendors are state-linked or state-regulated and can be compelled to share data. Limit vendor access, segment networks, and avoid hosting sensitive data locally.

The TIDE team tracks 17 threat actors that list Egypt among their targets. By attributed nexus, they break down as 7 cybercriminal, 3 Iran-nexus, 3 unattributed or other, 1 Russia-nexus, 1 Turkey-nexus, 1 China-nexus, and 1 hacktivist. The most frequently targeted sectors are government (13), banking and financial services (7), technology (6), industrial and manufacturing (5), and telecommunications (5). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and arrest.** Social media posts and chat content have led to prosecution, and police have stopped people to inspect phones.
- **Fake-profile and entrapment risk.** Dating-app entrapment has been used against LGBTQ people.
- **Fraud.** Bank, wallet, and delivery impersonation scams are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Egypt.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Egypt Level 2, Exercise Increased Caution, citing terrorism, other, crime, health. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Pervasive state monitoring, blocking of VPN services, documented spyware use, and reported police inspections of phones drive the rating.
- **What would change this rating.** Raise to Level 4 if detentions of foreigners or device inspections increase. Lower to Level 2 if monitoring and VPN blocking ease.

Public Wi-Fi

- Pervasive state monitoring, VPN blocking, and documented spyware use against dissidents and foreigners mean public Wi-Fi poses extreme risk; do not use public networks unless explicitly approved by your employer, and use only employer-provisioned devices with pre-approved connectivity.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid photographing military sites, bridges, and government buildings.
- Do not use dating apps in ways that could expose you to entrapment, and avoid demonstrations.
- Carry minimal data, since border and police checks can include electronics.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

EL SALVADOR

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2



CAPITAL
San Salvador

GOVERNMENT
Presidential republic

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued June 25, 2026)

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Documented spyware use against journalists and a state able to access in-country data.

Country Overview

El Salvador is the smallest and most densely populated country in Central America and has a Pacific coast and volcanic highlands. Pipil peoples lived in the area before Spain's conquest in 1525. El Salvador became independent in 1821 and endured a 1979 to 1992 civil war that killed about 75,000 people.

Gang violence then became one of the world's worst crises. President Nayib Bukele, in office since 2019, launched a state of exception in March 2022 that jailed tens of thousands of suspected gang members and cut homicides sharply. El Salvador adopted Bitcoin as legal tender in 2021 and later scaled back the policy under an IMF program. The country has about 6.3 million people.

Geopolitical Landscape

- **Security model.** The state of exception, renewed repeatedly, suspends some civil liberties, and rights groups criticize arbitrary detention. The model has high public approval and regional influence.
- **Concentrated power.** Constitutional changes in 2025 allow indefinite presidential reelection and extended the term.
- **U.S. partnership.** El Salvador agreed to hold deportees from the United States at its CECOT prison, a controversial arrangement.
- **Economy and Bitcoin.** Public debt and IMF conditions shape policy.

Cyber Threats | Organizations

- **State surveillance and spyware.** Citizen Lab and Access Now confirmed Pegasus infections on 35 journalists and civil society members between July 2020 and November 2021.
- **Public-sector breach risk.** Government and fintech systems carry breach risk because local security capacity is limited.
- **Financial sector.** Banks and the crypto sector face fraud and theft.
- **Gang-linked extortion.** Despite crackdowns, extortion tied to stolen personal data persists.
- **Employees based in country.** Employees face ordinary theft and bank-phishing risk, and staff in media, civil society, or politically exposed roles face state surveillance and spyware risk.
- **Vendor and supply chain risk.** Government-linked fintech and crypto vendors have had breaches, and the state can access data held in country. Review vendors that touch identity or payments.

The TIDE team tracks 2 threat actors that list El Salvador among their targets. By attributed nexus, they break down as 1 unattributed or other, and 1 cybercriminal. The most frequently targeted sectors are government (1), and banking and financial services (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring.** Journalists and activists face surveillance and legal pressure, and some have left the country.
- **Phishing and account takeover.** Bank and wallet impersonation is common.
- **Phone theft.** Opportunistic theft occurs in cities and tourist areas.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to El Salvador.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates El Salvador Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Spyware has been documented against journalists, the state can access data held in country, and ordinary theft and bank phishing persist. The security model has reduced violent crime for visitors.
- **What would change this rating.** Raise to Level 3 if the state of exception broadens surveillance of foreigners. Staff outside media, civil society, and politically exposed roles face closer to Level 1 conditions.

Public Wi-Fi

- Journalists, activists, and civil society staff have been targeted with Pegasus spyware; if your role is in sensitive sectors, verify VPN approval with your employer before using any public network.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Keep devices secured in public, and avoid political commentary during the trip.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

EQUATORIAL GUINEA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 3

CAPITAL
Malabo (administrative; Ciudad de la Paz is the planned capital)

GOVERNMENT
Presidential republic (authoritarian)

LANGUAGE
Spanish, French, and Portuguese

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued October 27, 2025)

Risk indicators: Crime, health, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Authoritarian control of telecoms, monitoring, internet restrictions, and sanctions exposure.

Country Overview

Equatorial Guinea is a small country in Central Africa made up of a mainland region, Rio Muni, and islands including Bioko, where the capital sits. Portugal and then Spain controlled the territory, and it became independent from Spain in 1968, the only Spanish-speaking country in sub-Saharan Africa.

Teodoro Obiang Nguema has ruled since a 1979 coup against his uncle, making him one of the world's longest-serving leaders. Oil discoveries in the 1990s made the country rich on paper, but wealth is concentrated among a small elite and rights groups report repression. The country has about 1.7 million people.

Geopolitical Landscape

- **Long-serving rule.** Obiang's family dominates politics and the economy, and succession is an open question.
- **Oil decline.** Falling oil output strains public finances.
- **Corruption and sanctions.** Obiang's relatives have faced asset seizures and charges in the United States and Europe.
- **Foreign partners.** Equatorial Guinea works with Russia, China, and Western energy firms.

Cyber Threats | Organizations

- **Oil sector.** Energy operators and contractors hold sensitive data and face espionage and fraud.
- **State control of telecoms.** Government-linked operators control the network, and authorities monitor communications.
- **Limited local security capacity.** Banks and public bodies face phishing with little incident response.
- **Sanctions and corruption exposure.** Business dealings can create compliance risk.
- **Employees based in country.** Staff should assume monitoring of communications, expect internet restrictions and unreliable service, and avoid commentary on the government or photography of official sites.
- **Vendor and supply chain risk.** State-linked telecoms and oil contractors control critical access, and compelled disclosure is likely. Limit vendor access to sensitive systems and screen for sanctions and corruption exposure.

The TIDE team does not currently track actors that list Equatorial Guinea among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Surveillance.** Activists and journalists face monitoring and arrest.
- **Internet controls.** Authorities have restricted social media and websites at sensitive moments.
- **Mobile fraud.** SMS and mobile money scams exist.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Equatorial Guinea.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Equatorial Guinea Level 2, Exercise Increased Caution, citing crime, health, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Authoritarian control of telecoms, monitoring of communications, internet restrictions at sensitive moments, and sanctions and corruption exposure drive the rating.
- **What would change this rating.** Raise to Level 4 if detentions of foreigners increase. Lower to Level 2 if restrictions ease.

Public Wi-Fi

- The state-controlled single telecom operator enables pervasive monitoring and internet restrictions; assume all connectivity is monitored and use a corporate VPN for any public network access only with explicit authorization.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Photography of government and security sites is restricted.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

ERITREA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 4

CAPITAL
Asmara

GOVERNMENT
One-party presidential republic

LANGUAGE
Tigrinya, Arabic, and English (working languages)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 24, 2026)

Risk indicators: Wrongful detention, other

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Extreme state control, single state telecom, near-total monitoring, and arbitrary detention.

Country Overview

Eritrea lies on the Red Sea in the Horn of Africa. Italy colonized it in the nineteenth century, Britain administered it after the Second World War, and the United Nations federated it with Ethiopia in 1952. Ethiopia annexed it in 1962, which triggered a 30-year independence war that ended in 1991. Eritrea became independent in 1993.

A 1998 to 2000 war with Ethiopia killed tens of thousands. President Isaias Afwerki has ruled since independence, elections have never been held, and the country has one of the world's most closed political systems, with indefinite national service. Eritrea has about 3.7 million people.

Geopolitical Landscape

- **Tension with Ethiopia.** Eritrea and Ethiopia, which made peace in 2018, are again at risk of war. Crisis Group listed Ethiopia and Eritrea as conflict risk alerts for October 2026, and Ethiopia's army commander accused Eritrea in September 2026 of backing rebels.
- **Isolation.** Eritrea has limited relations with Western governments and sanctions history, and has aligned with Russia, Egypt, and Gulf states.

- **Repression.** Arbitrary detention without trial, forced conscription, and tight media control are well documented.

Cyber Threats | Organizations

- **Extreme state control of connectivity.** Internet access is among the world's lowest and is state-controlled through a single operator, with no independent media.
- **Pervasive monitoring.** Communications are assumed monitored, and foreign organizations have almost no presence.
- **Diaspora targeting.** Eritrean diaspora groups report harassment and a diaspora tax enforced through coercion.
- **Employees based in country.** Staff should assume all communications and devices are monitored, expect minimal connectivity, and avoid unapproved contact with locals or photography.
- **Vendor and supply chain risk.** There is effectively one state telecom provider, so any vendor connectivity is state-controlled. Avoid dependency on in-country vendors for sensitive operations.

The TIDE team does not currently track actors that list Eritrea among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Surveillance and detention.** Citizens have been detained for contact with foreigners or online activity.
- **Connectivity limits.** Internet is slow, costly, and often unavailable.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Eritrea.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Eritrea Level 2, Exercise Increased Caution, citing wrongful detention, other. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A single state telecom provider, minimal connectivity, near-total monitoring, and arbitrary detention, with a risk of war with Ethiopia.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a major opening of communications and an end to arbitrary detention.

Public Wi-Fi

- A single state telecom provider enables near-total monitoring; do not use public Wi-Fi, and comply strictly with the approved corporate device and connectivity policy, as VPN use may attract official scrutiny.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Local practices

- Travel permits are required for movement outside Asmara, and photography restrictions are strict.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

ESTONIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Tallinn

GOVERNMENT
Parliamentary republic

LANGUAGE
Estonian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued March 31, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Highly digital, well-defended state facing Russia-linked activity and GPS interference near the border.

Country Overview

Estonia is a Baltic country on the Gulf of Finland bordering Russia and Latvia. Danes, Germans, Swedes, and Russians ruled its territory over the centuries, and Estonia first declared independence in 1918. The Soviet Union annexed it in 1940, and Estonia regained independence in 1991.

Estonia joined NATO and the EU in 2004 and the eurozone in 2011. It has about 1.4 million people and is famed for digital government, including e-residency, internet voting, and the X-Road data exchange. The NATO Cooperative Cyber Defence Centre of Excellence is based in Tallinn.

Geopolitical Landscape

- **Russia threat.** Estonia shares a border with Russia and is among Ukraine's strongest supporters. It has faced airspace violations, GPS jamming, and suspected sabotage.
- **NATO frontline.** Allied troops are stationed in Estonia, and the country spends a high share of GDP on defense.
- **Digital state.** Estonia's digital identity system underpins government and banking.
- **Baltic Sea infrastructure.** Undersea cable and pipeline incidents raised concern about hybrid threats.

Cyber Threats | Organizations

- **Russia-linked cyber activity.** Estonia suffered a landmark wave of denial-of-service attacks in 2007 and continues to face Russia-linked attacks and hacktivism.
- **GPS jamming and hybrid pressure.** Navigation interference affects aviation and shipping in the region.
- **Digital government dependence.** Heavy reliance on digital identity and data exchange makes resilience and supplier security central.
- **Ransomware and supply chain risk.** Estonian firms face ransomware, and heavy reliance on shared digital services makes supplier compromise a central concern.
- **Employees based in country.** Employees face bank and e-ID phishing and GPS interference near the eastern border and Gulf of Finland. Staff in government, defense, or critical-infrastructure roles may draw Russia-linked targeting.
- **Vendor and supply chain risk.** Estonia relies on a small set of digital-government and cloud suppliers, so supplier compromise can propagate widely. Require supplier assurance and monitor for Russia-linked targeting of providers.

The TIDE team tracks 9 threat actors that list Estonia among their targets. By attributed nexus, they break down as 3 Russia-nexus, 2 cybercriminal, 1 Belarus-nexus, 1 Iran-nexus, 1 unattributed or other, and 1 hacktivist. The most frequently targeted sectors are government (7), education and research (3), technology (2), critical infrastructure (general) (2), and energy (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and scams.** Bank and ID-card impersonation is common.
- **GPS and navigation interference.** Jamming can affect phone and vehicle location services near the border and Gulf of Finland.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Estonia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Estonia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Estonia is a highly digital, well-defended state. Visitors face GPS interference near the eastern border and Gulf of Finland, and government and defense staff may draw Russia-linked targeting.
- **What would change this rating.** Raise to Level 2 if Russian hybrid pressure or interference escalates.

Public Wi-Fi

- Russia-linked targeting of government and defense sectors, plus GPS jamming near the border, make credential theft a priority for adversaries; use a corporate VPN on all public networks if your role involves critical infrastructure or defense.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Expect GPS interference in some areas near the border, and carry offline maps.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

ESWATINI

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Mbabane (administrative) and Lobamba (legislative and royal)

GOVERNMENT
Absolute monarchy

LANGUAGE
siSwati and English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 10, 2026)

Risk indicators: Unrest, crime

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Absolute monarchy that restricted internet access during unrest, plus mobile-money fraud.

Country Overview

Eswatini, formerly Swaziland, is a small landlocked kingdom between South Africa and Mozambique. The Swazi nation coalesced in the early nineteenth century under King Sobhuza I, and Britain controlled it from 1903. It became independent in 1968.

King Mswati III has ruled since 1986 and holds executive power. Political parties are banned from contesting elections, and the 2021 prodemocracy protests were met with deadly force. Eswatini has about 1.2 million people and depends on South Africa's economy and customs revenues.

Geopolitical Landscape

- **Monarchical rule.** Calls for reform have been repressed, and the government monitors dissent.
- **U.S. deportee arrangement.** Eswatini agreed in 2025 to accept third-country deportees from the United States, a move criticized by rights groups.
- **Economic pressure.** High unemployment, HIV prevalence, and dependence on South Africa shape stability.

Cyber Threats | Organizations

- **Small, concentrated market.** A few banks and telecoms dominate, with limited security capacity.
- **Internet restrictions.** Authorities restricted internet access during the 2021 unrest.
- **Mobile money fraud.** SIM-swap and mobile money fraud are common.
- **Employees based in country.** Employees face mobile-money fraud and may face connectivity restrictions during unrest. Staff should avoid political activity.
- **Vendor and supply chain risk.** Small local vendors and South African parent firms carry most exposure. Verify subcontractor security and keep sensitive data off local infrastructure.

The TIDE team does not currently track actors that list Eswatini among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Monitoring.** Activists and journalists face surveillance and prosecution under laws including the 2008 Suppression of Terrorism Act; King Mswati III, Africa's last absolute monarch, holds a reported 10 percent stake in MTN Eswatini, the market leader.
- **Scams.** SMS and WhatsApp fraud targets mobile money users.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Eswatini.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Eswatini Level 2, Exercise Increased Caution, citing unrest, crime. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** An absolute monarchy that restricted internet access during unrest, plus mobile-money fraud and thin security capacity.
- **What would change this rating.** Raise to Level 3 if protests return with shutdowns.

Public Wi-Fi

- The government ordered a series of internet and social media shutdowns during the pro-democracy protests of 2021, including a full blackout in June and targeted platform blocks that October; mobile-money fraud is widespread. Use a corporate VPN to protect credentials if unrest recurs and connectivity is restricted.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, and carry offline plans if unrest occurs.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

ETHIOPIA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Addis Ababa

GOVERNMENT
Federal parliamentary republic

LANGUAGE
Amharic (federal working language) and others

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 27, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Dominant state telecom, long internet shutdowns, documented spyware use, and renewed war in the north.

Country Overview

Ethiopia is one of the world's oldest states, centered on the Aksumite kingdom and later Christian and imperial dynasties, and it was never colonized apart from a brief Italian occupation from 1936 to 1941. Emperor Haile Selassie ruled until the 1974 revolution brought a Marxist military junta, the Derg, followed by civil war.

The current federal system took shape in 1991 under the EPRDF coalition. Abiy Ahmed became prime minister in 2018 and won the 2019 Nobel Peace Prize for making peace with Eritrea. The 2020 to 2022 Tigray war killed hundreds of thousands. Ethiopia has about 112 million people and hosts the African Union headquarters.

Geopolitical Landscape

- **Renewed war in the north.** In September 2026, the Tigray People's Liberation Front launched a multi-pronged offensive with other rebels, large-scale fighting began around September 22 and 23, and Ethiopia responded with drone strikes. Crisis Group listed Ethiopia as deteriorated in September and a conflict risk alert for October, with a risk of drawing in Eritrea.
- **Ethiopia-Eritrea tension.** Addis Ababa accuses Eritrea, along with Sudan and Egypt, of supporting rebels, which raises the risk of interstate war.

- **Other conflicts.** Insurgencies in Amhara and Oromia continue.
- **Nile dam and sea access.** The Grand Ethiopian Renaissance Dam has strained relations with Egypt, and Ethiopia's push for sea access worries neighbors.

Cyber Threats | Organizations

- **Internet shutdowns.** Authorities have imposed long regional shutdowns, including in Tigray and Amhara, and national social media blocks. Plan for sudden loss of connectivity.
- **State surveillance and spyware.** Authorities monitor communications, and the dominant state-owned telecom operator, Ethio telecom, eases monitoring.
- **Financial and telecom sectors.** Banks and Ethio telecom face fraud and disruption.
- **Conflict-linked information operations.** All parties run disinformation campaigns, and diaspora networks are targeted.
- **Employees based in country.** Staff should expect shutdowns and social media blocks, assume monitoring through the dominant state telecom, and avoid political content. Travel outside Addis Ababa carries physical risk during the renewed fighting.
- **Vendor and supply chain risk.** The dominant state-owned telecom controls much of connectivity, and vendors in conflict regions can lose access abruptly. Plan continuity, segment vendor access, and avoid locating sensitive data in country.

The TIDE team tracks 3 threat actors that list Ethiopia among their targets. By attributed nexus, they break down as 2 China-nexus, and 1 unattributed or other. The most frequently targeted sectors are government (3), healthcare and pharmaceuticals (1), military (1), civil society and activism (1), and religious organizations (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and detention.** Journalists and activists face arrest, and authorities monitor social media.
- **Mobile money fraud.** Fraud affects telebirr and other wallets.
- **Disinformation.** False content spreads widely during conflict.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Ethiopia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Ethiopia Level 3, Reconsider Travel, citing unrest, crime, kidnapping or hostage-taking, terrorism, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions. Conditions in the north have worsened since September 2026, and the TIDE team would raise the level if fighting spreads to the capital or involves Eritrea.

TIDE Risk Level Rationale

- **Drivers.** The dominant state telecom enables monitoring, long regional shutdowns have occurred, spyware has been documented against dissidents, and war resumed in the north in September 2026.
- **What would change this rating.** Raise to Level 4 if fighting reaches the capital, Eritrea enters the war, or shutdowns become national. Lower to Level 2 if a ceasefire holds and restrictions end.

Public Wi-Fi

- Long regional internet shutdowns, state-enabled surveillance through the dominant telecom, and renewed warfare in the north mean connectivity is both monitored and unreliable; avoid public Wi-Fi entirely and rely only on employer-approved devices and connectivity outside conflict zones.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid the Tigray, Amhara, Afar, and border regions flagged in the advisory.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

FIJI

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Suva

GOVERNMENT
Parliamentary republic

LANGUAGE
English, Fijian, and Fiji Hindi

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued December 2, 2024)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk and ordinary tourist fraud; regional diplomatic hub and limited local security capacity.

Country Overview

Fiji is a Pacific archipelago of more than 300 islands, with most of its about 900,000 people on Viti Levu and Vanua Levu. Melanesian and Polynesian settlers arrived thousands of years ago, and Britain took control in 1874 and brought indentured laborers from India to work sugar plantations, which shaped the country's two largest communities. Fiji became independent in 1970.

Coups in 1987, 2000, and 2006 marked decades of ethnic and military politics. Frank Bainimarama governed from 2006 to 2022, and Sitiveni Rabuka has been prime minister since December 2022. The economy relies on tourism, sugar, remittances, and gold, and Suva hosts the Pacific Islands Forum Secretariat and many regional organizations.

Geopolitical Landscape

- **Great-power competition.** Australia, New Zealand, the United States, and China compete for influence in the Pacific through security, infrastructure, and policing agreements, and Fiji tries to balance them.
- **Elections.** A general election is due around the end of 2026 or early 2027, and Fiji's history of coups makes civil-military relations a continuing watch item.
- **Climate vulnerability.** Cyclones and sea-level rise drive policy, and Fiji is a leading voice on climate finance.
- **Regional hub.** Regional organizations in Suva make the city a target for diplomatic interest.

Cyber Threats | Organizations

- **Tourism and hospitality.** Resorts and airlines hold payment and passport data and face card fraud and ransomware.
- **Regional diplomatic targeting.** Pacific governments and regional bodies in Suva draw espionage interest from external powers.
- **Limited security capacity.** Public bodies and small firms rely on vendors and regional partners for cybersecurity, and public reporting of incidents is sparse.
- **Regulation.** Fiji has an Online Safety Act and a Cybercrime Act, and regional programs support capacity building.
- **Employees based in country.** Employees face tourist-area card fraud and theft, cyclone-related disruption, and phishing. Staff at regional organizations and diplomatic missions in Suva may draw targeted espionage interest.
- **Vendor and supply chain risk.** Small local vendors, regional telecoms, and cloud providers carry most of the exposure, and subsea cable dependence limits redundancy. Request continuity and incident notification terms.

The TIDE team tracks 1 threat actor that lists Fiji among their targets. By attributed nexus, they break down as 1 China-nexus. The most frequently targeted sectors are government (1), healthcare and pharmaceuticals (1), and industrial and manufacturing (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Tourist-targeted scams.** Fake booking and rental listings and card skimming target visitors.
- **Phishing and social media fraud.** Vodafone Fiji, Digicel Fiji, and Telecom Fiji operate the mobile networks; bank and telecom impersonation phishing is common on Facebook, and a cybersecurity industry estimate put Fijians' losses to online scams at more than US$2.2 million in 2024, including mobile money fraud.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Fiji.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Fiji Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low crime and light surveillance of visitors. Regional organizations in Suva and government staff may draw external espionage interest, and local security capacity is limited.
- **What would change this rating.** Raise to Level 2 if coup risk resurfaces around the coming election or targeting of regional bodies increases.

Public Wi-Fi

- Fiji is the Pacific's main submarine cable hub, landing the Southern Cross Cable Network and links to Samoa and Tonga, which reduces single-point-of-failure risk compared with its neighbors; phishing impersonating local banks remains active, so use a corporate VPN on hotel and public networks, and staff at diplomatic missions should verify VPN approval with their employer.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Cyclone season, November through April, can disrupt flights and connectivity.
- Keep devices secured on beaches and boats.

Return protocol

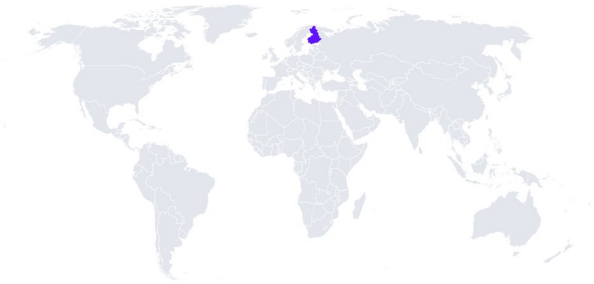
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

FINLAND

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Helsinki

GOVERNMENT
Parliamentary republic

LANGUAGE
Finnish and Swedish

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued March 13, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable, well-defended state; exposure is hacktivism, state-linked espionage, and GPS interference near the Russian border.

Country Overview

Finland sits in northern Europe between Sweden and Russia. Sweden ruled the territory for centuries until Russia took it in 1809 and made it a grand duchy. Finland declared independence in 1917 during the Russian Revolution and fought the Soviet Union in the Winter War of 1939 to 1940 and the Continuation War that followed, losing territory but keeping its independence.

Finland stayed militarily nonaligned during the Cold War, joined the EU in 1995, and joined NATO in April 2023 after Russia's invasion of Ukraine, which doubled the alliance's land border with Russia. The country has about 5.6 million people and a high-tech economy. Alexander Stubb has been president since March 2024, and Petteri Orpo has been prime minister since 2023.

Geopolitical Landscape

- **Border with Russia.** Finland shares a border of about 1,340 kilometers with Russia and closed its crossings in late 2023 after a surge of irregular arrivals that Helsinki said Russia orchestrated.
- **Baltic Sea infrastructure.** Suspected sabotage of undersea cables and pipelines in the Baltic Sea has raised hybrid-threat concerns.
- **Defense posture.** Finland has large reserves, high defense spending, and strong support for Ukraine.

- **GPS interference.** Jamming in the Baltic region affects aviation and shipping.

Cyber Threats | Organizations

- **State-linked espionage.** In August 2022 a Russian group claimed a denial-of-service attack on the Finnish Parliament's website, and Russia-linked and other actors target government, defense, and technology firms.
- **Healthcare data extortion.** Health and personal data are prime extortion targets, so vendors that hold such data should expect criminal attention.
- **Hacktivist DDoS.** Pro-Russia groups have attacked Finnish government and media sites, particularly around NATO decisions.
- **Critical infrastructure.** Energy, telecoms, and maritime operators are priority targets and are covered by NIS2 rules.
- **Employees based in country.** Employees face bank-ID and parcel phishing and GPS interference near the eastern border and Gulf of Finland. Staff in defense, energy, or government-adjacent roles may draw Russia-linked targeting.
- **Vendor and supply chain risk.** Telecom, maritime, and energy suppliers are priority targets for state-linked actors. NIS2 extends security duties to suppliers, so require attestations and incident notification.

The TIDE team tracks 9 threat actors that list Finland among their targets. By attributed nexus, they break down as 4 China-nexus, 3 cybercriminal, 1 Russia-nexus, and 1 Iran-nexus. The most frequently targeted sectors are government (7), technology (6), healthcare and pharmaceuticals (5), industrial and manufacturing (4), and banking and financial services (3). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, postal services, and authorities are common, and QR-code and bank-ID scams have grown.
- **GPS interference.** Jamming near the Gulf of Finland and eastern border can affect phone and vehicle location services.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Finland.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Finland Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Finland is stable and well-defended. Exposure comes from hacktivism, state-linked espionage, and GPS interference near the Russian border rather than from risks to ordinary visitors.

- **What would change this rating.** Raise to Level 2 if Russian hybrid pressure or interference escalates, particularly around the eastern border and Baltic infrastructure.

Public Wi-Fi

- State-linked espionage targeting government and technology sectors, along with phishing campaigns impersonating local authorities, make public networks in Finland attractive to both sophisticated and opportunistic adversaries; connect only through a corporate VPN if public networks must be used.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Expect GPS interference near the eastern border and in the Baltic, and carry offline maps.
- Eastern border crossings with Russia are closed.

Return protocol

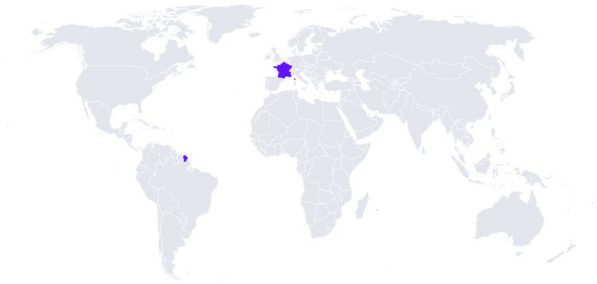
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

FRANCE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Paris

GOVERNMENT
Semi-presidential republic

LANGUAGE
French

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 28, 2025)

Risk indicators: Unrest, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Persistent state-linked and criminal targeting, phone snatching in Paris, and unrest and terrorism indicators from the State Department.

Country Overview

France has been a unified kingdom since the Middle Ages and a leading European power for centuries. The 1789 Revolution ended the monarchy and spread ideas of liberty and equality, Napoleon built an empire, and the Third Republic followed in 1870. France fought in both world wars, was occupied by Germany from 1940 to 1944, and rebuilt as a founder of the European Communities.

The Fifth Republic, founded in 1958 under Charles de Gaulle, created a strong presidency. France has about 69.1 million people, the second-largest economy in the EU, a permanent seat on the UN Security Council, and an independent nuclear deterrent. Emmanuel Macron has been president since 2017, and his term ends in 2027.

Geopolitical Landscape

- **Political fragmentation.** Macron's 2024 snap election produced a National Assembly split into three blocs without a governing majority. Sebastien Lecornu, reappointed in October 2025 after briefly resigning, is the fourth prime minister since the 2024 snap election, and he pushed the 2026 budget through parliament after months of turmoil. The 2027 presidential election is already shaping politics, and the National Rally is a leading contender.

- **Fiscal strain.** Credit agencies have downgraded France, citing political fragmentation and persistent deficits.
- **Russia and Ukraine.** France supports Ukraine, has attributed cyber operations to Russian intelligence, and faces disinformation and suspected sabotage.
- **Africa and overseas territories.** France has withdrawn forces from several Sahel and West African states, and unrest in New Caledonia in 2024 showed overseas tensions.
- **Terrorism and unrest.** The State Department cites terrorism and unrest, including periodic nationwide strikes and urban riots.

Cyber Threats | Organizations

- **State-linked espionage.** Chinese, Russian, and other actors target aerospace, defense, nuclear, and technology firms.
- **Ransomware and data breaches.** Hospitals, local authorities, and companies are frequent victims. A January 2024 breach at French health insurance companies affected 33 million people, and in April 2026 the national agency for secure credentials, ANTS, reported a breach affecting between 11 and 18 million accounts.
- **Hacktivism and event-driven attacks.** Pro-Russia DDoS groups target government and public-service sites, and a December 2025 attack knocked La Poste and La Banque Postale offline days before Christmas.
- **Regulation.** France implements NIS2, and the national agency ANSSI coordinates defense.
- **Employees based in country.** Employees face pickpocketing and phone snatching in Paris, bank and health-insurance phishing, and strike-related travel disruption. Staff in aerospace, defense, energy, or luxury sectors face elevated targeting.
- **Vendor and supply chain risk.** Hospitals, municipalities, and managed service providers are frequent ransomware victims, so supplier incidents can disrupt operations. NIS2 widens supplier security duties, so require attestations and incident notification.

The TIDE team tracks 152 threat actors that list France among their targets. By attributed nexus, they break down as 90 cybercriminal, 29 China-nexus, 9 Iran-nexus, 8 Russia-nexus, 5 North Korea-nexus, 5 unattributed or other, 3 hacktivist, 1 Belarus-nexus, 1 Turkey-nexus, and 1 Lebanon-nexus. The most frequently targeted sectors are healthcare and pharmaceuticals (82), government (80), industrial and manufacturing (65), technology (63), and banking and financial services (49). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, health insurance, tax, and delivery services are widespread.
- **Identity fraud after breaches.** Large breaches fuel convincing phishing and account takeover.
- **Phone theft.** Pickpocketing and phone snatching are common in Paris, especially on metro lines and at tourist sites.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to France.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates France Level 2, Exercise Increased Caution, citing unrest, terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** State-linked and criminal actors persistently target French organizations, phone snatching is common in Paris, and the State Department cites unrest and terrorism. Political fragmentation raises the chance of strikes and disruption.
- **What would change this rating.** Lower to Level 1 for travelers outside sensitive sectors if unrest subsides. Raise to Level 3 if sabotage or large-scale cyberattacks affect transport or telecoms.

Public Wi-Fi

- Ransomware campaigns and state-linked espionage targeting French enterprises, combined with recent large-scale breaches of health and credential systems, create elevated risk on public networks; use a corporate VPN if a public network is unavoidable.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Keep phones secured on the metro and at tourist sites.
- Strikes and demonstrations can disrupt transport, so confirm itineraries.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

GABON

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Libreville

GOVERNMENT
Presidential republic

LANGUAGE
French

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued March 30, 2026)

Risk indicators: Unrest, crime, health

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Post-coup government, an internet shutdown precedent, mobile-money fraud, and thin local security capacity.

Country Overview

Gabon is a rainforest-covered country on Africa's Atlantic coast. France colonized it in the nineteenth century, and it became independent in 1960. The Bongo family ruled for 55 years, with Omar Bongo from 1967 to 2009 and his son Ali Bongo from 2009 until a military coup in August 2023.

General Brice Oligui Nguema led the transition and was elected president in April 2025. Gabon has about 2.5 million people and relies on oil, manganese, and timber. It has one of Africa's higher per-capita incomes but sharp inequality.

Geopolitical Landscape

- **Post-transition government.** Oligui Nguema won the April 2025 presidential election by a large margin, and legislative elections followed. Critics note the dominant role of the former junta leader.
- **Partners.** Gabon remains close to France while courting China, the Gulf, and the United States for investment.
- **Resource dependence.** Oil decline and debt pressures shape the budget.

Cyber Threats | Organizations

- **Oil and mining.** Energy and manganese operators hold valuable data and face espionage and ransomware risk.
- **Connectivity controls.** Authorities cut internet access around the August 2023 election, and shutdowns are a precedent.
- **Financial and mobile money.** Banks and wallet providers face fraud and account takeover.
- **Limited local capacity.** Public bodies have few security resources.
- **Employees based in country.** Employees face mobile-money fraud and possible connectivity restrictions around political events. Oil and mining staff are higher-value targets for elicitation.
- **Vendor and supply chain risk.** Oil and logistics contractors and the main telecom operators hold sensitive data with limited local security capacity. Segment vendor access and limit locally stored data.

The TIDE team tracks 1 threat actor that lists Gabon among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile money and SMS fraud.** Gabon Telecom and Airtel Gabon split the market; SIM-swap and OTP scams are common.
- **Monitoring.** Authorities ordered a roughly four-day internet shutdown around the disputed August 2023 election; hours after the official result was announced, the military deposed President Ali Bongo and restored internet access, and post-coup authorities have been documented monitoring phone calls and personal mail.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Gabon.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Gabon Level 2, Exercise Increased Caution, citing unrest, crime, health. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A post-coup government, an internet shutdown during the 2023 election, mobile-money fraud, and thin local security capacity.
- **What would change this rating.** Raise to Level 3 if political unrest brings shutdowns or monitoring of dissent. Lower to Level 1 as institutions stabilize.

Public Wi-Fi

- The August 2023 election-period shutdown and the surveillance practices documented since the military took power show that public networks can be both cut and monitored around politically sensitive events; connect through a corporate VPN if public networks must be used.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Keep devices out of sight in Libreville traffic, where snatch theft occurs.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

GAMBIA, THE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Banjul

GOVERNMENT
Presidential republic

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued January 16, 2026)

Risk indicators: Crime, health, other

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk with tourism and mobile-money fraud; election period in December 2026.

Country Overview

The Gambia is a narrow country that follows the Gambia River into Senegal and is the smallest on mainland Africa. Britain established a colony there in the nineteenth century, and the country became independent in 1965. Dawda Jawara led until a 1994 coup brought Yahya Jammeh to power, and his 22-year rule was marked by repression until he lost the December 2016 election and left in early 2017.

Adama Barrow has been president since 2017 and won reelection in 2021. The Gambia has about 2.4 million people and depends on tourism, remittances, and groundnuts. A presidential election is scheduled for December 2026.

Geopolitical Landscape

- **December 2026 election.** Barrow is expected to seek another term, and campaign periods can bring tension and online disinformation.
- **Transitional justice.** Efforts to prosecute Jammeh-era abuses continue.
- **Economic fragility.** Debt, inflation, and tourism dependence shape politics.
- **Regional ties.** The Gambia is surrounded by Senegal and cooperates with ECOWAS.

Cyber Threats | Organizations

- **Tourism sector.** Hotels and tour operators hold payment and passport data and face card fraud.
- **Mobile money and banking.** Wallet providers and banks face SIM-swap and social engineering.
- **Limited local capacity.** Public bodies have few security resources, and public reporting is limited.
- **Employees based in country.** Employees face tourist-area fraud, mobile-money scams, and limited connectivity and power. Campaign periods may bring online disinformation.
- **Vendor and supply chain risk.** Small vendors and a handful of telecom and bank providers carry most exposure, with limited security capacity. Verify subcontractor controls.

The TIDE team does not currently track actors that list The Gambia among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile fraud.** Africell and QCell dominate the market, with QMoney and AfriMoney as the main mobile-money platforms; INTERPOL's 2025 Africa Cyberthreat Assessment placed the Gambia among the continent's top ransomware targets, with 1,729 detections logged in 2024, and smishing impersonating telecom operators is common.
- **Tourist-targeted scams.** Fake booking listings and card skimming target visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to The Gambia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates The Gambia Level 2, Exercise Increased Caution, citing crime, health, other. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with tourism fraud and mobile-money scams as the main exposure. Weak power and connectivity affect operations.
- **What would change this rating.** Raise to Level 2 if the December 2026 election period brings unrest or online restrictions.

Public Wi-Fi

- Ransomware and phishing activity are well above the regional average, and GM-CSIRT, operationalized under the telecom regulator PURA, issues regular phishing alerts; avoid mobile-money transactions over public Wi-Fi, and use a corporate VPN if a public network is necessary.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Power cuts and weak connectivity are common, so carry power banks and offline plans.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

GEORGIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2

CAPITAL
Tbilisi

GOVERNMENT
Parliamentary republic

LANGUAGE
Georgian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued March 13, 2025)

Risk indicators: Unrest, crime, other

Note: The United States recognizes Georgia within its internationally recognized borders. Abkhazia and South Ossetia are Russian-occupied and are recognized as independent by Russia and a small number of states.

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Rising pressure on civil society and media, Russia-linked targeting, and protest policing; low risk for typical visitors.

Country Overview

Georgia lies in the South Caucasus between the Black Sea and the Caucasus mountains. Ancient kingdoms including Colchis and Iberia preceded a medieval golden age, and the country adopted Christianity in the fourth century. Russia absorbed the territory in 1801. Georgia briefly gained independence in 1918, became a Soviet republic in 1921, and became independent again in 1991.

A 2003 Rose Revolution brought pro-Western reformers to power, and a 2008 war with Russia ended with Russian forces entrenched in the breakaway regions of Abkhazia and South Ossetia, about a fifth of Georgian territory. Georgia has about 3.9 million people. The Georgian Dream party, founded by billionaire Bidzina Ivanishvili, has governed since 2012.

Geopolitical Landscape

- **Contested 2024 election and EU course.** Georgian Dream claimed victory in the disputed October 26, 2024 election. The EU had already frozen Georgia's accession process in June 2024 after a foreign-influence law,

and in November 2024 Prime Minister Irakli Kobakhidze announced Georgia would suspend EU accession talks until 2028, triggering mass protests and police crackdowns. Georgia has been an EU candidate since December 2023. This profile does not independently verify later developments.

- **Western response.** The United States suspended its strategic partnership with Georgia and sanctioned the interior minister in December 2024.
- **Russia.** Critics say the government has tilted toward Moscow while it maintains it is committed to the constitutional goal of EU membership.
- **Occupied regions.** Russian forces in Abkhazia and South Ossetia continue incremental border movement, and the situation remains frozen.

Cyber Threats | Organizations

- **Russia-linked cyber activity.** The 2008 war included cyberattacks, and U.S. intelligence officials concluded that the Russian government was behind them.
- **Pressure on civil society and media.** Laws on foreign funding and tighter control of media increase risk for NGOs, journalists, and their vendors.
- **Government and critical infrastructure.** Government, energy, and transit networks along the Caucasus corridor draw regional espionage interest.
- **IT and outsourcing sector.** Georgia hosts growing IT services and relocated Russian technology workers, which creates vetting and supply chain considerations.
- **Employees based in country.** Employees face ordinary fraud risk, and staff in media, civil society, or politically exposed roles face monitoring, phishing, and legal pressure. Avoid demonstrations.
- **Vendor and supply chain risk.** Relocated and local IT contractors, telecoms, and media-adjacent vendors may face political pressure or Russia-linked targeting. Review developer access and ownership, and segment vendor connections.

The TIDE team tracks 3 threat actors that list Georgia among their targets. By attributed nexus, they break down as 2 cybercriminal, and 1 Russia-nexus. The most frequently targeted sectors are banking and financial services (2), government (2), civil society and activism (1), diplomatic and foreign affairs (1), and business and professional services (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Protesters, activists, and journalists face surveillance, fines, and detention.
- **Disinformation.** Politically themed false content spreads widely on Facebook and messaging apps.
- **Phishing and fraud.** Bank and delivery impersonation scams circulate in Georgian and Russian.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Georgia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Georgia Level 1, Exercise Normal Precautions, citing unrest, crime, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Government pressure on civil society and media has grown, Russia-linked actors target the country, and protests have met forceful policing. Typical visitors face low cyber risk, so the rating reflects role-based exposure.
- **What would change this rating.** Raise to Level 3 if surveillance or detention of foreigners increases or restrictions on communications are imposed. Lower to Level 1 if the political situation stabilizes.

Public Wi-Fi

- Russia-linked cyber activity and targeting of civil society, media, and critical infrastructure create elevated espionage risk on Georgian public networks, especially for staff in sensitive roles; connect through a corporate VPN if public networks must be used.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, which have involved water cannons and detentions.
- Do not approach the administrative boundary lines with Abkhazia and South Ossetia.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

GERMANY

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Berlin

GOVERNMENT
Federal parliamentary republic

LANGUAGE
German

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 13, 2025)

Risk indicators: Terrorism

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; main exposure is ransomware, industrial espionage, and pickpocketing.

Country Overview

Germany was a patchwork of states within the Holy Roman Empire before Otto von Bismarck unified most of it in 1871. Defeat in the First World War ended the empire, the Weimar Republic collapsed in 1933, and Nazi rule led to the Second World War and the Holocaust. After 1945 the country was divided, with the Federal Republic in the west and the communist German Democratic Republic in the east, until reunification on October 3, 1990.

Germany is a founding member of the EU and NATO, has about 84 million people, and has the largest economy in Europe. Friedrich Merz became chancellor in May 2025 leading a coalition of his CDU and the SPD.

Geopolitical Landscape

- **Ukraine and rearmament.** Germany is a leading supplier of aid to Ukraine and in 2025 loosened its constitutional debt brake to allow large increases in defense and infrastructure spending.
- **Russian hybrid threats.** Berlin has attributed cyberattacks and disinformation to Russian intelligence and faces suspected sabotage and espionage cases.
- **Domestic politics.** The far-right AfD finished second in the February 2025 federal election, and migration and the economy dominate debate.

- **Economic strain.** Industry faces high energy costs, weak growth, and U.S. tariffs, and trade ties with China are being reassessed.

Cyber Threats | Organizations

- **Ransomware and extortion.** Cybercriminal groups account for most threats, and manufacturers, municipalities, and hospitals are frequent victims.
- **State-linked espionage.** Germany publicly attributed the 2024 compromise of the SPD party's email accounts to Russia's APT28, and China-, Russia-, and Iran-linked actors target industry, research, and government.
- **Industrial base and supply chain.** Mittelstand suppliers and software vendors are routes into larger manufacturers, and intellectual property theft is a persistent concern.
- **Regulation.** Germany implements NIS2 through the BSI, and critical-infrastructure operators face strict reporting duties.
- **Employees based in country.** Employees face parcel and bank phishing and pickpocketing at stations and events. Staff in manufacturing, defense, and research may draw state-linked targeting.
- **Vendor and supply chain risk.** Mittelstand suppliers and managed service providers are common entry points for ransomware and intellectual property theft. NIS2 broadens supplier obligations, so require attestations and incident notification.

The TIDE team tracks 168 threat actors that list Germany among their targets. By attributed nexus, they break down as 99 cybercriminal, 29 China-nexus, 10 Russia-nexus, 9 Iran-nexus, 9 unattributed or other, 6 North Korea-nexus, 2 Turkey-nexus, 2 hacktivist, 1 Belarus-nexus, and 1 Lebanon-nexus. The most frequently targeted sectors are healthcare and pharmaceuticals (92), government (80), industrial and manufacturing (72), technology (69), and banking and financial services (55). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Bank, parcel, and tax impersonation is common in German.
- **Fraud via messaging apps.** Scammers impersonate relatives with a new phone number.
- **Marketplace and rental fraud.** Fake listings and payment-link scams are widespread.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Germany.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Germany Level 2, Exercise Increased Caution, citing terrorism. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Germany is stable and well-regulated. Exposure is ransomware, industrial espionage, and pickpocketing, and state-linked actors target industry and government more than visitors.
- **What would change this rating.** Raise to Level 2 if state-linked targeting of travelers or major sabotage affects transport and logistics.

Public Wi-Fi

- Ransomware crews and state-linked espionage targeting German industry and government, including the 2024 APT28 compromise of political party infrastructure, make German public networks attractive targets; use a corporate VPN if a public network is necessary.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Pickpocketing occurs at major train stations, markets, and events.
- Rail and airport strikes occur periodically, so confirm itineraries.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

GHANA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Accra

GOVERNMENT
Presidential republic

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 7, 2026)

Risk indicators: Crime, other, health

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Large fraud ecosystem, mobile-money scams, and snatch theft in traffic.

Country Overview

Ghana lies on the Gulf of Guinea and takes its name from the medieval Ghana Empire, though the empire lay farther northwest. The Ashanti Empire dominated the interior, and European traders, then Britain, ruled the coast as the Gold Coast. In 1957 Ghana became the first sub-Saharan African colony to gain independence, under Kwame Nkrumah.

Coups marked the decades after independence, and since 1992 Ghana has been a stable multiparty democracy with peaceful transfers of power. John Mahama returned as president in January 2025 after winning the December 2024 election. The country has about 34 million people and relies on gold, cocoa, and oil. Ghana defaulted on its external debt in 2022 and has been rebuilding under an IMF program.

Geopolitical Landscape

- **Economic recovery.** Debt restructuring and an IMF program have steadied the economy after the 2022 default, and the cedi and inflation remain key concerns.
- **Illegal mining.** Unregulated gold mining, called galamsey, damages rivers and is a major political issue.
- **Northern security spillover.** Jihadist violence in neighboring Burkina Faso raises risk in the north.

- **Regional diplomacy.** Ghana engages with the Sahel juntas while remaining in ECOWAS.

Cyber Threats | Organizations

- **Fraud ecosystem.** Ghana is a base for romance, advance-fee, and business email compromise networks that target victims abroad, which also creates insider and mule-account risk for local banks and telecoms.
- **Mobile money.** MTN MoMo and other wallets face SIM-swap and social engineering.
- **Public and financial sector.** The Cyber Security Authority, created under a 2020 law, coordinates response, and banks face phishing and account takeover.
- **Gold and cocoa supply chains.** Traders and exporters hold valuable data and face invoice fraud.
- **Employees based in country.** Employees face mobile-money fraud, phone snatching in traffic, and invoice and payment-redirection fraud in business settings.
- **Vendor and supply chain risk.** Local fintech, telecom, and outsourcing vendors face an active fraud ecosystem, and compromised vendor mailboxes are a common way to redirect payments. Require strong authentication and out-of-band verification of payment changes.

The TIDE team does not currently track actors that list Ghana among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile money fraud.** SIM-swap and fake-agent scams are widespread.
- **Romance and investment scams.** Local and foreign victims are targeted.
- **Phone theft.** Snatch theft occurs in Accra traffic.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Ghana.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Ghana Level 2, Exercise Increased Caution, citing crime, other, health. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A large fraud ecosystem, mobile-money scams, snatch theft in traffic, and invoice and payment-redirection fraud in business settings.
- **What would change this rating.** Lower to Level 1 as fraud and theft decline. Raise to Level 3 if northern security spillover reaches major cities.

Public Wi-Fi

- Ghana-based fraud networks targeting mobile-money and business email compromise, combined with SIM-swap attacks, create elevated risk for credentials and financial data on public networks; connect through a corporate VPN if public networks must be used.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Keep devices out of sight in traffic, and use hotel-arranged or app-based transport.
- Avoid the far north border areas flagged in the advisory.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

GREECE

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Athens

GOVERNMENT
Parliamentary republic

LANGUAGE
Greek

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued October 23, 2025)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable; exposure is tourist-area theft, hacktivism, and a past spyware scandal.

Country Overview

Greece is the birthplace of democracy and much of Western philosophy, and ancient Athens, Sparta, and Macedon shaped the classical world. Rome conquered the region, the Byzantine Empire preserved Greek culture, and the Ottomans ruled for roughly four centuries until the independence war that began in 1821.

The modern state expanded in the early twentieth century, suffered occupation in the Second World War and a civil war, and lived under a military junta from 1967 to 1974. Greece joined the EU in 1981 and the eurozone in 2001. A debt crisis from 2010 brought bailouts and austerity. The country has about 10.4 million people and a tourism and shipping economy. Kyriakos Mitsotakis has been prime minister since 2019.

Geopolitical Landscape

- **Turkey and the Aegean.** Greece and Turkey dispute maritime boundaries, airspace, and energy rights, and relations have alternated between tension and calm.
- **Cyprus.** Athens backs the Republic of Cyprus in the division dispute.
- **Migration.** Greece is a primary entry point into the EU for irregular arrivals by sea and land.
- **Domestic accountability.** The 2022 Predator spyware scandal continues to affect trust in institutions.

Cyber Threats | Organizations

- **Spyware and surveillance scandal.** Predator spyware was found on phones of politicians and journalists in 2022, and a February 2026 ruling convicted four people linked to Intellexa's Predator.
- **Ransomware.** Hospitals, municipalities, and companies are frequent victims.
- **Hacktivism.** Turkish- and pro-Russia-aligned hacktivists have targeted Greek sites around political events.
- **Shipping and tourism.** Maritime operators and hotels hold high-value data and face business email compromise and card fraud.
- **Employees based in country.** Employees face tourist-area pickpocketing and card fraud, and staff in shipping or energy roles may draw business email compromise attempts.
- **Vendor and supply chain risk.** Shipping agents, port services, and tourism platforms hold high-value data, and a vendor compromise can redirect payments. Verify payment-change requests out of band.

The TIDE team tracks 13 threat actors that list Greece among their targets. By attributed nexus, they break down as 5 cybercriminal, 4 China-nexus, 2 Turkey-nexus, 1 Russia-nexus, and 1 unattributed or other. The most frequently targeted sectors are government (9), technology (5), energy (4), education and research (4), and healthcare and pharmaceuticals (4). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, couriers, and public agencies are common in Greek.
- **Tourist scams.** Fake rental listings, overcharging, and card skimming target visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Greece.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Greece Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Greece is stable. Exposure is tourist-area theft and card fraud, hacktivism, and trust concerns left by the 2022 spyware scandal.
- **What would change this rating.** Raise to Level 2 if hostilities or hybrid activity with Turkey escalate or surveillance abuses recur.

Public Wi-Fi

- Ransomware affecting hospitals and government, spyware scandals targeting journalists and political figures, and business email compromise against maritime firms create a hostile environment for unprotected networks; use a corporate VPN if a public network is necessary.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Pickpocketing occurs at Athens transit hubs and tourist sites.
- Wildfires and strikes can disrupt travel in summer, so confirm itineraries.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

GRENADA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Saint George's

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued January 5, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk with ordinary tourist fraud and hurricane disruption.

Country Overview

Grenada is a three-island nation in the southeastern Caribbean known as the Spice Isle for its nutmeg and mace. France and Britain contested it, and Britain took control in 1763. It became independent in 1974.

A 1979 revolution brought Maurice Bishop's government to power, and a 1983 coup against Bishop was followed by a U.S.-led invasion. Democracy was restored. Grenada has about 109,000 people and an economy based on tourism and agriculture, and Hurricanes Ivan in 2004 and Beryl in 2024 caused severe damage. Dickon Mitchell has been prime minister since 2022.

Geopolitical Landscape

- **Climate vulnerability.** Hurricane risk shapes budgets and resilience planning.
- **Citizenship by investment.** Grenada runs a program that draws scrutiny from the United States and EU over vetting.
- **Regional integration.** Grenada belongs to CARICOM and the Organisation of Eastern Caribbean States.

Cyber Threats | Organizations

- **Tourism and small business.** Hotels and local firms face payment fraud and ransomware.
- **Investment migration providers.** Agents hold identity documents and financial records.
- **Limited security capacity.** Government depends on vendors and regional partners.
- **Employees based in country.** Employees face tourist-area fraud, opportunistic theft, and hurricane disruption. Investment-migration staff face tailored phishing.
- **Vendor and supply chain risk.** Small local vendors and regional cloud providers carry most exposure, and investment-migration agents hold identity files that warrant vetting.

The TIDE team does not currently track actors that list Grenada among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Tourist-targeted scams.** Fake rental and tour listings and card skimming target visitors.
- **Phishing in English.** Digicel and Flow (roughly 82 percent of internet subscriptions) provide mobile service; card fraud reports rose sharply in 2023, prompting the Royal Grenada Police Force to stand up dedicated cyber investigation units, and Grenada became the first English-speaking Caribbean country to join the Budapest Convention on Cybercrime.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Grenada.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Grenada Level 2, Exercise Increased Caution, citing crime. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk with ordinary tourist fraud and hurricane disruption.
- **What would change this rating.** Raise to Level 2 if a major breach hits investment-migration providers or fraud against visitors rises.

Public Wi-Fi

- Limited local security capacity and investment-migration agents handling sensitive identity documents mean public networks often lack protection against payment fraud and tailored phishing; connect through a corporate VPN if public networks must be used, particularly in tourist areas such as Grand Anse Beach and cruise-ship districts.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Hurricane season, June through November, can interrupt travel and connectivity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

GUATEMALA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 2

CAPITAL
Guatemala City

GOVERNMENT
Presidential republic

LANGUAGE
Spanish (with 24 recognized Mayan languages)

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued March 12, 2026)

Risk indicators: Crime, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Gang extortion using stolen data, express kidnapping, phone theft, and a State Department Level 3.

Country Overview

Guatemala was the heart of the Maya civilization, and its highlands remain home to a large indigenous population. Spain conquered the region in the 1520s, and Guatemala became independent in 1821. A 1954 coup backed by the United States overthrew an elected government, and a civil war from 1960 to 1996 killed an estimated 200,000 people, mostly indigenous Maya, before peace accords were signed.

Guatemala has about 18.3 million people and the largest economy in Central America, and it depends on agriculture, remittances, and manufacturing. Bernardo Arevalo took office in January 2024 after a contested transition in which prosecutors tried to block his inauguration.

Geopolitical Landscape

- **Rule of law contest.** Arevalo's anti-corruption agenda has met resistance from prosecutors and parts of the judiciary, and the country has faced repeated legal challenges to his government.
- **Gang violence.** Gangs such as Barrio 18 and MS-13 and drug trafficking groups drive violence, and authorities have repeatedly used states of exception.
- **Migration.** Guatemala is a transit and origin country for migration to the United States and cooperates with Washington on deportations.

- **Belize dispute.** Guatemala's territorial claim against Belize is before the International Court of Justice.

Cyber Threats | Organizations

- **Ransomware and fraud.** Banks, public bodies, and companies face ransomware and account takeover, and public incident reporting is limited.
- **Extortion.** Gangs extort businesses and transport operators, using stolen personal data and phone threats.
- **Public sector weaknesses.** Government systems have limited security capacity and have been breached.
- **Maquila and logistics.** Exporters and logistics firms face business email compromise.
- **Employees based in country.** Employees face extortion calls, phone theft on streets and buses, and express kidnapping risk. Managers and business owners are priority extortion targets.
- **Vendor and supply chain risk.** Logistics, security, and payment vendors can leak staff and route data to extortion gangs. Limit shared personal data, vet vendor staff, and monitor for insider-enabled extortion.

The TIDE team tracks 5 threat actors that list Guatemala among their targets. By attributed nexus, they break down as 2 China-nexus, 2 unattributed or other, and 1 cybercriminal. The most frequently targeted sectors are government (4), banking and financial services (2), diplomatic and foreign affairs (1), energy (1), and hospitality and travel (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Extortion calls and virtual kidnapping.** Callers claim to hold relatives and demand payment, often with data from breaches.
- **SIM swap and banking fraud.** Mobile and banking account takeover is common.
- **Phone theft.** Street and bus robberies target phones.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Guatemala.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Guatemala Level 3, Reconsider Travel, citing crime, terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Gangs use stolen personal data for extortion, express kidnapping and phone theft occur, and the State Department rates the country Level 3 for crime and terrorism.
- **What would change this rating.** Raise to Level 3 if extortion or violence against business travelers increases. Lower to Level 1 only on sustained declines in crime.

Public Wi-Fi

- Gang-based extortion operations exploiting stolen personal data and ransomware targeting public bodies create elevated risks of targeting and fraud on public networks, particularly for business managers; use a corporate VPN if a public network is necessary.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Use hotel-arranged or app-based transport, and avoid public buses and walking at night.
- Avoid areas flagged in the advisory, including parts of Guatemala City and border zones.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

GUINEA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Conakry

GOVERNMENT
Presidential republic (military-led transition)

LANGUAGE
French

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued February 25, 2026)

Risk indicators: Unrest, crime, health

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Military-led politics, social media and internet throttling during unrest, and mobile-money fraud.

Country Overview

Guinea is a West African country on the Atlantic coast that holds major bauxite and iron ore deposits. France colonized it, and Guinea became independent in 1958 under Ahmed Sekou Toure after voting to reject continued French ties. Lansana Conte ruled from a 1984 coup until his death in 2008, and a military coup followed.

Alpha Conde became the first elected president in 2010 and was overthrown in a September 2021 coup led by Colonel Mamady Doumbouya. In a September 2025 referendum, which the opposition boycotted, voters approved a new constitution that lifted the ban on junta members running, and Doumbouya won the December 28, 2025 presidential election with about 87 percent of the vote and a seven-year mandate. Guinea has about 17.5 million people. The Simandou iron ore project, one of the world's largest, was officially launched in November 2025.

Geopolitical Landscape

- **Military-led politics.** Doumbouya's win in the December 2025 election was widely expected, since opposition leaders Alpha Conde and Cellou Dalein Diallo are in exile and opposition figures rejected the official turnout figures. The junta restricted political parties and media during the transition and prosecuted opponents, and several critics have disappeared.

- **Simandou.** The Simandou project, backed by Chinese and Western interests, could transform the economy and draws strategic competition.
- **Regional position.** Guinea engages with both ECOWAS and the juntas of the Alliance of Sahel States.

Cyber Threats | Organizations

- **Mining and logistics.** Bauxite, alumina, and iron ore operators and rail and port builders hold high-value data and face espionage and fraud.
- **State control of connectivity.** Authorities have throttled social media and internet access during unrest.
- **Mobile money and banking.** Wallets and banks face SIM-swap and social engineering.
- **Limited local capacity.** Public bodies have few security resources.
- **Employees based in country.** Employees face possible social media and internet restrictions during unrest, mobile-money fraud, and political monitoring. Mining and logistics staff are higher-value targets.
- **Vendor and supply chain risk.** Mining, rail, and port contractors and state-linked telecoms hold sensitive data and operate under political pressure. Segment vendor access and limit locally stored data.

The TIDE team does not currently track actors that list Guinea among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Monitoring and arrest.** Opponents and journalists face surveillance and detention, and social media restrictions have been imposed.
- **Mobile fraud.** SMS and WhatsApp scams impersonate operators and banks.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Guinea.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Guinea Level 2, Exercise Increased Caution, citing unrest, crime, health. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** The military-led government restricts media, has throttled social media and internet access during unrest, and mobile-money fraud is common.
- **What would change this rating.** Raise to Level 3 if shutdowns or monitoring of dissent increase. Lower to Level 1 as political space reopens.

Public Wi-Fi

- Government control of connectivity, mobile-money fraud, and past internet throttling during unrest mean public networks are vulnerable to monitoring and credential theft; connect through a corporate VPN if public networks must be used.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations and political gatherings, and expect possible connectivity restrictions.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

GUINEA-BISSAU

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3

CAPITAL
Bissau

GOVERNMENT
Military-led transitional government

LANGUAGE
Portuguese (Kriol widely spoken)

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued December 11, 2025)

Risk indicators: Unrest, health, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Military seizure of power in November 2025, fragile institutions, illicit-finance exposure, and sudden disruption risk.

Country Overview

Guinea-Bissau is a small West African country on the Atlantic coast with a mainland and the Bijagos archipelago. Portugal ruled it as Portuguese Guinea until a liberation war led by Amilcar Cabral's PAIGC won independence in 1974. Political instability followed, including coups and a civil war in 1998 and 1999.

The country has about 1.9 million people, depends on cashew exports, and has served as a transit point for cocaine moving from Latin America to Europe. Presidential and legislative elections were held on November 23, 2025. On November 26, soldiers seized power while results were pending and arrested President Umaro Sissoco Embalo. General Horta N'Tam was sworn in on November 27 as transitional president for a planned one-year period.

Geopolitical Landscape

- **Military transition.** ECOWAS and the United Nations condemned the coup and called for a return to constitutional order. Elections have been scheduled for December 2026, and observers note that military transitions in the region have often been extended.

- **Drug trafficking.** Traffickers exploit weak institutions and the Bijagos islands, and some military figures have been accused of involvement.
- **Economic fragility.** Growth depends on cashew prices, and public services are thin.

Cyber Threats | Organizations

- **Minimal formal digital footprint.** A small banking and telecom sector depends on foreign parent firms and has limited local security capacity.
- **Political instability and connectivity.** Coups and unrest can bring sudden business closures and connectivity disruption.
- **Illicit finance exposure.** Drug-trafficking links create sanctions and anti-money-laundering risk for any financial counterparty.
- **Employees based in country.** Employees face sudden security-driven closures, limited connectivity and power, and monitoring during political tension. Mobile-money fraud is the main everyday cyber risk.
- **Vendor and supply chain risk.** A few banks and telecoms with foreign parents dominate. Vendors face sanctions and illicit-finance risk, so screen counterparties and keep sensitive data off local infrastructure.

The TIDE team does not currently track actors that list Guinea-Bissau among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile fraud.** Orange (roughly 58 percent share) and MTN provide mobile service; SMS and mobile money scams exist.
- **Monitoring during political tension.** Authorities and security forces may monitor communications and detain critics; the country has experienced repeated political crises, including an attempted coup in November 2023 and a military takeover in November 2025, during which the army moved to cut internet access.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Guinea-Bissau.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Guinea-Bissau Level 3, Reconsider Travel, citing unrest, health, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** The military seized power in November 2025 while election results were pending, institutions are fragile, drug-trafficking links create illicit-finance exposure, and sudden closures and connectivity disruption are possible.

- **What would change this rating.** Raise to Level 4 if fighting breaks out or detentions of foreigners occur. Lower to Level 2 if a credible civilian transition proceeds.

Public Wi-Fi

- Guinea-Bissau's first undersea fiber link, the ACE cable, reached the country in 2023, but connectivity outside Bissau remains minimal; political instability has produced both suspected government-linked outages, such as a four-hour Orange disruption in July 2024, and a deliberate internet cut attempted during the November 2025 coup. Use a corporate VPN if a public network must be used, and expect outages during periods of political tension.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid military sites, demonstrations, and areas near government buildings.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

GUYANA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 2

CAPITAL
Georgetown

GOVERNMENT
Presidential republic

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 26, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Venezuela border dispute, oil-sector targeting, and street crime; a State Department Level 3.

Country Overview

Guyana is the only English-speaking country in South America, with a rainforest interior and a populated Atlantic coast. The Dutch and then the British ruled it, and it became independent as a Commonwealth state in 1966 and a republic in 1970. Politics have long been divided between largely Afro-Guyanese and Indo-Guyanese communities.

The country has fewer than one million people. ExxonMobil's 2015 discovery in the Stabroek Block turned Guyana into a major oil producer and one of the world's fastest-growing economies. Irfaan Ali has been president since 2020, and his party won reelection on September 1, 2025, taking 36 of 65 seats, while the new We Invest in Nationhood party led by U.S.-sanctioned businessman Azruddin Mohamed became the main opposition with 16.

Geopolitical Landscape

- **Essequibo dispute.** Venezuela claims about two-thirds of Guyana's territory, the Essequibo region, and the case is before the International Court of Justice. Venezuela held a referendum on the claim in December 2023, and the dispute remains a security concern.

- **Oil wealth.** Rapid oil revenue brings governance and inflation challenges, and the country is a focus of U.S. and regional security cooperation.
- **Crime.** The State Department rates Guyana Level 3 for crime, citing violent crime and risks in some areas.

Cyber Threats | Organizations

- **Oil and gas sector.** Operators, contractors, and logistics firms hold sensitive production and financial data and face espionage, fraud, and ransomware risk.
- **Government and infrastructure.** Rapid digitization outpaces security capacity.
- **Financial sector.** Banks and mobile wallets face account takeover and card fraud.
- **Venezuela-related risk.** Border tension raises the risk of state-linked activity against Guyanese government and energy interests.
- **Employees based in country.** Employees face street crime and phone theft in Georgetown and phishing. Oil and gas staff are higher-value targets for elicitation and fraud.
- **Vendor and supply chain risk.** Rapid growth has pulled in many contractors and new vendors with uneven security. Require access controls, logging, and incident notification for vendors that touch oil and gas or financial systems.

The TIDE team does not currently track actors that list Guyana among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **State-linked phishing.** In February 2023, a suspected China-linked campaign (tracked as Operation Jacana) sent spear-phishing emails referencing Guyanese politics to government agencies, deploying a backdoor that let operators run commands and manipulate the Windows registry; researchers found the campaign's malware hosted on a compromised Vietnamese government server.
- **Phone theft and street crime.** Robbery and snatch theft occur in Georgetown.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Guyana.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Guyana Level 3, Reconsider Travel, citing crime. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** The Venezuela border dispute, oil-sector targeting, and street crime drive the rating, and the State Department rates the country Level 3 for crime.

- **What would change this rating.** Raise to Level 3 if tension with Venezuela escalates or state-linked activity against Guyanese energy interests increases. Lower to Level 1 as crime declines.

Public Wi-Fi

- Guyana's telecommunications rely on Digicel and GTT, with offshore-oil connectivity served by the Suriname-Guyana Submarine Cable System and the Deep Blue One cable; the documented state-linked espionage campaign against government networks, combined with Venezuela-related border tensions and the ExxonMobil-led offshore oil sector, creates elevated risk for corporate and government staff on public networks. Connect through a corporate VPN if public networks must be used.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Use hotel-arranged or app-based transport and avoid walking at night.
- Avoid the Venezuela border area flagged in the advisory.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

HAITI

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4

CAPITAL
Port-au-Prince

GOVERNMENT
Interim government led by a prime minister (the Transitional Presidential Council ended on February 7, 2026)

LANGUAGE
French and Haitian Creole

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued July 10, 2026)

Risk indicators: Unrest, crime, health, kidnapping or hostage-taking, terrorism

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Gang control of much of the capital, kidnapping, a political vacuum after February 2026, mass displacement, and no meaningful consular support.

Country Overview

Haiti occupies the western third of the island of Hispaniola. France colonized it as Saint-Domingue, the richest colony in the Caribbean, built on enslaved labor. A slave revolt that began in 1791 led to independence on January 1, 1804, making Haiti the first Black republic and the second independent nation in the Americas. France later forced Haiti to pay an indemnity for its independence, a burden that lasted well into the twentieth century.

The United States occupied Haiti from 1915 to 1934, and the Duvalier family dictatorship ruled from 1957 to 1986. Instability, coups, a devastating 2010 earthquake, and the July 2021 assassination of President Jovenel Moise followed. Haiti has about 11.9 million people and is the poorest country in the Western Hemisphere.

Geopolitical Landscape

- **Political vacuum.** The Transitional Presidential Council formed in April 2024 ended its mandate on February 7, 2026 without achieving its goals of restoring security and holding elections. Prime Minister Alix Didier Fils-Aime now governs largely by decree with U.S. support. Haiti has held no national election since 2016, and the electoral authority postponed the planned vote in October 2026 as gang violence prevents it.

- **Gang control.** Gangs control much of Port-au-Prince and large parts of the countryside, and more than 1.4 million people are displaced.
- **International security force.** A UN-backed Gang Suppression Force, authorized in September 2025 under Security Council Resolution 2793, is replacing the Kenya-led mission that never reached its planned strength.
- **Humanitarian crisis.** Hunger, disease, and the collapse of public services compound the security emergency.

Cyber Threats | Organizations

- **Minimal formal digital footprint.** Banks, telecommunications operators, remittance firms, and NGOs form most of the footprint, with unreliable power and connectivity and little local incident response.
- **Physical-safety consequences of data exposure.** Leaks of staff names, residences, routes, or beneficiary locations can enable kidnapping and extortion, so minimizing and protecting location data is critical.
- **Gang-controlled infrastructure.** Gangs control roads, ports, and some utilities, which disrupts logistics and creates extortion exposure for operators and vendors.
- **Financial sector.** Banks and mobile wallets face fraud and account takeover.
- **Employees based in country.** Employees face kidnapping, extortion, and severe connectivity and power disruption. Any exposure of names, locations, or movements can have life-safety consequences, so minimize stored personal data and avoid location-revealing apps.
- **Vendor and supply chain risk.** Logistics, security, telecom, and banking vendors operate under gang pressure and can leak staff or route data. Vet vendor personnel, limit shared location and contact data, and plan for sudden loss of vendor access.

The TIDE team does not currently track actors that list Haiti among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Kidnapping and extortion.** Kidnappings for ransom are widespread, and criminals use social media and phone data to target victims.
- **Connectivity disruption.** Power, fuel, and network outages are frequent.
- **Mobile-money fraud.** SMS and wallet scams are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Haiti.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Haiti Level 4, Do Not Travel, citing unrest, crime, health, kidnapping or hostage-taking, terrorism. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has very limited ability to assist in Haiti.

TIDE Risk Level Rationale

- **Drivers.** Gangs control much of the capital and major roads, kidnapping and extortion are widespread, the political authorities lack a mandate after February 2026, and the United States has very limited ability to assist. Exposure of names or locations can have life-safety consequences.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require sustained security gains from the Gang Suppression Force and a credible electoral path.

Public Wi-Fi

- Gang-controlled infrastructure and minimal local incident response capacity mean data exposure on public networks can have severe physical-safety consequences for staff; use a corporate VPN if a public network must be used.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

HONDURAS

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 2

CAPITAL
Tegucigalpa

GOVERNMENT
Presidential republic

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 25, 2026)

Risk indicators: Crime, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Extortion using stolen data, express kidnapping, phone theft, and limited local security capacity.

Country Overview

Honduras is a mountainous Central American country with coasts on the Caribbean and the Pacific. The Maya city of Copan flourished in its west, and Spain conquered the territory in the 1520s. Honduras became independent in 1821 and in the twentieth century was the archetypal banana republic, dominated by U.S. fruit companies.

A 2009 coup ousted President Manuel Zelaya, and Juan Orlando Hernandez, president from 2014 to 2022, was convicted in the United States of drug trafficking and pardoned by President Trump in late 2025. Xiomara Castro governed from 2022 to 2026. Nasry Asfura, a businessman endorsed by Trump, narrowly won the disputed November 30, 2025 election with about 40 percent of the vote and took office on January 27, 2026. Honduras has about 10.2 million people and relies on remittances, textiles, and agriculture.

Geopolitical Landscape

- **Gangs and security.** MS-13 and Barrio 18 and drug trafficking organizations drive violence, and a state of exception targeting gangs has been in force since December 2022.
- **New administration.** Asfura took office in January 2026, and he is expected to align more closely with the United States on security and migration.

- **Taiwan and China.** Honduras switched diplomatic recognition from Taiwan to the People's Republic in 2023.
- **Migration and remittances.** Honduras is a major origin and transit country for migration, and remittances are a large share of the economy.

Cyber Threats | Organizations

- **Ransomware and fraud.** Banks, public bodies, and companies face ransomware and account takeover, and public incident reporting is limited.
- **Extortion.** Gangs extort businesses and transport operators using stolen personal data.
- **Maquila and logistics.** Exporters face business email compromise and payment-redirection fraud.
- **Public sector weakness.** Government systems have limited security capacity.
- **Employees based in country.** Employees face extortion calls, phone theft, and express kidnapping risk. Managers and business owners are priority extortion targets.
- **Vendor and supply chain risk.** Logistics, security, and payment vendors can leak staff and route data to extortion gangs. Limit shared personal data, vet vendor staff, and verify payment-change requests out of band.

The TIDE team tracks 4 threat actors that list Honduras among their targets. By attributed nexus, they break down as 3 China-nexus, and 1 cybercriminal. The most frequently targeted sectors are government (2), banking and financial services (2), diplomatic and foreign affairs (1), energy (1), and hospitality and travel (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Extortion calls and virtual kidnapping.** Callers claim to hold relatives and demand payment.
- **SIM swap and banking fraud.** Mobile and bank account takeover is common.
- **Phone theft.** Street and bus robberies target phones.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Honduras.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Honduras Level 3, Reconsider Travel, citing crime, terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Gangs use stolen personal data for extortion, express kidnapping and phone theft occur, and local security capacity is limited. The State Department rates the country Level 3 for crime and terrorism.

- **What would change this rating.** Raise to Level 3 if extortion or violence against business travelers increases. Lower to Level 1 only on sustained declines in crime.

Public Wi-Fi

- Gang-based extortion networks exploiting stolen data and ransomware targeting public infrastructure create elevated targeting and fraud risks on public networks, especially for business owners and managers; connect through a corporate VPN if a public network is necessary.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Use hotel-arranged or app-based transport, and avoid public buses and walking at night.
- Avoid areas flagged in the advisory.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

HONG KONG

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 3



CAPITAL
None (seat of government in Central)

GOVERNMENT
Special Administrative Region of the People's Republic of China

LANGUAGE
Chinese (Cantonese) and English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 4, 2026)

Risk indicators: Other (arbitrary enforcement of local laws)

Note: The United States recognizes Hong Kong as part of the People's Republic of China but treats it separately for certain legal and trade purposes under U.S. law.

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: National security laws that allow compelled assistance and data access, expanding content controls, heavy state-linked targeting, and proximity to mainland rules.

Country Overview

Hong Kong sits on the southern coast of China at the mouth of the Pearl River. The Qing Empire ceded Hong Kong Island to Britain in 1842 after the First Opium War, Britain added Kowloon in 1860 and leased the New Territories for 99 years in 1898. Hong Kong grew into a global trading and financial center.

Britain returned Hong Kong to China on July 1, 1997 under the "one country, two systems" framework, which promised a high degree of autonomy. Mass protests in 2019 were followed by a National Security Law imposed by Beijing in 2020 and a locally enacted security law in 2024. Hong Kong has about 7.5 million people and remains a leading financial center.

Geopolitical Landscape

- **National security framework.** The 2020 National Security Law and the 2024 Safeguarding National Security Ordinance criminalize secession, subversion, terrorism, and collusion with foreign forces, and prosecutions have included prominent opposition figures and media tycoon Jimmy Lai.

- **Political changes.** Electoral rules adopted in 2021 limit candidates to those deemed patriotic, and the opposition has largely been removed from politics.
- **U.S. policy.** The United States ended Hong Kong's special treatment for export controls and other purposes in 2020 and has sanctioned officials.
- **Financial role.** Hong Kong remains a gateway for capital flows to and from mainland China, which draws sanctions and compliance scrutiny.

Cyber Threats | Organizations

- **National security powers over data.** Implementing rules under the security law allow police to require assistance, passwords, and data from people and organizations in certain cases, so organizations should assume authorities can compel access.
- **Open internet with growing controls.** Hong Kong does not use the mainland's Great Firewall, but content takedown and blocking powers have expanded.
- **State-linked targeting.** China-nexus groups target government, finance, media, and civil society.
- **Financial sector.** Banks and asset managers face business email compromise and deepfake fraud, including a 2024 case in which a Hong Kong employee transferred about 25 million dollars after a deepfake video call.
- **Employees based in country.** Employees face deepfake and impersonation fraud and national-security-law exposure for commentary on politics and protests. Anyone crossing into mainland China should apply the mainland China precautions.
- **Vendor and supply chain risk.** Local vendors, banks, and law and accounting firms can be compelled to provide data under national security rules, and staff may be subject to mainland data laws. Segment vendor access and review where sensitive data is stored.

The TIDE team tracks 34 threat actors that list Hong Kong among their targets. By attributed nexus, they break down as 22 China-nexus, 7 cybercriminal, 3 North Korea-nexus, and 2 Iran-nexus. The most frequently targeted sectors are government (20), education and research (13), technology (13), telecommunications (10), and defense and defense industrial base (8). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Online speech, posts, and group membership can bring national security prosecution.
- **Phishing and impersonation.** Messages impersonating banks and government are common, and WhatsApp and Telegram scams are widespread.
- **Deepfake and investment fraud.** Voice and video deepfakes and fake investment platforms are growing.
- **Border device checks.** Authorities and border officers can examine devices, and travel between Hong Kong and the mainland carries mainland rules.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Hong Kong.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Hong Kong Level 2, Exercise Increased Caution, citing arbitrary enforcement of local laws, including the national security law. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** National security laws allow authorities to compel assistance and data, content controls are expanding, China-linked actors target the territory, and mainland travel brings mainland rules. Typical visitors face moderate risk, so the rating reflects role-based exposure.
- **What would change this rating.** Raise to Level 4 if device inspections or detentions of foreign business travelers increase or Hong Kong is brought fully under mainland internet controls. Lower to Level 2 if compelled-access powers narrow.

Public Wi-Fi

- National security laws enabling compelled data access, China-nexus state-linked targeting, and recent deepfake fraud cases affecting financial staff create elevated risk on public networks; use a corporate VPN if a public network is necessary.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, finance, media, or civil-society roles, with encryption, phishing-resistant authentication, and remote wipe.
- Assume hotel and carrier networks can be observed, and avoid political commentary on social media during the trip.
- Apply the full mainland China policy to any onward travel to the mainland: no company devices, no company-linked accounts, and no log-ins to company infrastructure.

Local practices

- Carry minimal data, since border officials may examine devices.
- Be alert to deepfake and impersonation fraud involving payment requests, and verify them out of band.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

HUNGARY

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Budapest

GOVERNMENT
Parliamentary republic

LANGUAGE
Hungarian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued April 15, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: A stable EU member with a new government; residual concern from past spyware use and exposure to state-linked investment.

Country Overview

Hungary lies in the Carpathian Basin in Central Europe. The Magyars settled there in the late ninth century, and Stephen I was crowned the first king around the year 1000. Ottoman rule split the country in the sixteenth century, the Habsburgs took it back, and the Austro-Hungarian dual monarchy was formed in 1867.

The 1920 Treaty of Trianon stripped Hungary of about two-thirds of its territory, a trauma that still shapes politics. A communist regime took power after the Second World War, and the 1956 uprising was crushed by Soviet forces. Hungary joined NATO in 1999 and the EU in 2004. The country has about 9.6 million people.

Geopolitical Landscape

- **Change of government.** Peter Magyar's Tisza party defeated Viktor Orban's Fidesz in the April 12, 2026 election with about 53 percent of the vote and 141 of 199 seats, a two-thirds majority, ending Orban's 16 years in power. Turnout was a record near 79 percent, and Orban conceded.
- **EU relations and funds.** Tisza campaigned to restore the rule of law and unlock EU funds frozen under rule-of-law conditionality, and the new government is expected to improve relations with Brussels.
- **Russia and energy.** The new foreign minister has announced a gradual phase-out of ties with Russia, while acknowledging that Hungary cannot drop Russian fuel supplies quickly.

- **Ukraine.** Policy toward Ukraine was a campaign flashpoint, and Magyar denies the claim that he would drag Hungary into the war.

Cyber Threats | Organizations

- **State surveillance legacy.** Hungary was one of ten countries where the 2021 Pegasus Project found phone numbers selected for possible Pegasus targeting, including journalists. The new government's approach to surveillance and data access is still taking shape.
- **Ransomware and fraud.** Hospitals, municipalities, and companies are frequent ransomware victims, and business email compromise is common.
- **Foreign-linked investment and technology.** Large Chinese and Russian-linked investments, including in energy and batteries, create supply chain and state-access considerations.
- **Regulation.** Hungary implements NIS2 and the GDPR.
- **Employees based in country.** Employees face parcel and bank phishing and tourist-area overcharging and card fraud in Budapest. Staff in media or politically exposed roles should note the history of spyware targeting.
- **Vendor and supply chain risk.** Municipal, healthcare, and managed service providers are frequent ransomware victims, and foreign-linked energy and battery investors raise state-access questions. Require supplier attestations under NIS2 and review ownership.

The TIDE team tracks 9 threat actors that list Hungary among their targets. By attributed nexus, they break down as 5 China-nexus, 2 Russia-nexus, and 2 unattributed or other. The most frequently targeted sectors are government (7), civil society and activism (5), education and research (3), telecommunications (2), and diplomatic and foreign affairs (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Bank and parcel impersonation is common in Hungarian.
- **Tourist-area scams.** Overcharging and card fraud occur in Budapest nightlife areas.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Hungary.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Hungary Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Hungary is a stable EU member with a new government since April 2026. The rating reflects residual concern from past spyware use and state-linked investment, not risk to ordinary visitors.

- **What would change this rating.** Raise to Level 2 if surveillance abuses resurface or Russia-linked targeting of Hungarian networks escalates.

Public Wi-Fi

- Pegasus spyware targeting and ransomware affecting hospitals and public bodies, combined with large Russian and Chinese investments in critical infrastructure, create elevated surveillance and compromise risk on public networks; connect through a corporate VPN if public networks must be used.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Beware of overcharging at Budapest bars and taxis, and use licensed taxis or ride-hailing apps.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

ICELAND

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Reykjavik

GOVERNMENT
Parliamentary republic

LANGUAGE
Icelandic

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 5, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and low crime; exposure is concentrated in data centers and undersea cable dependence.

Country Overview

Iceland is a volcanic island in the North Atlantic settled by Norse and Celtic people from about 874. Its parliament, the Althing, was founded in 930 and is among the world's oldest. Iceland came under Norwegian and then Danish rule and became fully independent in 1944.

Iceland has about 400,000 people, no standing army, and a founding membership in NATO. The 2008 banking collapse caused a deep crisis followed by a strong recovery driven by tourism and fisheries, and geothermal and hydropower supply nearly all its energy. Volcanic eruptions on the Reykjanes peninsula since 2021 have repeatedly forced evacuations near Grindavik.

Geopolitical Landscape

- **Security cooperation.** Iceland relies on NATO and a bilateral defense agreement with the United States, and has increased attention to North Atlantic and undersea infrastructure security.
- **EU question.** The government has pledged a referendum on whether to resume EU accession talks, and the matter is under debate.
- **Volcanic risk.** Eruptions affect infrastructure, tourism, and the energy supply.

Cyber Threats | Organizations

- **Data centers and energy.** Iceland's cheap renewable power attracts data centers and cryptocurrency mining, which hold concentrated assets.
- **Undersea cables.** Iceland depends on a few subsea cables for connectivity, and damage would disrupt services.
- **Ransomware and fraud.** Small and midsize companies face phishing and business email compromise.
- **Regulation.** Iceland applies the GDPR and NIS-based rules through the EEA.
- **Employees based in country.** Employees face ordinary phishing and booking fraud. Staff at data centers and energy operators may draw targeted attempts.
- **Vendor and supply chain risk.** Data center operators and a small set of connectivity providers carry concentrated risk, and subsea cable damage could disrupt services. Review redundancy and incident notification terms.

The TIDE team tracks 1 threat actor that lists Iceland among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), hospitality and travel (1), and retail and e-commerce (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Bank and delivery impersonation circulates in Icelandic and English.
- **Tourist scams.** Fake rental listings and booking fraud target visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Iceland.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Iceland Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Iceland is stable and low crime. Exposure is concentrated in data centers and dependence on a few undersea cables.
- **What would change this rating.** Raise to Level 2 if cable sabotage or targeting of Icelandic infrastructure increases.

Public Wi-Fi

- Concentrated asset risk at data centers and energy operators, combined with dependency on a small number of submarine cables, means targeted attacks on public networks can disrupt critical infrastructure; use a corporate VPN if a public network must be used.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Check volcanic and weather alerts before travel, and carry offline maps for remote areas.

Return protocol

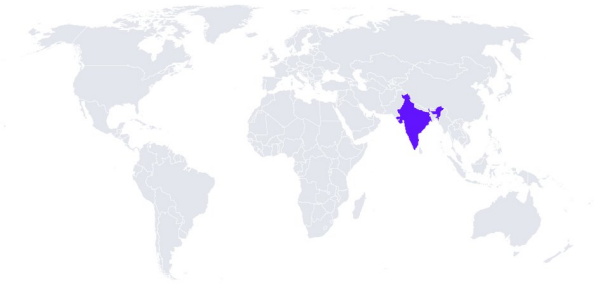
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

INDIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
New Delhi

GOVERNMENT
Federal parliamentary republic

LANGUAGE
Hindi and English (22 scheduled languages)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued June 16, 2025)

Risk indicators: Unrest, crime, terrorism, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Pervasive payment fraud, impersonation scams, regional internet shutdowns, and heavy targeting of IT and outsourcing providers.

Country Overview

India is home to one of the world's oldest civilizations, from the Indus Valley cities more than four thousand years ago through the Mauryan, Gupta, and Mughal empires. The British East India Company and then the British Crown ruled much of the subcontinent until independence on August 15, 1947, which came with the partition of British India into India and Pakistan and mass violence and displacement.

India adopted its constitution in 1950, liberalized its economy in 1991, and has become the world's most populous country, with about 1.43 billion people, and one of its fastest-growing large economies. Narendra Modi has been prime minister since 2014 and began a third term in June 2024 leading a BJP-led coalition.

Geopolitical Landscape

- **Pakistan.** After the April 2025 Pahalgam attack in Kashmir, which India attributed to Pakistan-based militants and which Pakistan denied any role in, India and Pakistan fought a four-day conflict in May 2025 involving missiles and drones before a ceasefire, and relations remain hostile.
- **China.** Relations improved after a 2024 border patrolling agreement, but the unresolved boundary and strategic rivalry persist.

- **United States.** U.S. tariffs on Indian goods and trade negotiations strained relations during 2025, and Washington and New Delhi continue to cooperate through the Quad and on defense.
- **Neighbors.** Ties with Bangladesh have been strained since 2024, and India shelters Sheikh Hasina.
- **Domestic politics.** Religious polarization and state-level tensions, including in Manipur, shape domestic security.

Cyber Threats | Organizations

- **Ransomware and data breaches.** A November 2022 attack on an Indian hospital cut off its networks and patient records for nearly two weeks, which illustrates persistent exposure. CERT-In rules require reporting of incidents within six hours.
- **State-linked espionage.** Pakistan-nexus and China-nexus actors target government, defense, energy, and telecoms, and many Indian organizations also support supply chains for foreign firms.
- **IT services and outsourcing.** Indian IT and BPO providers hold client data for organizations worldwide, so they are major supply chain nodes and targets.
- **Internet shutdowns.** Authorities regularly impose regional internet shutdowns, among the highest counts in the world, during unrest and exams.
- **Regulation.** The Digital Personal Data Protection Act of 2023 sets new duties for handling personal data.
- **Employees based in country.** Employees face UPI and impersonation fraud, phone theft in crowds, and regional internet shutdowns. Staff at IT and outsourcing firms handling client data face elevated phishing and insider-recruitment risk.
- **Vendor and supply chain risk.** Indian IT, BPO, and managed service providers are among the largest third-party concentrations in the world, so a vendor compromise can affect many clients at once. Require strong access controls, segmentation, logging, and incident notification, and verify subcontractor chains.

The TIDE team tracks 109 threat actors that list India among their targets. By attributed nexus, they break down as 47 cybercriminal, 32 China-nexus, 8 unattributed or other, 7 North Korea-nexus, 7 Iran-nexus, 3 Pakistan-nexus, 1 Russia-nexus, 1 India-nexus, 1 Lebanon-nexus, 1 Belarus-nexus, and 1 hacktivist. The most frequently targeted sectors are government (56), healthcare and pharmaceuticals (45), technology (44), banking and financial services (38), and industrial and manufacturing (36). These figures count actors, not incidents.

Cyber Threats | Individuals

- **UPI and payment fraud.** Fraud through the UPI payment system, fake customer-care numbers, and QR-code scams is widespread.
- **Digital arrest scams.** Scammers pose as police or officials on video calls and demand money.
- **Loan-app and investment fraud.** Predatory apps and fake trading platforms target users.
- **Phone theft.** Snatch theft occurs in crowded areas.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors that carry a public government attribution to India. Security vendors track several India-nexus espionage clusters whose targeting aligns with Indian strategic interests, but India does not acknowledge them, and the table below reflects vendor assessments.

GROUP	ALSO KNOWN AS	ATTRIBUTED SPONSOR	FOCUS	ACTIVE
SideWinder	Rattlesnake, Razor Tiger, APT-C-17	India-nexus; no government attribution	Espionage	2012 to 2025
Patchwork	Dropping Elephant, Quilted Tiger, APT-C-09	India-nexus; no government attribution	Espionage	2013 to 2026
Bitter	T-APT-17, APT-C-08, Hazy Tiger	India-nexus; no government attribution	Espionage	2013 to present
Donot Team	APT-C-35, Viceroy Tiger	India-nexus; no government attribution	Espionage	2016 to present
Confucius	APT-C-22	India-nexus; no government attribution	Espionage	2013 to present

Pakistan- and China-nexus actors target Indian organizations, and TIDE tracking lists those groups under the countries they are linked to.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates India Level 2, Exercise Increased Caution, citing unrest, crime, terrorism, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Payment and impersonation fraud is pervasive, regional internet shutdowns are frequent, and IT and outsourcing providers are heavily targeted. State surveillance of ordinary visitors is moderate.
- **What would change this rating.** Raise to Level 3 if conflict with Pakistan resumes or shutdowns and device inspections broaden. Lower to Level 1 as fraud declines.

Public Wi-Fi

- State-linked espionage from Pakistan and China, regular internet shutdowns, and ransomware affecting hospitals and government systems create elevated risk for corporate data on Indian public networks; connect through a corporate VPN if a public network must be used.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid the Kashmir border regions, Manipur, and other areas flagged in the advisory.
- Use hotel-arranged or app-based transport, and watch for fake taxi and customer-care scams.
- Expect regional internet shutdowns, and keep offline copies of key details.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

INDONESIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Jakarta

GOVERNMENT
Presidential republic

LANGUAGE
Indonesian

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 7, 2026)

Risk indicators: Unrest, natural disaster, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Major government and bank ransomware incidents, widespread payment and loan-app fraud, and protest and disaster disruption.

Country Overview

Indonesia is the world's largest archipelago, with more than 17,000 islands stretching between the Indian and Pacific oceans. The Srivijaya and Majapahit empires once dominated maritime trade, and the Dutch ruled most of the islands for centuries. Indonesia declared independence on August 17, 1945 and won international recognition in 1949.

Sukarno led the country until Suharto's authoritarian New Order from 1967 to 1998, after which democratic reform, called reformasi, began. Indonesia has about 288 million people, is the world's largest Muslim-majority country, and is a member of the G20. Prabowo Subianto became president in October 2024.

Geopolitical Landscape

- **2025 unrest.** Large protests and riots in August 2025 over lawmakers' perks and police conduct led to deaths and a cabinet reshuffle, and public frustration over living costs remains.
- **Foreign policy.** Indonesia joined BRICS in January 2025 while maintaining ties with the United States, China, and its neighbors.

- **Resources.** The government is pushing nickel processing and downstreaming, which draws Chinese investment and environmental concern.
- **Regional security.** Disputes in the South China Sea near the Natuna Islands and a long-running conflict in Papua remain concerns.

Cyber Threats | Organizations

- **Government ransomware.** In June 2024 a ransomware attack on the national data center disrupted immigration and other services across many agencies, and the incident exposed backup and governance failures.
- **Financial sector.** Bank Syariah Indonesia suffered a major ransomware attack in 2023, and banks and e-wallets face fraud and account takeover.
- **Online gambling and loan apps.** Illegal online gambling and predatory loan apps create fraud, money laundering, and insider risk.
- **Regulation.** The 2022 Personal Data Protection Law sets new duties, and the national cyber agency BSSN coordinates response.
- **Employees based in country.** Employees face courier and customer-care impersonation scams, snatch theft, and disruption from protests and natural disasters. Staff in banking and public-sector roles face elevated phishing.
- **Vendor and supply chain risk.** Government-run platforms and local fintech vendors have had major outages and breaches. Verify backup, recovery, and incident notification terms, and avoid concentrating data in a single national provider.

The TIDE team tracks 33 threat actors that list Indonesia among their targets. By attributed nexus, they break down as 18 China-nexus, 10 cybercriminal, 3 unattributed or other, 1 Lebanon-nexus, and 1 Iran-nexus. The most frequently targeted sectors are government (22), healthcare and pharmaceuticals (12), defense and defense industrial base (10), education and research (10), and banking and financial services (10). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Payment and impersonation fraud.** Fake courier messages, fake customer-care contacts, and QR-code scams are widespread.
- **Loan-app harassment.** Illegal loan apps harvest contacts and harass borrowers.
- **Phone theft.** Snatch theft occurs in Jakarta and tourist areas.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Indonesia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Indonesia Level 2, Exercise Increased Caution, citing unrest, natural disaster, terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Major ransomware incidents hit government and banks, payment and loan-app fraud is widespread, and protests and natural disasters can disrupt operations.
- **What would change this rating.** Raise to Level 3 if unrest returns with internet restrictions. Lower to Level 1 as fraud and theft decline.

Public Wi-Fi

- Ransomware affecting government and banking infrastructure, including a 2024 national data center attack, combined with predatory loan apps and financial sector fraud, create elevated risk on Indonesian public networks; use a corporate VPN if a public network is necessary.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, and monitor volcanic and earthquake alerts.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

IRAN

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Tehran

GOVERNMENT
Islamic republic

LANGUAGE
Persian

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued December 5, 2025)

Risk indicators: Unrest, kidnapping or hostage-taking, terrorism, wrongful detention, other

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Active war with the United States and Israel, pervasive state monitoring, wartime connectivity restrictions, wrongful detention of foreign and dual nationals, and severe sanctions.

Country Overview

Iran is the heir to Persia, one of history's great empires, which reached its height under the Achaemenids and later the Safavids, who made Twelver Shia Islam the state religion in the sixteenth century. The Qajar and Pahlavi dynasties modernized the state while facing foreign pressure, and a 1953 coup backed by the United States and Britain restored the shah.

The 1979 Islamic Revolution overthrew the shah and created a theocratic republic led by Ayatollah Ruhollah Khomeini, followed by the 1980 to 1988 war with Iraq. Iran has about 87.1 million people, large oil and gas reserves, and a nuclear program that has driven decades of sanctions and confrontation. Supreme Leader Ali Khamenei, in power since 1989, was killed in the opening strikes of the 2026 war. An interim Leadership Council assumed his constitutional duties, and the Assembly of Experts named his son, Mojtaba Khamenei, as the new Supreme Leader about a week later.

Geopolitical Landscape

- **2026 war with the United States and Israel.** The United States and Israel began strikes on Iran on February 28, 2026, killing Khamenei and many other officials. Iran retaliated with missiles and drones against Israel, U.S. bases, and Gulf states and disrupted shipping through the Strait of Hormuz.
- **Ceasefire and collapse.** A ceasefire took effect on April 7 and 8, Pakistan mediated talks, and the United States imposed a naval blockade. The two sides signed a memorandum on June 17, but it collapsed on July 8 after Iranian attacks on commercial vessels in the Strait of Hormuz and formally expired in August.
- **Continuing exchanges.** The United States struck Iranian targets on September 1 and Iran retaliated against U.S. sites in Jordan, Kuwait, Bahrain, and Iraq's Kurdistan region, according to Crisis Group. On October 8 President Trump said the United States would not resume strikes before the November 3 midterm elections.
- **Earlier conflict.** The war followed the Twelve-Day War of June 2025, in which U.S. strikes hit Iranian nuclear sites.
- **Sanctions.** U.S. and UN sanctions affect banking, energy, and technology, and the United States continues to add designations, including more than 30 in February 2026.

Cyber Threats | Organizations

- **Wartime state control of connectivity.** Authorities restrict the internet during war and unrest, filter foreign services heavily, and run a national information network. Plan for sudden loss of connectivity.
- **Compelled access and monitoring.** Foreign organizations should assume the state can monitor and compel access to data and communications.
- **Cyber conflict.** Israel-linked groups attacked Iranian institutions such as Bank Sepah and the Nobitex exchange in June 2025, and Iran-nexus actors target Israeli, U.S., Gulf, and critical-infrastructure systems, including industrial controllers.
- **Sanctions exposure.** Almost any commercial relationship with Iran carries severe U.S. and EU sanctions risk.
- **Regional supply chain risk.** Vendors with Gulf or Iraq operations may be affected by Iranian retaliation and by hacktivism.
- **Employees based in country.** Staff should assume all communications and devices are monitored, expect wartime connectivity restrictions, and recognize that foreign and dual nationals face a high risk of detention. Remove all company access from personal devices before any entry.
- **Vendor and supply chain risk.** Any vendor or contractor connected to Iran creates severe sanctions exposure and state-access risk, and vendors in neighboring states can be disrupted by Iranian retaliation. Remove Iran-based vendors, screen supply chains, and segment regional vendor access.

The TIDE team tracks 21 threat actors that list Iran among their targets. By attributed nexus, they break down as 14 Iran-nexus, 4 unattributed or other, 2 China-nexus, and 1 hacktivist. The most frequently targeted sectors are government (14), civil society and activism (8), energy (7), diplomatic and foreign affairs (4), and telecommunications (4). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Pervasive monitoring.** Authorities monitor communications, inspect phones, and arrest people for online activity, including contact with foreigners.
- **Wrongful detention.** Foreign nationals and dual nationals have been detained as leverage, and state media has aired confessions.
- **VPN and platform restrictions.** Most Western platforms are blocked, and VPN use is common but monitored.

State-Sponsored Cyber Threats

Iran conducts state cyber operations through the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS), supported by contractors. The groups below carry public government or vendor attribution.

GROUP	ALSO KNOWN AS	ATTRIBUTED SPONSOR	FOCUS	ACTIVE
APT33	Elfin, Magnallium, Refined Kitten, Holmium	IRGC	Espionage and disruption	2013 to 2025
APT34 (OilRig)	Helix Kitten, Chrysene, Hazel Sandstorm	Ministry of Intelligence and Security (MOIS)	Espionage	2014 to 2025
APT42	TA453, Mint Sandstorm, Charming Kitten	IRGC Intelligence Organization	Espionage and credential phishing	2015 to 2026
MuddyWater	Static Kitten, Seedworm, Mango Sandstorm	MOIS	Espionage	2017 to 2026
Imperial Kitten	Tortoiseshell, TA456, Crimson Sandstorm	IRGC	Espionage	2017 to present
CyberAv3ngers	Cyber Toufan, Agonizing Serpens	IRGC Cyber-Electronic Command	Attacks on industrial control systems and influence	2020 to 2026
Agrius	BlackShadow, Pink Sandstorm	MOIS	Destructive attacks and hack-and-leak	2020 to 2025
Scarred Manticore	Storm-0861, Void Manticore, Homeland Justice	MOIS	Espionage and destructive operations (including the 2022 Albania attack)	2019 to present
Fox Kitten	Pioneer Kitten, Parisite, UNC757	Iran-based government-affiliated contractor	Espionage and initial access brokering	2017 to present

Dozens of additional Iran-nexus clusters are tracked under differing names, and some overlap. Scarred Manticore and Homeland Justice share the Void Manticore designation in vendor reporting. This list excludes U.S. agencies by design.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Iran Level 4, Do Not Travel, citing unrest, kidnapping or hostage-taking, terrorism, and wrongful detention. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The United States has no embassy in Iran.

TIDE Risk Level Rationale

- **Drivers.** The country is in an unresolved war with the United States and Israel, authorities monitor communications and restrict connectivity in wartime, foreign and dual nationals face a high risk of detention, and severe sanctions apply.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable end to hostilities, release of detained foreign nationals, and an end to wartime restrictions, none of which is in sight.

Public Wi-Fi

- VPN use is restricted or blocked in Iran; do not use public Wi-Fi at all. Authorities restrict the internet during war and unrest, filter foreign services heavily, and run a national information network, making any public network inherently compromised. Use only approved devices and connectivity plans.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications from personal devices before travel, and do not access company or vendor infrastructure.
- Block sign-ins from Iran with geo-based conditional access, and alert on every attempt.
- The TIDE team does not recommend business travel to Iran. U.S. citizens face a severe risk of detention, and U.S. sanctions apply.

Connectivity and communications

- Expect nationwide connectivity restrictions and blocked services, and assume communications are monitored.

Legal exposure

- Involve counsel on sanctions and export controls before any engagement, and prepare a family and employer contact plan.

Return protocol

- Treat any device that traveled as untrusted, wipe it, rotate credentials from a trusted network, and hold a debrief.

WORLDBOOK

IRAQ

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Baghdad

GOVERNMENT
Federal parliamentary republic

LANGUAGE
Arabic and Kurdish

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued August 29, 2026)

Risk indicators: Unrest, kidnapping or hostage-taking, terrorism, other, crime, health

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Spillover from the Iran war, militia and state surveillance, recurring shutdowns, kidnapping risk, and a U.S. Level 4 advisory.

Country Overview

Iraq occupies ancient Mesopotamia, where Sumer, Babylon, and Assyria produced some of humanity's earliest writing, law, and cities. Baghdad became the capital of the Abbasid Caliphate in the eighth century. The Ottomans ruled for centuries before Britain took control after the First World War, and the monarchy that followed fell in a 1958 coup.

The Baath Party and Saddam Hussein ruled from 1968 to 2003, with wars against Iran and Kuwait and international sanctions. A 2003 U.S.-led invasion toppled Saddam and was followed by insurgency and sectarian conflict, and the Islamic State seized a third of the country in 2014 before being defeated in 2017. Iraq has about 46 million people and depends on oil for most government revenue.

Geopolitical Landscape

- **Iran war spillover.** Iraq sits between the United States and Iran. Iranian forces struck U.S. sites in Iraq's Kurdistan region in September 2026, according to Crisis Group, and Iran-aligned militias in the Popular Mobilization Forces operate inside the state.

- **Government formation.** Iraq held parliamentary elections on November 11, 2025, in which outgoing prime minister Mohammed Shia al-Sudani's coalition won the most seats, 46 of 329. After months of deadlock, including a January 2026 nomination of Nouri al-Maliki that President Trump publicly opposed, parliament elected Nizar Amedi as president on April 11, 2026 and approved a new government led by Ali al-Zaidi, a little-known businessman, about six months after the vote. Several key ministries remained unfilled amid disagreements between Tehran and Washington.
- **Kurdistan.** The Kurdistan Regional Government governs the north with its own security forces and relies on Baghdad for budget payments.
- **Militants.** Islamic State remnants remain active in rural areas.

Cyber Threats | Organizations

- **Connectivity shutdowns.** Authorities cut internet access during national exams and unrest, and the practice recurs yearly.
- **State and militia surveillance.** Security services and militias can monitor communications, and foreign organizations should assume state access to data.
- **Energy sector.** Oil and gas operators and contractors are targets for espionage, disruption, and physical attack.
- **Iran-linked targeting.** Iran-nexus actors target Iraqi government and regional networks, and Iraq is also a conduit for operations against Gulf and Western targets.
- **Employees based in country.** Staff should expect connectivity shutdowns, assume monitoring by state and militia actors, and recognize kidnapping and political violence risk. Remove company access from personal devices and keep location data minimal.
- **Vendor and supply chain risk.** Local telecom, security, and logistics vendors operate under political and militia pressure and can be compelled to share data. Segment vendor access, vet ownership, and plan for sudden disruption.

The TIDE team tracks 15 threat actors that list Iraq among their targets. By attributed nexus, they break down as 11 Iran-nexus, 3 unattributed or other, and 1 Turkey-nexus. The most frequently targeted sectors are government (13), telecommunications (9), energy (3), defense and defense industrial base (3), and civil society and activism (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and arrest.** Online criticism of the government, militias, or religious figures can bring arrest or violence.
- **Kidnapping and extortion.** Kidnapping for ransom and political reasons occurs.
- **Mobile fraud.** SMS and wallet scams are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Iraq.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Iraq Level 4, Do Not Travel, citing unrest, kidnapping or hostage-taking, terrorism, other, crime, health. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has limited ability to assist and the advisory warns of terrorism, kidnapping, and armed conflict.

TIDE Risk Level Rationale

- **Drivers.** Spillover from the Iran war, militia and state surveillance, recurring shutdowns, kidnapping risk, and a U.S. Level 4 advisory drive the rating.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require durable de-escalation with Iran and improved security.

Public Wi-Fi

- Public Wi-Fi in Iraq is subject to state and militia surveillance and periodic shutdowns during unrest. Assume hotel and carrier networks are monitored; avoid public networks entirely and route all traffic through a corporate VPN if travel is authorized.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

IRELAND

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Dublin

GOVERNMENT
Parliamentary republic

LANGUAGE
Irish and English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued March 20, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; exposure is ransomware, phishing, and targeting of multinational technology and pharmaceutical firms.

Country Overview

Ireland is an island nation in the North Atlantic whose Celtic culture was shaped by Viking and Norman invasions. English and later British rule from the twelfth century produced conflict, famine, and emigration, including the Great Famine of the 1840s. The 1916 Easter Rising and a war of independence led to the creation of the Irish Free State in 1922, and Ireland became a republic in 1949.

Ireland joined the European Community in 1973, built a global technology and pharmaceutical hub, and suffered a banking crisis in 2008. The Republic has about 5.5 million people. Micheal Martin became Taoiseach in January 2025, and Catherine Connolly became president in November 2025.

Geopolitical Landscape

- **Trade and tariffs.** Ireland's economy depends on U.S. multinationals in technology and pharmaceuticals, which makes U.S. tariff policy and tax changes a major risk.
- **Neutrality.** Ireland maintains military neutrality outside NATO while supporting Ukraine, and it has debated defense and cable-security spending.
- **Northern Ireland and Brexit.** The border with Northern Ireland and post-Brexit arrangements remain a political focus.

- **Housing and data centers.** Housing shortages and data center energy use dominate domestic debate.

Cyber Threats | Organizations

- **Ransomware and healthcare.** A 2021 Conti ransomware attack on the Health Service Executive disrupted hospitals nationwide for months and remains a defining case.
- **Technology and pharma hub.** Multinational data centers and European headquarters hold vast data and intellectual property, drawing state-linked espionage and ransomware.
- **Undersea cables.** Ireland hosts landing points for transatlantic cables, which makes cable security a national priority.
- **Regulation.** The Data Protection Commission leads GDPR enforcement for many global platforms, and Ireland implements NIS2.
- **Employees based in country.** Employees face bank and delivery phishing and opportunistic theft in Dublin. Staff at technology, pharmaceutical, and data center firms may draw targeted state-linked and criminal attention.
- **Vendor and supply chain risk.** Cloud, data center, and managed service providers concentrated in Ireland are high-value third parties. Require supplier attestations under NIS2 and test continuity plans.

The TIDE team tracks 11 threat actors that list Ireland among their targets. By attributed nexus, they break down as 9 cybercriminal, and 2 unattributed or other. The most frequently targeted sectors are healthcare and pharmaceuticals (9), education and research (7), industrial and manufacturing (7), government (6), and banking and financial services (6). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, Revenue, and delivery services are common.
- **Fraud and scams.** Investment scams and fake marketplace listings are widespread.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Ireland.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Ireland Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Ireland is stable and well-regulated. Exposure is ransomware, phishing, and state-linked and criminal targeting of multinational technology and pharmaceutical firms.
- **What would change this rating.** Raise to Level 2 if undersea cable sabotage or large attacks on Irish infrastructure occur.

Public Wi-Fi

- While Ireland is stable, ransomware and state-linked targeting of technology firms remain concerns. Apply standard protections: use full-disk encryption, multi-factor authentication, and a corporate VPN for any public network access.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Opportunistic theft occurs in central Dublin, so secure phones and bags.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

ISRAEL

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3

CAPITAL
Jerusalem (the United States recognizes Jerusalem as Israel's capital, and its status is disputed internationally)

GOVERNMENT
Parliamentary republic

LANGUAGE
Hebrew and Arabic

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 26, 2026)

Risk indicators: Unrest, terrorism

Note: The State Department issues separate advisories for Israel, the West Bank, and Gaza. The West Bank and Gaza will appear in their own profile.

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Active conflict with Iran and Hezbollah, Iran-linked phishing and influence operations, GPS interference, and wartime disruption.

Country Overview

Israel lies on the eastern Mediterranean and sits in a land with deep significance for Judaism, Christianity, and Islam. The Zionist movement of the late nineteenth century encouraged Jewish immigration to Ottoman and then British-ruled Palestine. After the Holocaust and a 1947 UN partition plan, Israel declared independence on May 14, 1948 and fought the first Arab-Israeli war.

Israel captured the West Bank, Gaza, the Sinai, and the Golan Heights in 1967, signed peace treaties with Egypt in 1979 and Jordan in 1994, and normalized relations with several Arab states under the 2020 Abraham Accords. Israel has about 10.3 million people and a leading technology and defense sector. Benjamin Netanyahu is in his longest period as prime minister.

Geopolitical Landscape

- **Election on October 27, 2026.** Israel votes on October 27, the latest date allowed by law, in the first national election since the October 7, 2023 attack. Netanyahu, 76, is seeking reelection against challengers including

former army chief Gadi Eisenkot, and Naftali Bennett and Yair Lapid merged their parties in April 2026. Accountability for October 7 and security policy dominate the campaign.

- **War with Iran.** Israel joined the United States in striking Iran on February 28, 2026. Iranian attacks killed about 20 Israeli civilians before the April 7 ceasefire, according to the Congressional Research Service. The ceasefire between the United States and Iran later collapsed, and tension continues.
- **Lebanon.** Israel has been in direct conflict with Hezbollah again since March 2026.
- **Gaza.** A ceasefire took effect in October 2025 and the living hostages were released, but Israel holds a zone behind the so-called Yellow Line that covers nearly 65 percent of Gaza, and the ceasefire framework remains fragile.
- **Diplomatic isolation.** Israel faces growing international criticism and partial diplomatic isolation.

Cyber Threats | Organizations

- **Iran-linked cyber operations.** Iran-nexus groups target Israeli government, defense, water, energy, and technology organizations, and hacktivist personas have run hack-and-leak and disruptive campaigns.
- **GPS interference.** Widespread GPS jamming and spoofing in the region affects aviation, shipping, and navigation apps.
- **Technology and supply chain.** Israeli cybersecurity, defense, and software firms are high-value suppliers for global customers and are therefore priority targets for state-linked actors.
- **Wartime disruption.** Missile alerts and mobilization disrupt operations and staffing.
- **Spyware sector.** Israel hosts a commercial spyware industry that has drawn sanctions and scrutiny.
- **Employees based in country.** Employees face Iran-linked phishing and fake-alert messages, GPS interference, and operational disruption from missile alerts. Staff in government, defense, technology, and media roles are priority targets.
- **Vendor and supply chain risk.** Israeli technology and cybersecurity vendors are priority targets and may face wartime staffing and availability disruption. Review continuity plans, verify software update integrity, and segment vendor access to sensitive environments.

The TIDE team tracks 55 threat actors that list Israel among their targets. By attributed nexus, they break down as 25 Iran-nexus, 15 cybercriminal, 6 China-nexus, 4 unattributed or other, 2 hacktivist, 1 Lebanon-nexus, 1 North Korea-nexus, and 1 Russia-nexus. The most frequently targeted sectors are government (40), industrial and manufacturing (19), energy (18), technology (18), and healthcare and pharmaceuticals (17). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Targeted phishing and influence.** Iran-linked actors run fake-persona campaigns and phishing against officials, researchers, and journalists, and impersonate recruiters and alerts.
- **Alert-app spoofing.** Fake missile-alert and news messages circulate during conflict.
- **Fraud.** Bank and delivery impersonation and investment scams are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Israel.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Israel Level 3, Reconsider Travel, citing unrest, terrorism. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Israel is in active conflict with Iran and Hezbollah, Iran-linked actors run phishing and influence campaigns, GPS interference is widespread, and missile alerts disrupt operations. The State Department rates Israel Level 3.
- **What would change this rating.** Raise to Level 4 if large-scale missile attacks resume or the conflict widens significantly. Lower to Level 2 if the Iran and Lebanon fronts quiet and election tensions pass.

Public Wi-Fi

- Hotel and carrier networks are monitored during active conflict with Iran and Hezbollah; GPS interference is widespread and alert-app spoofing occurs. Assume public networks are compromised and use a corporate VPN, and avoid public USB charging.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Follow Home Front Command alerts, and expect GPS interference and sudden airspace closures.
- Avoid areas flagged in the advisory, including near Gaza, the Lebanese and Syrian borders, and parts of the West Bank.

Return protocol

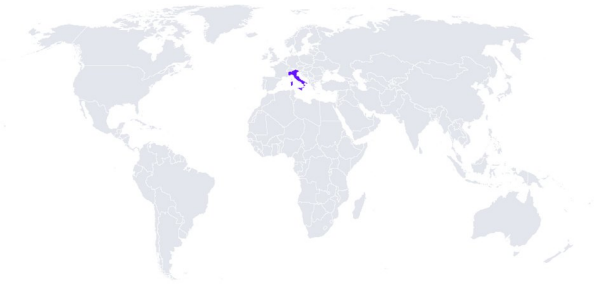
- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

ITALY

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Rome

GOVERNMENT
Parliamentary republic

LANGUAGE
Italian

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 10, 2026)

Risk indicators: Terrorism

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable; exposure is ransomware, hacktivism, tourist-area theft, and a 2025 spyware affair.

Country Overview

Italy was the heart of the Roman Republic and Empire, and its city-states, including Florence, Venice, and Genoa, drove the Renaissance. The peninsula was politically fragmented until unification in 1861 under the Kingdom of Sardinia. Benito Mussolini's fascist regime ruled from 1922 to 1943, and Italy became a republic by referendum in 1946.

Italy is a founding member of the EU and NATO, has about 59 million people, and has the third-largest economy in the eurozone, with strong manufacturing, fashion, and tourism sectors. Giorgia Meloni has been prime minister since October 2022, leading one of the country's longest-serving postwar governments.

Geopolitical Landscape

- **Stable government.** Meloni's coalition has been unusually durable, with a general election due by 2027.
- **Ukraine and defense.** Italy supports Ukraine and NATO while balancing energy and economic interests.
- **Migration.** Italy is a main arrival point for Mediterranean migration and has agreements with Albania and Libya.
- **Fiscal position.** High public debt remains a constraint.

Cyber Threats | Organizations

- **Ransomware.** Hospitals, municipalities, and manufacturers are frequent victims of ransomware.
- **Pro-Russia hacktivism.** DDoS campaigns by groups such as NoName057(16) target Italian government, transport, and financial sites, especially around political decisions on Ukraine.
- **Spyware affair.** In 2025 Paragon's Graphite spyware was found on devices of a journalist and activists in Italy, the government acknowledged targeting two activists, and Paragon ended its Italian contracts.
- **Industrial base.** Small and midsize manufacturers and design firms face intellectual property theft and supply chain compromise.
- **Regulation.** Italy's national cybersecurity agency ACN coordinates response, and Italy implements NIS2.
- **Employees based in country.** Employees face pickpocketing on transit and in tourist areas, bank and postal phishing, and rental fraud. Staff at manufacturers and design firms face intellectual property targeting.
- **Vendor and supply chain risk.** Small and midsize suppliers and managed service providers are common entry points for ransomware and IP theft. NIS2 broadens supplier obligations, so require attestations and incident notification.

The TIDE team tracks 53 threat actors that list Italy among their targets. By attributed nexus, they break down as 34 cybercriminal, 6 China-nexus, 4 Iran-nexus, 3 Russia-nexus, 3 unattributed or other, 2 hacktivist, and 1 Turkey-nexus. The most frequently targeted sectors are healthcare and pharmaceuticals (33), government (32), industrial and manufacturing (25), education and research (23), and technology (19). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, postal services, and tax authorities are widespread.
- **Tourist scams.** Pickpocketing, fake rental listings, and card fraud target visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Italy.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Italy Level 2, Exercise Increased Caution, citing terrorism. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Italy is stable. Exposure is ransomware, hacktivism, tourist-area theft, and trust issues from the 2025 spyware affair.
- **What would change this rating.** Raise to Level 2 if hacktivist or state-linked attacks begin to disrupt transport or health services.

Public Wi-Fi

- Ransomware and hacktivism target Italian infrastructure, and the 2025 spyware affair exposed trust issues in security practices. Public Wi-Fi in tourist areas like Rome and Venice carries pickpocketing risk and network eavesdropping; use a corporate VPN if access is unavoidable.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Pickpocketing is common in Rome, Florence, Venice, and Naples, especially on public transport and at tourist sites.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

JAMAICA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Kingston

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English (Jamaican Patois widely spoken)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued June 23, 2026)

Risk indicators: Crime, health, natural disaster

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Call-center fraud ecosystem, phone theft, high violent crime, and hurricane disruption.

Country Overview

Jamaica is a mountainous Caribbean island south of Cuba. The Taino people lived there before Spain's arrival in 1494, and Britain took control in 1655 and built a sugar economy on enslaved African labor. Jamaica became independent in 1962 and is a Commonwealth realm.

The country has about 2.8 million people and an economy based on tourism, remittances, bauxite, and services. Andrew Holness has been prime minister since 2016, and his party won a third term in September 2025. Hurricane Melissa struck Jamaica in October 2025 and caused catastrophic damage.

Geopolitical Landscape

- **Hurricane recovery.** Recovery from Hurricane Melissa and climate resilience dominate economic and political planning.
- **Violent crime.** Gang violence has given Jamaica one of the Caribbean's highest homicide rates, and authorities periodically declare states of emergency in affected areas.
- **Regional role.** Jamaica is a CARICOM member, a leader in Caribbean debates on reparations, and a participant in efforts to support Haiti.

Cyber Threats | Organizations

- **Lottery and impersonation scams.** Jamaica hosts organized call-center fraud networks that target victims abroad, which creates insider and mule-account risk for local banks, telecoms, and call-center vendors.
- **Public-sector incidents.** Government bodies have suffered ransomware and data breaches, and security capacity is limited.
- **Tourism sector.** Resorts and airlines hold payment and passport data and face card fraud and ransomware.
- **Financial sector.** Banks and mobile wallets face account takeover.
- **Employees based in country.** Employees face tourist-area card fraud, phone theft, and hurricane disruption. Staff at call centers and outsourcing firms face insider-recruitment and social engineering pressure.
- **Vendor and supply chain risk.** Call-center and outsourcing vendors hold customer data and sit next to an active fraud ecosystem. Require strong access controls, monitoring, and incident notification.

The TIDE team tracks 2 threat actors that list Jamaica among their targets. By attributed nexus, they break down as 1 cybercriminal, and 1 unattributed or other. The most frequently targeted sectors are government (2), banking and financial services (1), construction and engineering (1), healthcare and pharmaceuticals (1), and industrial and manufacturing (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Tourist-targeted fraud.** Fake rental listings and card skimming target visitors.
- **Impersonation scams.** Callers and messages impersonating banks and officials are common.
- **Phone theft.** Opportunistic theft occurs in tourist areas and in Kingston.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Jamaica.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Jamaica Level 2, Exercise Increased Caution, citing crime, health, natural disaster. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** An organized call-center fraud ecosystem, phone theft, high violent crime, and hurricane disruption drive the rating. State surveillance of visitors is limited.
- **What would change this rating.** Raise to Level 3 if violence or fraud directed at travelers increases or a major breach hits government or banks. Lower to Level 1 as crime declines.

Public Wi-Fi

- An organized call-center fraud ecosystem operates locally, and phone theft is common in tourist areas and Kingston. Public hotel and airport networks can be compromised by insider fraud; connect through a corporate VPN and enable remote wipe.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid areas flagged in the advisory, and use hotel-arranged transport at night.
- Hurricane season, June through November, can disrupt travel and connectivity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

JAPAN

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Tokyo

GOVERNMENT
Parliamentary constitutional monarchy

LANGUAGE
Japanese

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 15, 2025)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; exposure is smishing, credential theft, ransomware against suppliers, and state-linked targeting of sensitive sectors.

Country Overview

Japan is an island nation off the east coast of Asia with a continuous imperial institution that dates back more than a millennium. Shogun-led feudal rule lasted from the twelfth century until the Meiji Restoration of 1868, which launched rapid modernization. Japan built an empire in the early twentieth century and was defeated in the Second World War in 1945.

Postwar Japan adopted a pacifist constitution, grew into one of the world's largest economies, and became a close U.S. ally. It has about 123 million people and an aging population. Sanae Takaichi became the first woman prime minister in October 2025, and her Liberal Democratic Party won a landslide in a snap election on February 8, 2026.

Geopolitical Landscape

- **Takaichi government.** The LDP won 316 of 465 seats on February 8, 2026, the first two-thirds majority for the party in the postwar era, and Takaichi was reappointed on February 18. She has pledged to strengthen defense, create a national intelligence agency, and move toward an anti-espionage law.

- **Tension with China.** After Takaichi said in November 2025 that a Chinese attack on Taiwan could be an existential threat to Japan, Beijing responded with restrictions on seafood imports and exports of dual-use items including critical minerals.
- **Alliance and defense.** Japan is raising defense spending and deepening cooperation with the United States and partners such as the Philippines and Australia.
- **Regional threats.** North Korean missile launches and Russian military activity near Japan are continuing concerns.

Cyber Threats | Organizations

- **State-linked espionage.** Japanese authorities have attributed long-running campaigns, including MirrorFace activity, to China-linked actors, and defense, technology, and research organizations are priority targets.
- **Ransomware and supply chain.** Major incidents have hit large companies, including the September 2025 ransomware attack on Asahi Group Holdings, which Qilin claimed and which halted production at most of its domestic factories. Japan's space agency also disclosed attacks on its networks in 2023.
- **DDoS and hacktivism.** Pro-Russia and other groups have attacked airlines, banks, and government sites.
- **Policy.** Confirm current incident reporting and data handling obligations with local counsel before relying on assumptions from other jurisdictions.
- **Employees based in country.** Employees face SMS and delivery impersonation, credential phishing, and shoulder-surfing and device-loss risk in crowded transit. Staff in manufacturing, defense, and technology may draw state-linked targeting.
- **Vendor and supply chain risk.** Subcontractors, parts suppliers, and managed service providers are the main route into large Japanese manufacturers, and the Asahi incident showed how disruption spreads. Require supplier attestations, segmentation, and incident notification.

The TIDE team tracks 112 threat actors that list Japan among their targets. By attributed nexus, they break down as 51 China-nexus, 44 cybercriminal, 10 North Korea-nexus, 4 unattributed or other, 1 Lebanon-nexus, 1 Iran-nexus, and 1 hacktivist. The most frequently targeted sectors are government (58), technology (54), healthcare and pharmaceuticals (46), industrial and manufacturing (41), and defense and defense industrial base (38). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Smishing and impersonation.** SMS messages impersonating delivery firms, banks, and utilities are very common.
- **Account takeover and crypto theft.** Credential theft targets online banking and exchanges, and North Korea-linked actors have stolen cryptocurrency from Japanese exchanges.
- **Fake support scams.** Pop-up tech support and fake invoice scams target residents and visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Japan.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Japan Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Japan is stable and well-regulated. Exposure is smishing, credential theft, ransomware against suppliers, and state-linked targeting of defense and technology staff, which is role-based.
- **What would change this rating.** Raise to Level 2 for staff in sensitive sectors if China-linked targeting of travelers or tension over Taiwan escalates.

Public Wi-Fi

- China-linked espionage targets defense and technology organizations, and credential phishing is common via SMS. Public Wi-Fi in crowded transit areas carries device-loss risk and shoulder-surfing; use a corporate VPN and avoid public USB charging.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Earthquake and typhoon alerts can disrupt travel, so enable emergency alerts and carry a charged power bank.
- Devices left on trains are usually returned, but secure them and use a screen lock.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

JORDAN

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3

CAPITAL
Amman

GOVERNMENT
Constitutional monarchy

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 29, 2026)

Risk indicators: Terrorism, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Regional escalation after the Iran war, documented spyware use, state monitoring of speech, and a U.S. Level 3 advisory.

Country Overview

Jordan lies at a crossroads of the Levant and the Arabian Peninsula and contains the ancient city of Petra. The Ottoman Empire ruled the area until the First World War, after which Britain created the Emirate of Transjordan. Jordan became independent in 1946 and is ruled by the Hashemite dynasty, which claims descent from the Prophet Muhammad.

King Abdullah II has reigned since 1999. Jordan has about 11.9 million people, limited water and energy resources, and a large refugee population from Palestine, Iraq, and Syria. It signed a peace treaty with Israel in 1994 and is a close partner of the United States.

Geopolitical Landscape

- **Iran war spillover.** Iran retaliated against U.S. sites in Jordan in early September 2026, according to Crisis Group, after earlier Iranian missile and drone strikes across the region in the war that began on February 28, 2026. The State Department rates Jordan Level 3.

- **Gaza and the West Bank.** The war in Gaza and Israeli policy in the West Bank strain Jordan, whose population is largely of Palestinian origin.
- **Domestic politics.** Authorities banned the Muslim Brotherhood in 2025 and have prosecuted online speech under the 2023 cybercrime law.
- **Economic strain.** Unemployment and debt remain high, and Jordan depends on foreign aid.

Cyber Threats | Organizations

- **Iran-linked and regional targeting.** Government, military, and energy organizations draw Iran-linked and other regional actor interest, particularly during escalations.
- **State monitoring.** Security services monitor communications, and the 2023 cybercrime law expands penalties for online speech.
- **Spyware.** Citizen Lab and Access Now documented Pegasus spyware on the phones of Jordanian activists, journalists, and lawyers.
- **Financial and telecom sectors.** Banks and telecoms face phishing, business email compromise, and fraud.
- **Employees based in country.** Employees should assume communications are monitored, expect regional escalation to disrupt travel and airspace, and avoid political content online. Staff in government, defense, and energy roles face elevated targeting.
- **Vendor and supply chain risk.** State-linked telecoms and regional managed service providers can be disrupted during Iran-related escalations and may be compelled to share data. Segment vendor access and plan for airspace and connectivity disruption.

The TIDE team tracks 12 threat actors that list Jordan among their targets. By attributed nexus, they break down as 7 Iran-nexus, 2 unattributed or other, 1 India-nexus, 1 Turkey-nexus, and 1 China-nexus. The most frequently targeted sectors are government (10), telecommunications (8), defense and defense industrial base (5), civil society and activism (4), and education and research (3). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Social media posts about the monarchy, security services, or Israel can lead to prosecution.
- **Spyware targeting.** Activists and journalists are targets.
- **Fraud.** Bank and wallet impersonation scams are common in Arabic and English.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Jordan.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Jordan Level 3, Reconsider Travel, citing terrorism, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Iranian retaliation reached U.S. sites in Jordan in September 2026, spyware has been documented against activists, authorities monitor and prosecute online speech, and the State Department rates Jordan Level 3.
- **What would change this rating.** Raise to Level 4 if regional hostilities escalate to attacks on Jordanian territory or airspace closures. Lower to Level 2 if U.S.-Iran de-escalation holds.

Public Wi-Fi

- Authorities monitor communications and prosecute online speech, and Iranian retaliation reached U.S. sites in Jordan in September 2026. Assume hotel and carrier networks are monitored; use a corporate VPN and avoid public Wi-Fi entirely when handling company data.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid the Syrian and Iraqi border areas and demonstrations.

Return protocol

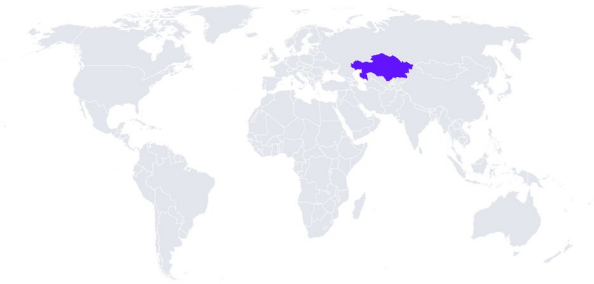
- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

KAZAKHSTAN

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2



CAPITAL
Astana

GOVERNMENT
Presidential republic

LANGUAGE
Kazakh and Russian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued August 18, 2026)

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: State ability to shut down and intercept traffic, sanctions-evasion scrutiny, and espionage interest in energy and minerals.

Country Overview

Kazakhstan is the world's largest landlocked country and spans the Eurasian steppe. Turkic and Mongol powers ruled the region, and Russia absorbed it in the eighteenth and nineteenth centuries. It became a Soviet republic and gained independence in December 1991.

Nursultan Nazarbayev led for nearly three decades. Kassym-Jomart Tokayev became president in 2019. Large January 2022 unrest, which Russian-led troops helped suppress, led to constitutional changes. Kazakhstan has about 20.6 million people and large oil, gas, and uranium reserves.

Geopolitical Landscape

- **Balancing powers.** Kazakhstan pursues a multi-vector policy among Russia, China, and the West, remains in Russian-led groupings, and has avoided recognizing Russian annexations in Ukraine.
- **Sanctions evasion concerns.** Western governments scrutinize re-export of sanctioned goods to Russia through Central Asia.
- **Energy and minerals.** The country is a major supplier of oil, uranium, and critical minerals and attracts Western and Chinese investment.
- **Political control.** Power remains concentrated in the presidency, and civic space is limited.

Cyber Threats | Organizations

- **State access to communications.** The government has used internet shutdowns, as in January 2022, and has attempted to intercept encrypted traffic through government-issued certificates.
- **Spyware and surveillance.** Reporting has documented commercial spyware and lawful-intercept systems used against activists.
- **Energy and mining.** Operators and contractors hold valuable commercial data and face espionage and ransomware.
- **Banks and fintech.** Rapid digitization has increased fraud and account takeover.
- **Employees based in country.** Employees should assume communications can be monitored and plan for possible internet shutdowns during unrest. Energy and mining staff are higher-value targets.
- **Vendor and supply chain risk.** Telecoms and local IT vendors can be compelled to provide access, and sanctions-evasion scrutiny creates compliance risk for some suppliers. Segment vendor access and screen counterparties.

The TIDE team tracks 12 threat actors that list Kazakhstan among their targets. By attributed nexus, they break down as 7 China-nexus, 3 Russia-nexus, and 2 cybercriminal. The most frequently targeted sectors are government (9), defense and defense industrial base (8), diplomatic and foreign affairs (4), industrial and manufacturing (4), and aerospace (3). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring.** Online criticism can lead to prosecution, and authorities monitor social media.
- **Fraud.** Phishing and impersonation scams circulate in Kazakh and Russian.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Kazakhstan.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Kazakhstan Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** The state can shut down and intercept traffic, sanctions-evasion scrutiny creates counterparty risk, and espionage interest in energy and minerals is high. Typical visitors face moderate risk.
- **What would change this rating.** Raise to Level 3 if unrest brings shutdowns or detentions of foreigners. Lower to Level 1 if monitoring practices ease.

Public Wi-Fi

- Kazakhstan has demonstrated the ability to shut down and intercept encrypted traffic using government-issued certificates. Plan for possible internet shutdowns during unrest; use a managed device with full-disk encryption and a corporate VPN, and carry only essential trip data.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, and keep offline copies of key details in case of connectivity disruption.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

KENYA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Nairobi

GOVERNMENT
Presidential republic

LANGUAGE
English and Swahili

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 28, 2026)

Risk indicators: Unrest, crime, health, kidnapping or hostage-taking, terrorism, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Pervasive mobile-money fraud, phone snatching, protest-related disruption, and episodic connectivity throttling.

Country Overview

Kenya lies on the equator in East Africa and spans coast, savanna, highlands, and the Rift Valley. Swahili coastal city-states traded across the Indian Ocean for centuries, and Britain made Kenya a colony in the early twentieth century. The Mau Mau uprising in the 1950s helped drive independence in 1963.

Jomo Kenyatta, Daniel arap Moi, and later presidents shaped a country that is now East Africa's largest economy and a regional tech and financial hub. Kenya has about 54.2 million people. William Ruto has been president since 2022, and the next general election is scheduled for August 2027.

Geopolitical Landscape

- **Protests.** Youth-led protests over taxes and governance in June 2024 and again in 2025 were met with force, and deaths were reported. Public anger over costs and police conduct persists.
- **Regional security.** Kenya borders Somalia, where al-Shabaab attacks continue, and South Sudan, and it has led international support for Haiti's security mission.
- **Debt and economy.** High debt service costs constrain budgets and have driven tax disputes.
- **2027 election.** Political maneuvering ahead of the August 2027 vote is increasing tension.

Cyber Threats | Organizations

- **Mobile money and fintech.** M-Pesa and other platforms are central to the economy and face SIM-swap, social engineering, and insider fraud.
- **Hacktivism and DDoS.** In July 2023 pro-Russian attackers disrupted Kenya's eCitizen government services platform for several days, and hacktivists continue to target public sites.
- **Connectivity controls.** Authorities and carriers have throttled or disrupted internet access around protests, according to civil society monitors.
- **Regulation.** Kenya's Data Protection Act and Computer Misuse and Cybercrimes Act shape duties and speech risk.
- **Employees based in country.** Employees face mobile-money fraud, phone snatching in Nairobi traffic, and travel disruption during protests. Staff in media, civil society, or finance face elevated phishing.
- **Vendor and supply chain risk.** Fintech, telecom, and outsourcing vendors hold sensitive financial and customer data, and fraud rings use compromised vendor mailboxes. Require strong authentication, logging, and out-of-band verification of payment changes.

The TIDE team tracks 4 threat actors that list Kenya among their targets. By attributed nexus, they break down as 2 cybercriminal, and 2 China-nexus. The most frequently targeted sectors are government (3), technology (3), healthcare and pharmaceuticals (2), defense and defense industrial base (2), and education and research (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile money fraud.** Fake agent, fake reversal, and SIM-swap scams are widespread.
- **Phone theft.** Snatch theft occurs in Nairobi traffic and crowded areas.
- **Monitoring and speech risk.** Online criticism of officials can lead to arrest, and journalists and activists have been targeted.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Kenya.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Kenya Level 2, Exercise Increased Caution, citing unrest, crime, health, kidnapping or hostage-taking, terrorism, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Mobile-money fraud and phone snatching are pervasive, protests have disrupted travel and connectivity, and fraud rings use compromised vendor mailboxes.

- **What would change this rating.** Raise to Level 3 if protests intensify with internet restrictions ahead of the 2027 election. Lower to Level 1 as fraud and theft decline.

Public Wi-Fi

- Pervasive mobile-money fraud and phone snatching occur in Nairobi traffic and crowded areas; authorities have throttled internet during protests. Keep devices out of sight in traffic, use app-based transport, and connect through a corporate VPN to avoid fraud interception.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations and the Somali border region flagged in the advisory.
- Keep devices out of sight in traffic, and use app-based transport.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

KIRIBATI

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Tarawa

GOVERNMENT
Presidential republic

LANGUAGE
English and Gilbertese (I-Kiribati)

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued December 2, 2024)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Very limited connectivity and low crime; diplomatic staff may draw external interest.

Country Overview

Kiribati is a Pacific nation of 33 low-lying coral atolls scattered across an area as wide as the continental United States. Micronesian peoples settled the islands thousands of years ago, Britain made them a protectorate in the nineteenth century, and Kiribati became independent in 1979.

The country has about 120,000 people and one of the world's most climate-vulnerable territories, with sea-level rise threatening its habitability. The economy depends on fishing license fees, remittances from seafarers, and aid. Kiribati switched diplomatic recognition from Taiwan to China in 2019. Taneti Maamau has been president since 2016.

Geopolitical Landscape

- **Climate threat.** Rising seas threaten land and fresh water, and the government seeks international support and migration options.
- **Great-power competition.** China, the United States, Australia, and New Zealand compete for influence through security and infrastructure agreements, and Chinese police and infrastructure projects have drawn regional attention.
- **Fisheries dependence.** License revenue from the world's largest tuna fishery zone funds much of the budget.

Cyber Threats | Organizations

- **Minimal digital footprint.** Connectivity depends on limited satellite and subsea links, and local security capacity is very limited.
- **Regional diplomatic targeting.** Government and diplomatic networks in the Pacific draw external espionage interest.
- **Vendor dependence.** Government and businesses rely on a few external providers for connectivity and IT.
- **Employees based in country.** Employees face very limited and costly connectivity and basic phishing risk. Diplomatic and aid staff may draw external interest.
- **Vendor and supply chain risk.** A small set of external vendors provide connectivity and IT, so loss of a single provider or link can cause outages. Plan for offline operation.

The TIDE team does not currently track actors that list Kiribati among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Limited connectivity.** Vodafone Kiribati and Oceanlink provide 2G/3G/4G service; internet is slow and costly, and social media is a main channel for news and scams.
- **Phishing and fraud.** Basic phishing and mobile fraud exist, though formal consumer-fraud reporting is limited.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Kiribati.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Kiribati Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity is very limited and crime is low. Diplomatic and aid staff may draw external interest.
- **What would change this rating.** Raise to Level 2 if great-power security arrangements increase targeting of local networks.

Public Wi-Fi

- Connectivity depends on the Kiritimati Island Cable, completed in 2022, and the East Micronesia Cable System, which reached Tarawa in 2025, ending heavy reliance on costly satellite links; local security capacity remains minimal. Carry offline copies of key documents, use a corporate VPN for any public network access, and plan for frequent outages.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Carry offline copies of key documents, since connectivity is limited.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

KOSOVO

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Pristina

GOVERNMENT
Parliamentary republic

LANGUAGE
Albanian and Serbian

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 25, 2026)

Risk indicators: Unrest, terrorism

Note: The United States and most EU states recognize Kosovo as independent. Serbia, Russia, and China do not.

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Prolonged political crisis, Serbia- and Russia-linked influence activity, and tension in the north.

Country Overview

Kosovo is a landlocked Balkan territory with an ethnic Albanian majority and a Serb minority concentrated in the north. It was part of the medieval Serbian state, then of the Ottoman Empire for centuries, and later of Yugoslavia. Repression of Kosovo Albanians in the 1990s led to the 1998 to 1999 war, which ended after a NATO bombing campaign forced Serbian forces out.

Kosovo declared independence on February 17, 2008. A NATO-led force, KFOR, remains. Kosovo has about 1.6 million residents and a large diaspora. The economy relies on remittances and services.

Geopolitical Landscape

- **Prolonged political crisis.** Kosovo has held three elections in about 18 months, in February 2025, December 2025, and June 7, 2026. Albin Kurti's Vetevendosje party won the most votes each time, 43 percent in June, but could not get the two-thirds quorum needed to elect a president. The presidency has been vacant since April 2026, and parliament confirmed Kurti's new government in September 2026 with 62 of 120 votes.

- **Serbia.** Tension remains high over the Serb-majority north and the unimplemented association of Serb-majority municipalities. EU measures imposed after 2023 clashes cost Kosovo hundreds of millions of euros in funding, according to analysts.
- **EU and NATO paths.** Kosovo seeks EU membership, but five EU states do not recognize it, and Serbia and Russia oppose its international standing.
- **Defense.** Kosovo is converting its security force into an army by 2028.

Cyber Threats | Organizations

- **State-linked and nationalist targeting.** Kosovo's government and critical infrastructure draw Serbia-aligned and Russia-linked attention, and hacktivism spikes with political tension.
- **Disinformation.** Narratives about the north, the army, and elections spread widely online.
- **Ransomware and fraud.** Public bodies and small firms have limited security capacity.
- **Banking sector.** Foreign-owned banks face phishing and fraud.
- **Employees based in country.** Employees face phishing and political disinformation, and tension in northern municipalities can disrupt travel. Government-adjacent staff may draw targeted phishing.
- **Vendor and supply chain risk.** Public bodies and small local vendors have limited security capacity, and hacktivism spikes during political tension. Verify vendor controls and keep sensitive data off local infrastructure where possible.

The TIDE team does not currently track actors that list Kosovo among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, couriers, and public agencies circulate in Albanian and Serbian.
- **Disinformation.** Politically charged false content spreads on social media.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Kosovo.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Kosovo Level 2, Exercise Increased Caution, citing unrest, terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A prolonged political crisis, Serbia- and Russia-linked influence activity, and periodic tension in the north drive the rating, with moderate risk to ordinary visitors.

- **What would change this rating.** Raise to Level 3 if violence flares in the north or hacktivist attacks on infrastructure increase. Lower to Level 1 as the political crisis ends.

Public Wi-Fi

- Serbia-aligned and Russia-linked targeting spikes during political tension, and hacktivism affects public infrastructure. Phishing messages impersonate banks and public agencies in Albanian and Serbian; use a corporate VPN, avoid demonstrations, and exercise heightened scrutiny of unsolicited communications.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid the north, including Mitrovica, during periods of tension, and avoid demonstrations.
- Border crossings with Serbia can close or require special documents, so confirm before travel.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

KUWAIT

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Kuwait City

GOVERNMENT
Constitutional emirate

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 28, 2026)

Risk indicators: Crime, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Iranian strikes on Gulf states and U.S. sites, Iran-linked targeting, state monitoring, and a U.S. Level 3 advisory.

Country Overview

Kuwait is a small, oil-rich Gulf state at the head of the Persian Gulf. The Al Sabah family has ruled since the eighteenth century, and Kuwait came under British protection in 1899 and became independent in 1961. Iraq invaded in 1990, and a U.S.-led coalition expelled Iraqi forces in 1991.

Kuwait has about 4.9 million people, most of them foreign workers, and one of the world's highest per-capita incomes from oil. Emir Mishal al-Ahmad Al Sabah took the throne in December 2023 and suspended parliament in May 2024.

Geopolitical Landscape

- **Iran war.** Iranian missile and drone strikes during the war that began on February 28, 2026 hit Gulf states including Kuwait, and Iran retaliated against U.S. sites in Kuwait again in early September 2026, according to Crisis Group. The State Department rates Kuwait Level 3.
- **Suspended parliament.** The emir's 2024 suspension of parliament concentrated power, and authorities have revoked citizenship in many cases.

- **U.S. presence.** Kuwait hosts U.S. forces and bases, which makes it a focus of Iranian retaliation.
- **Economic reform.** Kuwait faces pressure to diversify and reform spending.

Cyber Threats | Organizations

- **Iran-linked targeting.** Government, energy, finance, and telecommunications organizations are targeted by Iran-nexus actors, especially during escalations.
- **Oil sector.** Producers and contractors hold valuable data and run industrial systems that regional actors have probed.
- **State monitoring.** Authorities monitor communications and prosecute online speech critical of the emir.
- **Financial sector.** Banks face phishing, business email compromise, and fraud.
- **Employees based in country.** Employees should expect regional escalation to disrupt flights and airspace, assume monitoring of communications, and avoid political content online. Energy, finance, and government staff face elevated Iran-linked phishing.
- **Vendor and supply chain risk.** Gulf-wide telecoms and managed service providers can be disrupted during Iran-related escalations, and oil-sector contractors face elevated state-actor targeting. Segment vendor access and plan for airspace and connectivity disruption.

The TIDE team tracks 14 threat actors that list Kuwait among their targets. By attributed nexus, they break down as 10 Iran-nexus, 3 cybercriminal, and 1 unattributed or other. The most frequently targeted sectors are telecommunications (9), government (7), banking and financial services (4), energy (4), and technology (3). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Criticism of the emir or government online can lead to prosecution and citizenship loss.
- **Phishing and fraud.** Bank and delivery impersonation is common in Arabic and English.
- **VoIP limits.** Some voice-over-IP services are restricted.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Kuwait.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Kuwait Level 3, Reconsider Travel, citing crime, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Iranian strikes hit Gulf states including Kuwait during the war, Iran retaliated against U.S. sites there again in September 2026, authorities monitor speech, and the State Department rates Kuwait Level 3.

- **What would change this rating.** Raise to Level 4 if attacks on Kuwaiti territory resume or airspace closes. Lower to Level 2 if U.S.-Iran de-escalation holds.

Public Wi-Fi

- Iranian strikes hit Gulf states and U.S. sites in Kuwait during 2026 escalations, and authorities monitor communications and prosecute online speech. Assume hotel and carrier networks are monitored; do not use public Wi-Fi and route all traffic through a corporate VPN.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Confirm airline and evacuation arrangements before travel, since airspace closures have occurred during regional escalations.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

KYRGYZ REPUBLIC, THE

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2

CAPITAL
Bishkek

GOVERNMENT
Presidential republic

LANGUAGE
Kyrgyz and Russian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued February 10, 2026)

Risk indicators: Unrest

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Growing pressure on media and civil society, sanctions-related counterparty risk, and limited local security capacity.

Country Overview

The Kyrgyz Republic is a mountainous Central Asian country long inhabited by nomadic Turkic peoples. Russia absorbed the territory in the nineteenth century, and it became a Soviet republic and then independent in 1991. Revolutions in 2005 and 2010 toppled presidents.

The country has about 7.4 million people and depends on remittances, gold mining, and trade. Sadyr Japarov has been president since 2021, and power has become more concentrated while media and civil society face growing pressure, including a 2024 law on foreign-funded organizations.

Geopolitical Landscape

- **Russia and China.** The country is a member of Russian-led economic and security groupings and a major route for goods to and from Russia, which draws sanctions scrutiny. China is a leading investor and creditor.
- **Political space.** Authorities have arrested journalists and opponents and tightened controls on media and NGOs.
- **Border tensions.** A 2022 conflict with Tajikistan over borders ended with a 2025 agreement.
- **Remittance dependence.** Remittances, largely from Russia, are a large share of the economy.

Cyber Threats | Organizations

- **Sanctions and re-export exposure.** Banks and traders face scrutiny over transactions linked to Russia, which creates compliance and counterparty risk.
- **Limited security capacity.** Public bodies and banks have limited security staffing and have been targets of phishing and ransomware.
- **State access to data.** Authorities have the ability to monitor and block online content.
- **Regional espionage.** Government and diplomatic networks draw interest from regional actors.
- **Employees based in country.** Employees face ordinary phishing and fraud, and political content online can bring legal exposure. Staff in finance and trade face sanctions-related counterparty risk.
- **Vendor and supply chain risk.** Local banks, payment providers, and traders can create sanctions and compliance exposure. Screen counterparties and avoid concentrating sensitive data with local providers.

The TIDE team tracks 6 threat actors that list the Kyrgyz Republic among their targets. By attributed nexus, they break down as 3 China-nexus, 2 Russia-nexus, and 1 cybercriminal. The most frequently targeted sectors are government (5), defense and defense industrial base (4), diplomatic and foreign affairs (3), technology (2), and aerospace (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring.** Online criticism of officials can lead to prosecution, and some websites are blocked.
- **Fraud.** Phishing and impersonation scams circulate in Kyrgyz and Russian.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to the Kyrgyz Republic.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates the Kyrgyz Republic Level 1, Exercise Normal Precautions, citing unrest. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Pressure on media and civil society is growing, sanctions-related counterparty risk is rising, and local security capacity is limited. Typical visitors face low risk.
- **What would change this rating.** Raise to Level 3 if monitoring or detentions of foreigners increase. Lower to Level 1 if civic space reopens.

Public Wi-Fi

- Authorities have the ability to block online content and monitor communications, and political speech carries legal risk. Use a managed device with full-disk encryption, a corporate VPN, and phishing-resistant multi-factor authentication; carry only essential trip data.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, and expect mountain-region connectivity gaps.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

LAOS

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 3



CAPITAL
Vientiane

GOVERNMENT
One-party socialist republic

LANGUAGE
Lao

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 28, 2026)

Risk indicators: Unrest, crime, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Scam compound ecosystem, state monitoring of communications, and thin local security capacity.

Country Overview

Laos is a landlocked, mountainous country in Southeast Asia on the Mekong River. The Lan Xang kingdom unified the region in the fourteenth century, France ruled it as part of French Indochina, and Laos became independent in 1953. The country was bombed heavily during the Vietnam War era, and the communist Pathet Lao took power in 1975.

The Lao People's Revolutionary Party holds a monopoly on power. Laos has about 7.7 million people, one of the region's lowest incomes, and heavy debt to China, tied to projects such as the Laos-China railway that opened in 2021. Laos chaired ASEAN in 2024.

Geopolitical Landscape

- **Debt and China.** High external debt, much of it owed to China, strains public finances and has led to concessions over infrastructure and energy assets.
- **Golden Triangle scams.** The Golden Triangle Special Economic Zone in the northwest hosts large online scam operations, which has drawn U.S. sanctions and international pressure.
- **Political control.** The one-party state restricts media and civil society.

- **Hydropower.** Dams on the Mekong and its tributaries shape relations with downstream neighbors.

Cyber Threats | Organizations

- **Scam compound ecosystem.** Criminal syndicates run industrial-scale fraud from special zones using trafficked workers, creating money-laundering, insider, and trafficking risk for payment providers and telecoms.
- **State monitoring.** Authorities monitor communications and prosecute online criticism, and telecoms are state-linked.
- **Limited security capacity.** Banks and public bodies have thin security staffing.
- **Regional espionage.** Government networks draw interest from regional powers.
- **Employees based in country.** Employees face trafficking-linked job scams in the northwest, monitoring of communications, and limited connectivity. Online criticism of the government can lead to arrest.
- **Vendor and supply chain risk.** State-linked telecoms and local vendors can be compelled to share data, and special-zone entities can be tied to sanctioned networks. Screen vendor ownership and sanctions exposure and limit access to sensitive systems.

The TIDE team tracks 7 threat actors that list Laos among their targets. By attributed nexus, they break down as 6 China-nexus, and 1 Vietnam-nexus. The most frequently targeted sectors are government (5), telecommunications (4), media and journalism (2), defense and defense industrial base (2), and aerospace (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Scam recruitment.** Fake job offers lure people to scam compounds where they may be held and forced to commit fraud.
- **Monitoring and speech risk.** Online criticism of the government can lead to arrest.
- **Phishing and fraud.** Wallet and bank impersonation exist.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Laos.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Laos Level 2, Exercise Increased Caution, citing unrest, crime, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A scam compound ecosystem, state monitoring of communications, and thin local security capacity drive the rating.

- **What would change this rating.** Raise to Level 4 if detention risk for foreigners increases. Lower to Level 2 if compound crackdowns succeed.

Public Wi-Fi

- A scam compound ecosystem and state monitoring of communications create elevated risk; local security capacity is thin. Do not use public Wi-Fi and route all traffic through a corporate VPN; assume hotel and carrier networks are monitored and avoid all unsolicited job offers.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Treat unsolicited job offers in the region with extreme caution, and avoid the Golden Triangle special economic zone.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

LATVIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Riga

GOVERNMENT
Parliamentary republic

LANGUAGE
Latvian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued April 1, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable NATO and EU member; exposure is Russia-linked hacktivism, GPS interference near the border, and espionage.

Country Overview

Latvia is a Baltic country on the Gulf of Riga, bordering Estonia, Lithuania, Russia, and Belarus. German crusaders, Poland-Lithuania, Sweden, and Russia ruled its lands in succession. Latvia declared independence in 1918, was annexed by the Soviet Union in 1940, and regained independence in 1991.

Latvia joined NATO and the EU in 2004 and the eurozone in 2014. It has about 1.8 million people, a substantial Russian-speaking minority, and a services and logistics economy. A NATO-led multinational brigade is stationed in the country.

Geopolitical Landscape

- **Russia threat.** Latvia is among Ukraine's strongest supporters and a frontline NATO state, and it has faced airspace incidents, GPS jamming, cyberattacks, and suspected sabotage.
- **Border with Belarus.** Latvia has strengthened its border after Belarus-facilitated irregular migration, and it has closed or restricted some crossings.
- **Defense spending.** Latvia is raising defense spending sharply and has reintroduced conscription.
- **Russian-speaking minority.** Policy on language and citizenship is a political sensitivity.

Cyber Threats | Organizations

- **Russia-linked cyber activity.** Pro-Russia hacktivists conduct frequent DDoS attacks on Latvian government, media, and financial sites, and state-linked actors target defense and government networks.
- **GPS interference.** Jamming from Russian territory affects aviation, shipping, and navigation.
- **Financial sector.** Latvian banks have faced scrutiny over sanctions and money laundering, and they face phishing and fraud.
- **Regulation.** Latvia implements NIS2, and national CERT-LV coordinates response.
- **Employees based in country.** Employees face bank and parcel phishing and GPS interference near the eastern border. Staff in defense, logistics, or government-adjacent roles may draw Russia-linked targeting.
- **Vendor and supply chain risk.** Logistics, telecom, and financial suppliers are targets for state-linked actors and hacktivists. NIS2 extends security duties to suppliers, so require attestations and incident notification.

The TIDE team tracks 8 threat actors that list Latvia among their targets. By attributed nexus, they break down as 3 Russia-nexus, 2 China-nexus, 1 Belarus-nexus, 1 hacktivist, and 1 cybercriminal. The most frequently targeted sectors are government (7), diplomatic and foreign affairs (3), energy (3), education and research (3), and civil society and activism (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, postal services, and authorities are common.
- **GPS interference.** Jamming can affect phone and vehicle location services near the eastern border.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Latvia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Latvia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Latvia is a stable NATO and EU member. Exposure is Russia-linked hacktivism, GPS interference near the border, and role-based espionage targeting.
- **What would change this rating.** Raise to Level 2 if Russian hybrid pressure or sabotage escalates.

Public Wi-Fi

- Russia-linked cyberattacks and hacktivism target Latvian government and finance networks frequently; GPS jamming from Russian territory affects border areas. Use a corporate VPN for public networks, expect GPS interference near the eastern border, and carry offline maps.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Expect GPS interference near the eastern border, and carry offline maps.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

LEBANON

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Beirut

GOVERNMENT
Parliamentary republic with confessional power-sharing

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued August 21, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, other

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Active conflict with Israel, multi-actor surveillance, tampered-hardware precedent, GPS interference, and a U.S. Level 4 advisory.

Country Overview

Lebanon lies on the eastern Mediterranean and is home to the ancient Phoenician cities of Tyre, Sidon, and Byblos. The Ottomans ruled for centuries, France held a mandate after the First World War, and Lebanon became independent in 1943 with a power-sharing system among its Christian, Sunni, Shia, and Druze communities.

A civil war from 1975 to 1990 killed about 150,000 people, and Syria and Israel both occupied parts of the country. Hezbollah, a Shia militia and political party backed by Iran, became the dominant armed force. Lebanon has about 5.5 million people and suffered a financial collapse from 2019 that destroyed the value of the currency. Joseph Aoun became president in January 2025 and Nawaf Salam prime minister.

Geopolitical Landscape

- **2026 war between Israel and Hezbollah.** Hezbollah fired rockets at Israel in early March 2026 after the killing of Iran's supreme leader, and Israel launched a campaign in Lebanon. Lebanon's Health Ministry put the death toll at more than 3,000, with more than a million displaced, by the time a U.S.-brokered ceasefire took effect in mid-April.

- **Direct talks with Israel.** Lebanon and Israel opened their first direct negotiations in decades, with rounds held in Washington through the summer. Hezbollah rejects the talks and disarmament. In a September 15 interview, President Aoun said he wants a security agreement with Israel once Israeli forces withdraw from the south and that disarming Hezbollah is not negotiable.
- **Disarmament and civil-war risk.** The government has committed to a state monopoly on arms, and officials warn of the risk of internal conflict.
- **UNIFIL.** The UN Security Council voted to end the UNIFIL mandate on December 31, 2026.
- **Economy.** The post-2019 financial collapse limits state capacity and public services.

Cyber Threats | Organizations

- **Wartime disruption.** Strikes and displacement disrupt power, telecoms, and operations, and airspace closures affect travel.
- **State-linked and militia targeting.** Hezbollah-linked and Israeli-linked cyber and surveillance activity affect telecoms, government, and civil society, and the 2024 pager attacks showed supply chain compromise at scale.
- **GPS interference.** Widespread jamming and spoofing affects aviation and navigation.
- **Financial sector.** Banks operate under capital controls and face fraud and account takeover.
- **Fragile infrastructure.** Power outages are frequent, and local security capacity is limited.
- **Employees based in country.** Employees face wartime disruption, GPS interference, power and connectivity outages, and surveillance by multiple actors. Remove company access from personal devices and keep location data minimal.
- **Vendor and supply chain risk.** Local telecom, security, and logistics vendors operate under political and militia pressure, and tampered hardware has been used in attacks. Verify hardware provenance, segment vendor access, and plan for sudden loss of access.

The TIDE team tracks 6 threat actors that list Lebanon among their targets. By attributed nexus, they break down as 3 Iran-nexus, 2 cybercriminal, and 1 Lebanon-nexus. The most frequently targeted sectors are government (3), civil society and activism (2), media and journalism (2), healthcare and pharmaceuticals (2), and law and legal services (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Surveillance.** Multiple actors can monitor communications, and activists and journalists face risk.
- **Supply chain tampering.** The 2024 pager and radio attacks demonstrated risk from tampered devices.
- **Kidnapping and extortion.** Kidnapping risk exists, and fraud targets people hit by the financial crisis.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Lebanon.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Lebanon Level 4, Do Not Travel, citing unrest, crime, kidnapping or hostage-taking, terrorism, other. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has limited ability to assist, and the advisory warns of armed conflict, terrorism, and kidnapping.

TIDE Risk Level Rationale

- **Drivers.** Active conflict with Israel, surveillance by multiple actors, the 2024 tampered-hardware precedent, GPS interference, and frequent outages drive the rating. The State Department rates Lebanon Level 4.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable ceasefire, a security agreement with Israel, and progress on disarmament.

Public Wi-Fi

- Multiple actors conduct surveillance, power and connectivity outages are frequent, and the 2024 pager attacks demonstrated supply chain tampering at scale. Do not bring company devices; if authorized, use a clean loaner with a corporate VPN, assume all networks are monitored, and wipe devices on return.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

LESOTHO

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Maseru

GOVERNMENT
Parliamentary constitutional monarchy

LANGUAGE
Sesotho and English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued June 17, 2026)

Risk indicators: Crime, health

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is mobile-money fraud, phone theft, and thin local security capacity.

Country Overview

Lesotho is a mountainous kingdom entirely surrounded by South Africa, with the highest lowest point of any country. King Moshoeshoe I united Basotho clans in the 1820s and sought British protection against Boer expansion. Lesotho became independent in 1966.

The country has about 2.1 million people, one of the world's highest HIV rates, and an economy that depends on textiles, diamonds, water exports to South Africa, and remittances. Sam Matekane has been prime minister since 2022. U.S. tariffs imposed in 2025 hit its garment industry hard.

Geopolitical Landscape

- **Tariff uncertainty.** U.S. tariffs imposed in 2025 on Lesotho's textile exports threatened tens of thousands of jobs, and later legal and policy changes to U.S. tariffs have left the garment industry facing uncertainty.
- **Political instability.** Coups and coalition collapses have been common, and the army has intervened in politics in the past.
- **Dependence on South Africa.** Lesotho relies on South African trade, customs revenue, and labor markets.

Cyber Threats | Organizations

- **Limited digital footprint.** A small banking and telecom sector depends on South African parent firms and vendors.
- **Garment and mining exporters.** Firms hold buyer and pricing data and face invoice fraud.
- **Limited local capacity.** Government has few security resources.
- **Employees based in country.** Employees face mobile-money fraud, phone theft, and weather-related road disruption in the highlands. Garment-sector staff face invoice and payment fraud attempts.
- **Vendor and supply chain risk.** South African parent companies and a few local vendors carry most exposure. Verify subcontractor security and out-of-band payment verification.

The TIDE team does not currently track actors that list Lesotho among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile money fraud.** Vodacom Lesotho (M-Pesa) and Econet Telecom Lesotho (EcoCash) run a mobile-money duopoly; phishing and SIM-swap fraud target both platforms.
- **Government ransomware.** A September 2023 ransomware attack on the Ministry of Defence leaked a reported 1.6 terabytes of personal data, and a December 2023 attack on the Central Bank of Lesotho disrupted the national payments system, suspending interbank transactions for about two weeks.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Lesotho.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Lesotho Level 2, Exercise Increased Caution, citing crime, health. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with mobile-money fraud, phone theft, and thin local security capacity as the main exposure.
- **What would change this rating.** Raise to Level 2 if political instability or unrest brings connectivity restrictions.

Public Wi-Fi

- Mobile-money fraud and the documented Central Bank and Defence Ministry ransomware incidents show that both financial and government infrastructure have been targeted; surveillance risk is low but local security capacity is thin, and Lesotho's national CSIRT only launched in July 2026. Use standard protections: full-disk encryption, multi-factor authentication, and a corporate VPN for public network access.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Mountain roads and weather can disrupt travel, so allow extra time.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

LIBERIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Monrovia

GOVERNMENT
Presidential republic

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued December 11, 2025)

Risk indicators: Unrest, crime, health

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Mobile-money fraud, phone snatching, unreliable infrastructure, and thin security capacity.

Country Overview

Liberia lies on the Atlantic coast of West Africa. It was founded in the early nineteenth century by freed African Americans, with support from the American Colonization Society, and declared independence in 1847. The Americo-Liberian minority dominated politics until a 1980 coup.

Two civil wars between 1989 and 2003 killed an estimated 250,000 people and devastated infrastructure. Ellen Johnson Sirleaf became Africa's first elected woman head of state in 2006, and Joseph Boakai has been president since January 2024. Liberia has about 5.2 million people and depends on mining, rubber, and aid.

Geopolitical Landscape

- **Post-war recovery.** Liberia remains among the poorest countries in the world, and electricity, roads, and public services are limited.
- **Peacekeeping legacy.** The UN mission left in 2018, and Liberian forces and police now carry out security with limited resources.
- **Governance.** Corruption and weak institutions affect services and the investment climate.
- **Mining and regional ties.** Iron ore, gold, and rubber attract Chinese and Western investment.

Cyber Threats | Organizations

- **Mobile money and telecoms.** Operators and banks face SIM-swap, social engineering, and insider fraud.
- **Limited security capacity.** Public bodies and banks have thin security staffing and poor infrastructure.
- **Shipping registry.** Liberia hosts a major ship registry whose corporate and vessel data are valuable to fraud and state-linked actors.
- **Mining firms.** Operators hold commercial data and face espionage and fraud.
- **Employees based in country.** Employees face mobile-money fraud, phone snatching in Monrovia, and unreliable power and connectivity.
- **Vendor and supply chain risk.** The ship registry operator, mining contractors, and telecoms hold sensitive commercial data with thin local security. Segment vendor access and verify payment-change requests out of band.

The TIDE team does not currently track actors that list Liberia among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile money fraud.** SIM-swap and fake-agent scams are common.
- **Phone theft.** Snatch theft occurs in Monrovia.
- **Phishing.** Impersonation by SMS and WhatsApp is common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Liberia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Liberia Level 2, Exercise Increased Caution, citing unrest, crime, health. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Mobile-money fraud, phone snatching, unreliable infrastructure, and thin security capacity drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest or restrictions increase. Lower to Level 1 as infrastructure and security capacity improve.

Public Wi-Fi

- Mobile-money fraud, phone snatching in Monrovia, and unreliable infrastructure create ongoing risk; thin local security capacity limits incident response. Keep devices out of sight in traffic, carry power banks for frequent outages, and use a corporate VPN for all public network access.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Keep devices out of sight in traffic, and carry power banks, since outages are frequent.

Return protocol

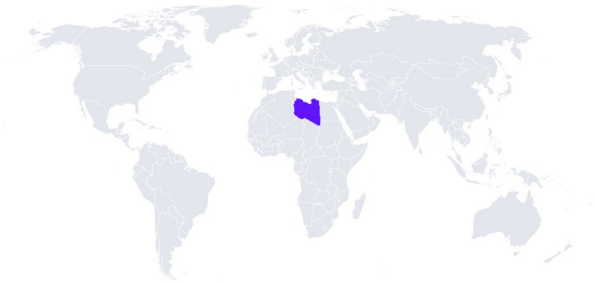
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

LIBYA

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Tripoli

GOVERNMENT
Divided transitional authorities (a Government of National Unity in Tripoli and eastern authorities aligned with Khalifa Haftar)

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued August 31, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, other, health

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Divided governments and militia control of infrastructure, kidnapping risk, unreliable power and connectivity, sanctions exposure, and a U.S. Level 4 advisory.

Country Overview

Libya spans the Mediterranean coast and Saharan interior of North Africa. Phoenicians, Greeks, Romans, Arabs, and Ottomans ruled parts of the territory, and Italy invaded in 1911 and held it until the Second World War. Libya became independent as a monarchy in 1951.

Colonel Muammar Gaddafi seized power in 1969 and ruled until a 2011 uprising backed by NATO airstrikes ended his regime. Since then Libya has been split by rival governments and militias, with civil wars in 2014 to 2020. The country has about 7.5 million people and Africa's largest proven oil reserves, which make the oil sector the center of political competition.

Geopolitical Landscape

- **Divided country.** A UN-recognized government in Tripoli and eastern authorities backed by Haftar's armed forces control separate territory, and elections planned for 2021 were never held. Armed groups inside Tripoli clashed in May 2025 after the killing of a prominent militia leader.

- **Foreign involvement.** Turkey, Russia, the UAE, Egypt, and others support different factions, and Russian forces are present at bases in the east and south.
- **Oil.** Blockades of oil facilities have repeatedly cut production, and control of revenue is a central dispute.
- **Migration.** Libya is a major departure point for migrants crossing the central Mediterranean, and abuses in detention centers are well documented.

Cyber Threats | Organizations

- **Militia control of infrastructure.** Armed groups control or influence ports, airports, telecoms, and utilities, and operations depend on security arrangements that can shift quickly.
- **Connectivity disruption.** Power cuts, damaged networks, and deliberate interruptions are frequent.
- **Oil and energy sector.** The National Oil Corporation, operators, and contractors hold sensitive data and face espionage, disruption, and physical attack.
- **Sanctions and illicit finance.** Fuel smuggling and arms embargo violations create sanctions exposure for traders and shippers.
- **Employees based in country.** Employees face kidnapping risk, militia surveillance, and unreliable power and connectivity. Remove company access from personal devices, and keep location and contact data minimal.
- **Vendor and supply chain risk.** Local telecom, logistics, and security vendors depend on militia arrangements and can be compelled to share data or lose access suddenly. Sanctions exposure is significant, so screen ownership and plan for loss of vendor access.

The TIDE team tracks 3 threat actors that list Libya among their targets. By attributed nexus, they break down as 2 unattributed or other, and 1 Iran-nexus. The most frequently targeted sectors are government (3), civil society and activism (2), diplomatic and foreign affairs (1), energy (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Surveillance by multiple actors.** Militias and security services monitor communications, and activists and journalists face abduction.
- **Kidnapping and extortion.** Kidnapping for ransom occurs.
- **Mobile and wallet fraud.** Banking cash shortages have encouraged informal payment schemes and fraud.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Libya.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Libya Level 4, Do Not Travel, citing unrest, crime, kidnapping or hostage-taking, terrorism, other, health. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has no embassy operations in Libya and very limited ability to assist.

TIDE Risk Level Rationale

- **Drivers.** Rival governments and militias control infrastructure, kidnapping occurs, power and connectivity are unreliable, sanctions exposure is significant, and the United States has very limited ability to assist.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require unified institutions, durable disarmament of militias, and restored consular presence.

Public Wi-Fi

- Rival governments and militias control infrastructure and surveil communications; kidnapping occurs and power and connectivity are unreliable. Do not bring company devices or access company infrastructure; power cuts and deliberate interruptions are frequent, making corporate VPN reliance impractical.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

LIECHTENSTEIN

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Vaduz

GOVERNMENT
Constitutional monarchy

LANGUAGE
German

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued August 18, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and low crime; exposure is targeted fraud against wealthy clients and financial-sector data theft.

Country Overview

Liechtenstein is a tiny Alpine principality between Switzerland and Austria. The Liechtenstein family acquired the territory in 1699 and 1712, and the principality was established as a sovereign state in 1719. It became fully independent in 1806 after the Holy Roman Empire dissolved and has been neutral since.

The country has about 41,000 people, uses the Swiss franc, and is in a customs union with Switzerland. It is a member of the European Economic Area. Prince Hans-Adam II holds substantial constitutional powers, and his son Hereditary Prince Alois acts as regent. The economy is highly industrialized and built on precision manufacturing and private banking.

Geopolitical Landscape

- **Financial transparency.** Liechtenstein has moved from a bank-secrecy model to international tax transparency, a shift accelerated by a 2008 theft of client data from a Liechtenstein bank.
- **Low-profile neutrality.** The principality has no army and no active disputes.
- **Regional integration.** It relies on Switzerland and the EEA for market access and diplomacy.

Cyber Threats | Organizations

- **Financial sector.** Private banks, trusts, and asset managers hold high-value client data and face business email compromise, targeted phishing, and data theft.
- **Precision manufacturing.** Industrial firms hold intellectual property and face ransomware and espionage.
- **Small-state resourcing.** Local security capacity is small, and firms rely on Swiss and Austrian vendors.
- **Employees based in country.** Employees face targeted phishing and payment fraud, especially in wealth-management roles. Everyday theft risk is low.
- **Vendor and supply chain risk.** Swiss and Austrian vendors and a small number of trust and banking service providers carry most exposure. Verify subcontractor controls for client data.

The TIDE team tracks 1 threat actor that lists Liechtenstein among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), construction and engineering (1), government (1), healthcare and pharmaceuticals (1), and industrial and manufacturing (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Wealth-targeted fraud.** Residents with high net worth face tailored fraud and extortion.
- **Phishing.** Bank and delivery impersonation in German is common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Liechtenstein.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Liechtenstein Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Liechtenstein is stable and low crime. Exposure is targeted fraud against wealthy clients and data theft at financial firms.
- **What would change this rating.** Raise to Level 2 if targeted campaigns against Liechtenstein banks or trusts emerge.

Public Wi-Fi

- Financial sector staff should avoid public Wi-Fi networks entirely, as wealth-management professionals are targets for business email compromise and data theft. If public Wi-Fi is unavoidable, use only a corporate VPN with phishing-resistant multi-factor authentication.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Liechtenstein is reached via Switzerland or Austria, and border checks follow Swiss and Schengen practice.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

LITHUANIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Vilnius

GOVERNMENT
Semi-presidential republic

LANGUAGE
Lithuanian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued April 28, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable NATO and EU member; exposure is Russia-linked hacktivism, GPS interference, and hybrid activity near the Belarus and Kaliningrad borders.

Country Overview

Lithuania was once the center of the Grand Duchy of Lithuania, one of Europe's largest states, which united with Poland in 1569 to form the Polish-Lithuanian Commonwealth. Russia absorbed the territory in the late eighteenth century. Lithuania declared independence in 1918, was annexed by the Soviet Union in 1940, and in March 1990 became the first Soviet republic to declare independence.

Lithuania joined NATO and the EU in 2004 and the eurozone in 2015. It has about 2.9 million people, a growing technology and logistics economy, and a German brigade stationed on its territory. Vilnius also hosts exile opposition from Belarus.

Geopolitical Landscape

- **Belarus pressure.** Lithuania has faced irregular migration facilitated by Belarus and, in October 2025, smuggling balloons from Belarus that closed Vilnius airport and border crossings repeatedly.
- **Russia threat.** Lithuania borders Russia's Kaliningrad exclave and is a leading supporter of Ukraine. Western officials attribute incendiary parcel plots and other sabotage in Europe to Russian services.
- **Defense posture.** Lithuania is sharply increasing defense spending, and a permanent German brigade is being established.

- **China.** A dispute over a Taiwanese representative office strained ties with Beijing in 2021.

Cyber Threats | Organizations

- **Pro-Russia hacktivism.** Groups such as NoName057(16) frequently launch DDoS attacks on Lithuanian government, transport, and media sites.
- **State-linked espionage.** Russia- and Belarus-linked actors, including the Ghostwriter operation, target government and defense.
- **GPS interference.** Jamming and spoofing from Russian territory affect aviation and navigation.
- **Hybrid threats.** Sabotage and disinformation target infrastructure and elections.
- **Regulation.** Lithuania implements NIS2.
- **Employees based in country.** Employees face bank and parcel phishing and GPS interference near the Belarus and Kaliningrad borders. Staff in defense, logistics, or government-adjacent roles may draw Russia- or Belarus-linked targeting.
- **Vendor and supply chain risk.** Logistics, telecom, and energy suppliers are priority targets for state-linked actors and hacktivists. NIS2 extends security duties to suppliers, so require attestations and incident notification.

The TIDE team tracks 12 threat actors that list Lithuania among their targets. By attributed nexus, they break down as 4 China-nexus, 3 Russia-nexus, 2 Belarus-nexus, 2 cybercriminal, and 1 hacktivist. The most frequently targeted sectors are government (10), diplomatic and foreign affairs (3), energy (3), defense and defense industrial base (3), and media and journalism (3). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, postal services, and police are common.
- **GPS interference.** Jamming can affect phone and vehicle location services near the borders.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Lithuania.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Lithuania Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Lithuania is a stable NATO and EU member. Exposure is Russia-linked hacktivism, GPS interference, and hybrid activity near the Belarus and Kaliningrad borders.
- **What would change this rating.** Raise to Level 2 if sabotage, border closures, or interference escalate.

Public Wi-Fi

- Public Wi-Fi near borders with Belarus and Kaliningrad presents elevated risk due to GPS interference and Russian-linked espionage. Connect through a corporate VPN if public networks are unavoidable, and confirm border status before travel.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Expect GPS interference near the borders, and confirm border-crossing status with Belarus before any trip nearby.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

LUXEMBOURG

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Luxembourg City

GOVERNMENT
Constitutional monarchy (Grand Duchy)

LANGUAGE
Luxembourgish, French, and German

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued April 8, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and low crime; exposure is targeted phishing and payment fraud against financial and EU-institution staff.

Country Overview

Luxembourg is a small, landlocked grand duchy between Belgium, France, and Germany. Its fortress city was one of Europe's strongest and changed hands among Spanish, French, Austrian, and Dutch rulers. The Congress of Vienna created the Grand Duchy in 1815, and Luxembourg became fully independent in 1890 when it separated from the Dutch crown.

Germany occupied Luxembourg in both world wars. The country was a founding member of NATO, the EU, and the Benelux union. It has about 690,000 people, one of the world's highest incomes per person, and a leading financial center. Grand Duke Henri abdicated in October 2025 and was succeeded by his son Guillaume. Luc Frieden has been prime minister since 2023.

Geopolitical Landscape

- **Financial center.** Luxembourg is a major hub for investment funds, banking, and data centers, and it has faced pressure over tax practices and anti-money-laundering controls.
- **EU institutions.** The Court of Justice of the EU, the European Investment Bank, and other bodies sit in Luxembourg, which draws espionage interest.
- **Security.** Luxembourg relies on NATO and has increased defense spending.

Cyber Threats | Organizations

- **Financial sector.** Banks, fund administrators, and custodians hold high-value data and face business email compromise, phishing, and state-linked espionage.
- **Data centers and cloud.** Luxembourg's data center cluster hosts concentrated assets for many clients.
- **EU institutions.** Staff and contractors of EU bodies face targeted phishing.
- **Regulation.** Luxembourg implements NIS2 and DORA, and the CSSF regulates financial-sector resilience.
- **Employees based in country.** Employees face targeted phishing and payment fraud, and staff at EU bodies, banks, and fund administrators draw elevated attention.
- **Vendor and supply chain risk.** Fund administrators, custodians, and data center operators are concentrated third parties for many firms. DORA and NIS2 extend resilience duties to them, so require attestations and exit and recovery plans.

The TIDE team tracks 2 threat actors that list Luxembourg among their targets. By attributed nexus, they break down as 2 China-nexus. The most frequently targeted sectors are aerospace (2), defense and defense industrial base (2), energy (2), government (2), and banking and financial services (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Bank and delivery impersonation circulates in French, German, and English.
- **Wealth-targeted fraud.** Residents with high net worth face tailored fraud and extortion.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Luxembourg.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Luxembourg Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Luxembourg is stable and low crime. Exposure is targeted phishing and payment fraud against finance and EU-institution staff.
- **What would change this rating.** Raise to Level 2 for staff in those roles if state-linked targeting of the financial sector intensifies.

Public Wi-Fi

- EU institution and financial sector staff face targeted phishing on public networks. Use a corporate VPN when accessing public Wi-Fi, and staff at banks, fund administrators, and EU bodies should avoid public networks wherever possible.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Everyday theft risk is low, though pickpocketing occurs at Luxembourg City rail hubs.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MACAU

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
None (seat of government in Macau Peninsula)

GOVERNMENT
Special Administrative Region of the People's Republic of China

LANGUAGE
Chinese (Cantonese) and Portuguese

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 4, 2026)

Risk indicators: Other (arbitrary enforcement of local laws)

Note: The United States recognizes Macau as part of the People's Republic of China but treats it separately for certain legal and trade purposes under U.S. law.

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Mainland-aligned security laws that permit compelled access, a casino sector with illicit-finance exposure, and impersonation fraud.

Country Overview

Macau lies on the Pearl River Delta west of Hong Kong. Portugal established a trading settlement in the sixteenth century and administered Macau until it returned to China on December 20, 1999 under the "one country, two systems" framework.

Macau has about 690,000 people and an economy dominated by casinos and tourism, which make it the world's largest gambling center by revenue. Sam Hou Fai became chief executive in December 2024. A national security law framework applies, including amendments passed in 2023.

Geopolitical Landscape

- **Close alignment with Beijing.** Macau's political system is tightly aligned with the mainland, and opposition space is minimal.
- **Economic diversification.** The government is trying to reduce reliance on casinos through technology and tourism, tied to the Greater Bay Area.

- **Financial crime scrutiny.** Casinos and junket operators have drawn scrutiny over money laundering and capital flight, and Beijing has cracked down on the junket industry.

Cyber Threats | Organizations

- **Casino and tourism sector.** Casino operators hold high-value customer and financial data and face ransomware, card fraud, and insider threats.
- **Financial crime.** Illicit finance and cross-border payment schemes create counterparty and compliance risk.
- **State access.** Security laws and mainland influence mean authorities can compel assistance and data, and foreign firms should assume access is possible.
- **State-linked targeting.** China-nexus actors target government, finance, and gaming interests in the region.
- **Employees based in country.** Employees face casino-area card fraud, impersonation scams, and legal exposure for political commentary. Anyone entering the mainland should apply the mainland China precautions.
- **Vendor and supply chain risk.** Casino technology, payment, and junket-linked vendors present illicit-finance and compelled-access risk. Screen vendor ownership, segment access, and review where data is stored.

The TIDE team tracks 1 threat actor that lists Macau among their targets. By attributed nexus, they break down as 1 China-nexus. The most frequently targeted sectors are civil society and activism (1), and education and research (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Impersonation and investment fraud.** Messages impersonating officials and banks, deepfake scams, and fake investment platforms are common.
- **Monitoring.** Online speech about politics can have legal consequences, and mainland rules apply at the border crossings.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Macau.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Macau Level 2, Exercise Increased Caution, citing other (arbitrary enforcement of local laws). The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Mainland-aligned security laws permit compelled access, the casino sector carries illicit-finance exposure, and impersonation fraud is common. Typical visitors face moderate risk.
- **What would change this rating.** Raise to Level 3 if device inspections or security-law enforcement against foreigners increase. Lower to Level 1 if compelled-access powers narrow.

Public Wi-Fi

- Mainland-aligned security laws permit compelled access to data transiting Macau's networks, and casino areas present elevated card fraud and impersonation fraud risk. Use only a corporate VPN on all networks, including hotel and casino connections.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Keep devices secured in crowded casino and tourist areas.
- Apply the full mainland China policy to any onward travel to the mainland.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MADAGASCAR

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Antananarivo

GOVERNMENT
Military-led transitional government

LANGUAGE
Malagasy and French

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued December 4, 2025)

Risk indicators: Unrest, crime, health

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: A 2025 military takeover, outages, possible connectivity restrictions during unrest, and mobile-money fraud.

Country Overview

Madagascar is the world's fourth-largest island, off the southeast coast of Africa, with unique wildlife found nowhere else. Settlers from Southeast Asia and Africa arrived about two thousand years ago, and the Merina Kingdom unified much of the island in the nineteenth century. France colonized Madagascar in 1896, and independence came in 1960.

Coups and contested elections marked the decades since. Andry Rajoelina first took power in a 2009 coup and returned as president in 2019. The country has about 32.7 million people and is among the poorest in the world, with chronic power and water shortages.

Geopolitical Landscape

- **2025 coup.** Youth-led Gen Z protests over power and water shortages and corruption began in September 2025. The army unit CAPSAT joined the protesters, parliament impeached Rajoelina after he fled, and Colonel Michael Randrianirina announced on October 14 that the military had taken power. He was sworn in as president on October 17 and promised a transition of up to two years. The African Union suspended Madagascar, while the regional SADC bloc did not.

- **Transition.** Randrianirina submitted a transition roadmap by the end of February 2026, and critics question his commitment to a timetable.
- **Economy.** Poverty, outages, and fiscal weakness are the root drivers of unrest.

Cyber Threats | Organizations

- **Instability and outages.** Power cuts, unrest, and political change disrupt operations, and local security capacity is limited.
- **Mobile money and banking.** Wallets and banks face SIM-swap and social engineering.
- **Mining and export sectors.** Nickel, cobalt, vanilla, and textile exporters hold commercial data and face invoice fraud.
- **Connectivity controls.** Authorities have restricted connectivity during past unrest.
- **Employees based in country.** Employees face outages, possible connectivity restrictions during unrest, mobile-money fraud, and phone theft in Antananarivo.
- **Vendor and supply chain risk.** A small set of local telecom, banking, and logistics vendors with thin security capacity carry most exposure, and unrest can interrupt services. Verify continuity plans and out-of-band payment verification.

The TIDE team does not currently track actors that list Madagascar among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile fraud.** SMS and wallet scams are common.
- **Monitoring during unrest.** Authorities may monitor and restrict communications during political tension.
- **Phone theft.** Snatch theft occurs in Antananarivo.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Madagascar.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Madagascar Level 2, Exercise Increased Caution, citing unrest, crime, health. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A 2025 military takeover, power and water outages, possible connectivity restrictions during unrest, and mobile-money fraud drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest returns with shutdowns or the transition collapses. Lower to Level 1 as a credible civilian transition proceeds.

Public Wi-Fi

- Power outages and unrest can disrupt connectivity and restrict access to network services during political instability. Prepare offline plans and use a corporate VPN when public Wi-Fi is available.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations and expect power cuts, and carry power banks and offline plans.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MALAWI

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Lilongwe

GOVERNMENT
Presidential republic

LANGUAGE
English and Chichewa

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 14, 2026)

Risk indicators: Unrest, crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is mobile-money fraud, phone theft, and frequent outages.

Country Overview

Malawi is a landlocked country in southeastern Africa, centered on Lake Malawi. Bantu-speaking peoples established kingdoms there, and Britain created the Nyasaland Protectorate in the late nineteenth century. Malawi became independent in 1964 under Hastings Banda, who ruled as a one-party dictator until a 1994 transition to multiparty democracy.

The country has about 21 million people and one of the world's lowest incomes, with an economy based on agriculture, especially tobacco. In the September 2025 election former president Peter Mutharika defeated incumbent Lazarus Chakwera and returned to office.

Geopolitical Landscape

- **Economic crisis.** Foreign-exchange and fuel shortages, inflation, and debt strain households and the government.
- **New government.** Mutharika's return reflects public frustration with the economy, and policy priorities include currency stabilization and investment.
- **Climate shocks.** Droughts and cyclones drive food insecurity.

Cyber Threats | Organizations

- **Mobile money.** Airtel Money and TNM Mpamba face SIM-swap, social engineering, and insider fraud.
- **Banks and public bodies.** Limited security capacity and frequent power cuts make organizations vulnerable to phishing and ransomware.
- **Agricultural exporters.** Tobacco and commodity traders face invoice fraud.
- **Employees based in country.** Employees face mobile-money fraud, phone theft, and frequent power outages. Fuel and currency shortages can disrupt operations.
- **Vendor and supply chain risk.** A few banks, telecoms, and agricultural traders with thin security capacity carry most exposure. Verify payment changes out of band and plan for power and connectivity gaps.

The TIDE team does not currently track actors that list Malawi among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile-money fraud.** SMS and agent scams are common.
- **Phone theft.** Snatch theft occurs in Lilongwe and Blantyre.
- **Disinformation.** False content spreads on WhatsApp and Facebook.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Malawi.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Malawi Level 2, Exercise Increased Caution, citing unrest, crime. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with mobile-money fraud, phone theft, and frequent outages as the main exposure.
- **What would change this rating.** Raise to Level 2 if economic stress brings unrest or connectivity restrictions.

Public Wi-Fi

- Mobile-money fraud through SIM-swap and social engineering is common; public Wi-Fi compounds this risk when accessing financial accounts or applications. Connect through a corporate VPN and avoid financial transactions on public networks.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Carry power banks and offline plans, since outages are frequent.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MALAYSIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Kuala Lumpur (administrative capital: Putrajaya)

GOVERNMENT
Federal constitutional elective monarchy

LANGUAGE
Malay

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued February 22, 2026)

Risk indicators: Kidnapping or hostage-taking (eastern Sabah)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; exposure is impersonation scams, snatch theft, and concentrated data center targeting.

Country Overview

Malaysia combines the Malay Peninsula and the northern part of Borneo. The Malacca Sultanate flourished in the fifteenth century, and Portuguese, Dutch, and British colonial powers followed. Peninsular states gained independence in 1957, and Malaysia was formed in 1963 with Sabah, Sarawak, and Singapore, which left in 1965.

Malaysia has about 34 million people and a diversified economy based on manufacturing, electronics, palm oil, and energy. Anwar Ibrahim has been prime minister since November 2022. Malaysia chaired ASEAN in 2025 and helped broker the Thailand-Cambodia ceasefire.

Geopolitical Landscape

- **Balancing powers.** Malaysia keeps close trade ties with China while cooperating with the United States and others, and it has overlapping claims in the South China Sea.
- **Data center boom.** Johor has become one of Asia's largest data center hubs, drawing global investment and U.S. export-control scrutiny of chip flows.
- **Domestic politics.** Racial and religious politics and corruption cases shape government.

- **Eastern Sabah.** Kidnapping risk persists along the eastern coast of Sabah.

Cyber Threats | Organizations

- **Data center and cloud sector.** Concentrated hosting for regional and global clients makes the sector a high-value target for state-linked actors and ransomware groups.
- **Ransomware and fraud.** Banks, government bodies, and companies face ransomware and business email compromise, and scam operations and money mule networks are active.
- **State-linked espionage.** Government, defense, and technology organizations draw regional espionage interest.
- **Regulation.** Malaysia enacted a Cyber Security Act in 2024 and amended its personal data protection law, which sets duties for critical infrastructure and incident reporting.
- **Employees based in country.** Employees face impersonation scams, snatch theft by motorbike, and public Wi-Fi risk. Staff at data center, technology, and finance firms may draw targeted attention.
- **Vendor and supply chain risk.** Data center operators, cloud providers, and managed service providers are concentrated third parties. The Cyber Security Act sets duties for critical-infrastructure suppliers, so require attestations and incident notification.

The TIDE team tracks 44 threat actors that list Malaysia among their targets. By attributed nexus, they break down as 24 China-nexus, 16 cybercriminal, 1 India-nexus, 1 Lebanon-nexus, 1 unattributed or other, and 1 Iran-nexus. The most frequently targeted sectors are government (29), technology (16), healthcare and pharmaceuticals (15), banking and financial services (14), and defense and defense industrial base (13). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Scams.** Phone and messaging scams impersonating police and banks, and investment fraud, cause large losses.
- **Phone and bag theft.** Snatch theft by motorcycle occurs in Kuala Lumpur.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Malaysia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Malaysia Level 1, Exercise Normal Precautions, citing kidnapping or hostage-taking (eastern sabah). The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Malaysia is stable and well-regulated. Exposure is impersonation scams, snatch theft, and concentrated data center targeting.

- **What would change this rating.** Raise to Level 2 for data center and technology staff if state-linked targeting intensifies.

Public Wi-Fi

- Data center and technology sector staff face targeting from regional state-linked actors; impersonation scams are widespread on public networks. Use a corporate VPN on all public connections, particularly if your role involves sensitive infrastructure.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Keep phones secured when walking near roads, where motorbike snatch theft occurs.
- Avoid the eastern coast of Sabah areas flagged in the advisory.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MALDIVES

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Male

GOVERNMENT
Presidential republic

LANGUAGE
Dhivehi

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued October 7, 2025)

Risk indicators: Terrorism

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low crime and light surveillance of visitors; exposure is tourism fraud and resort-vendor concentration.

Country Overview

The Maldives is an island nation of about 1,200 coral islands in the Indian Ocean southwest of India. Buddhist and then Muslim kingdoms ruled the islands, which later became a British protectorate until independence in 1965.

Maumoon Abdul Gayoom ruled for 30 years until multiparty elections in 2008. The country has about 520,000 people, and tourism supplies most income. Mohamed Muizzu became president in November 2023 after campaigning to reduce Indian influence and has since balanced relations among India, China, and Gulf states. High debt and climate vulnerability are central concerns.

Geopolitical Landscape

- **India and China.** The Maldives sits on key Indian Ocean shipping lanes and is courted by India and China, with Muizzu moving between them.
- **Debt pressure.** High external debt and thin reserves create default risk and reliance on partner support.
- **Climate.** Rising seas threaten the low-lying islands.

- **Extremism.** The State Department cites terrorism risk, and some Maldivians have joined foreign jihadist groups.

Cyber Threats | Organizations

- **Tourism sector.** Resorts and airlines hold payment and passport data and face card fraud and ransomware.
- **Limited security capacity.** Public bodies and small firms rely on foreign vendors and have thin incident response.
- **Regional targeting.** Government and diplomatic networks draw interest from regional powers.
- **Financial sector.** Banks face phishing and fraud.
- **Employees based in country.** Employees face tourist-area card fraud and booking scams. Resort and aviation staff may draw targeted phishing.
- **Vendor and supply chain risk.** Resorts depend on a small number of foreign booking, payment, and IT vendors, so a vendor compromise can affect many properties. Require access controls and incident notification.

The TIDE team tracks 1 threat actor that lists Maldives among their targets. By attributed nexus, they break down as 1 India-nexus. The most frequently targeted sectors are banking and financial services (1), critical infrastructure (general) (1), defense and defense industrial base (1), education and research (1), and government (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Tourist-targeted fraud.** Fake booking and resort listings and card skimming target visitors.
- **Monitoring and legal risk.** Online criticism of religion or the government can lead to prosecution.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Maldives.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Maldives Level 2, Exercise Increased Caution, citing terrorism. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low crime and light surveillance of visitors. Exposure is tourism fraud and concentrated reliance on a few resort technology vendors.
- **What would change this rating.** Raise to Level 2 if political tension or debt stress brings connectivity or legal restrictions.

Public Wi-Fi

- Resorts operate on private islands with their own networks where payment fraud and ransomware are risks; apply the same precautions to resort Wi-Fi as to public networks. Require a corporate VPN for all Wi-Fi access.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Resorts operate on private islands with their own Wi-Fi, so follow the public Wi-Fi guidance there as well.

Return protocol

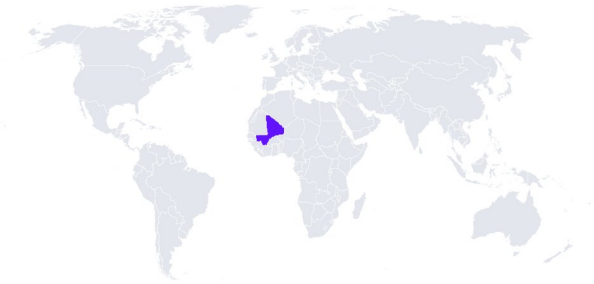
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MALI

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Bamako

GOVERNMENT
Military-led government

LANGUAGE
French (with Bambara and other national languages)

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued June 8, 2026)

Risk indicators: Crime, kidnapping or hostage-taking, terrorism, unrest, health

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Jihadist blockade of the capital, junta control of media and connectivity, abductions, thin infrastructure, and a U.S. Level 4 advisory.

Country Overview

Mali is a landlocked Sahel country that was the heart of three great West African empires: Ghana, Mali, and Songhai. Timbuktu was a leading center of Islamic scholarship and trade. France colonized the area and Mali became independent in 1960.

Coups in 1968, 1991, 2012, 2020, and 2021 mark a history of military rule. A 2012 Tuareg rebellion and jihadist takeover of the north led to French intervention in 2013. Colonel Assimi Goita took power in 2021, expelled French and UN forces, and brought in Russian paramilitaries, now called the Africa Corps. In July 2025 he named himself president for a renewable five-year term. Mali has about 23.9 million people.

Geopolitical Landscape

- **JNIM blockade.** Al-Qaeda affiliate JNIM imposed a fuel blockade on Bamako in September 2025 that caused severe shortages and blackouts and prompted Western governments to urge their citizens to leave. In April 2026 JNIM and the Tuareg-led Azawad Liberation Front launched offensives, Russian paramilitaries withdrew from Kidal, and JNIM announced a blockade of all roads into the capital, which Goita said was under control.

- **Alliance of Sahel States.** Mali, Burkina Faso, and Niger left ECOWAS and formed a separate alliance, and they rely on Russia and Turkey for security help.
- **Political repression.** The junta has dissolved political parties, suspended media, and detained critics.
- **Humanitarian crisis.** Displacement, hunger, and insecurity affect millions.

Cyber Threats | Organizations

- **Fuel and power disruption.** Blockade-driven shortages cause blackouts, closures, and logistics failure, so operations depend on generators and convoy security.
- **State control of connectivity and media.** Authorities have suspended foreign media and restricted social media.
- **Mining sector.** Gold and lithium operators and contractors hold valuable data and face attack, extortion, and espionage.
- **Staff safety.** Leaks of staff, site, or convoy information can create direct physical risk.
- **Employees based in country.** Employees face fuel and power outages, connectivity restrictions, monitoring, and physical risk if location data leaks. Remove company access from personal devices and keep movements confidential.
- **Vendor and supply chain risk.** Mining, logistics, security, and telecom vendors operate under blockade and junta pressure and may lose access abruptly. Limit shared location data, segment vendor access, and plan for sudden loss of services.

The TIDE team tracks 1 threat actor that lists Mali among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Surveillance and abduction.** Critics, lawyers, and journalists have been abducted, and authorities monitor communications.
- **Mobile money fraud.** SIM-swap and wallet scams are common.
- **Disinformation.** Pro-junta and pro-Russia narratives and jihadist propaganda circulate widely.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Mali.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Mali Level 4, Do Not Travel, citing crime, kidnapping or hostage-taking, terrorism, unrest, health. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has very limited ability to assist, and Western governments have urged their citizens to leave.

TIDE Risk Level Rationale

- **Drivers.** A jihadist blockade of the capital, junta control of media and connectivity, abductions of critics, fuel and power outages, and a U.S. Level 4 advisory drive the rating. Leaks of location data can create direct physical risk.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require the blockade to end and the security situation around Bamako to stabilize.

Public Wi-Fi

- Do not use public Wi-Fi or connect to company infrastructure of any kind due to jihadist blockade, junta connectivity control, and extreme surveillance risk. Follow the corporate policy: no device, no infrastructure.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

MALTA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Valletta

GOVERNMENT
Parliamentary republic

LANGUAGE
Maltese and English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 9, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable EU member; exposure is gaming-sector targeting, phishing, and tourist-area theft.

Country Overview

Malta is a Mediterranean archipelago south of Sicily whose strategic position drew Phoenicians, Romans, Arabs, Normans, and the Knights of St. John, who built Valletta. Britain took control in 1800, and Malta endured heavy bombing in the Second World War. It became independent in 1964 and a republic in 1974.

Malta joined the EU in 2004 and the eurozone in 2008. It has about 590,000 people, an economy built on tourism, online gaming, and financial services, and a policy of military neutrality. Robert Abela has been prime minister since 2020.

Geopolitical Landscape

- **Rule-of-law scrutiny.** The 2017 assassination of journalist Daphne Caruana Galizia exposed corruption concerns, and Malta was placed on the FATF grey list from 2021 to 2022 before being removed.
- **Migration.** Malta is a front-line state for Mediterranean arrivals.
- **Gaming and finance.** The online gaming and financial-services sectors draw regulatory attention and high-value targeting.

Cyber Threats | Organizations

- **Online gaming and fintech.** Gaming operators and payment firms hold large volumes of customer and financial data and face fraud, DDoS extortion, and ransomware.
- **Banking sector.** Banks and gaming firms are prime targets for fraud and extortion.
- **Pro-Russia hacktivism.** DDoS campaigns have targeted Maltese government sites.
- **Regulation.** Malta implements NIS2 and the GDPR.
- **Employees based in country.** Employees face phishing, tourist-area pickpocketing, and rental scams. Staff at gaming and fintech firms face elevated targeting.
- **Vendor and supply chain risk.** Gaming platforms, payment processors, and managed service providers hold concentrated data. NIS2 extends security duties to suppliers, so require attestations and incident notification.

The TIDE team tracks 2 threat actors that list Malta among their targets. By attributed nexus, they break down as 1 China-nexus, and 1 cybercriminal. The most frequently targeted sectors are civil society and activism (1), diplomatic and foreign affairs (1), government (1), banking and financial services (1), and cryptocurrency and digital assets (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Bank and delivery impersonation is common in English and Maltese.
- **Tourist-area theft and fraud.** Pickpocketing and rental scams affect visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Malta.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Malta Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Malta is a stable EU member. Exposure is targeting of gaming and fintech firms, phishing, and tourist-area theft.
- **What would change this rating.** Raise to Level 2 for gaming and fintech staff if state-linked or extortion campaigns intensify.

Public Wi-Fi

- Gaming and fintech sectors are targeted by phishing on public networks, and tourist areas present elevated fraud and theft risk. Use a corporate VPN for all public Wi-Fi access, particularly in financial and gaming districts.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Pickpocketing occurs on crowded buses and at Valletta and St. Julian's tourist areas.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MARSHALL ISLANDS

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Majuro

GOVERNMENT
Presidential republic in free association with the United States

LANGUAGE
Marshallese and English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 21, 2026)

Risk indicators: Health

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Very limited connectivity and low crime; registry and U.S.-facility staff may draw external interest.

Country Overview

The Marshall Islands is a Pacific nation of 29 atolls and five islands. Micronesian navigators settled the islands thousands of years ago, and Germany, Japan, and then the United States held them in turn. The United States carried out 67 nuclear tests at Bikini and Enewetak atolls between 1946 and 1958, with lasting health and environmental effects.

The country became self-governing in 1979 and fully independent in 1986 under a Compact of Free Association with the United States, which provides defense, funding, and access. It has about 42,000 people. Hilda Heine, a former education minister, became president in January 2024. Climate threats and a large international ship registry shape the economy.

Geopolitical Landscape

- **Compact relationship.** The United States provides security, financial support, and visa-free access under the compact, and it operates a missile test range at Kwajalein.
- **Climate threat.** Sea-level rise threatens the low-lying atolls, and the government is a leading voice on climate and displacement.

- **Nuclear legacy.** The government continues to press for compensation and cleanup related to U.S. nuclear testing.

Cyber Threats | Organizations

- **Ship registry.** The Marshall Islands registry is among the world's largest, and its corporate and vessel data are valuable to fraud and state-linked actors.
- **Limited digital footprint.** Connectivity depends on limited subsea and satellite links, and local security capacity is thin.
- **Strategic military role.** The Kwajalein range attracts foreign intelligence interest.
- **Employees based in country.** Employees face limited and costly connectivity and basic phishing risk. Staff linked to the ship registry or U.S. facilities may draw targeted interest.
- **Vendor and supply chain risk.** The registry operator and a few connectivity and IT providers carry concentrated exposure. Plan for outages and verify payment-change requests out of band.

The TIDE team does not currently track actors that list Marshall Islands among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Limited connectivity.** The state monopoly NTA/MINTA operates the only mobile network, running over the aging HANTRU-1 submarine cable from Guam; a March 2022 distributed denial-of-service attack, reportedly linked to the Russia-Ukraine conflict, disrupted DSL and mobile data for roughly ten days.
- **Phishing and fraud.** Basic phishing and romance scams circulate on Facebook, the primary social platform.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Marshall Islands.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Marshall Islands Level 1, Exercise Normal Precautions, citing health. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity is very limited and crime is low. Registry and U.S.-facility staff may draw external interest.
- **What would change this rating.** Raise to Level 2 if targeting of the ship registry or Kwajalein-related networks increases.

Public Wi-Fi

- A single aging submarine cable (HANTRU-1) creates critical dependency, with a Google-backed secondary cable in development; use a corporate VPN when connectivity is available, and rely on offline copies of essential documents given the outage risk.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Carry offline copies of key documents, since connectivity is limited.

Return protocol

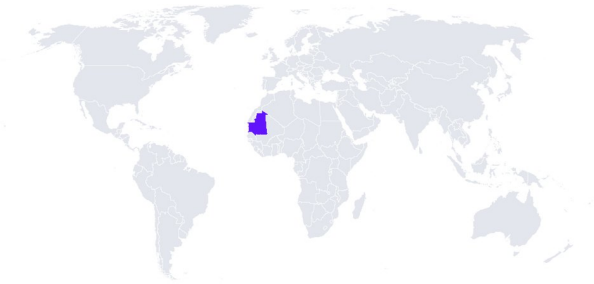
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MAURITANIA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Nouakchott

GOVERNMENT
Presidential republic

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 18, 2026)

Risk indicators: Crime, terrorism, health

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Mobile internet shutdowns around elections and protests, monitoring of speech, Sahel border risk, and a U.S. Level 3 advisory.

Country Overview

Mauritania lies in the western Sahara and Sahel, where Berber and Arab influences shaped the societies that built caravan trading cities such as Chinguetti. France colonized the territory, and Mauritania became independent in 1960. Coups in 1978, 1984, 2005, 2008, and others marked its political history.

The country has about 4.9 million people, a legacy of slavery that was formally abolished in 1981 and criminalized in 2007, and economic reliance on iron ore, fisheries, and new offshore gas. Mohamed Ould Ghazouani has been president since 2019 and was reelected in 2024.

Geopolitical Landscape

- **Sahel spillover.** Mauritania borders Mali, and refugees and jihadist activity on the frontier are concerns. It has avoided major attacks since 2011 through security and religious outreach.
- **Gas projects.** The Greater Tortue Ahmeyim gas project with Senegal is a major source of expected revenue.
- **Political space.** Authorities cut mobile internet access after the 2024 election and during protests.
- **Migration.** Mauritania is a departure route toward the Canary Islands.

Cyber Threats | Organizations

- **Connectivity shutdowns.** Authorities have cut mobile internet during elections and protests, and exam-period disruptions occur.
- **Mining and gas.** Iron ore, gold, and gas operators and contractors hold valuable data and face espionage and fraud.
- **Limited local capacity.** Banks, telecoms, and public bodies have thin security staffing.
- **Employees based in country.** Employees face possible mobile internet shutdowns, monitoring of communications, and mobile-money fraud. Online remarks about religion or the government carry legal risk.
- **Vendor and supply chain risk.** A few banks, telecoms, and extractive contractors with thin security capacity carry most exposure, and shutdowns can cut vendor access. Plan for offline continuity and segment vendor access.

The TIDE team does not currently track actors that list Mauritania among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Monitoring.** Authorities monitor online criticism of the government and religion, and blasphemy laws carry severe penalties; SIM registration has required biometric data since October 2023.
- **Mobile fraud.** Moov Mauritel, Mattel, and Chinguitel provide mobile service, and SMS and wallet scams are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Mauritania.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Mauritania Level 3, Reconsider Travel, citing crime, terrorism, health. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Authorities have cut mobile internet around elections and protests, monitor online speech, and the Sahel border adds risk. The State Department rates Mauritania Level 3.
- **What would change this rating.** Raise to Level 4 if Mali's conflict spills across the border or shutdowns become routine. Lower to Level 2 if restrictions end.

Public Wi-Fi

- Authorities have repeatedly cut mobile internet during elections and unrest, most recently for 22 days in July 2024 after disputed presidential election results, and online speech is monitored for religious or political

commentary. Avoid public Wi-Fi entirely; if travel is authorized, use a corporate VPN with no personal device access to company infrastructure.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid the Mali border region flagged in the advisory.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

MAURITIUS

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Port Louis

GOVERNMENT
Parliamentary republic

LANGUAGE
English (official), French, and Mauritian Creole

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued December 8, 2025)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable democracy; exposure is offshore-sector fraud, tourism scams, and a recent surveillance controversy.

Country Overview

Mauritius is an Indian Ocean island nation east of Madagascar that was uninhabited until the Dutch, then the French, and then the British settled it. Sugar plantations worked first by enslaved Africans and later by indentured laborers from India shaped its diverse society.

Mauritius became independent in 1968 and a republic in 1992. It has about 1.2 million people and one of Africa's most stable democracies, with an economy built on tourism, textiles, financial services, and information technology. Navin Ramgoolam returned as prime minister in November 2024.

Geopolitical Landscape

- **Chagos agreement.** Mauritius and the United Kingdom signed a treaty in May 2025 to transfer sovereignty over the Chagos Archipelago to Mauritius while the UK leases back the Diego Garcia base. Ratification and implementation have drawn debate.
- **Surveillance scandal.** In November 2024 authorities blocked social media for about 24 hours after leaked recordings of phone calls by politicians, journalists, and diplomats surfaced, which raised questions about surveillance practices and civil liberties.
- **Financial center.** Mauritius has worked to leave financial watchlists and tighten transparency.

Cyber Threats | Organizations

- **Financial and offshore sector.** Global business companies, banks, and fund administrators hold high-value client data and face business email compromise, phishing, and extortion.
- **Tourism and IT.** Resorts and outsourcing firms hold payment and customer data.
- **Government data.** Public bodies have faced leaks and breaches.
- **Regulation.** Mauritius has a Data Protection Act aligned with GDPR principles.
- **Employees based in country.** Employees face phishing and tourist-area fraud, and staff in offshore finance face targeted payment fraud.
- **Vendor and supply chain risk.** Corporate service providers, fund administrators, and IT outsourcing firms hold concentrated client data. Verify subcontractor controls and require incident notification.

The TIDE team does not currently track actors that list Mauritius among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Phishing and impersonation.** Bank and delivery impersonation scams circulate in English, French, and Creole.
- **Tourist-targeted fraud.** Fake rental listings and card skimming target visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Mauritius.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Mauritius Level 2, Exercise Increased Caution, citing crime. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Mauritius is a stable democracy. Exposure is offshore-sector fraud, tourism scams, and a recent surveillance controversy.
- **What would change this rating.** Raise to Level 2 if surveillance practices or online restrictions expand.

Public Wi-Fi

- Tourist-area fraud and a recent surveillance controversy create risks on public networks for business travelers. Use a corporate VPN for all public Wi-Fi, and offshore finance staff should avoid accessing client data on public networks.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Cyclone season, November through April, can disrupt travel and connectivity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MEXICO

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Mexico City

GOVERNMENT
Federal presidential republic

LANGUAGE
Spanish (with 68 recognized indigenous languages)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 29, 2026)

Risk indicators: Crime, kidnapping or hostage-taking, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Extortion using leaked data, express kidnapping, SIM-swap and bank-impersonation fraud, phone theft, and nearshoring-driven vendor exposure.

Country Overview

Mexico was the home of the Olmec, Maya, and Aztec civilizations. Spain conquered the Aztec Empire in 1521 and ruled New Spain for three centuries. Independence came in 1821 after a decade of war, and the nineteenth century brought the loss of Texas and other territory to the United States, French intervention, and the dictatorship of Porfirio Diaz.

The 1910 revolution produced the 1917 constitution, and the Institutional Revolutionary Party dominated politics for seven decades. Mexico joined NAFTA in 1994 and is now the largest trading partner of the United States. It has about 130 million people. Claudia Sheinbaum, the first woman president, took office on October 1, 2024 and leads the Morena party, which has deepened its dominance.

Geopolitical Landscape

- **Pressure from Washington.** President Trump has used tariffs and threats of military action against cartels to press Mexico on drugs, migration, and water deliveries. The United States has designated Mexican cartels as terrorist organizations, indicted a Mexican governor on cartel-related charges, and demanded more security cooperation, while Sheinbaum has extradited dozens of cartel figures and deployed troops to the border.

- **USMCA review.** The joint review of the U.S.-Mexico-Canada Agreement began in mid-2026, and steel, aluminum, and auto tariffs continue to affect exporters. Roughly 80 percent of Mexican exports depend on the U.S. market.
- **Cartel violence.** Violence, disappearances, and extortion persist, especially in states such as Sinaloa.
- **Institutional changes.** Constitutional reforms, including the election of judges, have raised concerns about checks and balances and the investment climate.

Cyber Threats | Organizations

- **Extortion and cartel influence.** Cartels extort businesses and infiltrate local institutions, and stolen personal data supports threats against employees and managers.
- **State-linked and criminal intrusions.** In September 2022 attackers took six terabytes of data from the Defense Ministry, and Citizen Lab and Mexican groups documented Pegasus infections of journalists and a human rights defender between 2019 and 2021.
- **Ransomware.** Government bodies, banks, and manufacturers face ransomware, and nearshoring brings foreign manufacturers into the same threat environment.
- **Banking and fintech.** Instant payments through SPEI and wallets are targeted by fraud and account takeover.
- **Regulation.** Mexico is updating its data protection and telecom frameworks, which creates compliance uncertainty.
- **Employees based in country.** Employees face extortion calls using leaked data, SIM-swap and bank-impersonation fraud, phone theft, and express kidnapping risk. Managers and employees at manufacturing sites in cartel-affected states are priority extortion targets.
- **Vendor and supply chain risk.** Nearshoring has brought many logistics, security, payment, and manufacturing vendors into a high-extortion environment, and vendor staff data can leak to criminal groups. Vet vendor personnel, limit shared staff data, and require strong authentication for payment changes.

The TIDE team tracks 47 threat actors that list Mexico among their targets. By attributed nexus, they break down as 31 cybercriminal, 6 China-nexus, 4 unattributed or other, 3 Iran-nexus, 2 Russia-nexus, and 1 North Korea-nexus. The most frequently targeted sectors are government (29), healthcare and pharmaceuticals (29), industrial and manufacturing (25), education and research (22), and technology (18). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Extortion and virtual kidnapping.** Callers claim to hold relatives or threaten the victim, often using leaked data.
- **SIM swap and banking fraud.** Account takeover is common, and fake bank-security calls are widespread.
- **Phone theft.** Snatch theft and robberies target phones in Mexico City and other major cities.
- **Express kidnapping.** Criminals use fake taxis and dating apps to target travelers.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Mexico.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Mexico Level 2, Exercise Increased Caution, citing crime, kidnapping or hostage-taking, terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Extortion using leaked data, express kidnapping, SIM-swap and bank-impersonation fraud, and phone theft are widespread, and nearshoring has brought many vendors into a high-extortion environment.
- **What would change this rating.** Raise to Level 3 if U.S. military action against cartels or retaliatory violence disrupts travel and business. Lower to Level 1 only on sustained declines in extortion and kidnapping.

Public Wi-Fi

- Extortion using leaked data and SIM-swap fraud are widespread; public Wi-Fi compounds risk of credential compromise used for extortion calls or account takeover. Use a corporate VPN on all public networks and avoid financial applications on public Wi-Fi.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Use hotel-arranged or app-based transport, and avoid hailing street taxis.
- Avoid areas flagged in the advisory, including parts of Sinaloa, Michoacan, Guerrero, Tamaulipas, and other states with severe cartel violence.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MICRONESIA, FEDERATED STATES OF

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Palikir

GOVERNMENT
Federal republic in free association with the United States

LANGUAGE
English (with eight indigenous languages)

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 7, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Very limited connectivity and low crime; government and aid staff may draw external interest.

Country Overview

The Federated States of Micronesia spans more than 600 islands across the western Pacific, grouped into four states: Chuuk, Kosrae, Pohnpei, and Yap. Navigators settled the islands thousands of years ago, and Spain, Germany, Japan, and then the United States administered them in turn. The islands became self-governing in 1979 and fully independent in 1986 under a Compact of Free Association with the United States.

The country has about 76,000 people and depends on compact funding, fishing license fees, and remittances. Wesley Simina has been president since 2023. Climate change, limited infrastructure, and great-power competition for influence in the Pacific are central issues.

Geopolitical Landscape

- **Compact relationship.** The United States provides defense, funding, and access under the compact, which is a major factor in Micronesia's alignment, and Washington has renewed the economic provisions.
- **Great-power competition.** China, the United States, Japan, and Australia compete for influence through infrastructure and security agreements.
- **Climate vulnerability.** Rising seas and storms threaten low-lying atolls.

Cyber Threats | Organizations

- **Minimal digital footprint.** Connectivity depends on a few subsea cable and satellite links, and local security capacity is very limited.
- **Regional diplomatic targeting.** Government and diplomatic networks in the Pacific draw external espionage interest.
- **Vendor concentration.** Telecom and IT services rely on a small set of external providers.
- **Employees based in country.** Employees face limited and costly connectivity and basic phishing risk. Government, aid, and defense-adjacent staff may draw external interest.
- **Vendor and supply chain risk.** A small set of external vendors supply connectivity and IT, so the loss of one provider or link can cause outages. Plan for offline operation.

The TIDE team does not currently track actors that list the Federated States of Micronesia among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Limited connectivity.** The state-owned FSM Telecommunications Corporation runs a monopoly 4G network with roughly 80 percent coverage; the East Micronesia Cable System became operational in January 2026, giving FSM its first submarine cable after decades of satellite dependence.
- **Phishing and fraud.** Romance and advance-fee scams circulate via social media; a March 2025 ransomware attack forced the Yap State Department of Health to shut down its systems, with no group claiming responsibility.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to the Federated States of Micronesia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates the Federated States of Micronesia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity is very limited and crime is low. Government, aid, and defense-adjacent staff may draw external interest.
- **What would change this rating.** Raise to Level 2 if great-power security arrangements increase targeting of local networks.

Public Wi-Fi

- The East Micronesia Cable System ended decades of satellite-only connectivity in January 2026, though redundancy remains limited; use a corporate VPN on public networks, which still carry standard phishing risk at hotels and resorts.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Carry offline copies of key documents, since connectivity is limited.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MOLDOVA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Chisinau

GOVERNMENT
Parliamentary republic

LANGUAGE
Romanian (called Moldovan in some contexts)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 7, 2026)

Risk indicators: Unrest, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Sustained Russia-linked influence and cyber operations, energy coercion, and a separatist region with separate surveillance risk.

Country Overview

Moldova is a landlocked country between Romania and Ukraine that was part of the historic region of Bessarabia. The Ottoman, Russian, and Romanian states ruled it in turn, and it became a Soviet republic in 1940. Moldova declared independence in 1991, and a short war in 1992 left the Russian-backed breakaway region of Transnistria outside government control.

Moldova has about 2.4 million people, is one of Europe's poorest countries, and relies on remittances and agriculture. It became an EU candidate in 2022, and accession talks opened in 2024. President Maia Sandu was reelected in 2024 in a vote marked by interference allegations.

Geopolitical Landscape

- **September 2025 election.** Sandu's pro-EU Party of Action and Solidarity won about 50 percent of the vote and roughly 55 of 101 seats in the September 28, 2025 election, keeping a single-party majority despite what observers called unprecedented Russian interference, including vote buying and influence operations. Opposition leaders alleged fraud.

- **Transnistria and energy.** Russia stopped gas supplies to Transnistria on January 1, 2025, which triggered an energy crisis, and about 1,500 Russian troops remain in the region. Moldova has been cutting its dependence on Russian gas.
- **EU path.** The government aims for an accession treaty by 2028 and EU membership by 2030.
- **Gagauzia.** The pro-Russian autonomous region of Gagauzia remains a source of political tension.

Cyber Threats | Organizations

- **Russia-linked influence and cyber operations.** Moldova faces sustained disinformation, vote-buying networks, phishing, and DDoS attacks, and government and energy bodies are priority targets.
- **Energy sector.** Gas, power, and grid operators are exposed to supply coercion and attacks as the country decouples from Russia.
- **Financial sector.** Banks face fraud and money-laundering scrutiny, and past large bank frauds shaped regulation.
- **Limited security capacity.** Public bodies and small firms rely on EU and partner support.
- **Employees based in country.** Employees face election-themed phishing and disinformation, and travel to Transnistria carries separate legal and surveillance risk. Government, energy, and media staff face elevated targeting.
- **Vendor and supply chain risk.** Energy suppliers, telecoms, and small IT vendors have limited security capacity and are exposed to Russia-linked targeting. Verify supplier controls and segment vendor access.

The TIDE team tracks 1 threat actor that lists Moldova among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Disinformation.** Politically themed false content spreads on Telegram, TikTok, and Facebook.
- **Phishing and impersonation.** Messages impersonating banks and authorities circulate in Romanian and Russian.
- **Monitoring risk in Transnistria.** Authorities in the breakaway region monitor communications.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Moldova.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Moldova Level 2, Exercise Increased Caution, citing unrest, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Sustained Russia-linked influence and cyber operations, energy coercion, and a breakaway region with its own surveillance practices drive the rating. Typical visitors face moderate risk.
- **What would change this rating.** Raise to Level 3 if the situation in Transnistria escalates or attacks on Moldovan infrastructure intensify. Lower to Level 1 as accession progresses and interference abates.

Public Wi-Fi

- Russia-linked disinformation and phishing campaigns target election-related communications; a breakaway region with separate surveillance practices creates additional legal and monitoring risk. Use a corporate VPN on all public networks and avoid travel to Transnistria.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid Transnistria unless necessary, since the U.S. government has limited ability to assist there.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MONACO

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Monaco

GOVERNMENT
Constitutional monarchy (principality)

LANGUAGE
French

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 28, 2025)

Risk indicators: Unrest, terrorism

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and low crime; exposure is targeted fraud against wealthy clients and spear-phishing of finance staff.

Country Overview

Monaco is a tiny principality on the Mediterranean coast, ruled by the Grimaldi family since 1297. It lies entirely within France, covers about two square kilometers, and has about 39,000 residents, most of them foreign nationals. France guarantees its defense under treaty.

Prince Albert II has reigned since 2005. Monaco's economy rests on banking, real estate, and luxury tourism, including its casino and the Grand Prix. It uses the euro and has a customs union with France but is not an EU member.

Geopolitical Landscape

- **Financial transparency.** Monaco has tightened anti-money-laundering rules and exchanged tax data under pressure from the OECD and Moneyval, and it was removed from the FATF grey list in 2024.
- **Reliance on France.** Security, customs, and much law enforcement depend on France.
- **Low geopolitical profile.** Monaco has no active disputes.

Cyber Threats | Organizations

- **Wealth-targeted fraud.** Private banks, family offices, and yacht and real estate firms hold high-value client data and face business email compromise, spear-phishing, and extortion.
- **Hospitality and events.** Hotels, casinos, and events such as the Grand Prix hold payment data and face fraud and DDoS.
- **Small-state resourcing.** Local security capacity is small, and firms rely on French and Italian vendors.
- **Employees based in country.** Employees face targeted payment fraud and spear-phishing, especially in banking and wealth-management roles. Everyday theft risk is low.
- **Vendor and supply chain risk.** Private banks and service providers rely on a handful of French and Italian technology vendors. Verify subcontractor controls for client data and require incident notification.

The TIDE team does not currently track actors that list Monaco among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Wealth-targeted social engineering.** Residents and visitors with high net worth face tailored fraud, romance scams, and extortion.
- **Card fraud.** Skimming and payment fraud target tourists.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Monaco.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Monaco Level 2, Exercise Increased Caution, citing unrest, terrorism. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Monaco is stable and low crime. Exposure is targeted fraud against wealthy clients and spear-phishing of finance staff.
- **What would change this rating.** Raise to Level 2 if targeted campaigns against Monaco's financial firms intensify.

Public Wi-Fi

- Wealth-management and finance professionals face spear-phishing and targeted payment fraud on public networks; crowds at events attract pickpockets. Use a corporate VPN for all public Wi-Fi, particularly in banking and wealth-management districts.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Crowds at events such as the Grand Prix attract pickpockets, so secure devices.

Return protocol

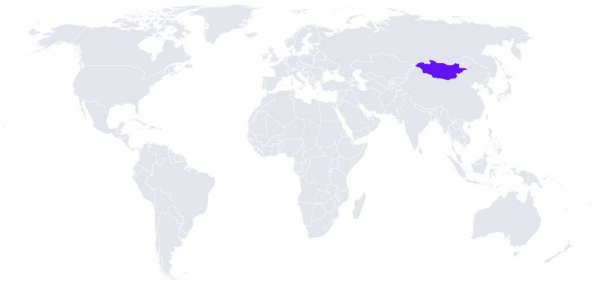
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MONGOLIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Ulaanbaatar

GOVERNMENT
Semi-presidential republic

LANGUAGE
Mongolian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 29, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is phone theft, phishing, and targeting of mining and government staff.

Country Overview

Mongolia is a vast, landlocked country between Russia and China, and the center of the empire Genghis Khan founded in 1206, which became the largest contiguous land empire in history. After the Mongol Empire fragmented, the region fell under Qing Chinese control, and Mongolia declared independence in 1911.

Mongolia became a Soviet satellite in 1924 and carried out a peaceful democratic revolution in 1990. It has about 3.6 million people, a large nomadic herding tradition, and a mining-driven economy based on coal, copper, and gold. Politically it has had frequent changes of government, including leadership turnover during 2025.

Geopolitical Landscape

- **Third neighbor policy.** Mongolia balances dependence on Russia and China, which together take nearly all its energy and exports, with outreach to the United States, Japan, South Korea, and the EU.
- **Political churn.** Protests over corruption and living costs and a series of prime ministerial changes in 2025 reflect volatile coalition politics.
- **Mining dependence.** Coal exports to China and the Oyu Tolgoi copper mine dominate revenue.
- **Russia gas pipeline.** Mongolia is a proposed transit route for Russia-China gas pipelines.

Cyber Threats | Organizations

- **Mining sector.** Operators and contractors hold valuable commercial data and face espionage and fraud.
- **State-linked targeting.** China-nexus and other regional actors target government, diplomatic, and mining networks.
- **Limited security capacity.** Public bodies and banks have thin security staffing.
- **Regulation.** Mongolia has a cyber security law and a personal data protection law, with limited enforcement capacity.
- **Employees based in country.** Employees face pickpocketing and phone theft in Ulaanbaatar and phishing. Mining and government-adjacent staff may draw state-linked targeting.
- **Vendor and supply chain risk.** Mining contractors and a few banks and telecoms carry most exposure, with thin local security capacity. Segment vendor access and verify payment-change requests out of band.

The TIDE team tracks 8 threat actors that list Mongolia among their targets. By attributed nexus, they break down as 8 China-nexus. The most frequently targeted sectors are government (7), defense and defense industrial base (3), technology (3), religious organizations (2), and aerospace (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and wallet fraud.** Mobicom, Unitel, and Skytel provide mobile service; bank and delivery impersonation circulates in Mongolian.
- **Phone theft.** Pickpocketing and phone snatching occur in Ulaanbaatar.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Mongolia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Mongolia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with phone theft, phishing, and role-based targeting of mining and government staff as the main exposure.
- **What would change this rating.** Raise to Level 2 if political instability or regional tension increases targeting of Mongolian networks.

Public Wi-Fi

- All of Mongolia's international internet traffic transits overland through Chinese and Russian carriers via the ERMC cable system, since the country has no direct ocean cable access; a satellite initiative (Steppe Road)

aims to reduce this dependence, but overland routes remain primary. Treat public Wi-Fi as subject to monitoring by both neighboring states, use a corporate VPN with a non-China, non-Russia endpoint, and carry offline maps and documents given that remote terrain and winter conditions can limit connectivity entirely.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Winter cold and remote terrain limit connectivity and rescue, so carry offline maps and power banks.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MONTENEGRO

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Podgorica

GOVERNMENT
Parliamentary republic

LANGUAGE
Montenegrin

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued August 27, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable NATO member; the 2022 national ransomware incident shows public-sector fragility, but visitor risk is low.

Country Overview

Montenegro is a small Balkan country on the Adriatic coast whose mountainous terrain helped it resist Ottoman conquest for centuries. It was an independent principality and kingdom before joining Yugoslavia after the First World War. After Yugoslavia's breakup, Montenegro stayed in union with Serbia until a 2006 referendum led to independence.

Montenegro joined NATO in 2017 and is a front-runner for EU membership, aiming to complete accession talks by 2028. It has about 620,000 people and an economy driven by tourism. Milojko Spajic has been prime minister since 2023.

Geopolitical Landscape

- **EU accession.** Montenegro is the most advanced candidate and is working to close negotiating chapters, with reforms of the judiciary and media a focus.
- **Serbia and Russia influence.** Pro-Serbian and Russia-friendly political currents and the influence of the Serbian Orthodox Church create political fault lines.
- **Organized crime.** Montenegro is a transit point for drug trafficking, and clan violence affects politics.

Cyber Threats | Organizations

- **2022 national cyberattack.** In August 2022 a cyberattack on several Montenegrin state bodies disrupted government services, and the defense minister said there was sufficient evidence to suspect Russia, which showed the exposure of small public sectors.
- **Hacktivism.** DDoS campaigns target government sites around political events.
- **Tourism and banking.** Hotels and banks hold payment data and face fraud and ransomware.
- **Regulation.** Montenegro is aligning with NIS2 and GDPR as part of accession.
- **Employees based in country.** Employees face phishing and coastal tourist fraud. Government-adjacent staff may draw state-linked targeting.
- **Vendor and supply chain risk.** Small public-sector and tourism vendors have limited security capacity, and the 2022 incident showed how a single compromise can disrupt many services. Require recovery and incident notification terms.

The TIDE team does not currently track actors that list Montenegro among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks and public agencies circulate in Montenegrin and English.
- **Tourist scams.** Fake rental listings and card skimming target visitors on the coast.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Montenegro.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Montenegro Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Montenegro is a stable NATO member, but the 2022 national ransomware incident shows public-sector fragility. Visitor risk is low.
- **What would change this rating.** Raise to Level 2 if Russia-linked attacks on Montenegrin institutions return.

Public Wi-Fi

- The 2022 national ransomware attack on government bodies shows public-sector fragility; government and tourist-area phishing remain active. Use a corporate VPN on all public Wi-Fi connections, especially in coastal tourist areas.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Summer coastal traffic and ferry delays are common, so confirm itineraries.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MOROCCO

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Rabat

GOVERNMENT
Constitutional monarchy

LANGUAGE
Arabic and Tamazight (French widely used)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 4, 2026)

Risk indicators: Terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Documented spyware use, a hack-and-leak rivalry with Algeria, legal risk for speech, and phone snatching in medinas.

Country Overview

Morocco is a North African kingdom with coasts on the Atlantic and the Mediterranean, shaped by Berber, Arab, and Andalusian cultures. The Idrisid, Almoravid, Almohad, and Alaouite dynasties ruled, and the Alaouites have held the throne since the seventeenth century. France and Spain established protectorates in 1912, and Morocco became independent in 1956.

King Mohammed VI has reigned since 1999 and holds broad powers. Morocco has about 37 million people and an economy built on agriculture, phosphates, automotive manufacturing, and tourism. It is co-hosting the 2030 World Cup.

Geopolitical Landscape

- **Western Sahara.** Morocco controls most of Western Sahara and proposes autonomy under its sovereignty, while the Polisario Front, backed by Algeria, seeks independence. A UN Security Council resolution in October 2025 backed autonomy as a basis for talks, which strengthened Rabat's position.
- **Gen Z protests.** Youth-led protests in September and October 2025 over health, education, and spending priorities drew a security response and arrests.

- **Algeria.** Relations with Algeria remain ruptured, with a closed border and rival alliances.
- **Foreign alignment.** Morocco normalized relations with Israel in 2020 and maintains close ties with the United States, France, and Gulf states.

Cyber Threats | Organizations

- **Hack-and-leak between rivals.** In 2025 attackers linked to Algeria leaked data from Morocco's national social security fund, and Moroccan and Algerian hacktivists exchange attacks.
- **State surveillance and spyware.** The 2021 Pegasus Project identified Morocco as one of ten countries where phone numbers were selected for possible Pegasus targeting, including those of journalists.
- **Financial and energy sectors.** Banks, phosphate producers, and renewable energy firms hold valuable data and face fraud and espionage.
- **Outsourcing sector.** Call-center and IT outsourcing firms hold client data for European firms.
- **Employees based in country.** Employees face impersonation fraud, phone snatching in medinas, and legal exposure for commentary on the monarchy or Western Sahara. Outsourcing and finance staff face elevated phishing.
- **Vendor and supply chain risk.** Call-center, IT outsourcing, and telecom vendors hold client data and sit in a hack-and-leak rivalry with Algeria. Require access controls, logging, and incident notification, and segment vendor access.

The TIDE team tracks 4 threat actors that list Morocco among their targets. By attributed nexus, they break down as 2 cybercriminal, 1 unattributed or other, and 1 Iran-nexus. The most frequently targeted sectors are government (3), banking and financial services (2), hospitality and travel (1), retail and e-commerce (1), and civil society and activism (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Criticism of the monarchy, religion, or territorial integrity can lead to prosecution, and journalists have been prosecuted.
- **Spyware targeting.** Activists and journalists are targets.
- **Fraud.** Bank and delivery impersonation scams circulate in Arabic and French.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Morocco.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Morocco Level 2, Exercise Increased Caution, citing terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Spyware has been documented against journalists and activists, a hack-and-leak rivalry with Algeria continues, speech about the monarchy carries legal risk, and phone snatching occurs in medinas.
- **What would change this rating.** Raise to Level 3 if surveillance of foreign business travelers or unrest increases. Lower to Level 1 as monitoring practices ease.

Public Wi-Fi

- Documented Pegasus spyware targeting, hack-and-leak rivalry with Algeria, and legal risk for speech create elevated surveillance and data theft risk on public networks. Use a corporate VPN on all public Wi-Fi, and outsourcing and finance staff should avoid public networks entirely.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid commentary on the monarchy and Western Sahara, and avoid demonstrations.
- Keep phones secured in crowded medinas, where snatch theft occurs.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

MOZAMBIQUE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Maputo

GOVERNMENT
Presidential republic

LANGUAGE
Portuguese

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 21, 2026)

Risk indicators: Unrest, crime, health, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Post-election repression and connectivity restrictions, northern insurgency, and mobile-money fraud.

Country Overview

Mozambique stretches along the southeast coast of Africa. Swahili and Arab traders and then Portugal, which colonized it for nearly five centuries, shaped the coast. Independence came in 1975 under the Frelimo movement, followed by a civil war with the Renamo rebels from 1977 to 1992 that killed about a million people.

Frelimo has governed since independence. Mozambique has about 35 million people and large natural gas reserves off its northern coast. Daniel Chapo became president in January 2025 after a disputed October 2024 election that triggered months of deadly protests.

Geopolitical Landscape

- **Post-election unrest.** Protests against the 2024 result were met with lethal force, and hundreds were reported killed. Chapo has sought dialogue while Frelimo retains dominance.
- **Cabo Delgado insurgency.** An Islamic State-linked insurgency has attacked northern Cabo Delgado province since 2017, displacing hundreds of thousands and delaying large gas projects.
- **Economic strain.** High debt and the effects of unrest and cyclones constrain growth.

Cyber Threats | Organizations

- **Gas and extractive sector.** LNG developers and contractors hold valuable data and operate under insurgent and political risk.
- **Connectivity restrictions.** Authorities restricted mobile internet and social media during the post-election protests.
- **Mobile money and banking.** M-Pesa and bank customers face SIM-swap and social engineering.
- **Limited local capacity.** Public bodies and banks have thin security staffing.
- **Employees based in country.** Employees face possible connectivity restrictions during unrest, mobile-money fraud, and phone theft in Maputo. Staff in the north face insurgency risk.
- **Vendor and supply chain risk.** Gas-project contractors, security firms, and telecom vendors operate under insurgent and political risk, and connectivity can be restricted abruptly. Segment vendor access and plan for outages.

The TIDE team tracks 2 threat actors that list Mozambique among their targets. By attributed nexus, they break down as 1 China-nexus, and 1 unattributed or other. The most frequently targeted sectors are banking and financial services (2), government (1), telecommunications (1), defense and defense industrial base (1), and diplomatic and foreign affairs (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and arrest.** Protesters, activists, and journalists faced arrest and intimidation.
- **Mobile money fraud.** SMS and wallet scams are common.
- **Phone theft.** Snatch theft occurs in Maputo.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Mozambique.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Mozambique Level 2, Exercise Increased Caution, citing unrest, crime, health, terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Post-election repression, connectivity restrictions during unrest, a northern insurgency, and mobile-money fraud drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest returns with shutdowns or insurgent attacks spread south. Lower to Level 1 as politics and security stabilize.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Post-election repression and connectivity restrictions, coupled with mobile-money fraud, make unsecured networks particularly risky, so use a corporate VPN if a public network is unavoidable.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid Cabo Delgado and demonstrations, and keep devices out of sight in Maputo traffic.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

NAMIBIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Windhoek

GOVERNMENT
Presidential republic

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 15, 2026)

Risk indicators: Crime, health

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is mobile-money fraud, opportunistic theft, and telecom incidents.

Country Overview

Namibia lies on Africa's southwestern coast and contains the Namib and Kalahari deserts. Germany colonized it as South West Africa in the 1880s and committed the Herero and Nama genocide in the early twentieth century, and South Africa then administered it until independence in 1990 after a long liberation struggle led by SWAPO.

Namibia has about 3 million people and one of the world's lowest population densities. The economy relies on mining, including diamonds and uranium, fishing, and tourism. Netumbo Nandi-Ndaitwah of SWAPO became its first woman president in March 2025. Large offshore oil discoveries and green hydrogen plans shape its outlook.

Geopolitical Landscape

- **New government.** Nandi-Ndaitwah won the November 2024 election, the first presidential election with notable opposition gains, and took office in March 2025.
- **Resource pipeline.** Offshore oil, uranium, and green hydrogen projects attract international investment and competition.
- **Germany reparations.** A joint declaration with Germany on the colonial genocide remains contested.

Cyber Threats | Organizations

- **Telecom data leak.** A ransomware attack on Telecom Namibia in late 2024 led to the leak of customer data, which illustrates exposure at national operators.
- **Mining and energy.** Diamond, uranium, and oil operators hold valuable data and face espionage and fraud.
- **Financial sector.** Banks and mobile wallets face phishing and account takeover.
- **Regulation.** Namibia is developing data protection and cybercrime laws.
- **Employees based in country.** Employees face mobile-money fraud and opportunistic theft in Windhoek. Mining and energy staff are higher-value targets for elicitation.
- **Vendor and supply chain risk.** Telecom operators, mining contractors, and logistics providers hold sensitive data, and the 2024 telecom leak shows supplier incidents can expose customers. Require incident notification and segment access.

The TIDE team does not currently track actors that list Namibia among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile money and impersonation fraud.** SMS and wallet scams are common.
- **Phone theft.** Opportunistic theft occurs in Windhoek and coastal towns.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Namibia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Namibia Level 2, Exercise Increased Caution, citing crime, health. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with mobile-money fraud, opportunistic theft, and telecom-sector incidents as the main exposure.
- **What would change this rating.** Raise to Level 2 if targeting of the energy and mining sector increases.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. The 2024 telecom ransomware attack and mobile-money fraud create targeted threat vectors on unsecured networks, so connect through a corporate VPN if a public network must be used.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Keep devices out of sight in vehicles, and carry offline maps for remote desert areas.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

NAURU

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Yaren (de facto)

GOVERNMENT
Presidential republic

LANGUAGE
Nauruan and English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued December 2, 2024)

Risk indicators: Health

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Single-cable connectivity and low crime; government and immigration-system staff may draw external interest.

Country Overview

Nauru is the world's smallest island republic, a single coral island of about 21 square kilometers in the central Pacific. Phosphate mining, started under German and then British, Australian, and New Zealand administration, stripped much of the island's interior. Nauru became independent in 1968.

The country has about 12,000 people and has relied on phosphate revenue, fishing license fees, and payments for hosting an Australian offshore immigration processing center. Nauru switched diplomatic recognition from Taiwan to China in January 2024, and the president is David Adeang, in office since October 2023.

Geopolitical Landscape

- **Australia dependence.** Australia provides budget support, security guarantees under a 2024 treaty, and migration processing revenue.
- **China switch.** Nauru's January 2024 switch to Beijing adds to great-power competition in the Pacific.
- **Passport sales.** A citizenship-by-investment program adopted in 2024 draws scrutiny over vetting.

Cyber Threats | Organizations

- **Minimal digital footprint.** Connectivity depends on one subsea cable and satellite links, and local security capacity is extremely limited.
- **Government and diplomatic targeting.** Pacific governments draw external espionage interest.
- **Identity data.** Citizenship and immigration systems hold sensitive personal data.
- **Employees based in country.** Employees face very limited connectivity and basic phishing risk, and staff linked to government or immigration processing may draw external interest.
- **Vendor and supply chain risk.** A single subsea cable and a few external vendors provide connectivity and IT, so outages are likely if one fails. Plan for offline operation.

The TIDE team does not currently track actors that list Nauru among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Limited connectivity.** Digicel Pacific provides mobile service, historically dependent on satellite links now being supplemented by the East Micronesia Cable System.
- **Investment scams.** Nauru's Financial Intelligence Unit warned of the BG Wealth Sharing and DSJ Exchange cryptocurrency schemes, which promised guaranteed returns and then restricted withdrawals once investors recruited others.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Nauru.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Nauru Level 1, Exercise Normal Precautions, citing health. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity depends on a single cable and crime is low. Government and immigration-system staff may draw external interest.
- **What would change this rating.** Raise to Level 2 if great-power competition increases targeting of Nauruan systems.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Nauru's near-total dependence on satellite and a single developing submarine cable means a compromise of that infrastructure affects all users, so use a corporate VPN if any public network is necessary.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Carry offline copies of key documents, since connectivity is limited.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

NEPAL

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Kathmandu

GOVERNMENT
Federal parliamentary republic

LANGUAGE
Nepali

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 4, 2026)

Risk indicators: Natural disaster

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Platform bans and volatile connectivity policy, mobile-wallet fraud, and protest disruption.

Country Overview

Nepal is a Himalayan country between India and China that contains eight of the world's ten highest peaks, including Mount Everest. The Shah dynasty unified it in the eighteenth century, and it was never colonized. A Maoist insurgency from 1996 to 2006 and the abolition of the monarchy in 2008 created a federal democratic republic.

Nepal has about 30 million people, relies on remittances and tourism, and has been governed by a long series of short-lived coalitions since becoming a republic. The economy is closely tied to India.

Geopolitical Landscape

- **2025 Gen Z uprising.** A government ban on 26 social media platforms in September 2025 triggered youth-led protests over corruption. Security forces shot protesters, and about 76 people were killed. Prime Minister KP Sharma Oli resigned on September 9, and former chief justice Sushila Karki led an interim government.
- **March 2026 election.** The Rastriya Swatantra Party led by former rapper and Kathmandu mayor Balendra Shah won 182 of 275 seats on March 5, 2026, and Shah was sworn in as prime minister on March 27, after defeating Oli in his own district.

- **India and China.** Nepal balances ties with its two neighbors, who compete for influence through trade and infrastructure.
- **Economy.** Unemployment drives millions of Nepalis to work abroad, and the new government has pledged job creation and anti-corruption action.

Cyber Threats | Organizations

- **Platform controls.** The 2025 social media ban shows authorities' willingness to restrict platforms and the volatility of connectivity policy.
- **Financial sector.** Banks and payment systems have suffered intrusions and fraud, and mobile wallets face account takeover.
- **Tourism and trekking.** Operators hold passport and payment data and face fraud.
- **Limited security capacity.** Public bodies have thin security staffing.
- **Employees based in country.** Employees face mobile-wallet fraud, tourist scams, and possible platform restrictions or protest disruption. Trekking staff face weather and altitude risk.
- **Vendor and supply chain risk.** Local banks, payment providers, and tour operators have thin security capacity, and platform restrictions can disrupt vendor communications. Verify payment changes out of band.

The TIDE team tracks 14 threat actors that list Nepal among their targets. By attributed nexus, they break down as 6 China-nexus, 3 India-nexus, 1 Russia-nexus, 1 Pakistan-nexus, 1 cybercriminal, 1 Lebanon-nexus, and 1 North Korea-nexus. The most frequently targeted sectors are government (11), military (6), defense and defense industrial base (5), diplomatic and foreign affairs (4), and education and research (4). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Platform and speech risk.** Online speech has led to arrests, and the government's approach to platform regulation is evolving.
- **Mobile wallet fraud.** SMS and wallet scams are common.
- **Tourist fraud.** Fake trekking and booking offers target visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Nepal.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Nepal Level 2, Exercise Increased Caution, citing natural disaster. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Platform bans and volatile connectivity policy, mobile-wallet fraud, and protest disruption drive the rating, with moderate risk to typical visitors.
- **What would change this rating.** Raise to Level 3 if unrest returns with shutdowns. Lower to Level 1 as the new government stabilizes policy.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. The 2025 social media ban and volatile platform controls, combined with mobile-wallet fraud, create unpredictable connectivity and targeted risks on open networks, so connect through a corporate VPN if a public network is unavoidable.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, and check monsoon and earthquake alerts.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

NETHERLANDS

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Amsterdam (the seat of government is The Hague)

GOVERNMENT
Parliamentary constitutional monarchy

LANGUAGE
Dutch

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 18, 2026)

Risk indicators: Terrorism

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; role-based exposure for semiconductor, logistics, and research staff.

Country Overview

The Netherlands is a low-lying country on the North Sea whose history is defined by its fight against flooding and its maritime trade. The Dutch revolted against Spanish Habsburg rule in the sixteenth century and founded the Dutch Republic, which became a global commercial power in the Golden Age. Napoleon's conquest led to the Kingdom of the Netherlands in 1815.

Germany occupied the country in the Second World War. The Netherlands is a founding member of NATO and the EU, hosts the International Criminal Court and the OPCW in The Hague, and has about 18 million people. Rotterdam is Europe's largest port. Rob Jetten became prime minister on February 23, 2026.

Geopolitical Landscape

- **New minority government.** Jetten's centrist D66 narrowly won the October 29, 2025 snap election, called after Geert Wilders' PVV left the previous coalition. D66, the CDA, and the VVD formed a minority cabinet with 66 of 150 seats, sworn in on February 23, 2026 after 117 days of talks. It must secure opposition support to pass laws.
- **Defense and Ukraine.** The Netherlands supports Ukraine strongly and is raising defense spending.

- **Chip export controls.** Dutch firm ASML makes the world's most advanced chip-making equipment, which places the Netherlands at the center of U.S.-China technology controls.
- **Hybrid threats.** Russian sabotage plots and drone activity have been reported in Europe.

Cyber Threats | Organizations

- **State-linked espionage.** Dutch authorities have repeatedly named Russia- and China-linked actors as threats, including a 2018 disrupted GRU operation against the OPCW, and technology, port, and research organizations are targeted.
- **Hacktivism and DDoS.** Pro-Russia groups launched DDoS attacks on Dutch government and municipal sites, including around NATO events.
- **Ransomware.** Hospitals, universities, municipalities, and logistics firms are frequent victims.
- **Data centers and ports.** Amsterdam is a major internet exchange and data center hub, and Rotterdam is a critical logistics node.
- **Regulation.** The Netherlands implements NIS2.
- **Employees based in country.** Employees face bank and delivery phishing and pickpocketing in Amsterdam. Staff in semiconductor, logistics, and research roles face elevated state-linked targeting.
- **Vendor and supply chain risk.** Semiconductor suppliers, port and logistics operators, and data center providers are high-value third parties and targets for state-linked actors. NIS2 extends security duties to suppliers, so require attestations and incident notification.

The TIDE team tracks 55 threat actors that list Netherlands among their targets. By attributed nexus, they break down as 29 cybercriminal, 9 China-nexus, 6 Iran-nexus, 4 Russia-nexus, 2 Turkey-nexus, 2 unattributed or other, 2 North Korea-nexus, and 1 hacktivist. The most frequently targeted sectors are healthcare and pharmaceuticals (30), government (29), industrial and manufacturing (22), education and research (20), and technology (20). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, DigiD, and delivery services are common.
- **Marketplace and rental fraud.** Fake listings and payment-link fraud affect buyers.
- **Bike and pickpocket theft.** Pickpocketing is common in Amsterdam tourist areas.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Netherlands.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Netherlands Level 2, Exercise Increased Caution, citing terrorism. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** The Netherlands is stable and well-regulated. Exposure is role-based, centered on semiconductor, logistics, and research staff targeted by state-linked actors.
- **What would change this rating.** Raise to Level 2 for staff in those sectors if state-linked targeting of travelers escalates.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. State-linked espionage targeting technology and research staff extends to public networks in Amsterdam and other hubs, so use a corporate VPN if a public network must be used.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Pickpocketing is common at Amsterdam Centraal, on trams, and at tourist sites.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

NEW ZEALAND

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Wellington

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English, Maori, and New Zealand Sign Language

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued April 29, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; exposure is scams, vehicle break-ins, and state-linked targeting of government and research staff.

Country Overview

New Zealand, known to Maori as Aotearoa, was settled by Polynesian voyagers around the thirteenth century. Britain annexed it after the 1840 Treaty of Waitangi, which remains a foundational and debated agreement between the Crown and Maori. It became a self-governing dominion in 1907 and fully independent in practice by the mid-twentieth century.

New Zealand has about 5.3 million people and an economy built on agriculture, tourism, and services. It is a member of the Five Eyes alliance and a nuclear-free state. Christopher Luxon has been prime minister since 2023, and a general election is due in late 2026.

Geopolitical Landscape

- **Election year.** A general election is due in late 2026, and cost of living and economic growth dominate the campaign.
- **Pacific and China.** New Zealand competes with China and Australia for influence in the Pacific while maintaining China as its largest trading partner.
- **Security alignment.** New Zealand is deepening defense ties with Australia and the United States while preserving its nuclear-free policy.

- **Natural hazards.** Earthquakes and severe weather affect infrastructure.

Cyber Threats | Organizations

- **State-linked espionage.** New Zealand's intelligence agencies have publicly attributed campaigns, including a 2024 advisory on China's APT40, and government, research, and Pacific-focused organizations are targeted.
- **Denial-of-service.** In July 2023 a Russian state-linked threat actor took the New Zealand Parliament's websites offline with a denial-of-service attack and cited New Zealand's support for Ukraine.
- **Supply chain.** Managed service and cloud providers are common routes into public bodies.
- **Regulation.** The Privacy Act requires breach notification, and cyber rules for critical infrastructure are evolving.
- **Employees based in country.** Employees face impersonation scams and vehicle break-ins at tourist sites. Staff in government, research, and Pacific-focused organizations may draw state-linked targeting.
- **Vendor and supply chain risk.** Managed service providers and cloud vendors serving public bodies are common compromise paths, as the 2022 incident showed. Require supplier attestations and incident notification.

The TIDE team tracks 16 threat actors that list New Zealand among their targets. By attributed nexus, they break down as 10 cybercriminal, 4 China-nexus, 1 unattributed or other, and 1 Iran-nexus. The most frequently targeted sectors are education and research (11), healthcare and pharmaceuticals (11), government (10), industrial and manufacturing (9), and technology (7). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Scams.** Investment, impersonation, and marketplace scams cause large losses.
- **Account takeover.** Credential theft targets banking and email.
- **Vehicle break-ins.** Thieves target tourist vehicles, so devices left in cars are often stolen.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to New Zealand.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates New Zealand Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** New Zealand is stable and well-regulated. Exposure is scams, vehicle break-ins, and state-linked targeting of government and research staff.
- **What would change this rating.** Raise to Level 2 if targeting of travelers or critical infrastructure increases.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. State-linked targeting of government and research staff, combined with vehicle break-in risks at tourist sites, make device security paramount on public networks, so connect through a corporate VPN if a public network is unavoidable.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Never leave devices in parked vehicles, since break-ins at trailheads and tourist sites are common.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

NICARAGUA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3

CAPITAL
Managua

GOVERNMENT
Presidential republic (authoritarian co-presidency)

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued May 14, 2026)

Risk indicators: Crime, health, wrongful detention, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Pervasive state monitoring, wrongful detention of foreign nationals, state-controlled telecoms, sanctions exposure, and a U.S. Level 3 advisory.

Country Overview

Nicaragua is the largest country in Central America, with lakes, volcanoes, and coasts on both the Pacific and the Caribbean. Spain colonized it in the sixteenth century, and independence followed in 1821. U.S. occupation in the early twentieth century and the long Somoza family dictatorship, overthrown by the Sandinista revolution in 1979, shaped its modern history.

A 1980s civil war pitted the Sandinista government against U.S.-backed Contras. Daniel Ortega lost power in 1990 and returned in 2007. His government has jailed or exiled opponents, closed independent media and thousands of non-governmental organizations, and stripped many critics of citizenship. A constitutional reform in January 2025 made his wife, Rosario Murillo, co-president. Nicaragua has about 6.9 million people.

Geopolitical Landscape

- **Authoritarian consolidation.** The Ortega-Murillo government controls the legislature, courts, and security forces, and the opposition has been dismantled. Rights groups report arbitrary detention and forced exile.

- **Sanctions and U.S. pressure.** The United States and other governments have imposed sanctions and trade measures on officials and sectors, and the State Department flags wrongful detention of U.S. citizens.
- **Russia and China.** Nicaragua has deepened ties with Russia and China, including security cooperation and a trade agreement with Beijing.
- **Migration.** Nicaragua has become a transit route for migrants moving north.

Cyber Threats | Organizations

- **State surveillance.** Security services monitor communications and online activity, and critics have faced prosecution for posts and contacts.
- **Sanctions exposure.** State-linked companies and officials are sanctioned, so vendor and counterparty screening is essential.
- **Control of telecoms and media.** The government controls much of the telecom and media sector.
- **Spyware.** Authorities monitor communications and online activity.
- **Employees based in country.** Staff should assume communications are monitored, avoid political content, and recognize that foreign nationals have been detained. Remove company access from personal devices before travel where policy requires.
- **Vendor and supply chain risk.** State-linked telecoms and companies can be compelled to share data, and many entities are sanctioned. Screen all vendors for ownership and sanctions exposure, and segment access.

The TIDE team tracks 2 threat actors that list Nicaragua among their targets. By attributed nexus, they break down as 1 unattributed or other, and 1 cybercriminal. The most frequently targeted sectors are energy (1), government (1), military (1), telecommunications (1), and banking and financial services (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and arrest.** Social media posts and messages critical of the government can lead to arrest, and foreigners have been detained.
- **Device checks.** Border and police officers have inspected phones.
- **Fraud.** Phishing and impersonation scams circulate in Spanish.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Nicaragua.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Nicaragua Level 3, Reconsider Travel, citing crime, health, wrongful detention, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions. The State Department flags the risk of wrongful detention of U.S. citizens.

TIDE Risk Level Rationale

- **Drivers.** Pervasive state monitoring, wrongful detention of foreign nationals, state-controlled telecoms, and sanctions exposure drive the rating, and the State Department rates Nicaragua Level 3.
- **What would change this rating.** Raise to Level 4 if detentions of foreign business travelers increase. Lower to Level 2 if monitoring and detention practices ease.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Pervasive state monitoring and state-controlled telecoms mean all communications are at risk, so do not use public Wi-Fi without a corporate VPN and assume that connectivity is monitored regardless.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

NIGER

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Niamey

GOVERNMENT
Military-led government

LANGUAGE
French (with Hausa, Zarma, and other national languages)

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued July 9, 2026)

Risk indicators: Unrest, crime, health, kidnapping or hostage-taking, terrorism

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Attacks and mutiny in the capital, junta control of connectivity and media, insurgent threat near strategic assets, and a U.S. Level 4 advisory.

Country Overview

Niger is a vast, landlocked Sahel country that is mostly Sahara. Trans-Saharan trade shaped Hausa, Tuareg, and Songhai states, and France colonized the territory, which became independent in 1960. Military coups in 1974, 1996, 1999, and 2010 and a 2023 coup mark a history of unstable rule.

General Abdourahamane Tiani seized power in July 2023 and ousted President Mohamed Bazoum. Niger has about 27.5 million people, one of the world's youngest and fastest-growing populations, and large uranium, oil, and gold resources. It ranks among the poorest countries.

Geopolitical Landscape

- **Jihadist attacks reach the capital.** Islamic State Sahel Province attacked the Niamey airport and military base on January 29, 2026, and the al-Qaeda affiliate JNIM claimed another attack on the airport in June. On August 29, 2026, mutinous soldiers attacked the airport and the presidency, briefly knocking state television off the air. Mass-casualty attacks on the army and civilians continue.

- **Break with the West.** The junta ended security cooperation with France and the United States, deepened ties with Russia, left ECOWAS, and formed the Alliance of Sahel States with Mali and Burkina Faso.
- **Uranium dispute.** Niger nationalized Orano's Somair mine in June 2025, reallocated former Orano and GoviEx permits to state-backed firms in August 2026, and faces legal challenges from Orano.
- **Benin tension.** Relations with Benin and the oil pipeline route have been disputed, though contacts resumed in 2026.

Cyber Threats | Organizations

- **Insecurity near strategic assets.** Attacks near the Niamey airport and uranium stockpiles show risk to logistics, mining, and aviation.
- **State control of connectivity and media.** Authorities have suspended media and restricted communications, and the junta controls the information environment.
- **Mining and oil.** Operators and contractors hold valuable data and face attack, extortion, and espionage.
- **Staff safety.** Leaks of staff, site, or convoy information can create direct physical risk.
- **Employees based in country.** Employees face connectivity restrictions, monitoring, attacks and mutiny risk in the capital, and physical danger if location data leaks. Remove company access from personal devices and keep movements confidential.
- **Vendor and supply chain risk.** Mining, logistics, security, and telecom vendors operate under junta and insurgent pressure and may lose access abruptly. Limit shared location data, segment vendor access, and plan for sudden loss of services.

The TIDE team tracks 1 threat actor that lists Niger among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Surveillance and detention.** Critics, journalists, and activists face arrest, and authorities monitor communications.
- **Mobile money fraud.** SMS and wallet scams are common.
- **Disinformation.** Pro-junta and pro-Russia narratives circulate widely.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Niger.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Niger Level 4, Do Not Travel, citing unrest, crime, health, kidnapping or hostage-taking, terrorism. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has very limited ability to assist, and attacks have reached the capital.

TIDE Risk Level Rationale

- **Drivers.** Attacks and a mutiny reached the capital in 2026, the junta controls connectivity and media, insurgents operate near strategic assets, and the State Department rates Niger Level 4.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require durable security in the capital and an end to communications restrictions.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Junta control of connectivity and communications, combined with proximity to insurgent threats and staff safety risks, means you should not rely on any public networks or VPN services that could expose your location.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

NIGERIA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Abuja

GOVERNMENT
Federal presidential republic

LANGUAGE
English (with Hausa, Yoruba, Igbo, and more than 500 other languages)

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued June 12, 2026)

Risk indicators: Unrest, crime, health, kidnapping or hostage-taking, terrorism

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Kidnapping risk, an extensive fraud ecosystem, episodic connectivity disruption, and a U.S. Level 3 advisory.

Country Overview

Nigeria is Africa's most populous country, with about 224 million people and hundreds of ethnic groups. The Hausa-Fulani Sokoto Caliphate, the Yoruba kingdoms, and the Igbo and other societies flourished before Britain colonized the area and merged it into a single territory in 1914. Nigeria became independent in 1960.

A civil war over Biafra from 1967 to 1970 killed about a million people, and military rule dominated until 1999. Nigeria is Africa's largest economy by some measures and its top oil producer, and its Lagos tech scene is a continental hub. Bola Tinubu has been president since May 2023.

Geopolitical Landscape

- **U.S. military cooperation.** After President Trump threatened action over attacks on Christians and designated Nigeria a Country of Particular Concern, the United States carried out strikes on Islamic State targets in Sokoto State on December 25, 2025, the first acknowledged U.S. combat action in Nigeria. About 200 U.S. personnel arrived in February 2026 for counterterrorism support. Tinubu said he consented, and critics worry about sovereignty and backlash.

- **Multiple insecurity crises.** Boko Haram and ISWAP attack in the northeast, banditry and kidnapping for ransom plague the northwest and Middle Belt, and farmer-herder violence persists.
- **2027 election.** Presidential and National Assembly elections are set for February 20, 2027, with campaigns starting in November 2026, and political tension is rising.
- **Economic reform.** Currency liberalization and removal of fuel subsidies have caused hardship and protests.

Cyber Threats | Organizations

- **Cybercrime ecosystem.** Nigeria hosts large romance, sextortion, and business email compromise networks, which creates insider and mule-account risk for banks, telecoms, and fintechs.
- **Fintech and banking.** Banks and fintech platforms face account takeover, SIM-swap, and large fraud, and the 2024 Nigeria Cybercrimes Act amendments created a levy and new enforcement.
- **Oil and gas.** Operators and contractors face theft, sabotage, and cyber espionage.
- **Internet restrictions.** Authorities blocked Twitter in 2021 and have throttled access during protests.
- **Employees based in country.** Employees face mobile and bank fraud, kidnapping risk on highways, and possible connectivity disruption during protests. Fintech and banking staff face insider-recruitment and social engineering pressure.
- **Vendor and supply chain risk.** Fintech, telecom, and outsourcing vendors sit next to an active fraud ecosystem, and compromised vendor mailboxes are routinely used to redirect payments. Require strong authentication, logging, and out-of-band verification of payment changes.

The TIDE team tracks 7 threat actors that list Nigeria among their targets. By attributed nexus, they break down as 2 cybercriminal, 2 China-nexus, 1 North Korea-nexus, 1 Iran-nexus, and 1 unattributed or other. The most frequently targeted sectors are government (5), telecommunications (3), defense and defense industrial base (2), military (2), and civil society and activism (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile and bank fraud.** SIM-swap, fake alerts, and social engineering are common.
- **Kidnapping.** Kidnapping for ransom affects travelers on highways and in some cities.
- **Monitoring and speech risk.** Cybercrime laws have been used to arrest critics and journalists.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Nigeria.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Nigeria Level 3, Reconsider Travel, citing unrest, crime, health, kidnapping or hostage-taking, terrorism. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Kidnapping risk, an extensive fraud ecosystem, episodic connectivity disruption, and the State Department's Level 3 advisory drive the rating.
- **What would change this rating.** Raise to Level 4 if violence or unrest intensifies around the 2027 election. Lower to Level 2 as security and fraud trends improve.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. An extensive cybercrime ecosystem and targeted social engineering of fintech and banking staff mean unsecured networks create significant fraud and infiltration risk, so use a corporate VPN if a public network is essential.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid the northeast, northwest, and other areas flagged in the advisory, and avoid road travel at night.
- Use hotel-arranged or armored transport where policy requires.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

NORTH KOREA

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4

CAPITAL
Pyongyang

GOVERNMENT
One-party state under a hereditary leadership (Democratic People's Republic of Korea)

LANGUAGE
Korean

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued April 29, 2025)

Risk indicators: Wrongful detention, other

Note: U.S. passports are not valid for travel to North Korea without a special validation, and the Department of State advises against all travel.

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Comprehensive state control and surveillance, wrongful detention risk, a U.S. passport restriction, and the world's most prolific state cyber-theft and fraudulent IT worker operations.

Country Overview

North Korea occupies the northern half of the Korean Peninsula, which was divided at the 38th parallel in 1945 after Japan's defeat. The Soviet-backed state led by Kim Il Sung was founded in 1948, and its invasion of South Korea in 1950 began the Korean War, which ended in a 1953 armistice rather than a peace treaty.

Kim Il Sung, his son Kim Jong Il, and since 2011 his grandson Kim Jong Un have ruled one of the world's most closed and militarized states, with about 26 million people, a command economy, and a nuclear weapons program. A 2024 treaty with Russia and the deployment of North Korean troops to fight in Ukraine have given it new revenue and diplomatic cover.

Geopolitical Landscape

- **Alliance with Russia.** North Korea signed a mutual defense treaty with Russia in June 2024 and sent troops to fight in Russia's war. The UK and others have sanctioned North Korean officials over the deployment, and delegations are exchanging visits on cooperation.

- **China.** China remains North Korea's economic lifeline, and Chinese state media said in June 2026 that Xi Jinping looks forward to talks with Kim.
- **Weapons programs.** North Korea continues to test missiles and engines and to expand nuclear production, and the United States and South Korea scheduled joint exercises for August 17 to 27, 2026.
- **Sanctions evasion.** Ten countries including the United States and South Korea urged the UN in May 2026 to designate vessels that violate sanctions, after the UN panel that monitored sanctions was disbanded in 2024.

Cyber Threats | Organizations

- **Cryptocurrency and financial theft.** North Korea has become the world's most prolific crypto thief. FBI attribution links the February 2025 Bybit theft of about 1.5 billion dollars to the Lazarus-linked TraderTraitor, and industry estimates credit North Korean actors with roughly 609 million dollars, about 55 percent of global crypto theft, in the first half of 2026, including an April 2026 theft of about 290 million dollars from KelpDAO.
- **Fraudulent IT workers.** North Korean operatives pose as remote IT contractors and employees to infiltrate companies worldwide, earn revenue for the state, and steal data. This is a hiring and vendor risk for any organization, wherever it operates.
- **Social engineering of crypto and defense firms.** Actors spend months posing as recruiters, investors, or trading firms, and even attend industry conferences in person.
- **No viable local presence.** Foreign organizations have almost no legitimate operations in North Korea.
- **Employees based in country.** Do not travel to or conduct business in North Korea. Employees anywhere should expect fake-recruiter and fake-investor approaches from North Korea-linked actors, especially in crypto, defense, and technology roles.
- **Vendor and supply chain risk.** Contractors and freelancers can be North Korean operatives using stolen or forged identities and proxy payments. Verify identity and location for remote vendors and developers, monitor for unusual access patterns, and screen payment recipients against sanctions.

The TIDE team tracks 2 threat actors that list North Korea among their targets. By attributed nexus, they break down as 1 unattributed or other, and 1 China-nexus. The most frequently targeted sectors are banking and financial services (2), defense and defense industrial base (2), diplomatic and foreign affairs (1), healthcare and pharmaceuticals (1), and electronics and semiconductors (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Total state surveillance.** Citizens use a closed national intranet, and foreign communications are tightly restricted and monitored.
- **Targeting of researchers and job seekers.** Kimsuky and Lazarus run credential phishing and fake job-offer campaigns against researchers, journalists, and developers worldwide.

State-Sponsored Cyber Threats

North Korea conducts cyber operations through the Reconnaissance General Bureau (RGB), which the U.S. Treasury has said controls Lazarus, BlueNoroff, and Andariel. The groups below carry public government or vendor attribution.

GROUP	ALSO KNOWN AS	ATTRIBUTED SPONSOR	FOCUS	ACTIVE
Lazarus Group	Hidden Cobra, Labyrinth Chollima, Diamond Sleet	Reconnaissance General Bureau (RGB), Lab 110	Financial theft, espionage, and destructive attacks	2009 to 2026
BlueNoroff	APT38, Stardust Chollima, Sapphire Sleet, TraderTraitor	RGB	Cryptocurrency and bank theft	2014 to 2026
Andariel	Silent Chollima, Onyx Sleet, Plutonium	RGB, 3rd Bureau	Espionage and ransomware for revenue	2009 to present
Kimsuky	APT43, Velvet Chollima, Black Banshee	RGB	Espionage and credential phishing	2012 to 2026
Konni	TA406, Vedalia, Opal Sleet	RGB (vendor assessment)	Espionage	2014 to present

Additional clusters, such as Famous Chollima and Moonstone Sleet, overlap with these groups under different names. This list excludes U.S. agencies by design.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates North Korea Level 4, Do Not Travel, citing the risk of wrongful detention, and U.S. passports are not valid for travel there without a special validation. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Comprehensive state control and surveillance, wrongful detention risk, a U.S. passport restriction, and the world's most prolific state cyber-theft and fraudulent IT-worker operations drive the rating. The defensive risk to organizations is global, not local.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require an opening of the country and an end to its state-run cyber theft, which is not in prospect.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Comprehensive state surveillance and control make all public networks monitored; VPN use is restricted or blocked in North Korea, so do not connect to any public Wi-Fi and rely exclusively on approved devices and the authorized connectivity plan.

Recommended corporate policy

- The TIDE team does not recommend any business travel to North Korea. Do not bring company or vendor devices or access company or vendor infrastructure.
- Treat any inbound approach from North Korea-linked recruiters, investors, or contractors elsewhere as a potential intrusion attempt.

Legal exposure

- North Korea is subject to comprehensive U.S., UN, and EU sanctions, so involve counsel on any engagement.

Return protocol

- Not applicable to travel, since the TIDE team does not recommend it. Apply the vendor and hiring checks above to defend against North Korean operatives.

WORLDBOOK

NORTH MACEDONIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Skopje

GOVERNMENT
Parliamentary republic

LANGUAGE
Macedonian (Albanian co-official in many areas)

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued September 10, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is phishing, marketplace fraud, and role-based targeting of government-adjacent staff.

Country Overview

North Macedonia is a landlocked Balkan country that was part of the Ottoman Empire until 1912 and then of Serbia and Yugoslavia. It declared independence in 1991 and avoided the wars of Yugoslavia's breakup, though an Albanian insurgency in 2001 ended with the Ohrid Agreement guaranteeing minority rights.

A long dispute with Greece over the country's name ended with the 2018 Prespa Agreement, and it joined NATO in 2020 as North Macedonia. It has about 1.8 million people and has been an EU candidate since 2005. Hristijan Mickoski has been prime minister since June 2024.

Geopolitical Landscape

- **EU stalemate.** Accession is blocked by a Bulgarian demand to amend the constitution to recognize a Bulgarian minority, and the government has resisted the change.
- **Corruption and tragedy.** A March 2025 nightclub fire in Kocani that killed at least 63 people exposed corruption in safety inspections and prompted protests.
- **Russian and regional influence.** The country is a target of disinformation and influence operations and has been the site of Russia-linked spying cases.

Cyber Threats | Organizations

- **Ransomware and fraud.** Public bodies and small firms face ransomware and phishing with limited security capacity.
- **Disinformation.** Politically charged false narratives spread on social media.
- **Banking.** Foreign-owned banks face fraud and account takeover.
- **Regulation.** North Macedonia is aligning with NIS2 and GDPR as part of accession.
- **Employees based in country.** Employees face phishing and marketplace fraud. Government-adjacent staff may draw state-linked targeting.
- **Vendor and supply chain risk.** Small local IT vendors and public-sector suppliers have limited security capacity. Verify supplier controls and incident notification terms.

The TIDE team does not currently track actors that list North Macedonia among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks and couriers circulate in Macedonian and Albanian.
- **Marketplace fraud.** Fake listings and payment-link scams affect buyers.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to North Macedonia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates North Macedonia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with phishing, marketplace fraud, and role-based targeting of government-adjacent staff as the main exposure.
- **What would change this rating.** Raise to Level 2 if Russia-linked targeting of institutions escalates.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Ransomware and phishing are common, and state-linked actors target government-adjacent staff, so connect through a corporate VPN if a public network must be used.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Hiking areas may have unmarked hazards, and mobile coverage is limited in mountains.

Return protocol

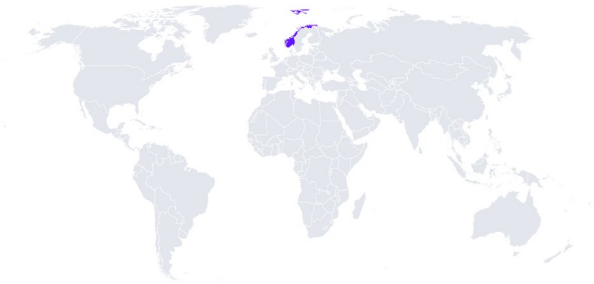
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

NORWAY

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Oslo

GOVERNMENT
Parliamentary constitutional monarchy

LANGUAGE
Norwegian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 6, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; exposure is role-based targeting in energy and defense and pro-Russia attacks on small utilities.

Country Overview

Norway is a Scandinavian country with a long Atlantic coastline and fjords. Viking-age kings unified the kingdom, and Norway later fell under Danish and then Swedish rule before becoming fully independent in 1905. Germany occupied it from 1940 to 1945.

Norway discovered oil in 1969 and built the world's largest sovereign wealth fund. It has about 5.6 million people, is a NATO founding member, and is not an EU member but is in the European Economic Area. Jonas Gahr Store has been prime minister since 2021, and his Labour party won the September 2025 election.

Geopolitical Landscape

- **Arctic and energy security.** Norway is Europe's main gas supplier after Russia's pivot away from Europe and shares a border and Arctic waters with Russia, and it has raised defense spending.
- **Undersea infrastructure.** Cable and pipeline protection in the North Sea and Arctic is a national priority.
- **Ukraine support.** Norway is among Ukraine's leading per-capita donors.
- **Domestic politics.** A stable center-left government continues after the 2025 election.

Cyber Threats | Organizations

- **Pro-Russia sabotage of industrial control systems.** In April 2025 attackers took control of a dam's valve in western Norway, and Norwegian security authorities later attributed the incident to pro-Russian attackers.
- **State-linked espionage.** Russia- and China-linked actors target government, defense, energy, and shipping, and a 2020 attack on parliament email was attributed to Russia.
- **Energy sector.** Oil and gas operators and suppliers are priority targets.
- **Regulation.** Norway applies NIS-based rules through the EEA.
- **Employees based in country.** Employees face BankID and parcel phishing. Staff in energy, defense, and shipping may draw state-linked targeting.
- **Vendor and supply chain risk.** Energy-sector suppliers and operators of industrial control systems are priority targets, and the 2025 dam incident showed exposure of small utilities. Require segmentation, remote-access controls, and incident notification.

The TIDE team tracks 18 threat actors that list Norway among their targets. By attributed nexus, they break down as 10 China-nexus, 5 cybercriminal, and 3 Russia-nexus. The most frequently targeted sectors are government (14), defense and defense industrial base (10), technology (8), healthcare and pharmaceuticals (8), and aerospace (7). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, BankID, and delivery services are common.
- **Marketplace fraud.** Fake listings and payment scams affect buyers.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Norway.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Norway Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Norway is stable and well-regulated. Exposure is role-based targeting in energy and defense and pro-Russia attacks on small utilities.
- **What would change this rating.** Raise to Level 2 for energy and defense staff if state-linked or sabotage activity escalates.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Pro-Russia sabotage of industrial systems and state-linked espionage targeting energy and defense staff create elevated targeting risk, so use a corporate VPN if a public network is necessary.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Remote Arctic areas have limited coverage and harsh weather, so carry offline maps.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

OMAN

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Muscat

GOVERNMENT
Absolute monarchy (Sultanate)

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 30, 2026)

Risk indicators: Terrorism, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Regional escalation after the Iran war, state monitoring of speech, Iran-linked targeting, and a U.S. Level 3 advisory.

Country Overview

Oman lies on the southeastern edge of the Arabian Peninsula and was a major maritime trading power with East Africa and India. The Al Said dynasty has ruled since the eighteenth century. Sultan Qaboos modernized the country after taking power in 1970 and ruled until his death in 2020.

Sultan Haitham bin Tariq has reigned since 2020. Oman has about 5.4 million people, oil and gas resources, and a tradition of neutral diplomacy that has made it a mediator between Iran and the West.

Geopolitical Landscape

- **Iran war and mediation.** Oman mediated the U.S.-Iran talks that failed in February 2026 before the United States and Israel struck Iran on February 28. Gulf states faced Iranian missile and drone strikes during the war, and the State Department rates Oman Level 3 in an advisory updated on August 30, 2026.
- **Houthis.** Yemen's Houthis border Oman, which has served as a communication channel with them.
- **Economic reform.** Oman is pursuing diversification under Vision 2040 and fiscal consolidation.

Cyber Threats | Organizations

- **Iran-linked and regional targeting.** Energy, government, and finance organizations draw Iran-linked and other regional actor interest, particularly during escalations.
- **State monitoring.** Authorities monitor communications and prosecute online criticism of the sultan and religion.
- **Energy sector.** Oil and gas operators and contractors run industrial systems that regional actors have probed.
- **Financial sector.** Banks face phishing and fraud.
- **Employees based in country.** Employees should assume communications are monitored, expect regional escalation to disrupt flights and airspace, and avoid political content online. Energy, finance, and government staff face elevated Iran-linked phishing.
- **Vendor and supply chain risk.** Gulf-wide telecoms and managed service providers can be disrupted during regional escalations, and energy contractors face elevated state-actor targeting. Segment vendor access and plan for airspace and connectivity disruption.

The TIDE team tracks 4 threat actors that list Oman among their targets. By attributed nexus, they break down as 2 cybercriminal, 1 Iran-nexus, and 1 unattributed or other. The most frequently targeted sectors are government (3), education and research (2), healthcare and pharmaceuticals (2), industrial and manufacturing (2), and defense and defense industrial base (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Criticism of the sultan, religion, or government online can lead to prosecution.
- **VoIP restrictions.** Some voice-over-IP services face restrictions.
- **Fraud.** Bank and delivery impersonation circulates in Arabic and English.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Oman.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Oman Level 3, Reconsider Travel, citing terrorism, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Regional escalation after the Iran war, state monitoring of speech, Iran-linked targeting, and the State Department's Level 3 advisory drive the rating.
- **What would change this rating.** Raise to Level 4 if hostilities reach Omani territory or airspace closes. Lower to Level 2 if U.S.-Iran de-escalation holds.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. State monitoring of communications and Iran-linked targeting during regional escalations mean unsecured networks are particularly risky, so connect through a corporate VPN if a public network must be used.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid the Yemen border area flagged in the advisory.

Return protocol

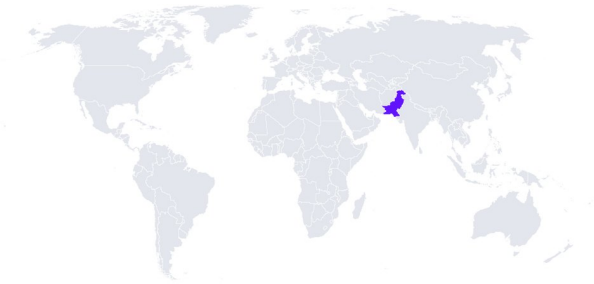
- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

PAKISTAN

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Islamabad

GOVERNMENT
Federal parliamentary republic with a dominant military

LANGUAGE
Urdu and English (with Punjabi, Sindhi, Pashto, and others)

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued June 16, 2026)

Risk indicators: Terrorism, crime, kidnapping or hostage-taking, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Terrorism and kidnapping risk, an active conflict with Afghanistan, internet throttling and platform blocks, state monitoring, and a U.S. Level 3 advisory.

Country Overview

Pakistan lies where South Asia meets Central Asia and the Middle East and is home to the ancient Indus Valley civilization. It was created in 1947 as a homeland for Muslims when British India was partitioned, and East Pakistan broke away as Bangladesh after the 1971 war with India.

Military governments ruled for much of Pakistan's history, and the army remains the dominant institution. Pakistan has about 242 million people, nuclear weapons, and a fragile economy supported by IMF programs. Imran Khan, prime minister until 2022, has been jailed since 2023.

Geopolitical Landscape

- **War with Afghanistan.** Pakistan and the Afghan Taliban have been in open confrontation in 2026. Pakistan launched Operation Ghazab lil Haq on February 26 and has conducted repeated airstrikes in Afghan provinces, including strikes in late September after drone incidents and a September 18 suicide attack. Pakistan accuses Kabul of sheltering the Tehrik-e-Taliban Pakistan (TTP), which the Taliban denies. A Pakistani research center counted 385 violent incidents and 1,415 deaths in the third quarter of 2026, the sharpest rise in nearly five years.

- **Mediator in the Iran conflict.** Pakistan mediated the April 2026 U.S.-Iran ceasefire and hosted talks in Islamabad, and it remains a channel between Washington and Tehran.
- **India.** Pakistan and India fought a four-day conflict in May 2025 and remain hostile.
- **Domestic politics.** Military dominance, jailed opposition leaders, and constitutional changes strengthen the army's role.

Cyber Threats | Organizations

- **State monitoring and internet controls.** Authorities have throttled the internet, blocked platforms including X for long periods, and expanded surveillance, and a firewall has been built to filter traffic.
- **Terrorism and physical risk.** Militant attacks affect infrastructure, security forces, and civilians, and kidnapping occurs.
- **Regional espionage and ransomware.** India-nexus and China-nexus groups target government and military networks, and banks and telecoms face ransomware and fraud.
- **IT outsourcing.** Pakistan has a large IT services sector that holds client data for overseas firms.
- **Employees based in country.** Employees face terrorism and kidnapping risk, internet throttling and platform blocks, monitoring of communications, and mobile-wallet fraud. Remove company access from personal devices where policy requires.
- **Vendor and supply chain risk.** IT outsourcing and call-center vendors hold client data and operate under state internet controls and security pressure. Segment vendor access, require logging and incident notification, and plan for connectivity disruption.

The TIDE team tracks 29 threat actors that list Pakistan among their targets. By attributed nexus, they break down as 9 China-nexus, 5 India-nexus, 5 unattributed or other, 4 cybercriminal, 3 Iran-nexus, 1 Russia-nexus, 1 Pakistan-nexus, and 1 Lebanon-nexus. The most frequently targeted sectors are government (22), defense and defense industrial base (10), telecommunications (9), diplomatic and foreign affairs (8), and education and research (7). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and speech risk.** Cybercrime laws have been used against critics, journalists, and activists, and platform blocks and VPN restrictions are common.
- **Mobile wallet fraud.** Fake agent, OTP, and prize scams affect users of JazzCash and Easypaisa.
- **Phone theft.** Snatch theft occurs in Karachi and Lahore.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors that carry a public government attribution to Pakistan. Security vendors track Pakistan-nexus espionage clusters that target India, listed below, but Pakistan does not acknowledge them.

GROUP	ALSO KNOWN AS	ATTRIBUTED SPONSOR	FOCUS	ACTIVE
Transparent Tribe	APT36, C-Major, Mythic Leopard, Earth Karkaddan	Pakistan-nexus; no government attribution	Espionage against Indian government and military	2013 to 2026
Gorgon Group	Subaat	Pakistan-nexus; no government attribution	Espionage and financially motivated activity	2017 to 2020

Pakistan is itself targeted by India-nexus actors, which TIDE tracking lists under India.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Pakistan Level 3, Reconsider Travel, citing terrorism, crime, kidnapping or hostage-taking, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Terrorism and kidnapping risk, an active conflict with Afghanistan, internet throttling and platform blocks, state monitoring, and the State Department's Level 3 advisory drive the rating.
- **What would change this rating.** Raise to Level 4 if the conflict with Afghanistan or militant violence reaches major cities or the capital. Lower to Level 2 if a durable ceasefire holds.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Internet throttling and state surveillance create both connectivity and targeting risk, and mobile-wallet fraud is endemic, so use a corporate VPN if a public network is unavoidable.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid the Afghan border areas, Balochistan, and Khyber Pakhtunkhwa areas flagged in the advisory, and avoid demonstrations.
- Use hotel-arranged or armored transport where policy requires.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

PALAU

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Ngerulmud

GOVERNMENT
Presidential republic in free association with the United States

LANGUAGE
Palauan and English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued January 7, 2026)

Risk indicators: Health, other

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Very limited connectivity and low crime; government and diplomatic staff may draw state-linked targeting.

Country Overview

Palau is a Pacific archipelago of about 340 islands, known for its marine reserves and diving. Spain, Germany, Japan, and the United States administered it in turn. Palau became independent in 1994 under a Compact of Free Association with the United States.

The country has about 17,000 people and depends on tourism and U.S. compact funds. Surangel Whipps Jr. has been president since January 2021 and was reelected in 2024. Palau is one of the few countries that recognize Taiwan.

Geopolitical Landscape

- **Taiwan recognition.** Palau maintains diplomatic ties with Taiwan, which exposes it to pressure from Beijing.
- **U.S. security role.** The compact gives the United States defense responsibility, and the United States has been developing radar and training facilities in Palau.
- **Climate and tourism.** Rising seas and reliance on visitors shape policy.

Cyber Threats | Organizations

- **Chinese pressure and targeting.** Palau recognizes Taiwan, which exposes it to pressure from Beijing, and government and diplomatic networks in the Pacific draw external espionage interest.
- **Minimal digital footprint.** Connectivity depends on a few subsea cable and satellite links, and local security capacity is limited.
- **Tourism sector.** Hotels and dive operators hold payment and passport data.
- **Employees based in country.** Employees face limited connectivity and basic phishing risk. Government, diplomatic, and defense-adjacent staff may draw state-linked targeting.
- **Vendor and supply chain risk.** A few external vendors provide connectivity and IT, so a single compromise or outage can disrupt services. Plan for offline operation and require incident notification.

The TIDE team does not currently track actors that list Palau among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Limited connectivity.** The state-owned PNCC (branded PalauCel) runs the mobile network over the Palau Cable 1 subsea link, operational since 2017.
- **Phishing and scams.** Palau's Financial Intelligence Unit and Office of the Special Prosecutor warned in 2025 and 2026 of a surge in social-media investment and romance scams, including AI-generated deepfakes and a fake financial-regulator website.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Palau.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Palau Level 1, Exercise Normal Precautions, citing health, other. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity is very limited and crime is low. Government and diplomatic staff may draw state-linked targeting.
- **What would change this rating.** Raise to Level 2 if Chinese pressure or attacks on Palauan systems increase.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Palau's government has suffered a documented string of attacks: a March 2024 ransomware incident disabled the Ministry of Finance's payroll system for weeks (President Whipps said investigators traced it to Malaysia, with possible Russia or China links), and separate ransomware incidents hit the Bureau of Customs and Border

Protection, the National Development Bank, and the Ministry of Health through early 2025. Connect through a corporate VPN if a public network is necessary.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Carry offline copies of key documents, since connectivity is limited.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

PANAMA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Panama City

GOVERNMENT
Presidential republic

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 19, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Card fraud, phone theft, strategic canal and logistics targeting, and strike disruption.

Country Overview

Panama links North and South America and is home to the Panama Canal, which opened in 1914 and carries a significant share of global shipping. Spain colonized the isthmus, and Panama split from Colombia in 1903 with U.S. backing. The United States ran the canal zone until a 1977 treaty returned the canal to Panama on December 31, 1999.

A U.S. invasion in 1989 removed dictator Manuel Noriega. Panama has about 4.1 million people and a service economy built on the canal, banking, and logistics. Jose Raul Mulino has been president since July 2024.

Geopolitical Landscape

- **Canal politics.** President Trump has pressed Panama over Chinese influence near the canal, and Panama withdrew from China's Belt and Road initiative in 2025. A deal for a Hong Kong-based company to sell ports on the canal drew scrutiny from Beijing and Washington.
- **Social unrest.** Protests over social security reform and mining policy in 2025 led to strikes and road blockades.
- **Darien Gap.** Migration through the jungle has fallen sharply since 2024.

- **Financial center.** Panama's offshore sector has faced scrutiny after the Panama Papers leak.

Cyber Threats | Organizations

- **Canal and logistics.** The canal authority, ports, and shipping firms hold valuable operational data and are targets for espionage and ransomware.
- **Financial and legal sector.** Banks and corporate service providers hold sensitive client data, which makes them prime targets for exfiltration and extortion.
- **Government incidents.** Public bodies have experienced ransomware and data theft.
- **Regulation.** Panama has a data protection law in force since 2021.
- **Employees based in country.** Employees face card fraud, phone theft in Panama City, and strike-related disruption. Staff in logistics, finance, and legal services face elevated targeted phishing.
- **Vendor and supply chain risk.** Law firms, corporate service providers, and logistics vendors hold sensitive data, and a single vendor breach can expose many clients. Require access controls, logging, and incident notification.

The TIDE team tracks 4 threat actors that list Panama among their targets. By attributed nexus, they break down as 2 cybercriminal, 1 unattributed or other, and 1 China-nexus. The most frequently targeted sectors are banking and financial services (3), healthcare and pharmaceuticals (3), government (2), hospitality and travel (2), and energy (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and card fraud.** Bank impersonation and card skimming are common.
- **Phone theft.** Snatch theft occurs in Panama City.
- **Express kidnapping.** Criminals use fake taxis in some areas.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Panama.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Panama Level 2, Exercise Increased Caution, citing crime. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Card fraud, phone theft, strategic targeting of canal and logistics firms, and strike disruption drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest or targeted attacks on canal operators escalate. Lower to Level 1 as crime and disruption decline.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Card fraud and phone theft are common, and strategic targeting of canal and logistics firms occurs over public networks, so use a corporate VPN if a public network must be used.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Use app-based or hotel-arranged transport, and avoid walking at night in flagged areas.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

PAPUA NEW GUINEA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Port Moresby

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English, Tok Pisin, and Hiri Motu (over 800 languages)

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued April 29, 2025)

Risk indicators: Unrest, crime, health, kidnapping or hostage-taking, natural disaster, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Violent crime and insecurity, limited connectivity, platform-restriction precedent, and a U.S. Level 3 advisory.

Country Overview

Papua New Guinea occupies the eastern half of the island of New Guinea and nearby islands, and it is among the world's most linguistically diverse countries. Germany and Britain divided the territory, Australia administered it, and it became independent in 1975.

The country has about 10.2 million people, rich resources in gold, copper, and natural gas, and widespread poverty. James Marape has been prime minister since 2019. A peace deal ended a civil conflict in Bougainville, which is now moving toward independence.

Geopolitical Landscape

- **Bougainville.** Bougainville voted overwhelmingly for independence in a 2019 referendum, and negotiations continue with Port Moresby over the process.
- **Australia security treaty.** Australia and Papua New Guinea have been negotiating a defense and security treaty amid regional competition with China.
- **Tribal and political violence.** Clan violence in the Highlands and deadly riots in Port Moresby in 2024 are recurring risks.

- **Resources.** Gas and mining projects shape revenue and relations with foreign investors.

Cyber Threats | Organizations

- **Limited digital footprint.** Connectivity is limited and costly, and security capacity is thin.
- **Platform restrictions.** Authorities tested a ban on Facebook in 2025, showing willingness to restrict platforms.
- **Mining and gas.** Operators and contractors hold valuable data and operate in insecure areas.
- **Staff safety.** Leaks of location data can create physical risk.
- **Employees based in country.** Employees face violent crime risk, connectivity gaps, and possible platform restrictions. Staff at mining and gas sites face insecurity and kidnapping risk.
- **Vendor and supply chain risk.** Mining, security, and telecom vendors operate in insecure areas with thin connectivity and can lose access abruptly. Limit shared location data and plan for outages.

The TIDE team does not currently track actors that list Papua New Guinea among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Violent crime.** Robbery and carjacking are common in Port Moresby and Lae.
- **Mobile and wallet fraud.** SMS and wallet scams exist.
- **Platform and speech risk.** Authorities have threatened action over social media content.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Papua New Guinea.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Papua New Guinea Level 3, Reconsider Travel, citing unrest, crime, health, kidnapping or hostage-taking, natural disaster, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Violent crime and insecurity, limited connectivity, a precedent of platform restrictions, and the State Department's Level 3 advisory drive the rating.
- **What would change this rating.** Raise to Level 4 if violence in the capital or highlands escalates. Lower to Level 2 as security and connectivity improve.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Violent crime, limited connectivity, and a precedent of platform restrictions mean device security is critical; use a corporate VPN if a public network is unavoidable and avoid revealing location data.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Use secure transport arranged by your employer, and avoid walking at night.
- Avoid areas flagged in the advisory, including parts of the Highlands.

Return protocol

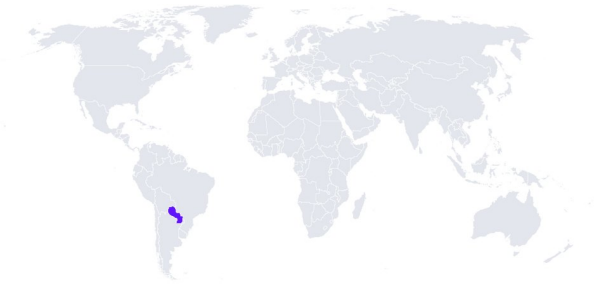
- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

PARAGUAY

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Asuncion

GOVERNMENT
Presidential republic

LANGUAGE
Spanish and Guarani

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued August 19, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is wallet fraud, phone theft, and counterparty risk near organized crime.

Country Overview

Paraguay is a landlocked South American country where Guarani culture and language remain central. Spain colonized it, and independence came in 1811. The War of the Triple Alliance from 1864 to 1870 devastated the country, and General Alfredo Stroessner ruled from 1954 to 1989.

Paraguay has about 6.1 million people and an economy built on agriculture, hydropower from the Itaipu and Yacyreta dams, and soy and beef exports. The Colorado Party dominates politics, and Santiago Pena has been president since 2023.

Geopolitical Landscape

- **Taiwan alliance.** Paraguay is one of the few countries that recognize Taiwan, and Beijing has pressed it to switch.
- **Organized crime.** The Tri-Border Area with Argentina and Brazil and groups such as the PCC use Paraguay for smuggling and money laundering.
- **Itaipu pricing.** Energy pricing under the Itaipu treaty has been a recurring source of friction with Brazil.

Cyber Threats | Organizations

- **Ransomware and fraud.** Public bodies and firms have limited security capacity and have faced ransomware and phishing.
- **Illicit finance.** Money laundering and smuggling networks create counterparty risk for financial and logistics vendors.
- **Energy sector.** Hydropower operators and utilities are strategic targets.
- **Employees based in country.** Employees face phishing and wallet fraud and phone theft in Asuncion. Logistics and finance staff face counterparty and fraud risk.
- **Vendor and supply chain risk.** Logistics, customs brokers, and money-service vendors operate near organized-crime networks, and public-sector suppliers have thin security. Screen counterparties and require incident notification.

The TIDE team tracks 1 threat actor that lists Paraguay among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and wallet fraud.** Bank and wallet impersonation scams are common in Spanish and Guarani.
- **Phone theft.** Snatch theft occurs in Asuncion.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Paraguay.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Paraguay Level 1, Exercise Normal Precautions, citing crime. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with wallet fraud, phone theft, and counterparty risk near organized crime as the main exposure.
- **What would change this rating.** Raise to Level 2 if organized-crime violence or targeting of Paraguayan institutions increases.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Organized-crime networks and wallet fraud create counterparty and financial risk, so connect through a corporate VPN if a public network must be used.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Avoid the border areas flagged in the advisory, and keep devices out of sight in traffic.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

PERU

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Lima

GOVERNMENT
Presidential republic

LANGUAGE
Spanish, Quechua, and Aymara

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 4, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Extortion using leaked data, phone snatching, wallet fraud, and mining-corridor disruption.

Country Overview

Peru was the heart of the Inca Empire, which Spain conquered in 1532, and Lima became the center of the Spanish viceroyalty in South America. Peru declared independence in 1821. Military coups, the Shining Path insurgency of the 1980s and 1990s, and Alberto Fujimori's authoritarian rule shaped recent history.

Peru has about 34 million people and is a leading producer of copper, gold, and silver, with a major new Chinese-built port at Chancay. Political instability has been extreme, with nine presidents in ten years. Keiko Fujimori took office on July 28, 2026.

Geopolitical Landscape

- **New president.** Fujimori, the daughter of Alberto Fujimori, won the June 7, 2026 runoff over leftist Roberto Sanchez by fewer than 50,000 votes after losing three earlier runoffs, and was proclaimed on July 3 and inaugurated on July 28. She succeeds interim president Jose Maria Balcazar, who took office in February. She has vowed to combat a wave of crime and faces a divided country.
- **U.S. and China.** Peru must balance the Trump administration with China, its largest trade partner, which operates the Chancay port.

- **Institutional change.** A Senate was restored in 2026 to the legislature to reduce the frequency of impeachments.
- **Crime and extortion.** Extortion by gangs against transport workers, businesses, and residents has surged.

Cyber Threats | Organizations

- **Extortion and doxxing.** Gangs use stolen personal data to threaten businesses and staff.
- **Mining sector.** Copper and gold operators and contractors hold valuable data and face espionage, protest-related disruption, and ransomware.
- **Financial sector.** Banks and the Yape and Plin wallets face SIM-swap, account takeover, and social engineering.
- **Ports and logistics.** The Chancay port and Callao handle strategic trade and attract foreign state interest.
- **Employees based in country.** Employees face extortion calls, phone snatching in Lima, wallet fraud, and protest-related disruption on mining corridors. Managers and business owners are priority extortion targets.
- **Vendor and supply chain risk.** Mining contractors, transport, and security vendors face extortion and can leak staff and route data. Vet vendor staff, limit shared personal data, and verify payment changes out of band.

The TIDE team tracks 10 threat actors that list Peru among their targets. By attributed nexus, they break down as 7 cybercriminal, 2 China-nexus, and 1 unattributed or other. The most frequently targeted sectors are government (7), banking and financial services (5), healthcare and pharmaceuticals (4), industrial and manufacturing (4), and technology (4). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Extortion and virtual kidnapping.** Callers claim to hold relatives and demand payment, often with leaked data.
- **Phone theft.** Snatch theft is common in Lima, often by thieves on motorbikes.
- **Wallet fraud.** Fake QR and transfer scams exploit Yape and Plin.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Peru.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Peru Level 2, Exercise Increased Caution, citing unrest, crime, kidnapping or hostage-taking, terrorism, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Extortion using leaked data, phone snatching, wallet fraud, and mining-corridor disruption drive the rating. A new government took office on July 28, 2026.

- **What would change this rating.** Raise to Level 3 if unrest or extortion violence escalates after the transition. Lower to Level 1 as crime declines.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Extortion rings use leaked personal data, and phone snatching is common in Lima, making unsecured networks a vector for social engineering and fraud, so use a corporate VPN if a public network is unavoidable.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Use hotel-arranged or app-based transport in Lima, and avoid hailing street taxis.
- Avoid areas flagged in the advisory, including the VRAEM region and parts of the border.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

PHILIPPINES

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Manila

GOVERNMENT
Presidential republic

LANGUAGE
Filipino and English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 1, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Pervasive smishing and wallet fraud, snatch theft, typhoon disruption, and heavy targeting of outsourcing providers.

Country Overview

The Philippines is an archipelago of more than 7,000 islands in Southeast Asia. Spain colonized it in the sixteenth century and ruled for over three centuries, and the United States took control after the Spanish-American War in 1898. Japan occupied it in the Second World War, and independence came in 1946.

Ferdinand Marcos Sr.'s dictatorship from 1965 to 1986 ended in the People Power revolution. The country has about 115 million people, a large overseas workforce, and a growing services economy. Ferdinand Marcos Jr. has been president since 2022 and chairs ASEAN in 2026.

Geopolitical Landscape

- **South China Sea.** The Philippines has confrontations with China at Scarborough Shoal and the Second Thomas Shoal, and ASEAN's Code of Conduct talks under the Philippine chairmanship have stalled. Manila has deepened its alliance with the United States and expanded access to bases.
- **Flood-control corruption scandal.** Investigations since September 2025 found that about 2 billion dollars in flood-control funds were misspent, with ghost projects and ties between politicians and contractors. The scandal hurt Marcos's approval and sparked large protests.

- **Marcos and Duterte feud.** Vice President Sara Duterte, who has announced a 2028 run, is at odds with Marcos, and former president Rodrigo Duterte faces an ICC case.
- **ASEAN chair.** The Philippines took over the 2026 ASEAN chairmanship early after Myanmar was bypassed.

Cyber Threats | Organizations

- **Outsourcing sector.** The Philippines hosts one of the world's largest call-center and business process outsourcing industries, which hold client data and are prime targets for social engineering and insider recruitment.
- **State-linked targeting.** China-nexus and other actors target government, defense, and maritime networks, and disinformation targets South China Sea narratives.
- **Scam hubs.** Online scam operations linked to illegal gaming businesses were targeted for closure, but fraud persists.
- **Financial sector.** E-wallets such as GCash and Maya and banks face phishing and account takeover.
- **Typhoons.** Storms regularly disrupt power, connectivity, and operations.
- **Employees based in country.** Employees face wallet and smishing fraud, snatch theft, and typhoon disruption. Staff at outsourcing firms face targeted insider-recruitment and social engineering pressure.
- **Vendor and supply chain risk.** Business process outsourcing and call-center vendors are among the largest third-party concentrations, holding client data across many industries. Require access controls, logging, segmentation, and incident notification, and verify subcontractor chains.

The TIDE team tracks 40 threat actors that list Philippines among their targets. By attributed nexus, they break down as 30 China-nexus, 6 cybercriminal, 2 unattributed or other, 1 Vietnam-nexus, and 1 Iran-nexus. The most frequently targeted sectors are government (32), telecommunications (12), technology (10), defense and defense industrial base (9), and education and research (9). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Wallet and SMS fraud.** Smishing and fake e-wallet messages are extremely common.
- **Phone theft.** Snatch theft occurs in Manila.
- **Online scams.** Investment, job, and romance scams cause large losses.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Philippines.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Philippines Level 2, Exercise Increased Caution, citing unrest, crime, kidnapping or hostage-taking, terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Pervasive smishing and wallet fraud, snatch theft, typhoon disruption, and heavy targeting of outsourcing providers drive the rating.
- **What would change this rating.** Raise to Level 3 if South China Sea tension escalates into conflict. Lower to Level 1 as fraud and theft decline.

Public Wi-Fi

- Avoid public Wi-Fi in every country, including hotel, airport, cafe, and conference networks. Pervasive smishing, wallet fraud, and targeted recruitment of outsourcing staff make public networks particularly risky, so connect through a corporate VPN if a public network must be used.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid the southern Mindanao and Sulu areas flagged in the advisory.
- Typhoon season, June through November, can disrupt travel, so monitor alerts.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

POLAND

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Warsaw

GOVERNMENT
Parliamentary republic

LANGUAGE
Polish

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued June 5, 2025)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable NATO and EU member; exposure is Russia-linked sabotage and cyber activity against infrastructure and logistics, and GPS interference near the borders.

Country Overview

Poland has been a kingdom since the tenth century and once ruled a vast Polish-Lithuanian Commonwealth. Russia, Prussia, and Austria partitioned it in the late eighteenth century, and Poland regained independence in 1918. Germany and the Soviet Union invaded in 1939, and the Second World War devastated the country.

Communist rule ended after the Solidarity movement's victory in 1989. Poland joined NATO in 1999 and the EU in 2004 and has about 37 million people and one of Europe's fastest-growing economies. Donald Tusk has been prime minister since December 2023, and conservative Karol Nawrocki became president in August 2025.

Geopolitical Landscape

- **Frontline state.** Poland borders Ukraine, Belarus, and Russia's Kaliningrad exclave, hosts NATO and U.S. forces, and spends a higher share of GDP on defense than any other NATO member.
- **Russian hybrid attacks.** Poland has faced sabotage and arson, drone incursions, and railway damage that officials link to Russian services, and it has closed its border with Belarus at times.
- **Cohabitation.** A government led by Tusk and a president from the opposing camp complicate legislation and judicial reform.

- **Ukraine support.** Poland is a key logistics hub and supporter of Ukraine, with tensions over trade and refugees.

Cyber Threats | Organizations

- **Russia-linked cyber operations.** Poland is among the most targeted European countries, with attacks on government, energy, water, rail, and logistics, and large DDoS and influence campaigns.
- **Ransomware.** Hospitals, municipalities, and companies are frequent victims.
- **Spyware affair.** Pegasus was used against opposition figures under the previous government, and the matter is under investigation.
- **Regulation.** Poland is implementing NIS2 and has a national cybersecurity system.
- **Employees based in country.** Employees face BLIK and courier phishing and GPS interference near the eastern borders. Staff in logistics, energy, and defense-adjacent roles may draw Russia-linked targeting.
- **Vendor and supply chain risk.** Logistics, rail, energy, and managed service providers are priority targets for Russia-linked actors. NIS2 extends security duties to suppliers, so require attestations and incident notification.

The TIDE team tracks 36 threat actors that list Poland among their targets. By attributed nexus, they break down as 19 cybercriminal, 8 Russia-nexus, 2 China-nexus, 2 North Korea-nexus, 2 Belarus-nexus, 2 unattributed or other, and 1 hacktivist. The most frequently targeted sectors are government (25), healthcare and pharmaceuticals (16), industrial and manufacturing (16), banking and financial services (13), and technology (11). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, couriers, and BLIK payments are common.
- **Marketplace fraud.** Fake listings and BLIK scams affect buyers.
- **GPS interference.** Jamming near Kaliningrad and Belarus affects navigation.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Poland.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Poland Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Poland is a stable NATO and EU member. Exposure is Russia-linked sabotage and cyber activity against infrastructure and logistics and GPS interference near the borders.

- **What would change this rating.** Raise to Level 2 for logistics, energy, and defense-adjacent staff if hybrid attacks escalate.

Public Wi-Fi

- Given the documented Russia-linked targeting of Polish logistics, rail, and energy staff, avoid public Wi-Fi networks at transportation hubs and industrial facilities; use a corporate VPN if such a network is unavoidable.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Expect GPS interference near the eastern borders, and confirm border crossing status with Belarus before any trip nearby.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

PORTUGAL

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Lisbon

GOVERNMENT
Semi-presidential republic

LANGUAGE
Portuguese

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued December 23, 2025)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable EU member; exposure is ransomware, tourist-area theft, and phishing.

Country Overview

Portugal is one of Europe's oldest nation-states, with borders largely unchanged since the thirteenth century. In the fifteenth and sixteenth centuries its navigators pioneered the Age of Discovery and built a global empire. The 1755 Lisbon earthquake and later wars weakened it, and Brazil became independent in 1822.

The Carnation Revolution of 1974 ended decades of dictatorship and led to decolonization and democracy. Portugal joined the EU in 1986 and the euro at its launch. It has about 11.4 million people and an economy driven by tourism and services. Luis Montenegro has been prime minister since 2024.

Geopolitical Landscape

- **Political stability.** A center-right government has governed after three elections in four years, and the far-right Chega party became the second-largest party in 2025.
- **Iberian blackout.** A power outage in April 2025 across Portugal and Spain shut down transport and communications for hours and prompted investigations into grid resilience.
- **Atlantic role.** Portugal hosts the Lajes air base in the Azores and has strengthened ties with partners in lusophone Africa and Brazil.

Cyber Threats | Organizations

- **Ransomware.** Hospitals, municipalities, airlines, and companies have been hit by ransomware, and public sector incidents have disrupted services.
- **Hacktivism.** Pro-Russia groups have launched DDoS attacks on Portuguese government and financial sites.
- **Tourism sector.** Hotels and booking platforms hold payment data and face fraud.
- **Regulation.** Portugal implements NIS2 through its national cybersecurity center.
- **Employees based in country.** Employees face phishing and pickpocketing on Lisbon trams and at tourist sites. Staff in tourism and logistics face elevated fraud.
- **Vendor and supply chain risk.** Municipal, healthcare, and managed service providers are frequent ransomware victims, and the 2025 blackout showed dependence on shared infrastructure. Require continuity plans and incident notification.

The TIDE team tracks 13 threat actors that list Portugal among their targets. By attributed nexus, they break down as 8 cybercriminal, 3 China-nexus, 1 Iran-nexus, and 1 hacktivist. The most frequently targeted sectors are government (10), healthcare and pharmaceuticals (9), technology (7), education and research (6), and industrial and manufacturing (6). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, postal services, and tax authorities are common.
- **Tourist-area theft and fraud.** Pickpocketing and rental scams are common in Lisbon and Porto.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Portugal.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Portugal Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Portugal is a stable EU member. Exposure is ransomware, tourist-area theft, and phishing.
- **What would change this rating.** Raise to Level 2 if attacks on critical services or tourist-area crime increase.

Public Wi-Fi

- Because ransomware affects Portuguese public sector and tourism infrastructure, avoid public Wi-Fi at hotels, cafes, and tourist destinations; connect through a corporate VPN if you must use a public network.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Pickpocketing is common on Lisbon's trams and in tourist areas, so secure phones and bags.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

QATAR

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Doha

GOVERNMENT
Constitutional emirate

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 28, 2026)

Risk indicators: Other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Iranian strikes on Qatari territory during the war, Iran-linked targeting, state monitoring, and a U.S. Level 3 advisory.

Country Overview

Qatar is a small peninsula nation on the Persian Gulf that became one of the world's richest countries per person through natural gas. The Al Thani family has ruled since the nineteenth century, and Qatar became independent from Britain in 1971.

Sheikh Tamim bin Hamad Al Thani has been emir since 2013. Qatar has about 3.4 million people, mostly foreign workers, hosts a major U.S. air base at Al Udeid, and has used its wealth and gas exports for outsized diplomacy, including mediation in Gaza, Afghanistan, and the Democratic Republic of the Congo. It hosted the 2022 World Cup.

Geopolitical Landscape

- **Iran war.** Iran has fired missiles and drones at locations across Qatar since the war began on February 28, 2026, including at Al Udeid, and civilians have been killed and injured. The State Department rates Qatar Level 3 in an advisory updated on August 28, 2026.

- **2025 Israeli strike.** Israel struck Hamas leaders in Doha in September 2025, which drew Gulf condemnation and U.S. security assurances to Qatar.
- **Mediation.** Qatar continues to mediate in Gaza and in the DRC-M23 talks.
- **Gas exports.** Qatar is a leading LNG exporter, and Hormuz disruptions threaten shipments.

Cyber Threats | Organizations

- **Iran-linked and regional targeting.** Energy, government, finance, and telecommunications organizations are targeted by Iran-nexus actors, especially during escalations, and hack-and-leak operations have targeted Qatar before.
- **Energy sector.** LNG operators, QatarEnergy contractors, and suppliers hold valuable data and run industrial systems that regional actors have probed.
- **State monitoring.** Authorities monitor communications, and some VoIP services are restricted.
- **Hack-and-leak history.** Qatar's role as a regional diplomatic and energy hub draws state-linked espionage and influence interest.
- **Employees based in country.** Employees should expect regional escalation to disrupt flights and airspace, assume monitoring of communications, and avoid political content online. Energy, finance, and government staff face elevated Iran-linked phishing.
- **Vendor and supply chain risk.** Gulf-wide telecoms and managed service providers can be disrupted during Iran-related escalations, and LNG contractors face elevated state-actor targeting. Segment vendor access and plan for airspace and connectivity disruption.

The TIDE team tracks 13 threat actors that list Qatar among their targets. By attributed nexus, they break down as 7 Iran-nexus, 2 unattributed or other, 2 cybercriminal, 1 Russia-nexus, and 1 Lebanon-nexus. The most frequently targeted sectors are government (8), telecommunications (5), defense and defense industrial base (4), civil society and activism (4), and technology (3). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Online criticism of the emir or government can lead to prosecution.
- **VoIP limits.** Some voice-over-IP services face restrictions.
- **Fraud.** Bank and delivery impersonation circulates in Arabic and English.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Qatar.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Qatar Level 3, Reconsider Travel, citing other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Iranian strikes hit Qatari territory during the war, Iran-linked actors target Gulf organizations, authorities monitor speech, and the State Department rates Qatar Level 3.
- **What would change this rating.** Raise to Level 4 if attacks on Qatar resume or airspace closes. Lower to Level 2 if U.S.-Iran de-escalation holds.

Public Wi-Fi

- Given Iran-linked targeting of Qatari energy and government organizations, assume hotel and airport networks may be monitored; connect through a corporate VPN before accessing any company infrastructure on public networks.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Confirm airline and evacuation arrangements before travel, since airspace closures have occurred during the conflict.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

ROMANIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Bucharest

GOVERNMENT
Semi-presidential republic

LANGUAGE
Romanian

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued October 14, 2025)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: EU and NATO member with Russia-linked influence operations and ransomware, but low risk to ordinary visitors.

Country Overview

Romania lies in southeastern Europe along the Danube and the Black Sea and was formed in 1859 by the union of Wallachia and Moldavia. It became an independent kingdom in 1881 and gained Transylvania after the First World War. A communist regime took power after the Second World War, and Nicolae Ceausescu's dictatorship ended in the violent revolution of December 1989.

Romania joined NATO in 2004 and the EU in 2007. It has about 19 million people and a growing economy, with a large IT sector. Nicusor Dan won the May 2025 presidential election after the Constitutional Court annulled the November 2024 first round over alleged Russian-backed manipulation of social media.

Geopolitical Landscape

- **Annulled election and rerun.** The court annulled the 2024 presidential vote after the surprise success of Russia-aligned candidate Calin Georgescu, citing a coordinated TikTok campaign and foreign interference. Dan, a pro-European mayor of Bucharest, won the rerun in May 2025.
- **Fiscal strain.** Romania has among the EU's largest budget deficits and has enacted austerity measures.
- **War in Ukraine.** Romania is a NATO frontline state on the Black Sea, with drone debris falling on its territory and a major NATO base at Mihail Kogalniceanu.

- **Black Sea gas.** Offshore gas projects are strategic for regional energy security.

Cyber Threats | Organizations

- **Russia-linked influence operations.** Romania's election systems faced more than 85,000 cyberattacks around the November 2024 presidential vote, which reporting attributed to Russian attackers, and election bodies and government remain priority targets.
- **Ransomware.** Hospitals, utilities, and companies have been hit by ransomware.
- **Pro-Russia hacktivism.** DDoS campaigns target government and financial sites.
- **IT outsourcing.** Romania's large IT and outsourcing sector holds data for clients across Europe.
- **Regulation.** Romania is implementing NIS2 through its national cybersecurity directorate.
- **Employees based in country.** Employees face bank and courier phishing, taxi overcharging, and disinformation. Staff at outsourcing and technology firms face elevated targeted phishing.
- **Vendor and supply chain risk.** IT outsourcing firms and hospital and utility suppliers are frequent targets, and the 2024 hospital ransomware showed how one incident can disrupt many sites. Require supplier attestations and incident notification.

The TIDE team tracks 15 threat actors that list Romania among their targets. By attributed nexus, they break down as 8 cybercriminal, 2 China-nexus, 2 Russia-nexus, 2 hacktivist, and 1 unattributed or other. The most frequently targeted sectors are government (12), energy (6), education and research (6), industrial and manufacturing (6), and banking and financial services (6). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks and couriers are common in Romanian.
- **Disinformation.** Politically themed false content spreads widely on social media.
- **Tourist scams.** Taxi overcharging and ATM skimming target visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Romania.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Romania Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Romania is an EU and NATO member with Russia-linked influence operations and ransomware, but risk to ordinary visitors is low.

- **What would change this rating.** Raise to Level 2 if Russia-linked attacks on infrastructure or election bodies escalate.

Public Wi-Fi

- Romania's IT outsourcing sector faces elevated phishing, and ransomware regularly disrupts hospitals and utilities; avoid public Wi-Fi if you work in outsourcing or technology, and use a corporate VPN if public access is unavoidable.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Use licensed taxis or ride-hailing apps to avoid overcharging, and use bank ATMs rather than standalone machines.

Return protocol

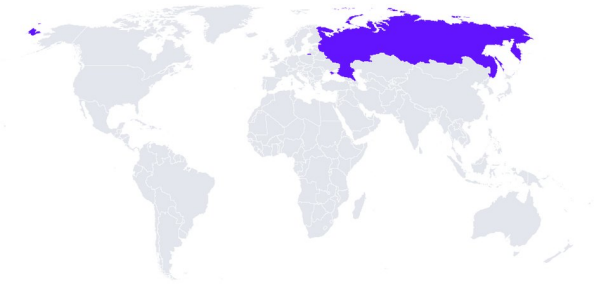
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

RUSSIA

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Moscow

GOVERNMENT
Federal semi-presidential republic

LANGUAGE
Russian

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued December 29, 2025)

Risk indicators: Unrest, terrorism, wrongful detention, other

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Compelled access under state security laws, pervasive monitoring, wartime connectivity restrictions and blocked services, detention risk, and severe sanctions.

Country Overview

Russia traces its origins to Kievan Rus', a medieval federation of East Slavic principalities centered on Kyiv that adopted Orthodox Christianity in the late tenth century. Mongol conquest in the thirteenth century fractured the region, and Moscow rose over the following two centuries and ended Mongol overlordship around 1480. Ivan IV was crowned the first tsar in 1547, the Romanov dynasty ruled from 1613, and Peter the Great proclaimed the Russian Empire in 1721.

The 1917 revolutions ended the monarchy, and the Bolsheviks founded the Soviet Union in 1922. The USSR emerged from the Second World War as a superpower and dissolved in December 1991, leaving the Russian Federation as its successor. A 1993 constitution established a strong presidency. Vladimir Putin has led the country since 1999, as president from 2000 to 2008, as prime minister from 2008 to 2012, and as president again since 2012.

Russia is the largest country in the world by area, spans eleven time zones, and has about 146 million people. It annexed Crimea in 2014 and declared the annexation of four more Ukrainian regions in 2022. The United Nations General Assembly and most governments do not recognize either claim.

Geopolitical Landscape

- **War in Ukraine.** Russia's full-scale invasion began in February 2022. As of an October 9, 2026 update from the Council on Foreign Relations, Russia occupies roughly 20 percent of Ukrainian territory, and U.S.-mediated talks have not produced a ceasefire.
- **Energy ceasefire claim.** On October 11, 2026, President Trump announced that Russia and Ukraine had agreed to stop striking each other's energy infrastructure. Neither government confirmed it, and Ukraine reported Russian strikes on six energy facilities the next day. Russia has privately tied any deal to sanctions relief.
- **Strikes inside Russia.** Ukraine's long-range drones have knocked out up to 40 percent of Russian refining capacity, according to the Council on Foreign Relations, and Ukraine has also struck Russian digital infrastructure including data centers.
- **Sanctions.** In October 2026 EU foreign ministers approved the largest sanctions package since the invasion, adding about 1,569 individuals and entities, while the U.S. Treasury issued a temporary license permitting the supply of Russian diesel to global markets on October 9. Visa and Mastercard suspended operations in 2022, so cards issued outside Russia generally do not work.
- **Information controls.** Mobile internet shutdowns since May 2025 reached central Moscow in March 2026, whitelists keep only state-approved services online, and foreign messaging platforms face blocking and throttling.

Cyber Threats | Organizations

- **Ukraine-aligned attacks.** Pro-Ukraine groups carry out disruptive attacks on Russian organizations. In July 2025, Silent Crow and the Belarusian Cyber Partisans claimed a year-long intrusion into Aeroflot that forced dozens of flight cancellations, and Russian prosecutors opened an investigation. Independent verification of the full scope remains pending.
- **State-directed connectivity restrictions.** Shutdowns, whitelists, and blocked foreign services interrupt e-commerce, payments, and remote work. A February 2026 law lets the FSB require mobile operators to suspend service.
- **State access to data.** Foreign organizations should assume state access to data stored or transmitted in country and should plan for compelled disclosure.
- **Sanctions-driven technology gaps.** Vendor withdrawals leave Russian organizations dependent on domestic and gray-market technology, which widens patching and supply chain gaps.
- **Employees based in country.** Employees and travelers should assume all communications and devices are monitored, expect mobile data outages and blocked Western apps, and recognize the risk of detention. Remove all company access from personal devices before any entry.
- **Vendor and supply chain risk.** Any vendor or contractor connected to Russia creates severe sanctions exposure and compelled-access risk, and local hosting and telecom providers must cooperate with security services. Remove Russia-based vendors, screen supply chains, and segment regional vendor access.

The TIDE team tracks 69 threat actors that list Russia among their targets. By attributed nexus, they break down as 18 cybercriminal, 15 China-nexus, 10 Russia-nexus, 9 unattributed or other, 7 North Korea-nexus, 4 Iran-nexus, 3 hacktivist, 1 Pakistan-nexus, 1 Lebanon-nexus, and 1 Belarus-nexus. The most frequently targeted

sectors are government (41), banking and financial services (27), defense and defense industrial base (16), technology (14), and healthcare and pharmaceuticals (13). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Communications monitoring.** Russian telecom operators must provide lawful interception access to security services, so calls, texts, and unencrypted traffic should be treated as observable.
- **Messaging platforms.** Authorities ordered the blocking of WhatsApp in February 2026 and began restricting Telegram on March 14, 2026, and Signal and Viber were already blocked. The state-backed Max messenger, preinstalled on new phones since September 2025, is regarded by many security experts as a surveillance tool.
- **VPN restrictions.** VPNs are not strictly illegal, but authorities remove VPN apps from app stores and detect and block common protocols, and a reported analysis found Max and other VK apps can detect VPN use.
- **Connectivity disruption.** Mobile data cannot be relied on for banking, navigation, or emergency contact.

State-Sponsored Cyber Threats

Russia conducts state cyber operations primarily through three services: the GRU (military intelligence), the SVR (foreign intelligence), and the FSB (federal security service). The groups below carry public attribution to one of these services.

GROUP	ALSO KNOWN AS	ATTRIBUTED SPONSOR	FOCUS	ACTIVE
APT28	Fancy Bear, Sofacy, Sednit, Forest Blizzard	GRU, 85th Main Special Service Center, Military Unit 26165	Espionage and disruption	2004 to 2026
APT29	Cozy Bear, Nobelium, The Dukes, Midnight Blizzard	SVR	Espionage	2008 to 2026
Sandworm	Voodoo Bear, Telebots, Seashell Blizzard, GRU Unit 74455	GRU, Main Centre for Special Technologies, Military Unit 74455	Disruption and destruction	2009 to 2026
Turla	Snake, Venomous Bear, Secret Blizzard, Waterbug	FSB Center 16	Espionage	1996 to 2026
Gamaredon	Primitive Bear, Shuckworm, Aqua Blizzard, Actinium	FSB, 18th Center of Information Security	Espionage	2013 to 2026
Berserk Bear	Dragonfly, Energetic Bear, Crouching Yeti, TEMP.Isotope	FSB Center 16	Espionage and pre-positioning	2010 to 2025
Cold River	Star Blizzard, Callisto, SEABORGIUM, TA446	FSB Center 18	Espionage	2017 to 2026
Cadet Blizzard	Ember Bear, DEV-0586, UAC-0056	GRU Unit 29155	Disruption and destruction	2020 to present

Russian-speaking cybercriminal groups and pro-Russia hacktivist fronts are also active. Some operate with state tolerance, and analysts assess that certain fronts have state ties. They are tracked separately. Berserk Bear

overlaps with Energetic Bear and Dragonfly, and Cold River overlaps with Callisto and Star Blizzard. This list excludes U.S. agencies by design.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Russia Level 4, Do Not Travel, citing the risk of harassment and wrongful detention by security officials, terrorism, and armed conflict. U.S. consulates in Russia have suspended operations, the embassy in Moscow has limited ability to assist detained U.S. citizens, commercial air options are few, and travelers should reconsider bringing electronic devices. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** State security laws compel access to data, communications and devices are monitored, shutdowns and blocked services disrupt operations, wrongful detention is a documented risk, and severe sanctions apply.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable end to the war, an end to wartime connectivity controls, and release of detained foreign nationals, none of which is in sight.

Public Wi-Fi

- Russia restricts VPNs and monitors all communications; do not use public Wi-Fi at all, and remove all company-linked applications from personal devices before entry.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices into Russia, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Require advance travel reporting. Block sign-ins from Russia with geo-based conditional access and alert on every blocked attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- For genuine business needs, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.

Connectivity and communications

- Expect mobile data outages and blocked Western messaging apps, and build check-in plans that do not depend on mobile data or a single app.
- Treat VPN use as a visible, higher-risk activity, and assume communications are monitored. Keep devices on your person, and treat rooms, vehicles, and restaurants as non-private.

Payments and logistics

- Cards issued outside Russia generally do not work, so confirm payment options through a travel provider and do not rely on foreign cards.
- Confirm that travel medical and evacuation coverage applies to Level 4 destinations and that the provider can operate in Russia.

Personal safety and legal exposure

- Do not wear company apparel or discuss work, and prepare a short approved cover answer. Treat unsolicited approaches with caution, including contacts through LinkedIn and social media before and after the trip.
- Wrongful detention is a documented risk, and a finding of wrongful detention does not guarantee release. Identify counsel before departure, and involve counsel on sanctions and export controls, including encryption on devices.

Return protocol

- Treat any personal device that traveled as untrusted and wipe it before re-enrolling it. Rotate passwords and revoke sessions for personal accounts used on the device, from a trusted network and device, starting with personal email.
- Hold a debrief to capture suspicious contacts or device behavior, and apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

RWANDA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3

CAPITAL
Kigali

GOVERNMENT
Presidential republic (dominant-party)

LANGUAGE
Kinyarwanda, English, French, and Swahili

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued June 4, 2026)

Risk indicators: Crime, health, unrest

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Pervasive state monitoring with documented spyware use, tight political control, and tension with the DRC and Burundi.

Country Overview

Rwanda is a small, mountainous, landlocked country in the African Great Lakes region. A Tutsi-led monarchy ruled for centuries before German and then Belgian colonization, and Rwanda became independent in 1962 after a Hutu-led revolution.

In 1994 Hutu extremists killed an estimated 800,000 Tutsi and moderate Hutu in about 100 days, until the Rwandan Patriotic Front led by Paul Kagame took control. Kagame has dominated the country since, formally as president since 2000. Rwanda has about 14.4 million people and is known for orderliness, rapid development, and strict political control.

Geopolitical Landscape

- **Conflict in eastern DRC.** UN experts say Rwandan forces played a critical role in the M23 offensive that seized Goma and Bukavu in early 2025. Rwanda denies backing M23 and says it acts in self-defense against Hutu militia. The United States brokered a Rwanda-DRC peace agreement in June 2025 and the Washington Accords in December 2025, but fighting continues.

- **Tension with Burundi.** Crisis Group reported that Burundian and Rwandan forces reportedly exchanged fire along their border in late summer 2026, and the border has been closed since 2024.
- **International pressure.** Western governments have sanctioned Rwandan officials and cut some aid over the DRC conflict.
- **Domestic control.** Opposition and media operate under tight constraints, and Kagame won the July 2024 election with about 99 percent of the vote.

Cyber Threats | Organizations

- **State monitoring and spyware.** The 2021 Pegasus Project identified Rwanda as one of ten countries where phone numbers were selected for possible Pegasus targeting.
- **Connectivity and platform controls.** Authorities monitor communications and online speech, and some platforms have been restricted.
- **Fintech and mobile money.** Rwanda is a regional fintech hub, with mobile money providers facing fraud and SIM-swap.
- **Conflict spillover.** Escalation with the DRC or Burundi could increase hacktivist and state-linked activity.
- **Employees based in country.** Employees should assume communications can be monitored, avoid commentary on politics or the DRC conflict, and expect mobile-money fraud attempts. Staff working on conflict or human-rights topics face elevated spyware risk.
- **Vendor and supply chain risk.** Telecoms and fintech vendors operate under state oversight and can be compelled to share data. Segment vendor access and keep sensitive data off local infrastructure where possible.

The TIDE team does not currently track actors that list Rwanda among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Monitoring and speech risk.** Online criticism of the government can lead to prosecution, and dissidents abroad have faced targeting.
- **Mobile money fraud.** SMS and wallet scams are common.
- **Low street crime.** Kigali is relatively safe, but opportunistic theft occurs.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Rwanda.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Rwanda Level 3, Reconsider Travel, citing crime, health, unrest. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Pervasive state monitoring with documented spyware use, tight political control, and tension with the DRC and Burundi drive the rating. Street crime is low.
- **What would change this rating.** Raise to Level 4 if the conflict with the DRC or Burundi escalates onto Rwandan territory. Lower to Level 2 if peace agreements hold and monitoring practices ease.

Public Wi-Fi

- Given documented state monitoring and spyware use against activists and civil society, avoid public Wi-Fi networks; use a corporate VPN if public access is required, and assume hotel networks are monitored.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid the DRC and Burundi borders flagged in the advisory.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

SAINT KITTS AND NEVIS

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Basseterre

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 7, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is tourism fraud and investment-migration data.

Country Overview

Saint Kitts and Nevis is a twin-island federation in the eastern Caribbean and the smallest sovereign state in the Americas by area and population. Britain established its first Caribbean colony on Saint Kitts in 1624, and sugar plantations built on enslaved labor shaped the islands. The federation became independent in 1983.

It has about 51,000 people and an economy based on tourism and one of the world's oldest citizenship-by-investment programs, launched in 1984. Terrance Drew has been prime minister since 2022.

Geopolitical Landscape

- **Citizenship by investment.** The program, a major source of revenue, has drawn scrutiny from the United States, EU, and others over vetting, and reforms are ongoing.
- **Climate vulnerability.** Hurricanes shape recovery and fiscal planning.
- **Regional integration.** The federation belongs to CARICOM and the Organisation of Eastern Caribbean States.

Cyber Threats | Organizations

- **Investment migration providers.** Agents and the program unit hold identity documents and financial records for thousands of applicants, a high-value target for fraud, extortion, and espionage.

- **Tourism and small business.** Hotels and local firms face payment fraud and ransomware.
- **Limited security capacity.** Government depends on vendors and regional partners.
- **Employees based in country.** Employees face tourist-area fraud and hurricane disruption, and staff at investment-migration firms face tailored phishing.
- **Vendor and supply chain risk.** Investment-migration agents hold identity files that warrant vetting, and small local vendors rely on regional cloud providers. Verify subcontractor controls.

The TIDE team does not currently track actors that list Saint Kitts and Nevis among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Tourist-targeted scams.** Fake rental and tour listings and card skimming target visitors.
- **Identity exposure and government ransomware.** The gov.kn domain was breached by the RansomHouse group in March 2023, exposing a reported 2.7 terabytes of data, and a separate ransomware incident hit Customs in December 2023; the Saint Kitts-Nevis-Anguilla National Bank issued a 2025 fraud alert over calls impersonating bank staff. People who hold or apply for citizenship through investment face targeted phishing using details from their applications.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Saint Kitts and Nevis.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Saint Kitts and Nevis Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with tourism fraud and investment-migration data as the main exposure.
- **What would change this rating.** Raise to Level 2 if a major breach hits investment-migration providers.

Public Wi-Fi

- Tourism fraud, the documented gov.kn ransomware breach, and identity exposure from the citizenship-by-investment program are the primary risks; use a corporate VPN on public Wi-Fi, especially at hotel networks that handle payment data, and never share financial details in response to an unsolicited call.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Hurricane season, June through November, can interrupt travel and connectivity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SAINT LUCIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Castries

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English (with Saint Lucian Creole)

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 10, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is tourism fraud and hurricane disruption.

Country Overview

Saint Lucia is a volcanic island in the eastern Caribbean known for the twin Pitons, a UNESCO World Heritage site. France and Britain fought over it for more than a century, and it changed hands about a dozen times before Britain gained firm control in 1814. It became independent in 1979.

The island has about 180,000 people and an economy based on tourism and banana exports. It is the birthplace of two Nobel laureates, economist Arthur Lewis and poet Derek Walcott. Hurricanes and climate change are central concerns.

Geopolitical Landscape

- **Climate vulnerability.** Storms and sea-level rise shape policy and recovery planning.
- **Citizenship by investment.** The program funds public spending and draws scrutiny from partners over vetting.
- **Regional integration.** Saint Lucia belongs to CARICOM and the Organisation of Eastern Caribbean States.

Cyber Threats | Organizations

- **Tourism and small business.** Hotels and local firms face payment fraud and ransomware.

- **Investment migration providers.** Agents hold identity documents and financial records.
- **Limited security capacity.** Government depends on vendors and regional partners.
- **Employees based in country.** Employees face tourist-area fraud and hurricane disruption.
- **Vendor and supply chain risk.** Small local vendors and regional cloud providers carry most exposure, and investment-migration agents hold identity files that warrant vetting.

The TIDE team does not currently track actors that list Saint Lucia among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Tourist-targeted scams.** Fake rental and tour listings and card skimming target visitors.
- **Phishing in English.** Digicel and LIME (Cable & Wireless) provide mobile service; a 2026 CIBC Caribbean alert warned of fraudulent calls impersonating bank staff, and a 2025 regional central bank advisory flagged romance and advance-fee scams.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Saint Lucia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Saint Lucia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with tourism fraud and hurricane disruption as the main exposure.
- **What would change this rating.** Raise to Level 2 if fraud against visitors or a major breach increases.

Public Wi-Fi

- Because hotels and tourism businesses face payment fraud and impersonation calls, avoid public Wi-Fi at resorts and cafes; connect through a corporate VPN if you must use a public network, and verify any banking contact through official channels rather than numbers provided in a call or message.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Hurricane season, June through November, can interrupt travel and connectivity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SAINT VINCENT AND THE GRENADINES

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Kingstown

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 7, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is tourism fraud and volcanic and hurricane disruption.

Country Overview

Saint Vincent and the Grenadines is an island nation in the Windward Islands made up of the main volcanic island and a chain of smaller islands. Indigenous Kalinago and Garifuna peoples resisted European settlement for generations, and Britain gained control in the late eighteenth century. The country became independent in 1979.

It has about 109,000 people and relies on tourism, agriculture, and remittances. The La Soufriere volcano erupted explosively in April 2021, forcing mass evacuations.

Geopolitical Landscape

- **Volcano and storms.** Volcanic activity and hurricanes strain infrastructure and public finances.
- **Taiwan recognition.** Saint Vincent and the Grenadines is one of the few states that recognize Taiwan.
- **Regional integration.** The country belongs to CARICOM and the Organisation of Eastern Caribbean States.

Cyber Threats | Organizations

- **Tourism and small business.** Hotels and yacht-charter firms face payment fraud and ransomware.
- **Limited security capacity.** Government depends on vendors and regional partners, and public incident reporting is limited.
- **Offshore services.** Corporate service providers hold client data.
- **Employees based in country.** Employees face tourist-area fraud and volcanic or hurricane disruption.
- **Vendor and supply chain risk.** Small local vendors and regional cloud providers carry most exposure. Verify subcontractor controls for client data.

The TIDE team does not currently track actors that list Saint Vincent and the Grenadines among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Tourist-targeted scams.** Fake rental and charter listings and card skimming target visitors.
- **Phishing in English.** Digicel and Flow provide mobile service; the Bank of Saint Vincent and the Grenadines has warned of fraudulent lookalike banking websites distributed by SMS, alongside shell-company investment scams flagged by regional regulators.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Saint Vincent and the Grenadines.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Saint Vincent and the Grenadines Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with tourism fraud and volcanic and hurricane disruption as the main exposure.
- **What would change this rating.** Raise to Level 2 if a major breach or disaster disrupts connectivity for an extended period.

Public Wi-Fi

- Tourism infrastructure and yacht-charter operations face payment fraud; the fraudulent banking websites distributed by SMS make URL verification essential before logging in. Use a corporate VPN on any public Wi-Fi, particularly at hotels and waterfront venues.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Check hurricane and volcanic alerts before travel.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SAMOA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Apia

GOVERNMENT
Parliamentary republic

LANGUAGE
Samoan and English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 7, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Limited connectivity and low crime; exposure is basic phishing and vendor concentration.

Country Overview

Samoa is a Polynesian island nation in the South Pacific whose culture, called fa'a Samoa, emphasizes chiefly titles and extended family. Germany and then New Zealand administered it, and in 1962 it became the first Pacific island nation to gain independence.

Samoa has about 210,000 people and an economy based on remittances, tourism, and agriculture. Political rivalry between factions of the long-dominant ruling party led to a constitutional crisis in 2021 and to snap elections in 2025. Cyclones and tsunamis are recurring threats.

Geopolitical Landscape

- **Political instability.** Splits in the governing party led to a prolonged crisis and early elections in 2025.
- **Great-power competition.** Australia, New Zealand, China, and the United States compete for influence in the Pacific, and Samoa balances their offers.
- **Climate vulnerability.** Cyclones and rising seas drive policy and aid requests.

Cyber Threats | Organizations

- **Limited digital footprint.** Connectivity depends on a few subsea and satellite links, and local security capacity is limited.
- **Regional diplomatic targeting.** Pacific governments draw external espionage interest.
- **Vendor concentration.** Telecom and banking services depend on a few providers.
- **Employees based in country.** Employees face limited connectivity and basic phishing risk, and cyclone season can disrupt travel.
- **Vendor and supply chain risk.** A few external vendors provide connectivity and banking services, so one outage can have wide effects. Plan for offline operation and verify incident notification terms.

The TIDE team does not currently track actors that list Samoa among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Phishing and fraud.** Vodafone Samoa and Digicel Samoa are the two mobile operators; scams and bank impersonation spread mainly through Facebook and WhatsApp, and the Central Bank of Samoa reported a sharp rise in fraud complaints, including investment, romance, and parcel-delivery scams, in its FY2025/2026 review.
- **Limited connectivity.** Internet access is slow and costly.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Samoa.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Samoa Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity is limited and crime is low. Exposure is basic phishing and vendor concentration.
- **What would change this rating.** Raise to Level 2 if political instability brings connectivity or legal restrictions.

Public Wi-Fi

- Connectivity runs through the single Tui-Samoa submarine cable linking Samoa to Fiji, creating vendor concentration risk; connect through a corporate VPN on public Wi-Fi to avoid single-cable compromise, and plan for outages during maintenance or storms.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Cyclone season, November through April, can disrupt travel and connectivity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SAN MARINO

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
San Marino

GOVERNMENT
Parliamentary republic (two Captains Regent serve as heads of state)

LANGUAGE
Italian

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 10, 2026)

Risk indicators: Terrorism

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and low crime; exposure is targeted fraud against finance staff.

Country Overview

San Marino is a tiny mountaintop republic entirely surrounded by Italy and claims to be the world's oldest surviving sovereign state and constitutional republic, with a founding tradition dating to 301. Its Sammarinese independence survived the unification of Italy.

The country has about 34,000 people and an economy built on tourism, banking, and manufacturing. Two Captains Regent, elected every six months, serve as joint heads of state. San Marino uses the euro under an agreement with the EU and is negotiating an association agreement with the bloc.

Geopolitical Landscape

- **EU association.** San Marino has negotiated an association agreement with the EU that would give it access to parts of the single market.
- **Financial transparency.** The country has adopted international tax transparency and anti-money-laundering standards after years of scrutiny.
- **Reliance on Italy.** Italy provides defense, customs, and many public services.

Cyber Threats | Organizations

- **Financial sector.** Banks and fiduciary firms hold client data and face business email compromise and targeted phishing.
- **Tourism.** Visitor-facing businesses face card fraud.
- **Small-state resourcing.** Local security capacity is limited, and firms rely on Italian vendors.
- **Employees based in country.** Employees face ordinary phishing and tourist-area theft. Staff in banking and fiduciary roles face tailored fraud.
- **Vendor and supply chain risk.** Italian vendors and a small set of local financial service providers carry most exposure. Verify subcontractor controls for client data.

The TIDE team does not currently track actors that list San Marino among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Phishing and parcel scams.** Messages impersonating banks and couriers circulate in Italian.
- **Tourist-area theft.** Pickpocketing occurs at crowded tourist sites.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to San Marino.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates San Marino Level 2, Exercise Increased Caution, citing terrorism. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** San Marino is stable and low crime. Exposure is targeted fraud against finance staff.
- **What would change this rating.** Raise to Level 2 if targeted campaigns against its financial firms emerge.

Public Wi-Fi

- San Marino's financial sector faces business email compromise and targeted phishing; banking and fiduciary staff should avoid public Wi-Fi entirely, and use a corporate VPN if access is essential.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- San Marino is reached through Italy, and border checks follow Italian practice.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SAO TOME AND PRINCIPE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Sao Tome

GOVERNMENT
Semi-presidential republic

LANGUAGE
Portuguese

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 4, 2026)

Risk indicators: Health

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Single-cable connectivity and low crime; political instability can bring sudden disruption.

Country Overview

Sao Tome and Principe is a two-island nation off the coast of Central Africa in the Gulf of Guinea. Portugal found the uninhabited islands in the 1470s and developed sugar and later cocoa plantations worked by enslaved and contract laborers. The country became independent in 1975.

It has about 210,000 people, depends on cocoa and aid, and is one of Africa's smallest and poorest states. Political instability has included a coup attempt in November 2022 and the dismissal of the prime minister in 2025. Elections were due in 2026, and offshore oil exploration has been a hoped-for source of revenue.

Geopolitical Landscape

- **Political instability.** Tension between the president and parliament has led to repeated government changes and a 2022 coup attempt.
- **Foreign partners.** Portugal, China, and the United States compete for influence in a strategic position in the Gulf of Guinea.
- **Economic fragility.** Debt and limited revenue constrain the state.

Cyber Threats | Organizations

- **Limited digital footprint.** Connectivity depends on a single subsea cable, and local security capacity is minimal.
- **Banking and telecom.** A few institutions with foreign parents carry most exposure.
- **Public sector.** Government systems have thin security staffing.
- **Employees based in country.** Employees face limited connectivity and basic fraud risk, and political tension can bring sudden disruption.
- **Vendor and supply chain risk.** A single cable and a few vendors provide connectivity and banking, so one outage can have wide effects. Plan for offline operation.

The TIDE team does not currently track actors that list Sao Tome and Principe among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Mobile fraud.** CST and Unitel STP provide mobile service; basic SMS and wallet scams exist, though the country's cybersecurity reporting capacity remains limited and a National Cybersecurity Strategy is still in development.
- **Limited connectivity.** Internet is slow and costly.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Sao Tome and Principe.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Sao Tome and Principe Level 2, Exercise Increased Caution, citing health. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity depends on a single cable and crime is low. Political instability can bring sudden disruption.
- **What would change this rating.** Raise to Level 2 if unrest or another coup attempt occurs.

Public Wi-Fi

- A single subsea cable provides all international connectivity, creating dependency on one telecom provider; use a corporate VPN on public Wi-Fi, and expect limited connectivity options outside major towns.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Carry offline copies of key documents, since connectivity is limited.

Return protocol

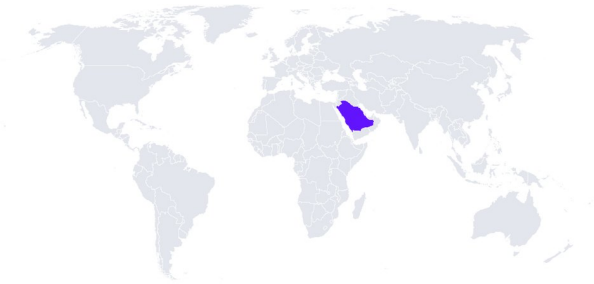
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SAUDI ARABIA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 4



CAPITAL
Riyadh

GOVERNMENT
Absolute monarchy

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued September 15, 2026)

Risk indicators: Terrorism, other

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Houthi strikes closed Riyadh's main international airport and killed at least 20 people in early October 2026, plus Iran-linked targeting, state monitoring of speech, and a U.S. Level 3 advisory.

Country Overview

Saudi Arabia occupies most of the Arabian Peninsula and contains Islam's two holiest cities, Mecca and Medina. The Al Saud family allied with the Wahhabi religious movement in the eighteenth century, and Abdulaziz Ibn Saud unified the modern kingdom in 1932. The discovery of oil in 1938 transformed the country.

Saudi Arabia has about 35 million people and the world's second-largest proven oil reserves. King Salman has reigned since 2015, and his son, Crown Prince Mohammed bin Salman, is the de facto ruler and has pursued social and economic change under Vision 2030 while tightening political control.

Geopolitical Landscape

- **Houthi war and Iran conflict.** The U.S.-Israeli war on Iran that began on February 28, 2026 has pulled Saudi Arabia into a renewed war with Yemen's Houthis. The Houthis declared a blockade of Saudi ports in July 2026, seized Yemen's Red Sea coast in September, and struck Saudi airports repeatedly between October 5 and 10, killing at least 20 people and wounding hundreds, including an October 10 missile strike on Riyadh's King Khalid International Airport that killed 12 and closed the kingdom's main international gateway through

at least October 17. Saudi Arabia and allied Yemeni forces launched a ground and air offensive in early October and retook Mokha. President Trump said on October 10 that he is considering strikes on the Houthis.

- **Gulf security.** Iranian attacks on Gulf states during the war and on shipping near the Strait of Hormuz affect Saudi oil exports and make the Red Sea route more important.
- **Domestic politics.** Authorities have imprisoned critics, clerics, and activists, and expression is tightly controlled.
- **Vision 2030.** Megaprojects such as NEOM and large events such as the 2034 World Cup drive investment and scrutiny.

Cyber Threats | Organizations

- **State-linked and hacktivist attacks.** Iran-nexus actors have targeted Saudi energy, government, and finance organizations for years, including the destructive Shamoon attacks on Saudi Aramco in 2012 and later waves, and escalations raise that risk.
- **Critical infrastructure.** Oil and gas, desalination, aviation, and airports run industrial systems that regional actors have probed, and physical attacks have disrupted airport operations.
- **State monitoring and spyware.** Authorities monitor communications and online speech, and Saudi-linked actors have used commercial spyware against dissidents.
- **Data localization and regulation.** The Personal Data Protection Law and National Cybersecurity Authority controls set strict duties for organizations operating in the kingdom.
- **Employees based in country.** Employees should expect missile and drone alerts and airport disruption, assume monitoring of communications, and avoid political content online. Energy, finance, and government staff face elevated Iran-linked phishing.
- **Vendor and supply chain risk.** Telecoms, managed service providers, and oil-sector contractors are priority targets for Iran-linked actors, and data localization rules require local hosting for some data. Segment vendor access, plan for airport and airspace disruption, and screen vendors for compelled-access risk.

The TIDE team tracks 44 threat actors that list Saudi Arabia among their targets. By attributed nexus, they break down as 20 Iran-nexus, 9 cybercriminal, 8 unattributed or other, 5 China-nexus, 1 India-nexus, and 1 Lebanon-nexus. The most frequently targeted sectors are government (30), telecommunications (15), energy (14), defense and defense industrial base (12), and healthcare and pharmaceuticals (11). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Social media posts critical of the government, monarchy, or religion have led to long prison sentences.
- **VoIP and platform limits.** Some voice-over-IP services face restrictions.
- **Fraud.** Bank, Absher, and delivery impersonation scams circulate in Arabic and English.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Saudi Arabia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Saudi Arabia Level 3, Reconsider Travel, citing terrorism, other. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Houthi missile and drone strikes killed at least 20 people and closed Riyadh's King Khalid International Airport, the kingdom's main gateway, through at least October 17, 2026, Iran-linked actors target Gulf organizations, authorities monitor speech, and the State Department rates Saudi Arabia Level 3 in an advisory updated on September 15, 2026.
- **What would change this rating.** Level 4 reflects the closure of Riyadh's main international airport and the intensified attack tempo. Lower to Level 3 if the airport reopens and the attack tempo eases, and to Level 2 if the Houthi front and the Iran conflict de-escalate.

Public Wi-Fi

- Iran-linked actors have targeted Saudi energy and finance organizations, and state monitoring is pervasive; assume hotel and airport networks are monitored, and use a corporate VPN before accessing any company systems.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid the Yemen border region and Abha, Jizan, Najran, and other southwestern areas under attack, and confirm airline and evacuation arrangements.
- Follow alert guidance, since attacks on Riyadh's airport have occurred.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

SENEGAL

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2

CAPITAL
Dakar

GOVERNMENT
Presidential republic

LANGUAGE
French (with Wolof and other national languages)

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued December 1, 2025)

Risk indicators: Crime, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Mobile-money fraud, snatch theft, and a precedent of connectivity restrictions during unrest.

Country Overview

Senegal lies on the westernmost point of Africa and has long been a center of trade, Sufi Islam, and cultural influence. France colonized it, and Dakar served as capital of French West Africa. Senegal became independent in 1960 under the poet-president Leopold Senghor and has never had a successful military coup.

The country has about 19.6 million people and a reputation as one of West Africa's more stable democracies. Bassirou Diomaye Faye won the March 2024 election as the candidate of the Pastef party led by Ousmane Sonko, who became prime minister. Offshore oil and gas production began in 2024.

Geopolitical Landscape

- **Debt shock.** The government revealed in 2025 that earlier administrations had understated public debt, which put Senegal's debt among the highest in the region and strained talks with the IMF.
- **Pastef government.** Faye and Sonko took office on a platform of sovereignty and reform, and the relationship between the two has drawn attention.
- **Sahel spillover.** Jihadist violence in Mali raises risk along the eastern border, and Senegal avoided the break with ECOWAS made by the Sahel juntas.

- **Oil and gas.** New production offers revenue but raises governance and contract questions.

Cyber Threats | Organizations

- **Connectivity restrictions.** Authorities cut mobile internet and restricted social media platforms during unrest in 2023 and 2024.
- **Financial and mobile money.** Wave, Orange Money, and banks face SIM-swap, social engineering, and fraud.
- **Public-sector incidents.** Government agencies have suffered data breaches and ransomware, and security capacity is limited.
- **Energy sector.** Oil and gas operators and contractors hold valuable data.
- **Employees based in country.** Employees face mobile-money fraud, snatch theft in Dakar, and possible connectivity restrictions during political unrest.
- **Vendor and supply chain risk.** Telecom, fintech, and energy contractors hold sensitive data with thin local security capacity, and government agencies have suffered breaches. Require logging, segmentation, and out-of-band verification of payment changes.

The TIDE team tracks 1 threat actor that lists Senegal among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile money fraud.** Fake agent and fake reversal scams are common.
- **Phone theft.** Snatch theft occurs in Dakar.
- **Monitoring and speech risk.** Online criticism of officials has led to arrests.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Senegal.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Senegal Level 1, Exercise Normal Precautions, citing crime, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Mobile-money fraud, snatch theft, and a precedent of connectivity restrictions during unrest drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest returns with shutdowns. Lower to Level 1 as fraud and tension decline.

Public Wi-Fi

- Mobile-money fraud and connectivity restrictions during unrest are documented; use a corporate VPN on public Wi-Fi, especially at cafes and hotels, and avoid public networks during political protests.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, and avoid the Casamance and eastern border areas flagged in the advisory.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SERBIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Belgrade

GOVERNMENT
Parliamentary republic

LANGUAGE
Serbian

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 27, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Election-period disinformation and protest disruption, documented spyware use against activists, and state-linked targeting.

Country Overview

Serbia is a Balkan country at the crossroads of Central and Southeastern Europe. A medieval Serbian kingdom and empire reached its height in the fourteenth century before Ottoman conquest, and Serbia regained autonomy in the nineteenth century. It was the core of Yugoslavia, whose breakup in the 1990s brought wars, NATO's 1999 bombing, and the loss of Kosovo.

Serbia has about 6.5 million people and has been an EU candidate since 2012, though its accession has stalled. Aleksandar Vucic has dominated politics as prime minister and then president since 2014.

Geopolitical Landscape

- **Snap election on October 25, 2026.** Vucic dissolved parliament on September 9 and called early parliamentary elections for October 25, a central demand of a student-led protest movement that began after the November 2024 collapse of a railway station canopy in Novi Sad killed 16 people. The students registered their own electoral list on September 14, and an early presidential election will be held separately. Vucic's party has agreed to put him forward as a candidate.

- **EU path stalled.** Serbia has not joined EU sanctions on Russia and keeps close ties with both Russia and China.
- **Kosovo.** Belgrade does not recognize Kosovo, and tensions in the north recur.
- **Protest crackdown.** Authorities accuse the movement of a foreign-funded revolution, and police have clashed with protesters.

Cyber Threats | Organizations

- **Spyware and surveillance.** Amnesty International found in 2024 that Serbian police and security services used Cellebrite phone-extraction tools and a spyware tool against activists and journalists.
- **Election-period activity.** Phishing, disinformation, and denial-of-service attacks tend to cluster around elections and protests.
- **State-linked targeting.** Government and critical infrastructure draw regional espionage interest, and Serbia's Chinese-built surveillance and safe-city systems raise data-access concerns.
- **IT sector.** Serbia has a growing IT outsourcing sector, including relocated Russian technology workers.
- **Employees based in country.** Employees face election-period phishing and disinformation and possible disruption from large protests in Belgrade. Staff in media, civil society, or politically exposed roles face monitoring and spyware risk.
- **Vendor and supply chain risk.** Local IT outsourcers, including relocated Russian technology firms, and state-linked surveillance suppliers raise vetting and data-access questions. Review developer access, ownership, and sanctions exposure.

The TIDE team tracks 1 threat actor that lists Serbia among their targets. By attributed nexus, they break down as 1 China-nexus. The most frequently targeted sectors are diplomatic and foreign affairs (1), energy (1), and government (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring.** Activists and journalists face phone searches, spyware, and legal pressure.
- **Phishing and impersonation.** Messages impersonating banks and couriers circulate in Serbian.
- **Disinformation.** Politically charged false content spreads on social media.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Serbia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Serbia Level 2, Exercise Increased Caution, citing crime. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Election-period disinformation and protest disruption, documented spyware use against activists, and state-linked targeting drive the rating, with moderate risk for typical visitors.
- **What would change this rating.** Raise to Level 3 if the October 25 election or its aftermath brings violence, shutdowns, or detentions of foreigners. Lower to Level 1 after a calm transition.

Public Wi-Fi

- Spyware tools have been used against activists during election periods, and election-related phishing clusters around voting; avoid public Wi-Fi around elections, and use a corporate VPN on any public network.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, particularly around the October 25 election and results, and keep to official updates.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SEYCHELLES

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Victoria

GOVERNMENT
Presidential republic

LANGUAGE
Seychellois Creole, English, and French

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued December 9, 2025)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and low crime; exposure is tourism fraud and offshore-sector payment fraud.

Country Overview

Seychelles is an archipelago of 115 islands in the Indian Ocean northeast of Madagascar that was uninhabited until French settlers arrived in the eighteenth century. Britain took control in 1814, and Seychelles became independent in 1976.

The country has about 120,000 people, the highest income per person in Africa, and an economy built on luxury tourism, fishing, and offshore financial services. A one-party state under France-Albert Rene ended in 1993. Patrick Herminie, an opposition leader, won the October 2025 presidential runoff against incumbent Wavel Ramkalawan.

Geopolitical Landscape

- **Change of government.** Herminie's victory in the October 2025 runoff marked a peaceful turnover of power in one of Africa's more stable democracies.
- **Indian Ocean competition.** India, China, the Gulf states, and Western partners compete for influence over Seychelles' strategic location and ports.
- **Climate and fisheries.** Sea-level rise and the tuna economy drive policy.

Cyber Threats | Organizations

- **Offshore financial sector.** Corporate service providers and banks hold client data and face business email compromise and targeted phishing.
- **Tourism sector.** Resorts and airlines hold payment and passport data and face card fraud.
- **Limited security capacity.** Government depends on vendors and partner support.
- **Employees based in country.** Employees face tourist-area card fraud and booking scams, and staff in offshore finance face tailored payment fraud.
- **Vendor and supply chain risk.** Corporate service providers and resort technology vendors carry concentrated client data. Verify subcontractor controls and require incident notification.

The TIDE team does not currently track actors that list Seychelles among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Tourist-targeted scams.** Fake booking listings and card skimming target visitors.
- **Phishing.** Airtel Seychelles and Cable & Wireless Seychelles provide mobile service, with Airtel Money as the main mobile-wallet platform; the offshore financial sector has drawn targeted attacks, including a data breach at the Seychelles Commercial Bank and a ransomware incident at the Development Bank of Seychelles.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Seychelles.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Seychelles Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Seychelles is stable and low crime. Exposure is tourism fraud and offshore-sector payment fraud.
- **What would change this rating.** Raise to Level 2 for offshore-finance staff if targeted campaigns intensify.

Public Wi-Fi

- The offshore finance sector and resorts hold concentrated client and payment data, and the documented bank breaches show foreign actors actively target the jurisdiction's financial institutions; staff in financial services should use a corporate VPN on all public Wi-Fi to avoid business email compromise.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Cyclone and monsoon seasons can disrupt travel and connectivity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SIERRA LEONE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Freetown

GOVERNMENT
Presidential republic

LANGUAGE
English (with Krio widely spoken)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 15, 2025)

Risk indicators: Unrest, crime, health

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Mobile-money fraud, phone snatching, unreliable infrastructure, and a precedent of restrictions during unrest.

Country Overview

Sierra Leone lies on the West African Atlantic coast and takes its name from the mountains near Freetown, which freed slaves and Black loyalists settled in the late eighteenth century. Britain governed it as a colony and protectorate until independence in 1961.

An eleven-year civil war from 1991 to 2002, famous for the blood-diamond trade, killed tens of thousands and displaced millions. A 2014 to 2016 Ebola epidemic also devastated the country. Julius Maada Bio has been president since 2018, was reelected in 2023, and chaired ECOWAS in 2025. The country has about 9.3 million people.

Geopolitical Landscape

- **Political tension.** The 2023 election was contested by the opposition, and a failed coup attempt in November 2023 led to arrests and trials.
- **Economic strain.** Inflation, currency weakness, and youth unemployment drive discontent, and past protests turned deadly.
- **Mining.** Iron ore, diamonds, and rutile are major exports, with investment from China and Western firms.

- **Regional role.** Bio's ECOWAS chairmanship put Sierra Leone at the center of regional mediation with the Sahel juntas.

Cyber Threats | Organizations

- **Connectivity restrictions.** Authorities restricted internet access during the August 2022 protests.
- **Mobile money and banking.** Wallets and banks face SIM-swap and social engineering.
- **Mining firms.** Operators and contractors hold commercial data and face fraud and espionage.
- **Limited local capacity.** Public bodies and banks have thin security staffing and unreliable power.
- **Employees based in country.** Employees face mobile-money fraud, phone snatching in Freetown, unreliable power and connectivity, and possible restrictions during unrest.
- **Vendor and supply chain risk.** Telecom, mining, and banking vendors have thin security capacity, and compromised mailboxes are used to redirect payments. Require logging and out-of-band verification of payment changes.

The TIDE team tracks 1 threat actor that lists Sierra Leone among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Mobile money fraud.** Africell and Orange Money dominate mobile money, which reaches more than 40 percent of adults; SIM-swap fraud and smishing are endemic, including lottery-win messages that extract incremental "processing fees," and regulators fined both Africell and Orange in October 2024 for operating mobile money services without proper licensing.
- **Phone theft.** Snatch theft occurs in Freetown.
- **Monitoring and speech risk.** Online criticism of officials has led to arrest under cybercrime laws.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Sierra Leone.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Sierra Leone Level 2, Exercise Increased Caution, citing unrest, crime, health. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Mobile-money fraud, phone snatching, unreliable infrastructure, and a precedent of restrictions during unrest drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest returns with shutdowns. Lower to Level 1 as infrastructure and security capacity improve.

Public Wi-Fi

- Mobile-money platforms face SIM-swap and social engineering at a documented, above-average rate, with occasional connectivity restrictions during unrest; Sierra Leone's national CSIRT and digital forensics lab only launched in January 2025. Use a corporate VPN on public Wi-Fi at hotels and cafes, and treat unsolicited lottery or prize messages as fraudulent.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Keep devices out of sight in traffic, and carry power banks, since outages are frequent.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SINGAPORE

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1



CAPITAL
Singapore

GOVERNMENT
Parliamentary republic

LANGUAGE
English, Malay, Mandarin, and Tamil

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued March 9, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Highly secure and well-regulated; exposure is impersonation scams and state-linked targeting of critical-infrastructure and finance staff.

Country Overview

Singapore is a city-state at the southern tip of the Malay Peninsula that grew from a British trading post founded by Stamford Raffles in 1819 into one of the world's busiest ports. Japan occupied it from 1942 to 1945. It joined Malaysia in 1963 and became independent in 1965 under Lee Kuan Yew.

The People's Action Party has governed since self-rule began in 1959. Singapore has about 6.1 million people, one of the world's highest incomes, and a leading role in finance, shipping, and technology. Lawrence Wong became prime minister in May 2024, and the PAP won the May 2025 election.

Geopolitical Landscape

- **Great-power balancing.** Singapore maintains ties with both the United States and China, its largest trading partner, and hosts U.S. military access.
- **Trade exposure.** As a trade hub, Singapore is exposed to U.S. tariffs and supply chain shifts.
- **Regional role.** Singapore is a leading ASEAN voice and a hub for regional finance and arbitration.

Cyber Threats | Organizations

- **State-linked espionage against critical infrastructure.** In July 2025 Singapore publicly named the China-nexus group UNC3886 as targeting its critical infrastructure and said it had ordered a response.
- **Financial and data center hub.** Banks, asset managers, and data centers hold concentrated regional data, drawing ransomware and espionage.
- **Scams.** Singapore sees very high scam losses, including impersonation of officials and investment fraud.
- **Regulation.** In February 2026 Singapore's Cyber Security Agency disclosed that the China-linked group UNC3886 had breached all four major telecom providers in a months-long espionage campaign, and the government ran an 11-month counteroperation to evict it. The Personal Data Protection Act sets breach duties.
- **Employees based in country.** Employees face impersonation scams and phishing, and staff at banks, data centers, and technology firms are priority targets for state-linked actors.
- **Vendor and supply chain risk.** Regional data centers, cloud providers, and managed service providers are concentrated third parties and critical-infrastructure suppliers. The amended Cybersecurity Act extends duties to them, so require attestations, segmentation, and incident notification.

The TIDE team tracks 56 threat actors that list Singapore among their targets. By attributed nexus, they break down as 30 cybercriminal, 18 China-nexus, 4 North Korea-nexus, 3 unattributed or other, and 1 Iran-nexus. The most frequently targeted sectors are government (29), banking and financial services (26), technology (26), healthcare and pharmaceuticals (26), and industrial and manufacturing (18). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Impersonation scams.** Fake government official, bank, and e-commerce scams are widespread.
- **Phishing and SIM fraud.** Account takeover is frequent.
- **Low street crime.** Theft is rare, but device loss still causes account exposure.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Singapore.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Singapore Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Singapore is highly secure and well-regulated. Exposure is impersonation scams and state-linked targeting of critical-infrastructure and finance staff, which is role-based.

- **What would change this rating.** Raise to Level 2 for staff in those sectors if state-linked targeting of travelers escalates.

Public Wi-Fi

- Singapore is highly secure, but impersonation scams are widespread and state-linked actors have targeted critical infrastructure; use a corporate VPN on public Wi-Fi if you work in finance, banking, or data centers.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Singapore has strict laws on drugs, vaping, and public conduct, so follow local rules.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SLOVAKIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Bratislava

GOVERNMENT
Parliamentary republic

LANGUAGE
Slovak

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued February 12, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable EU member; exposure is phishing, marketplace fraud, and role-based targeting.

Country Overview

Slovakia is a landlocked Central European country in the Carpathian Basin. It was part of the Kingdom of Hungary for a thousand years, then joined the Czechs in Czechoslovakia in 1918. It had a wartime fascist client state, and a communist regime followed. Czechoslovakia split peacefully in 1993.

Slovakia joined NATO and the EU in 2004 and the eurozone in 2009. It has about 5.4 million people and an economy built on automobile manufacturing. Robert Fico returned as prime minister in October 2023 and survived an assassination attempt in May 2024.

Geopolitical Landscape

- **Fico government.** Fico's government has criticized EU aid to Ukraine, slowed some sanctions packages, and kept energy ties with Russia, which has drawn criticism from Brussels and large domestic protests.
- **Rule of law concerns.** Changes to criminal law and public media drew EU scrutiny and protests.
- **Energy.** Slovakia depended heavily on Russian gas and oil, and the end of Ukrainian gas transit in 2025 forced adjustment.

Cyber Threats | Organizations

- **Russia-linked influence and cyber activity.** Disinformation, DDoS, and phishing target government and media, and espionage interest focuses on government and defense.
- **Ransomware.** Hospitals, municipalities, and manufacturers are frequent victims.
- **Automotive supply chain.** Auto suppliers hold intellectual property and face ransomware and business email compromise.
- **Regulation.** Slovakia is implementing NIS2.
- **Employees based in country.** Employees face bank and courier phishing and marketplace fraud. Staff in automotive and government-adjacent roles may draw targeted attention.
- **Vendor and supply chain risk.** Automotive suppliers and managed service providers are common entry points for ransomware and intellectual property theft. NIS2 extends security duties to suppliers, so require attestations and incident notification.

The TIDE team tracks 4 threat actors that list Slovakia among their targets. By attributed nexus, they break down as 2 Russia-nexus, 1 China-nexus, and 1 Belarus-nexus. The most frequently targeted sectors are government (4), critical infrastructure (general) (1), education and research (1), energy (1), and civil society and activism (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, couriers, and public agencies are common.
- **Marketplace fraud.** Fake listings and payment-link scams affect buyers.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Slovakia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Slovakia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Slovakia is a stable EU member. Exposure is phishing, marketplace fraud, and role-based targeting of automotive and government-adjacent staff.
- **What would change this rating.** Raise to Level 2 if Russia-linked targeting of Slovak institutions escalates.

Public Wi-Fi

- Ransomware frequently disrupts Slovak hospitals and manufacturers, and Russia-linked phishing targets automotive suppliers; use a corporate VPN on public Wi-Fi, particularly in industrial and manufacturing areas.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Demonstrations in Bratislava can disrupt travel, so avoid them.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SLOVENIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Ljubljana

GOVERNMENT
Parliamentary republic

LANGUAGE
Slovene

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 15, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable EU member; exposure is phishing, marketplace fraud, and role-based targeting of industrial staff.

Country Overview

Slovenia is a small Alpine and Adriatic country that was part of the Habsburg Empire for centuries and then of Yugoslavia. It declared independence in June 1991 and fought a brief ten-day war with Yugoslav forces, avoiding the larger conflicts that followed.

Slovenia joined NATO and the EU in 2004 and the eurozone in 2007. It has about 2.1 million people and a prosperous, export-oriented economy built on manufacturing and services. It is known for its capital Ljubljana, Lake Bled, and the Julian Alps.

Geopolitical Landscape

- **Stable EU and NATO member.** Slovenia is an advanced democracy with a record of orderly transfers of power, and it is increasing defense spending.
- **Balkans neighbor.** Slovenia supports EU enlargement in the Western Balkans and manages border disputes with Croatia through arbitration.
- **Energy and transit.** Slovenia is a transit corridor between Italy, Austria, Croatia, and Hungary and is diversifying away from Russian energy.

Cyber Threats | Organizations

- **Ransomware and fraud.** Public bodies, hospitals, and manufacturers are periodic ransomware victims, and business email compromise is common.
- **Pro-Russia hacktivism.** DDoS campaigns have targeted Slovenian government and media sites around political events.
- **Manufacturing and logistics.** Industrial firms and logistics operators hold intellectual property and face supply chain compromise.
- **Regulation.** Slovenia is implementing NIS2 and GDPR.
- **Employees based in country.** Employees face bank and courier phishing and marketplace fraud. Staff in manufacturing and logistics may draw targeted attention.
- **Vendor and supply chain risk.** Industrial suppliers and managed service providers are common entry points for ransomware and intellectual property theft. NIS2 extends security duties to suppliers, so require attestations and incident notification.

The TIDE team tracks 1 threat actor that lists Slovenia among their targets. By attributed nexus, they break down as 1 North Korea-nexus. The most frequently targeted sectors are banking and financial services (1), and cryptocurrency and digital assets (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, couriers, and public agencies are common in Slovene.
- **Marketplace and rental fraud.** Fake listings and payment-link scams affect buyers and visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Slovenia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Slovenia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Slovenia is a stable EU member. Exposure is phishing, marketplace fraud, and role-based targeting of industrial staff.
- **What would change this rating.** Raise to Level 2 if ransomware or Russia-linked attacks on Slovenian infrastructure intensify.

Public Wi-Fi

- Ransomware and business email compromise target Slovenian manufacturers and logistics operators; industrial and manufacturing staff should use a corporate VPN on all public Wi-Fi networks.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Mountain weather can change quickly in the Alps, so check conditions before outdoor activity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SOLOMON ISLANDS

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Honiara

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
English (with Pijin and about 70 indigenous languages)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued April 29, 2025)

Risk indicators: Unrest, crime, health, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Limited connectivity, basic phishing, and the potential for civil unrest in the capital.

Country Overview

The Solomon Islands is a Melanesian archipelago of nearly a thousand islands in the southwestern Pacific. Britain established a protectorate in 1893, and the island of Guadalcanal was the site of a major Pacific battle in 1942 and 1943. The country became independent in 1978.

The islands have about 750,000 people and an economy based on logging, fishing, and aid. Ethnic tension between Guadalcanal and Malaitan groups led to civil conflict from 1998 to 2003, which an Australian-led regional mission ended. Riots in Honiara in 2006, 2019, and 2021 reflected persistent grievances. Jeremiah Manele became prime minister in May 2024.

Geopolitical Landscape

- **China security pact.** A 2022 security agreement with China, and Beijing's later police cooperation, raised concern in Australia and the United States about Chinese influence in the Pacific.
- **Domestic fragility.** Riots over political and economic grievances, including the 2021 unrest, remain a recurring risk.
- **Provincial tensions.** Malaita province has resisted the government's 2019 switch of recognition from Taiwan to China.

Cyber Threats | Organizations

- **Limited digital footprint.** Connectivity depends on limited subsea and satellite links, and local security capacity is minimal.
- **Regional diplomatic targeting.** Pacific governments draw external espionage interest, including from Chinese actors.
- **Logging and fishing.** Operators hold commercial data and face fraud.
- **Employees based in country.** Employees face limited connectivity, basic phishing risk, and the potential for civil unrest in Honiara.
- **Vendor and supply chain risk.** A few external vendors provide connectivity and IT, so a single outage can have wide effects. Plan for offline operation and verify incident notification terms.

The TIDE team does not currently track actors that list Solomon Islands among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Phishing and fraud.** Our Telekom and Bmobile provide mobile service; Facebook is the main platform, and scams and impersonation spread there.
- **Limited connectivity.** Internet access outside Honiara is slow and costly.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Solomon Islands.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Solomon Islands Level 2, Exercise Increased Caution, citing unrest, crime, health, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity is limited, basic phishing is common, and civil unrest in Honiara is a recurring risk.
- **What would change this rating.** Raise to Level 3 if unrest returns with connectivity restrictions. Lower to Level 1 as political tension eases.

Public Wi-Fi

- The Coral Sea Cable System to Sydney was the sole international link until November 2025, when the Adamasia Cable System added redundancy; public Wi-Fi networks carry basic phishing risk alongside the documented Chinese espionage interest in Pacific governments. Use only a corporate VPN if internet access is unavoidable in hotel or airport networks, and plan for frequent connectivity loss given the limited infrastructure.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations in Honiara, and carry offline copies of key documents.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SOMALIA

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Mogadishu

GOVERNMENT
Federal parliamentary republic

LANGUAGE
Somali and Arabic

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued May 21, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, other, health

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Terrorism and kidnapping risk, surveillance by multiple armed actors, unreliable infrastructure, and a U.S. Level 4 advisory.

Country Overview

Somalia occupies the Horn of Africa and has the longest coastline on the African mainland. Italian and British colonies merged at independence in 1960. Siad Barre's military dictatorship collapsed in 1991, and the state broke apart into clan-based militias and warlord fiefdoms, followed by decades of civil war, famine, and piracy.

A federal government has operated since 2012, with Hassan Sheikh Mohamud as president since 2022. The northern region of Somaliland has governed itself since 1991 without international recognition. Somalia has about 20.3 million people and is among the world's poorest countries. The jihadist group al-Shabaab controls rural areas and conducts attacks in the capital.

Geopolitical Landscape

- **Al-Shabaab insurgency.** Al-Shabaab, an al-Qaeda affiliate, regained ground in 2025 against government and allied forces and carries out bombings and assaults in Mogadishu and elsewhere. The United States conducts regular airstrikes against it and the Islamic State's Somalia branch.

- **Political contest.** Disputes between the federal government and regional states over elections and constitutional changes make politics volatile.
- **International mission.** An African Union stabilization mission is replacing the earlier force, with funding gaps.
- **Humanitarian crisis.** Drought, conflict, and aid cuts leave millions in need.

Cyber Threats | Organizations

- **Insecurity and infrastructure.** Attacks, power cuts, and weak governance affect operations, and local security capacity is very limited.
- **Mobile money.** Hormuud's EVC Plus and other mobile money platforms are central to the economy and face fraud and SIM-swap.
- **State and militant surveillance.** Government and al-Shabaab both monitor communications, and al-Shabaab runs its own taxation and extortion networks.
- **Staff safety.** Leaks of staff, site, or convoy information can create direct physical risk.
- **Employees based in country.** Employees face terrorism and kidnapping risk, surveillance by multiple actors, and unreliable connectivity. Remove company access from personal devices and keep location and movements confidential.
- **Vendor and supply chain risk.** Local telecom, security, and logistics vendors operate under militant and clan pressure and may be forced to share data or lose access. Limit shared location data, segment vendor access, and plan for sudden loss of services.

The TIDE team does not currently track actors that list Somalia among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Extortion and surveillance.** Al-Shabaab uses phone and mobile-money data to extort and intimidate.
- **Kidnapping.** Kidnapping for ransom and political reasons occurs.
- **Mobile money fraud.** SMS and wallet scams are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Somalia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Somalia Level 4, Do Not Travel, citing unrest, crime, kidnapping or hostage-taking, terrorism, other, health. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has very limited ability to assist, and terrorism and kidnapping risk is high.

TIDE Risk Level Rationale

- **Drivers.** Terrorism and kidnapping risk, surveillance by multiple armed actors, unreliable infrastructure, and a U.S. Level 4 advisory drive the rating.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable reduction in al-Shabaab's reach and a functioning security system.

Public Wi-Fi

- Do not use any public network; connectivity itself is monitored by both the government and al-Shabaab for extortion and surveillance. This environment is Level 4 Maximum Cyber Precautions and prohibits bringing corporate devices or accessing corporate infrastructure regardless of VPN.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

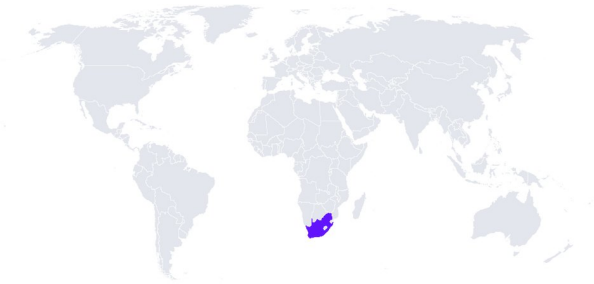
- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

SOUTH AFRICA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Pretoria (executive), Cape Town (legislative), Bloemfontein (judicial)

GOVERNMENT
Parliamentary republic

LANGUAGE
Eleven official languages, including Zulu, Xhosa, Afrikaans, and English

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 27, 2025)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Phone robbery, SIM-swap and banking fraud, carjacking risk, and extortion near organized crime.

Country Overview

South Africa is the southernmost country in Africa, with a diverse population and the continent's most industrialized economy. Dutch settlers founded Cape Town in 1652, and Britain took control of the Cape in the early nineteenth century. Gold and diamond discoveries drove conflict and economic change. The apartheid system of racial segregation was formalized in 1948.

Apartheid ended through negotiations, and Nelson Mandela was elected president in the country's first democratic election in 1994. The African National Congress governed alone for thirty years until it lost its majority in 2024 and formed a Government of National Unity with the Democratic Alliance and other parties. Cyril Ramaphosa is president. South Africa has about 63 million people and very high unemployment and inequality.

Geopolitical Landscape

- **Government of National Unity.** The ANC-led coalition, formed after the May 2024 election, has held together despite policy disputes, and local elections are due in 2026 and 2027.

- **Strained relations with the United States.** Washington expelled South Africa's ambassador in 2025, imposed tariffs, and criticized its land law and its genocide case against Israel at the International Court of Justice. The United States boycotted the November 2025 G20 summit that South Africa hosted.
- **Crime and extortion.** South Africa has one of the world's highest homicide rates, and extortion by so-called construction mafias affects projects and businesses.
- **Power and logistics.** Load shedding eased in 2024 and 2025, but port, rail, and grid reliability remain constraints.

Cyber Threats | Organizations

- **Ransomware.** Health, retail, logistics, and government bodies have been hit by ransomware, and national operators draw frequent attacks.
- **Banking and fintech.** Banks face account takeover, SIM-swap, and large fraud, and insiders have been recruited by fraud rings.
- **Critical infrastructure.** Ports, rail, and utilities are priority targets for criminals and for state-linked actors.
- **Regulation.** The Protection of Personal Information Act requires breach notification.
- **Employees based in country.** Employees face phone robbery, SIM-swap and banking fraud, and carjacking risk, and in some areas protest and unrest disrupt travel. Staff in logistics and finance face elevated targeted phishing.
- **Vendor and supply chain risk.** Logistics, security, and banking vendors operate near extortion and organized crime, and insider recruitment is a known risk. Vet vendor staff, limit shared personal data, and verify payment changes out of band.

The TIDE team tracks 26 threat actors that list South Africa among their targets. By attributed nexus, they break down as 17 cybercriminal, 5 China-nexus, 2 Iran-nexus, and 2 unattributed or other. The most frequently targeted sectors are government (16), healthcare and pharmaceuticals (16), industrial and manufacturing (12), technology (11), and education and research (11). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Violent crime and phone theft.** Smash-and-grab, carjacking, and phone robbery are common in major cities.
- **SIM swap and banking fraud.** Account takeover and fake bank calls are widespread.
- **Kidnapping.** Express kidnapping and extortion occur.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to South Africa.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates South Africa Level 2, Exercise Increased Caution, citing unrest, crime, kidnapping or hostage-taking, terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Phone robbery, SIM-swap and banking fraud, carjacking risk, and extortion near organized crime drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest or violence against business travelers escalates. Lower to Level 1 as crime and fraud decline.

Public Wi-Fi

- Public Wi-Fi in hotels and airports carries high risk from organized-crime networks and SIM-swap fraud rings known to target financial staff. If a public network must be used, always connect through a corporate VPN first and assume networks near financial districts are monitored.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Use hotel-arranged or app-based transport, avoid walking at night, and keep devices out of sight at traffic lights.
- Avoid townships and areas flagged in the advisory without a trusted local guide.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SOUTH KOREA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Seoul

GOVERNMENT
Presidential republic

LANGUAGE
Korean

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 28, 2025)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Secure and well-regulated; exposure is voice phishing and North Korean targeting of defense, technology, and crypto staff.

Country Overview

South Korea occupies the southern half of the Korean Peninsula, divided from North Korea after the Second World War. Japan colonized Korea from 1910 to 1945, and the 1950 to 1953 Korean War left the peninsula divided under an armistice. Authoritarian governments led rapid industrialization until democratization in 1987.

South Korea has about 51 million people and became one of the world's leading economies in electronics, shipbuilding, and automobiles. In December 2024 then-President Yoon Suk Yeol declared martial law, and the Constitutional Court removed him from office in April 2025. Lee Jae-myung won the June 2025 election and has been president since.

Geopolitical Landscape

- **Aftermath of martial law.** A Seoul court sentenced Yoon to life in prison on February 19, 2026 for leading an insurrection, after an earlier five-year sentence in January for obstructing his arrest, and he has appealed. Former prime minister Han Duck-soo received 23 years. The episode reshaped politics under a Democratic Party government.

- **North Korea.** South Korea and the United States held joint exercises in August 2026 amid continued North Korean missile tests and a deepening North Korea-Russia alliance, and a May 2026 joint statement urged the UN to designate sanctions-violating vessels.
- **U.S. alliance and trade.** Washington's tariff pressure and security-cost demands are tests for the alliance, and Seoul is balancing ties with China.
- **Demographics.** A very low birth rate and rapid aging weigh on the economy.

Cyber Threats | Organizations

- **Large breaches.** An April 2025 malware breach at SK Telecom exposed USIM data affecting its 23 million subscribers, and a December 2025 breach at the e-commerce platform Coupang compromised 33.7 million customer accounts.
- **North Korean targeting.** Lazarus, Kimsuky, and other North Korean groups target defense, government, research, and crypto firms with phishing and supply chain attacks.
- **Semiconductor and technology sector.** Chipmakers and suppliers hold valuable intellectual property and are targets for espionage.
- **Regulation.** South Korea has strict data protection rules and large penalties for breaches.
- **Employees based in country.** Employees face voice phishing and smishing and North Korean phishing lures, especially in technology, defense, and crypto roles. Street crime is low.
- **Vendor and supply chain risk.** Semiconductor suppliers, telecoms, and software vendors are priority targets for North Korean and Chinese actors, and breaches at one provider can affect many firms. Require supplier attestations, segmentation, and incident notification.

The TIDE team tracks 72 threat actors that list South Korea among their targets. By attributed nexus, they break down as 30 China-nexus, 18 cybercriminal, 11 North Korea-nexus, 7 unattributed or other, 5 Iran-nexus, and 1 hacktivist. The most frequently targeted sectors are government (42), technology (28), defense and defense industrial base (27), banking and financial services (24), and industrial and manufacturing (21). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Smishing and voice phishing.** Impersonation scams by phone and text, including fake prosecutors, are widespread.
- **Account takeover.** Credential theft targets online banking and gaming accounts.
- **Hidden cameras.** Spy-camera crimes have been a public concern.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to South Korea.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates South Korea Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** South Korea is secure and well-regulated. Exposure is voice phishing and North Korean targeting of defense, technology, and crypto staff.
- **What would change this rating.** Raise to Level 2 for staff in those sectors if North Korean targeting of travelers or tension on the peninsula escalates.

Public Wi-Fi

- While South Korea maintains strong infrastructure, North Korean-linked threat actors actively target public networks for supply chain attacks and phishing. Use a corporate VPN on any public network, particularly if you work in technology, defense, or crypto sectors.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Keep devices secured, and be cautious of unsolicited job or investment approaches from North Korea-linked recruiters.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SOUTH SUDAN

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Juba

GOVERNMENT
Transitional presidential republic

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued May 17, 2026)

Risk indicators: Crime, kidnapping or hostage-taking, unrest, health, other

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Armed conflict and kidnapping risk, state surveillance and shutdowns, negligible infrastructure, and a U.S. Level 4 advisory.

Country Overview

South Sudan is the world's youngest country, which gained independence from Sudan in July 2011 after decades of civil war and a referendum. It is landlocked, oil-rich, and among the poorest countries in the world, with about 15.8 million people.

A civil war between forces loyal to President Salva Kiir and Vice President Riek Machar began in December 2013 and killed hundreds of thousands. A 2018 peace deal created a power-sharing government, but implementation has stalled. Machar was placed under house arrest in March 2025 and put on trial that year, and elections have been repeatedly postponed.

Geopolitical Landscape

- **Fragile power-sharing.** Machar's detention and trial, fighting in Upper Nile and other states, and Kiir's moves to promote loyalists threaten to collapse the 2018 deal. Elections are scheduled for December 2026, and few expect them to be credible.

- **Economic collapse.** Oil exports depend on a pipeline through Sudan, whose war has repeatedly disrupted revenue, and civil servants go unpaid.
- **Sudan spillover.** Refugees and armed groups cross the border, and the Sudan war affects trade and security.
- **Humanitarian crisis.** Hunger, flooding, and aid cuts affect most of the population.

Cyber Threats | Organizations

- **Insecurity and infrastructure.** Fighting, banditry, and weak infrastructure disrupt operations, and local security capacity is minimal.
- **State surveillance.** The National Security Service monitors communications, has shut down internet access during unrest, and arrests critics.
- **Oil sector.** Operators and contractors hold valuable data and operate in insecure areas.
- **Staff safety.** Leaks of staff, site, or convoy information can create direct physical risk.
- **Employees based in country.** Employees face surveillance, detention, kidnapping, and connectivity shutdown risk. Remove company access from personal devices and keep location and movements confidential.
- **Vendor and supply chain risk.** Local telecom, security, and logistics vendors operate under state and armed-group pressure and may lose access abruptly. Limit shared location data, segment vendor access, and plan for sudden loss of services.

The TIDE team tracks 1 threat actor that lists South Sudan among their targets. By attributed nexus, they break down as 1 China-nexus. The most frequently targeted sectors are civil society and activism (1), and government (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Surveillance and detention.** Journalists, activists, and foreigners face arrest and monitoring.
- **Kidnapping.** Kidnapping and armed robbery occur, including on roads.
- **Mobile fraud.** SMS and wallet scams exist.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to South Sudan.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates South Sudan Level 4, Do Not Travel, citing crime, kidnapping or hostage-taking, unrest, health, other. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has very limited ability to assist, and armed conflict and crime are severe.

TIDE Risk Level Rationale

- **Drivers.** Armed conflict and kidnapping risk, state surveillance and shutdowns, negligible infrastructure, and a U.S. Level 4 advisory drive the rating.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable political settlement and security.

Public Wi-Fi

- Do not use any public network; both the National Security Service and armed groups monitor all communications for tracking and extortion. Connectivity may be shut down during unrest. This environment is Level 4 Maximum Cyber Precautions and prohibits bringing corporate devices or accessing corporate infrastructure regardless of VPN.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

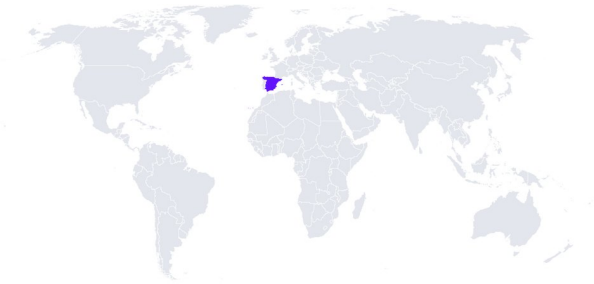
- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

SPAIN

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Madrid

GOVERNMENT
Parliamentary constitutional monarchy

LANGUAGE
Spanish (with Catalan, Galician, and Basque co-official regionally)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued August 1, 2026)

Risk indicators: Unrest, terrorism

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable EU member; exposure is pickpocketing, phishing, and a history of spyware use against political figures.

Country Overview

Spain occupies most of the Iberian Peninsula and was shaped by Roman, Visigothic, and Muslim rule. The Reconquista ended with the fall of Granada in 1492, the same year Columbus sailed, and Spain built a global empire. Decline and civil conflict followed, ending in the 1936 to 1939 Civil War and Francisco Franco's dictatorship.

Spain transitioned to democracy after Franco's death in 1975, joined the EU in 1986, and has about 49.8 million people. Tourism, services, and manufacturing drive the economy. Pedro Sanchez has been prime minister since 2018 and leads a minority coalition that relies on regional parties.

Geopolitical Landscape

- **Fragile minority government.** Sanchez's government depends on Catalan and Basque parties and has faced corruption scandals touching his party and family, which makes legislation difficult.
- **Catalonia.** The amnesty for Catalan separatist leaders remains politically contentious.
- **Iberian blackout.** A power outage on April 28, 2025 across Spain and Portugal shut down transport and communications for hours and led to investigations into grid resilience.

- **Migration and housing.** Arrivals through the Canary Islands and a severe housing crisis dominate debate.

Cyber Threats | Organizations

- **Ransomware.** Hospitals, telecoms, and companies have been hit by ransomware and data breaches.
- **Spyware affair.** Citizen Lab identified at least 65 people, including members of the European Parliament, Catalan presidents, and legislators, who were targeted or infected with mercenary spyware.
- **Hacktivism.** Pro-Russia DDoS campaigns target Spanish government and transport sites.
- **Tourism sector.** Hotels and booking platforms hold payment and passport data and face fraud and ransomware.
- **Regulation.** Spain implements NIS2 and the GDPR.
- **Employees based in country.** Employees face pickpocketing and phone theft in Barcelona and Madrid, bank and courier phishing, and rental fraud. Staff in government-adjacent or political roles should note the history of spyware targeting.
- **Vendor and supply chain risk.** Telecoms, hospitality platforms, and managed service providers hold concentrated data, and the 2025 blackout showed dependence on shared infrastructure. NIS2 extends duties to suppliers, so require attestations and incident notification.

The TIDE team tracks 69 threat actors that list Spain among their targets. By attributed nexus, they break down as 51 cybercriminal, 5 Iran-nexus, 4 China-nexus, 3 unattributed or other, 2 Russia-nexus, 2 hacktivist, 1 Pakistan-nexus, and 1 Turkey-nexus. The most frequently targeted sectors are healthcare and pharmaceuticals (42), industrial and manufacturing (33), government (31), technology (29), and education and research (24). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Pickpocketing and phone theft.** Theft is very common in Barcelona and Madrid tourist areas and on public transport.
- **Phishing and impersonation.** Messages impersonating banks, couriers, and the tax agency circulate in Spanish.
- **Rental and booking fraud.** Fake listings target visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Spain.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Spain Level 2, Exercise Increased Caution, citing unrest, terrorism. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Spain is a stable EU member. Exposure is pickpocketing, phishing, and confirmed historical spyware targeting of senior politicians, including Prime Minister Pedro Sanchez, between 2015 and 2021. Spain's own criminal probe into that targeting was shelved in January 2026 after Israeli authorities declined to cooperate, and no new, active targeting campaign has been documented since.
- **What would change this rating.** Raise to Level 2 for politically exposed, government, or advocacy-sector staff if a new or active spyware campaign, rather than the historical 2015 to 2021 infections, is documented.

Public Wi-Fi

- While Spain is a stable EU member, public networks in Barcelona and Madrid present elevated phishing and ransomware risk from organized-crime networks targeting tourists. Use a corporate VPN if public Wi-Fi must be used, particularly near tourist areas.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Keep phones and wallets secured in crowds, on the metro, and at tourist sites, where pickpocketing is common.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SRI LANKA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Sri Jayawardenepura Kotte (executive and legislative), Colombo (commercial)

GOVERNMENT
Presidential republic

LANGUAGE
Sinhala and Tamil (English widely used)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued October 14, 2025)

Risk indicators: Unrest, terrorism, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Monitoring of online speech under security and online-safety laws, tourist scams, and flood and protest disruption.

Country Overview

Sri Lanka is an island nation off the southern tip of India, with a history of Buddhist kingdoms dating back more than two thousand years. Portugal, the Netherlands, and Britain colonized coastal areas in turn, and Sri Lanka became independent as Ceylon in 1948.

A civil war between the government and the Tamil Tigers ran from 1983 to 2009 and killed an estimated 100,000 people. Sri Lanka has about 22 million people, a tourism and tea economy, and recovered from a 2022 sovereign default and mass protests that toppled the president. Anura Kumara Dissanayake of the left-leaning National People's Power coalition won the September 2024 presidential election.

Geopolitical Landscape

- **Economic recovery.** Sri Lanka completed a debt restructuring and continues an IMF program, while reforms and taxes weigh on households.
- **New government.** Dissanayake's government won a strong parliamentary majority in November 2024 on an anti-corruption platform.

- **Cyclone Ditwah.** Floods and landslides after a cyclone in late 2025 killed hundreds and damaged infrastructure.
- **India and China.** Colombo balances ties with its two large neighbors and has curbed Chinese research-vessel visits.
- **Online speech law.** The 2024 Online Safety Act drew criticism for threatening free expression.

Cyber Threats | Organizations

- **State monitoring.** Authorities monitor communications and online speech, and the Online Safety Act gives a commission broad powers.
- **Fintech and banking.** Banks and wallets face phishing and account takeover.
- **Tourism sector.** Hotels and booking platforms hold payment and passport data and face fraud.
- **Limited security capacity.** Public bodies have thin security staffing, and breaches have exposed personal data.
- **Employees based in country.** Employees face tourist-area scams, phishing, and possible disruption from floods or protests. Staff in media and civil society should note the legal risk around online speech.
- **Vendor and supply chain risk.** Local telecom, banking, and tourism vendors have thin security capacity. Verify supplier controls and out-of-band payment verification.

The TIDE team tracks 4 threat actors that list Sri Lanka among their targets. By attributed nexus, they break down as 3 India-nexus, and 1 China-nexus. The most frequently targeted sectors are government (4), military (3), defense and defense industrial base (2), education and research (2), and telecommunications (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and speech risk.** Online criticism can lead to arrest under security and online-safety laws.
- **Tourist-targeted scams.** Fake gem, taxi, and booking scams target visitors.
- **Phishing.** Bank and wallet impersonation circulates in Sinhala, Tamil, and English.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Sri Lanka.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Sri Lanka Level 2, Exercise Increased Caution, citing unrest, terrorism, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Monitoring of online speech under security and online-safety laws, tourist scams, and flood and protest disruption drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest returns with shutdowns or detentions of foreigners. Lower to Level 1 as the legal environment eases.

Public Wi-Fi

- Public networks carry phishing risk, and online activity is monitored under online-safety laws. Use a corporate VPN if a public network is necessary, and be cautious of bank and wallet impersonation messages circulating in local languages.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Monitor monsoon and cyclone alerts, and avoid demonstrations.

Return protocol

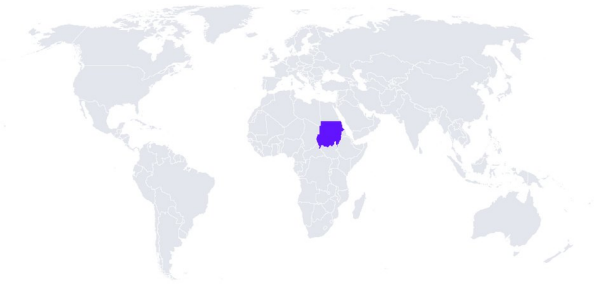
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SUDAN

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Khartoum (the army-aligned government operates from Port Sudan and elsewhere)

GOVERNMENT
Military-led transitional government in a state of civil war

LANGUAGE
Arabic and English

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued May 15, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, other, health

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Active civil war with drone strikes, detention, connectivity loss, no U.S. embassy operations, and a U.S. Level 4 advisory.

Country Overview

Sudan lies on the Nile in northeastern Africa and was home to the ancient Kingdom of Kush and Nubian civilizations. Egypt and Britain ruled it jointly until independence in 1956. Civil war between the north and south lasted most of the time until South Sudan seceded in 2011.

Omar al-Bashir ruled from 1989 until a 2019 popular uprising removed him. A 2021 coup by the army chief Abdel Fattah al-Burhan and Rapid Support Forces commander Mohamed Hamdan Dagalo, known as Hemedti, ended the civilian transition. The two then fought each other from April 2023, in a war that has killed tens of thousands, displaced about 12 million people, and created the world's largest humanitarian crisis.

Geopolitical Landscape

- **Civil war.** The army controls the north, east, and center, including Khartoum, which it retook in March 2025. The RSF captured El Fasher, the army's last Darfur stronghold, in October 2025 after an 18-month siege, with mass killings and other atrocities reported, and it now controls all five Darfur state capitals.

- **Fighting in Kordofan.** The army launched an offensive in late July 2026 that retook the Khartoum-El Obeid corridor and towns including Bara. The RSF launched kamikaze drone attacks on El Obeid, Atbara, Omdurman, and Khartoum on August 12 and continues to strike El Obeid, according to the Security Council Report and UN officials.
- **Failed diplomacy.** The RSF accepted a Quad humanitarian truce proposal in November 2025, but Burhan rejected a 90-day truce in September 2026 after Washington withheld his visa for the UN General Assembly, and the Security Council reports no breakthrough.
- **Foreign backing.** A September 2026 UN report found foreign recruitment and external support networks are fueling the conflict and upgrading drone capabilities on both sides.

Cyber Threats | Organizations

- **Drone strikes on infrastructure.** Drone attacks on power stations, fuel depots, and civilian sites have caused blackouts and disrupted operations.
- **Connectivity disruption.** The war has cut telecom networks and power repeatedly, and both sides can restrict access.
- **Surveillance by armed actors.** Both the army and RSF monitor communications, and civilians face abduction and extortion.
- **Staff safety.** Leaks of staff, site, or convoy information can create direct physical risk.
- **Employees based in country.** Employees face armed conflict, drone strikes, detention, and connectivity loss. Do not travel, and remove company access from personal devices of any staff in the country.
- **Vendor and supply chain risk.** Local telecom, logistics, and security vendors operate under both armies and the RSF and may lose access abruptly. Limit shared location data and plan for sudden loss of services.

The TIDE team tracks 3 threat actors that list Sudan among their targets. By attributed nexus, they break down as 1 Iran-nexus, 1 unattributed or other, and 1 Turkey-nexus. The most frequently targeted sectors are government (3), telecommunications (2), banking and financial services (1), defense and defense industrial base (1), and electronics and semiconductors (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Detention and extortion.** Checkpoints and armed groups detain, rob, and extort civilians and aid workers.
- **Communications disruption.** Starlink and local networks are contested, and shutdowns are frequent.
- **Mobile money fraud.** Fake agent and bank app scams spread among displaced people.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Sudan.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Sudan Level 4, Do Not Travel, citing unrest, crime, kidnapping or hostage-taking, terrorism, other, health. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has no embassy operations in Sudan and cannot assist, and conflict is ongoing.

TIDE Risk Level Rationale

- **Drivers.** Active civil war with drone strikes on cities, detention, connectivity loss, no U.S. embassy operations, and a U.S. Level 4 advisory drive the rating.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable ceasefire and restored basic services.

Public Wi-Fi

- Do not use any public network; armed actors and the National Security Service monitor all communications, and drone strikes on infrastructure create frequent outages. This environment is Level 4 Maximum Cyber Precautions and prohibits bringing corporate devices or accessing corporate infrastructure regardless of VPN.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

SURINAME

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Paramaribo

GOVERNMENT
Presidential republic

LANGUAGE
Dutch

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued September 8, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is phishing, opportunistic theft, and thin local security capacity.

Country Overview

Suriname is the smallest independent country in South America and has a diverse population descended from Indigenous peoples, enslaved Africans, indentured laborers from India and Java, and Dutch settlers. The Netherlands colonized it until independence in 1975, and a 1980 military coup led by Desi Bouterse began a period of dictatorship and a civil war in the 1980s.

Suriname has about 620,000 people and is covered largely by rainforest. Jennifer Geerlings-Simons became president in July 2025. The economy depends on gold, oil, and aid, and a large offshore oil project led by TotalEnergies promises new revenue starting in the late 2020s.

Geopolitical Landscape

- **Offshore oil.** A major offshore project is expected to begin production by 2028, and the government seeks to manage the revenue after a debt restructuring.
- **Political transition.** Geerlings-Simons became the first woman president after the 2025 election, following Chandrikapersad Santokhi's term.
- **Neighbors.** Suriname maintains a border dispute with Guyana over the Tigri area and works with Brazil, China, and the Netherlands.

Cyber Threats | Organizations

- **Small-state resourcing.** Government and firms have limited cybersecurity capacity and rely on a few vendors and Dutch support.
- **Mining and oil.** Operators and contractors hold valuable data and face fraud and espionage.
- **Banking.** A small banking sector faces phishing and fraud.
- **Employees based in country.** Employees face ordinary phishing and opportunistic theft in Paramaribo.
- **Vendor and supply chain risk.** A few local vendors and Dutch parent companies carry most exposure, and oil-project contractors are higher-value targets. Verify subcontractor controls.

The TIDE team does not currently track actors that list Suriname among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Phishing and wallet fraud.** State-owned Telesur (TeleG) and Digicel provide mobile service; bank impersonation circulates in Dutch and Sranan Tongo, and police have reported a rise in online sales fraud using forged bank-transfer receipts to obtain goods without payment.
- **Phone theft.** Opportunistic theft occurs in Paramaribo.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Suriname.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Suriname Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with phishing, opportunistic theft, and thin local security capacity as the main exposure.
- **What would change this rating.** Raise to Level 2 if targeting of the new oil sector increases.

Public Wi-Fi

- Connectivity relies on the Suriname-Guyana Submarine Cable System and the Americas II cable; public Wi-Fi carries low surveillance risk but basic phishing and the forged-payment-receipt scam pattern remain present. Use a corporate VPN if a public network must be used, and verify any payment receipt directly with your bank rather than accepting a forwarded image as proof of payment.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Keep devices out of sight in Paramaribo, and carry offline maps in the interior.

Return protocol

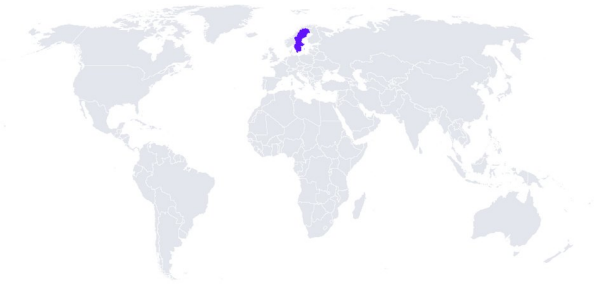
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SWEDEN

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Stockholm

GOVERNMENT
Parliamentary constitutional monarchy

LANGUAGE
Swedish

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 18, 2026)

Risk indicators: Terrorism

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; exposure is BankID phishing, gang violence in some areas, and role-based state-linked targeting.

Country Overview

Sweden is a Scandinavian country that was a major power in the seventeenth century and has avoided war since 1814, remaining neutral in both world wars. It built a high-tax welfare state and a strong export economy. Sweden joined the EU in 1995 but not the euro.

It has about 10.6 million people and joined NATO in March 2024 after two centuries of nonalignment. Gang violence, which includes shootings and bombings, rose sharply in the 2020s and became a defining political issue.

Geopolitical Landscape

- **2026 election.** The center-left opposition led by Magdalena Andersson's Social Democrats won 176 of 349 seats in the September 13 election, narrowly ahead of Prime Minister Ulf Kristersson's right-wing bloc with 173 seats. The far-right Sweden Democrats lost ground. Kristersson resigned on September 17 and leads a caretaker government while the speaker oversees formation of a new one. Parliament could vote on a new prime minister from September 29, and the left bloc faces internal divisions between the Left Party and the Centre Party.

- **Security posture.** As a NATO member on the Baltic Sea, Sweden is increasing defense spending and hosts allied forces, and it is concerned about Russian hybrid threats and undersea infrastructure.
- **Gang violence.** Organized criminal networks recruit children and use encrypted apps, and some attacks have been ordered from abroad, including by Iran-linked criminal proxies according to Swedish authorities.
- **Quran-burning aftermath.** Protests abroad over 2023 incidents contributed to a heightened terrorism threat level.

Cyber Threats | Organizations

- **State-linked espionage.** Russia- and China-linked actors target government, defense, and research, and Swedish authorities have warned of Russian sabotage plots.
- **Ransomware and supply chain.** In January 2024 a ransomware attack on Sweden's only digital service provider for government services affected operations at 120 government offices, which showed supplier concentration risk.
- **Hacktivism and DDoS.** Pro-Russia groups have targeted Swedish government and financial sites, especially around the NATO accession.
- **Regulation.** Sweden implements NIS2.
- **Employees based in country.** Employees face BankID phishing and pickpocketing in Stockholm. Staff in defense, energy, and technology roles may draw state-linked targeting.
- **Vendor and supply chain risk.** Managed service providers and software suppliers are concentrated third parties, as past incidents showed. NIS2 extends security duties to suppliers, so require attestations and incident notification.

The TIDE team tracks 29 threat actors that list Sweden among their targets. By attributed nexus, they break down as 17 cybercriminal, 5 China-nexus, 2 Russia-nexus, 2 Iran-nexus, 1 unattributed or other, 1 Turkey-nexus, and 1 hacktivist. The most frequently targeted sectors are government (21), healthcare and pharmaceuticals (18), industrial and manufacturing (16), education and research (14), and technology (12). These figures count actors, not incidents.

Cyber Threats | Individuals

- **BankID fraud.** Phishing and social engineering to steal BankID credentials are widespread.
- **Marketplace fraud.** Fake listings and payment-link scams affect buyers.
- **Pickpocketing.** Theft occurs on Stockholm transit and tourist areas.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Sweden.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Sweden Level 2, Exercise Increased Caution, citing terrorism. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Sweden is stable and well-regulated. Exposure is BankID phishing, gang violence in some areas, and role-based state-linked targeting.
- **What would change this rating.** Raise to Level 2 for staff in defense, energy, and technology if Russia-linked sabotage or targeting escalates.

Public Wi-Fi

- Sweden is a stable NATO member with strong security, but public networks in Stockholm present pickpocketing risk and state-linked espionage targeting defense and technology staff. Staff in those sectors should use a corporate VPN on any public network.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Avoid areas of gang-related violence flagged by local police, and keep devices secured on transit.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SWITZERLAND

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Bern

GOVERNMENT
Federal republic with direct democracy

LANGUAGE
German, French, Italian, and Romansh

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued August 14, 2026)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; exposure is targeted fraud in finance and state-linked targeting of diplomats and bankers.

Country Overview

Switzerland is an Alpine country that emerged from the medieval Swiss Confederacy, traditionally dated to 1291, and has been neutral since 1815. Its modern federal state was created in 1848. It has not fought a foreign war in over two centuries and remained neutral in both world wars.

Switzerland has about 9.2 million people, four national languages, and a highly developed economy based on finance, pharmaceuticals, machinery, and precision manufacturing. It is not a member of the EU or NATO but is in the Schengen Area and has extensive bilateral agreements with the EU.

Geopolitical Landscape

- **U.S. tariffs.** The United States imposed a 39 percent tariff on Swiss goods in August 2025 and later agreed to a lower rate in a November 2025 deal, which affected pharmaceuticals and watches.
- **Neutrality under pressure.** Switzerland adopted EU sanctions on Russia and debates arms-export rules and closer cooperation with NATO.
- **EU relations.** A package of bilateral agreements with the EU awaits approval by Swiss voters.
- **Banking.** The emergency takeover of Credit Suisse by UBS in 2023 raised concern about bank stability and led to new capital rules.

Cyber Threats | Organizations

- **Ransomware and data theft.** A May 2023 breach exposed about 65,000 Swiss federal administration documents, and municipalities and hospitals have also been hit.
- **State-linked espionage.** Geneva hosts international organizations, and Russia- and China-linked actors target diplomats, banks, and research.
- **Financial sector.** Private banks and asset managers hold high-value client data and face targeted phishing and extortion.
- **Regulation.** Critical infrastructure operators in Switzerland have cyberattack reporting duties, so confirm notification obligations with local counsel.
- **Employees based in country.** Employees face targeted phishing and payment fraud, especially in banking and wealth management, and staff at international organizations in Geneva face state-linked targeting.
- **Vendor and supply chain risk.** Managed service providers, fintechs, and IT suppliers to government and banks are concentrated third parties. Require attestations, segmentation, and incident notification.

The TIDE team tracks 26 threat actors that list Switzerland among their targets. By attributed nexus, they break down as 12 cybercriminal, 8 China-nexus, 3 Russia-nexus, 2 Iran-nexus, and 1 Turkey-nexus. The most frequently targeted sectors are government (12), banking and financial services (11), healthcare and pharmaceuticals (10), technology (9), and industrial and manufacturing (9). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, post, and police are common in German, French, and Italian.
- **Rental and marketplace fraud.** Fake listings and payment scams affect buyers and visitors.
- **Pickpocketing.** Theft occurs at stations and tourist sites.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Switzerland.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Switzerland Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Switzerland is stable and well-regulated. Exposure is targeted fraud in finance and state-linked targeting of diplomats and bankers.
- **What would change this rating.** Raise to Level 2 for staff in those roles if targeted campaigns intensify.

Public Wi-Fi

- Switzerland is well-regulated, but public networks in Geneva and financial districts face targeted phishing from state-linked actors and wealth management fraud schemes. Use a corporate VPN if a public network must be used, especially in banking areas.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Mountain weather changes quickly, so check conditions before outdoor activity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

SYRIA

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4

CAPITAL
Damascus

GOVERNMENT
Transitional government led by an interim president

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued August 7, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism, other

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Armed conflict and kidnapping risk, multi-actor surveillance, damaged infrastructure, residual sanctions, and a U.S. Level 4 advisory.

Country Overview

Syria lies in the heart of the Levant and contains some of the world's oldest continuously inhabited cities, including Damascus and Aleppo. The Ottoman Empire ruled it until the First World War, after which France held a mandate. Syria became independent in 1946.

The Assad family ruled from 1970, first Hafez al-Assad and then Bashar al-Assad from 2000. A 2011 uprising became a civil war that killed hundreds of thousands and displaced about half the population. In December 2024 an offensive led by Hayat Tahrir al-Sham toppled Assad. Ahmed al-Sharaa, the group's former leader, now leads an interim government.

Geopolitical Landscape

- **Transitional government.** Al-Sharaa governs with an appointed legislature chosen through indirect elections in October 2025 that excluded some areas. The government has had to manage sectarian violence on the coast in early 2025 and in the Druze-majority south in mid-2025.

- **SDF and the northeast.** After a January 2026 government advance, the government and the Kurdish-led SDF agreed on January 29, 2026 to integrate civilian and military institutions in the northeast, though al-Sharaa acknowledged implementation delays in July 2026.
- **Israel.** Israel struck Syrian targets and holds positions in the south, and al-Sharaa said in July 2026 that Damascus is seeking a security agreement with Israel.
- **Sanctions and economy.** The United States and others have lifted many sanctions, but al-Sharaa says relief will not take full effect while Syria stays on the U.S. list of state sponsors of terrorism.

Cyber Threats | Organizations

- **Fragile infrastructure.** Power, telecoms, and banking are damaged, and operations face frequent outages and an unsettled legal framework.
- **Armed-actor surveillance.** Multiple factions monitor communications, and civilians face detention and abduction.
- **Sanctions and counterparties.** Residual sanctions, designated individuals, and unclear ownership of companies create compliance risk.
- **Terrorist and criminal activity.** Islamic State cells remain active, and kidnapping and extortion occur.
- **Employees based in country.** Employees face armed-conflict, kidnapping, and detention risk, unreliable connectivity, and compliance exposure. Do not travel, and remove company access from personal devices of any staff in the country.
- **Vendor and supply chain risk.** Local telecom, logistics, and security vendors have unclear ownership and operate among competing armed actors, and sanctions exposure remains. Screen ownership, segment vendor access, and plan for sudden loss of services.

The TIDE team tracks 8 threat actors that list Syria among their targets. By attributed nexus, they break down as 3 unattributed or other, 2 Iran-nexus, 2 Turkey-nexus, and 1 hacktivist. The most frequently targeted sectors are government (5), civil society and activism (2), media and journalism (2), defense and defense industrial base (2), and telecommunications (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Detention and kidnapping.** Armed groups and security forces have detained and kidnapped civilians and foreigners.
- **Communications monitoring.** Authorities and factions monitor communications, and connectivity is unreliable.
- **Fraud.** Money-transfer and wallet scams are common in a cash-dependent economy.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Syria.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Syria Level 4, Do Not Travel, citing unrest, crime, kidnapping or hostage-taking, terrorism, other. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has very limited ability to assist, and armed conflict and kidnapping risks are severe.

TIDE Risk Level Rationale

- **Drivers.** Armed conflict and kidnapping risk, multi-actor surveillance, damaged infrastructure, residual sanctions, and a U.S. Level 4 advisory drive the rating.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require durable security across the country and a settled sanctions framework.

Public Wi-Fi

- Do not use any public network; multiple armed factions and security forces actively monitor all communications and detain civilians for their online activity. This environment is Level 4 Maximum Cyber Precautions and prohibits bringing corporate devices or accessing corporate infrastructure regardless of VPN.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

TAIWAN

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2

CAPITAL
Taipei

GOVERNMENT
Semi-presidential republic

LANGUAGE
Mandarin Chinese (with Taiwanese Hokkien, Hakka, and indigenous languages)

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued November 25, 2025)

Note: The United States maintains unofficial relations with Taiwan under the Taiwan Relations Act. It acknowledges the Chinese position that there is one China and takes no position on Taiwan's sovereignty.

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Heavy state-linked cyber activity, influence operations, and potential for sudden disruption from PLA drills or a crisis, with low risk to ordinary visitors.

Country Overview

Taiwan is an island off the southeastern coast of China with an Indigenous Austronesian population and later Dutch, Spanish, Qing Chinese, and Japanese rule. Japan took Taiwan in 1895 and held it until 1945. After the Chinese Civil War, the Republic of China government under Chiang Kai-shek retreated to Taiwan in 1949.

Taiwan ended martial law in 1987 and became a vibrant democracy, with a peaceful change of party in power in 2000. It has about 23 million people and dominates advanced semiconductor manufacturing. Lai Ching-te of the Democratic Progressive Party has been president since May 2024. The People's Republic of China claims Taiwan and has not ruled out force.

Geopolitical Landscape

- **Military pressure.** China held a large drill around Taiwan in late December 2025 after a record 11.1 billion dollar U.S. arms package, and its aircraft entered Taiwan's air defense zone more than 420 times in the first quarter of 2026. Gray-zone pressure through coast guard patrols, cyber operations, and influence campaigns continues.

- **U.S. policy uncertainty.** A package of about 14 billion dollars in U.S. arms sales was reportedly paused after President Trump discussed Taiwan with Xi Jinping, and Trump called arms sales a negotiating chip after his May visit to China. Xi's September 2026 Washington visit was the main diplomatic event, and the issue remains unresolved.
- **November 28 local elections.** Taiwan holds nine-in-one local elections on November 28, 2026. President Lai accused Beijing in August of using fake news and fabricated polls to interfere, and the National Security Bureau expects AI-generated deepfakes, false surveys, and illegal betting rings.
- **Domestic politics and defense.** The opposition-controlled legislature approved about 24.8 billion dollars of the roughly 40 billion dollars in defense spending Lai sought, and the cabinet approved a 2027 defense budget at about 3 percent of GDP.

Cyber Threats | Organizations

- **Massive intrusion volume.** The National Security Bureau said the government service network was attacked more than 173 million times in the first quarter of 2026 for intelligence gathering, surveillance, and data theft.
- **AI-assisted state operations.** AEI and ISW reported in August 2026 that suspected Chinese actors ran a largely autonomous attack that mapped 21 government systems, compromised more than 85 accounts, extracted more than 2,500 personnel records, and reached the Nuclear Safety Commission and at least seven energy companies.
- **Semiconductor and technology sector.** Chip makers, equipment suppliers, and design firms hold the world's most valuable manufacturing intellectual property and are priority targets for espionage, insider recruitment, and supply chain attacks.
- **Subsea cables and infrastructure.** Taiwan depends on a few subsea cables that have been cut, and energy and telecom networks are targets for disruption.
- **Insider recruitment.** A Taiwanese soldier was indicted in August 2026 for passing military records to a China-linked organization for money.
- **Employees based in country.** Employees face targeted phishing and influence campaigns, and staff in semiconductor, government, defense, and energy roles are priority targets for state-linked actors. Ordinary street crime is low.
- **Vendor and supply chain risk.** Semiconductor suppliers, equipment makers, and managed service providers are high-value targets for state-linked espionage and insider recruitment. A crisis in the Taiwan Strait could disrupt logistics and supply chains worldwide, so review concentration risk, require supplier attestations and segmentation, and plan for connectivity and shipping disruption.

The TIDE team tracks 71 threat actors that list Taiwan among their targets. By attributed nexus, they break down as 50 China-nexus, 16 cybercriminal, 1 North Korea-nexus, 1 India-nexus, 1 unattributed or other, 1 Iran-nexus, and 1 hacktivist. The most frequently targeted sectors are government (44), defense and defense industrial base (23), technology (23), education and research (15), and healthcare and pharmaceuticals (14). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Influence and disinformation.** AI-enabled deepfakes, false polls, and coordinated posting target voters, especially before the November elections.
- **Targeted phishing.** Officials, researchers, and journalists receive tailored phishing and fake-persona approaches.
- **Scams.** Investment, romance, and impersonation scams are widespread, including LINE-based fraud.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Taiwan.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Taiwan Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Heavy state-linked cyber activity, influence operations ahead of the November 28 elections, and the potential for sudden disruption from PLA drills or a crisis drive the rating. Risk to ordinary visitors is low.
- **What would change this rating.** Raise to Level 3 if a blockade, quarantine, or major escalation occurs, or if targeting of foreign visitors begins. Lower to Level 1 as cross-strait pressure eases.

Public Wi-Fi

- Taiwan faces massive state-linked intrusion volume targeting government and semiconductor networks, with 173 million attacks on government services alone in early 2026. Public networks present elevated risk of targeted phishing and AI-assisted surveillance, particularly for technology and defense staff; use a corporate VPN on any public network.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Monitor PLA drill announcements and airspace notices, which can disrupt flights and shipping with little warning.
- Be cautious of unsolicited job, investment, or networking approaches, which can be intelligence-gathering attempts.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

TAJIKISTAN

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Dushanbe

GOVERNMENT
Presidential republic (authoritarian)

LANGUAGE
Tajik (Russian widely used)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 4, 2026)

Risk indicators: Terrorism, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Blocked platforms and possible connectivity restrictions, state monitoring, and Afghan border risk.

Country Overview

Tajikistan is a mountainous Central Asian country, more than 90 percent of it covered by mountains, with a Persian-speaking population closely tied to the cultures of Iran and Afghanistan. Russia absorbed the region in the nineteenth century, and Tajikistan became a Soviet republic and then gained independence in 1991. A civil war from 1992 to 1997 killed tens of thousands.

President Emomali Rahmon has ruled since 1992 and is widely expected to hand power to his son, Rustam Emomali. Tajikistan has about 10.7 million people, relies heavily on remittances from migrant workers in Russia, and shares a long border with Afghanistan.

Geopolitical Landscape

- **Afghan border.** Instability across the border includes cross-border attacks that have killed Chinese workers in late 2025 according to reports, which prompted Chinese and Tajik security measures.
- **Dynastic succession.** Rahmon has built a system around his family, and a transfer of power to his son is anticipated.
- **Russia and terrorism.** Tajik nationals were arrested after the March 2024 Crocus City Hall attack in Moscow, which increased discrimination and scrutiny of Tajik migrants in Russia.

- **Political space.** Opposition and independent media are suppressed, and critics abroad face pressure.

Cyber Threats | Organizations

- **Connectivity controls.** Authorities block social media and messaging services and have restricted internet access during unrest.
- **State surveillance.** Security services monitor communications and online activity, and VPN use is restricted.
- **Remittance and banking sector.** Banks and transfer services face fraud and sanctions-related counterparty risk.
- **Limited security capacity.** Public bodies and firms have thin staffing and basic defenses.
- **Employees based in country.** Employees should assume communications can be monitored and expect blocked platforms and possible connectivity restrictions. Avoid political commentary and the Afghan border region.
- **Vendor and supply chain risk.** State-linked telecoms and local IT vendors can be compelled to share data, and banks carry sanctions-related counterparty risk. Segment vendor access and screen counterparties.

The TIDE team tracks 3 threat actors that list Tajikistan among their targets. By attributed nexus, they break down as 2 China-nexus, and 1 Russia-nexus. The most frequently targeted sectors are defense and defense industrial base (3), aerospace (2), government (2), healthcare and pharmaceuticals (1), and technology (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and arrest.** Online criticism of the government can lead to prosecution, and dissidents abroad have been targeted.
- **Device and network risk.** Mobile networks are monitored and some sites and apps are blocked.
- **Fraud.** Phishing and wallet scams circulate in Tajik and Russian.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Tajikistan.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Tajikistan Level 2, Exercise Increased Caution, citing terrorism, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Blocked platforms and possible connectivity restrictions, state monitoring, and Afghan border risk drive the rating.
- **What would change this rating.** Raise to Level 3 if instability on the Afghan border escalates or restrictions tighten. Lower to Level 1 if controls ease.

Public Wi-Fi

- State authorities actively monitor public networks and restrict social media and messaging platforms; VPN use itself may face scrutiny. Do not assume a VPN provides reliable protection, and plan for potential connectivity restrictions if unrest emerges.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid the Afghan border and the Gorno-Badakhshan region flagged in the advisory.

Return protocol

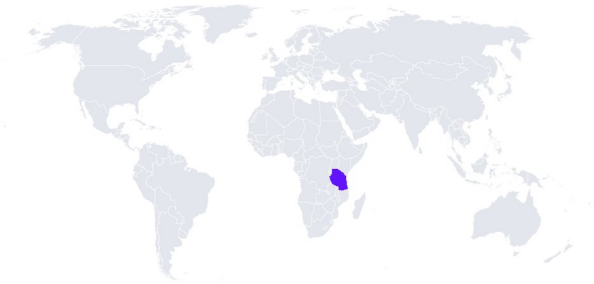
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

TANZANIA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Dodoma (Dar es Salaam is the commercial center)

GOVERNMENT
Presidential republic (dominant-party)

LANGUAGE
Swahili and English

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued October 31, 2025)

Risk indicators: Crime, terrorism, other, unrest

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Nationwide internet shutdown precedent, lethal force during the 2025 election, state monitoring, abductions of critics, and a U.S. Level 3 advisory.

Country Overview

Tanzania in East Africa includes Mount Kilimanjaro, the Serengeti, and the spice islands of Zanzibar. Swahili coastal trade and Omani rule shaped the coast, and Germany and then Britain colonized the mainland. Tanganyika became independent in 1961 and united with Zanzibar in 1964 to form Tanzania.

The Chama Cha Mapinduzi party has governed since independence. Tanzania has about 70 million people and a growing economy based on agriculture, gold, tourism, and gas. Samia Suluhu Hassan became president in 2021 after John Magufuli's death and won a full term in October 2025.

Geopolitical Landscape

- **October 2025 election crisis.** Samia won the October 29, 2025 election with about 98 percent of the vote after her main challengers were jailed or barred. Protests on election day met lethal force, a curfew and a roughly week-long nationwide internet shutdown followed, and the opposition Chadema said at least 800 people were killed, which the government has not confirmed. More than 200 people were charged with treason, and opposition leader Tundu Lissu remains on trial for treason.

- **International reaction.** SADC observers said the vote fell short of free and fair standards, and the State Department added an unrest indicator to its advisory on October 31, 2025.
- **Regional ties.** Tanzania's security forces clashed with Kenyan police at the border during the unrest, and activists from neighboring countries have been abducted in Tanzania.
- **Economy.** The internet shutdown cost an estimated hundreds of millions of dollars and rattled investors.

Cyber Threats | Organizations

- **State-imposed shutdowns.** Authorities cut internet access nationwide during the election, and online censorship has intensified.
- **State monitoring.** Security services monitor communications, and critics and foreign activists have been abducted.
- **Mobile money and banking.** M-Pesa and other platforms face SIM-swap, social engineering, and fraud.
- **Tourism and mining.** Operators hold payment, passport, and commercial data and face fraud and espionage.
- **Employees based in country.** Employees face possible nationwide internet shutdowns, monitoring, and violence during unrest. Avoid political content, and keep offline access to key contacts and documents.
- **Vendor and supply chain risk.** Telecoms and fintech vendors operate under state control and can be ordered to shut down or share data. Plan for sudden loss of connectivity, segment vendor access, and verify payment changes out of band.

The TIDE team tracks 2 threat actors that list Tanzania among their targets. By attributed nexus, they break down as 1 Iran-nexus, and 1 unattributed or other. The most frequently targeted sectors are government (2), banking and financial services (1), defense and defense industrial base (1), electronics and semiconductors (1), and industrial and manufacturing (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and arrest.** Online criticism of the government can lead to arrest, and social media content is monitored.
- **Abduction of critics.** Journalists and activists, including foreign visitors observing trials, have been detained or abducted.
- **Mobile money fraud.** SMS and wallet scams are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Tanzania.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Tanzania Level 3, Reconsider Travel, citing crime, terrorism, other, unrest. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A nationwide internet shutdown and lethal force around the October 2025 election, state monitoring, abductions of critics, and the State Department's Level 3 advisory drive the rating.
- **What would change this rating.** Raise to Level 4 if unrest returns with shutdowns or detentions of foreigners. Lower to Level 2 if restrictions lift and the treason cases ease.

Public Wi-Fi

- Tanzania has demonstrated willingness to impose nationwide internet shutdowns, as occurred during the October 2025 election violence. Do not rely on public Wi-Fi during political unrest, and assume all networks are monitored; if possible, avoid the trip during election seasons or political volatility.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid demonstrations and expect roadblocks and curfews during unrest, and avoid road travel at night.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

THAILAND

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2



CAPITAL
Bangkok

GOVERNMENT
Parliamentary constitutional monarchy

LANGUAGE
Thai

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 7, 2026)

Risk indicators: Unrest

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Phone and SMS fraud, lese-majeste legal risk, documented spyware use against activists, and border and southern insurgency disruption.

Country Overview

Thailand, known as Siam until 1939, was never colonized by a European power. The Sukhothai and Ayutthaya kingdoms preceded the Chakri dynasty, which has ruled from Bangkok since 1782. A 1932 revolution ended absolute monarchy, and the military has staged many coups since, most recently in 2014.

Thailand has about 70.3 million people and a diversified economy based on manufacturing, tourism, and agriculture. King Maha Vajiralongkorn has reigned since 2016, and lese-majeste laws carry long prison terms. Anutin Charnvirakul became prime minister in September 2025 after the Constitutional Court removed Paetongtarn Shinawatra.

Geopolitical Landscape

- **February 2026 election.** Anutin's conservative Bhumjaithai party won 193 seats in the February 8, 2026 election, which brought a degree of calm after four prime ministers in three years. Crisis Group describes a decisive victory.
- **Conflict with Cambodia.** Deadly border fighting in May and July 2025 ended in a ceasefire and the October Kuala Lumpur Peace Accord, but hostilities resumed. Thailand's cabinet annulled a 2001 maritime

memorandum in May 2026, both sides traded accusations of fire along the border, and the government is building a border barrier.

- **Southern insurgency.** Militant attacks in the deep south, including a May 2026 bombing that killed a police officer in Narathiwat, persist.
- **Scam networks.** Transnational scam compounds in neighboring countries have drawn Thai crackdowns on power, telecom, and border supplies.

Cyber Threats | Organizations

- **Scam and fraud ecosystem.** Banks, telecoms, and payment providers face large fraud flows and mule-account networks.
- **State monitoring and spyware.** Citizen Lab documented an extensive Pegasus operation against pro-democracy campaigners in Thailand, and authorities monitor online speech under lese-majeste and computer crime laws.
- **Tourism sector.** Hotels, airlines, and booking platforms hold payment and passport data and face fraud and ransomware.
- **Regulation.** The Personal Data Protection Act is in force, and the Cybersecurity Act gives authorities broad powers in an emergency.
- **Employees based in country.** Employees face phone and SMS fraud, tourist-area scams, and legal risk for commentary on the monarchy. Expect possible disruption near the Cambodian border and in the deep south.
- **Vendor and supply chain risk.** Telecoms, payment providers, and tourism vendors sit next to a large fraud ecosystem, and compromised mailboxes redirect payments. Require strong authentication, logging, and out-of-band verification of payment changes.

The TIDE team tracks 50 threat actors that list Thailand among their targets. By attributed nexus, they break down as 31 China-nexus, 14 cybercriminal, 2 unattributed or other, 1 North Korea-nexus, 1 Lebanon-nexus, and 1 Iran-nexus. The most frequently targeted sectors are government (35), healthcare and pharmaceuticals (16), banking and financial services (15), technology (15), and education and research (15). These figures count actors, not incidents.

Cyber Threats | Individuals

- **SMS and call-center scams.** Fake police, courier, and bank calls are widespread, and Thai authorities have cracked down on SIM registration.
- **Tourist-targeted fraud.** Jet-ski, taxi, and card-skimming scams affect visitors.
- **Speech risk.** Comments about the monarchy can lead to prosecution, including for foreign visitors.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Thailand.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Thailand Level 1, Exercise Normal Precautions, citing unrest. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Phone and SMS fraud, legal risk around the monarchy, documented spyware use against activists, and disruption near the Cambodian border and in the south drive the rating.
- **What would change this rating.** Raise to Level 3 if fighting with Cambodia escalates or unrest returns. Lower to Level 1 as the border calms and fraud declines.

Public Wi-Fi

- Public Wi-Fi in Bangkok and tourist areas faces high fraud volume from transnational scam networks, while authorities monitor online speech under lese-majeste laws and deploy spyware against activists. Use a corporate VPN on any public network, and avoid any commentary on the monarchy online.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid the Cambodian border areas and the deep southern provinces flagged in the advisory.
- Do not comment on the monarchy online or in person.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

TIMOR-LESTE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Dili

GOVERNMENT
Semi-presidential republic

LANGUAGE
Tetum and Portuguese

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 21, 2026)

Risk indicators: Unrest, crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Limited connectivity and low surveillance risk; unrest in the capital can disrupt travel.

Country Overview

Timor-Leste occupies the eastern half of the island of Timor, with an exclave on the west. Portugal colonized it for four centuries, and Indonesia invaded and annexed it in 1975, an occupation in which an estimated 100,000 to 200,000 people died. A 1999 referendum for independence triggered militia violence and an Australian-led peacekeeping force.

Timor-Leste became independent in 2002 and joined ASEAN as its eleventh member in October 2025. It has about 1.4 million people and depends on a sovereign wealth fund built from offshore oil and gas revenue that is running down. Xanana Gusmao has been prime minister since 2023.

Geopolitical Landscape

- **ASEAN membership.** Joining ASEAN was a long-sought goal that brings trade access and scrutiny of capacity.
- **Economic cliff.** Oil fields are depleting, and the government hopes the Greater Sunrise gas project and diversification can replace revenue.
- **Youth unrest.** Student protests over perks for lawmakers in 2025 and unemployment among a very young population are recurring risks.

Cyber Threats | Organizations

- **Minimal digital footprint.** Connectivity depends on a few cable and satellite links, and local security capacity is very limited.
- **Regional diplomatic targeting.** Government networks draw interest from regional powers.
- **Banking and telecoms.** A small number of foreign-owned institutions carry most exposure.
- **Employees based in country.** Employees face limited connectivity and opportunistic theft, and unrest in Dili can disrupt travel.
- **Vendor and supply chain risk.** A few foreign-owned vendors provide banking and connectivity, so one outage can have wide effects. Plan for offline operation.

The TIDE team tracks 1 threat actor that lists Timor-Leste among their targets. By attributed nexus, they break down as 1 China-nexus. The most frequently targeted sectors are aerospace (1), defense and defense industrial base (1), technology (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Limited connectivity.** Telemor, Timor Telecom, and Telkomcel provide mobile service with slow, costly internet, and Facebook is the main platform for news and scams.
- **Phone theft.** Opportunistic theft occurs in Dili.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Timor-Leste.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Timor-Leste Level 2, Exercise Increased Caution, citing unrest, crime. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity is limited and surveillance risk is low. Unrest in the capital can disrupt travel.
- **What would change this rating.** Raise to Level 2 if protests escalate or targeting of government networks increases.

Public Wi-Fi

- Timor-Leste's first international submarine cable, a link to Australia's North West Cable System, began commercial service in July 2026, ending the country's reliance on satellite connectivity; outages and unrest in Dili can still disrupt networks, so use a corporate VPN if a public network must be used and plan for interruptions.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Avoid demonstrations in Dili, and carry offline copies of key documents.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

TOGO

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Lome

GOVERNMENT
Parliamentary system with a President of the Council of Ministers as head of government

LANGUAGE
French (with Ewe, Kabiye, and other languages)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued March 9, 2026)

Risk indicators: Unrest, crime, kidnapping or hostage-taking, terrorism

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Documented spyware use, connectivity restrictions during protests, mobile-money fraud, and northern border risk.

Country Overview

Togo is a narrow West African country on the Gulf of Guinea. Germany colonized it in 1884, and after the First World War France and Britain divided it. French Togoland became independent in 1960.

The Gnassingbe family has ruled since 1967. Faure Gnassingbe took power in 2005 after his father Eyadema's death. Togo has about 8.1 million people, a major port at Lome, and an economy based on phosphates, agriculture, and transit trade.

Geopolitical Landscape

- **Constitutional change.** A 2024 constitution moved to a parliamentary system, and in May 2025 Gnassingbe became President of the Council of Ministers with no term limit, in effect extending his rule.
- **June 2025 protests.** Youth-led protests against the change and the cost of living were met with force, with deaths and arrests reported.
- **Sahel spillover.** Jihadist attacks in the northern Savanes region, near Burkina Faso, have killed soldiers and civilians.
- **Regional alignment.** Togo has sought closer ties with the Sahel states, and it mediates in regional disputes.

Cyber Threats | Organizations

- **State monitoring and spyware.** Togo was among the countries identified as a Pegasus client in the 2021 Pegasus Project reporting.
- **Connectivity restrictions.** Authorities have restricted social media and internet access during protests and elections.
- **Port and logistics.** Lome's port is a transit hub whose operators and brokers face fraud and ransomware.
- **Banking and mobile money.** Wallets and banks face SIM-swap and social engineering.
- **Employees based in country.** Employees face possible connectivity restrictions during unrest, monitoring, and mobile-money fraud. Avoid the northern border region.
- **Vendor and supply chain risk.** Port, logistics, and telecom vendors operate under state oversight and can be compelled to share data or restricted. Segment vendor access and plan for outages.

The TIDE team tracks 1 threat actor that lists Togo among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and arrest.** Online criticism of the government can lead to arrest.
- **Mobile money fraud.** SMS and wallet scams are common.
- **Phone theft.** Snatch theft occurs in Lome.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Togo.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Togo Level 2, Exercise Increased Caution, citing unrest, crime, kidnapping or hostage-taking, terrorism. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Documented spyware use, connectivity restrictions during protests, mobile-money fraud, and risk near the northern border drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest returns with shutdowns or jihadist attacks spread south. Lower to Level 1 as politics and security stabilize.

Public Wi-Fi

- Togo was identified as a Pegasus spyware client, and authorities have restricted social media and internet access during protests. Public networks carry monitoring risk and mobile-money fraud risk; use a corporate VPN if public Wi-Fi is necessary and avoid connectivity near demonstrations.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations and the northern Savanes region flagged in the advisory.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

TONGA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Nuku'alofa

GOVERNMENT
Constitutional monarchy

LANGUAGE
Tongan and English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued December 2, 2024)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Limited connectivity and low crime; exposure is basic phishing and vendor concentration.

Country Overview

Tonga is a Polynesian kingdom of about 170 islands in the South Pacific and was never fully colonized. It became a British protected state in 1900 and regained full independence in 1970. The Tupou dynasty has ruled since the nineteenth century, and King Tupou VI has reigned since 2012.

Tonga has about 100,000 people and depends on remittances from the large Tongan diaspora, tourism, and aid. A 2022 eruption of the Hunga Tonga-Hunga Ha'apai volcano and the resulting tsunami severed the island's undersea cable for weeks and isolated it.

Geopolitical Landscape

- **Disaster resilience.** Volcanic and cyclone risk and the 2022 cable cut shaped investment in redundant connectivity.
- **Great-power competition.** China, Australia, New Zealand, and the United States compete for influence in the Pacific, and Tonga carries significant debt to China.
- **Reform.** Pressure for political reform continues in a system where the monarch holds significant powers.

Cyber Threats | Organizations

- **Minimal digital footprint.** Connectivity depends on a few cable and satellite links, and local security capacity is limited.
- **Regional diplomatic targeting.** Government networks draw interest from regional powers.
- **Vendor concentration.** Telecom and banking services depend on a few providers.
- **Employees based in country.** Employees face limited connectivity and basic phishing risk, and cyclone season can disrupt travel.
- **Vendor and supply chain risk.** A few external vendors provide connectivity and banking, as the 2022 cable cut showed. Plan for offline operation and verify incident notification terms.

The TIDE team does not currently track actors that list Tonga among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Limited connectivity.** Digicel Tonga and the state-owned Tonga Communications Corporation provide mobile service, and internet is slow and costly.
- **Investment and romance scams.** The National Reserve Bank of Tonga has warned of Ponzi-style schemes (branded BG Wealth Sharing and DSJ Exchange) that recruit members through Facebook and WhatsApp with promises of guaranteed returns before blocking withdrawals.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Tonga.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Tonga Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity is limited and crime is low. Exposure is basic phishing and vendor concentration.
- **What would change this rating.** Raise to Level 2 if targeting of Tongan government networks increases.

Public Wi-Fi

- Tonga depends on a single subsea cable to Fiji; the January 2022 volcanic eruption severed it, cutting the country off for about five weeks until it was repaired. Use a corporate VPN if a public network must be used and plan for potential outages during cyclone season.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Cyclone season, November through April, can disrupt travel and connectivity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

TRINIDAD AND TOBAGO

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Port of Spain

GOVERNMENT
Parliamentary republic

LANGUAGE
English

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued April 13, 2026)

Risk indicators: Crime, terrorism, health

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Violent crime and extortion risk, express kidnapping, organized-crime insider risk, and a U.S. Level 3 advisory.

Country Overview

Trinidad and Tobago is a twin-island Caribbean nation just off the coast of Venezuela. Spain and then Britain ruled the islands, sugar plantations and indentured labor from India shaped a diverse population, and the country became independent in 1962 and a republic in 1976.

It has about 1.4 million people and one of the Caribbean's largest economies, built on oil, natural gas, and petrochemicals. Kamla Persad-Bissessar returned as prime minister in May 2025. Violent crime, driven by gangs and the drug trade, is a defining problem.

Geopolitical Landscape

- **State of emergency.** The government declared a state of emergency in 2025 to confront gang violence, after record homicide levels in 2024.
- **Venezuela and U.S. operations.** Trinidad and Tobago sits a few kilometers from Venezuela and supported the U.S. military buildup in the Caribbean, which strained relations with Caracas and ended a gas arrangement.
- **Energy dependence.** Declining gas output and refinery closures weigh on revenue.

Cyber Threats | Organizations

- **Organized crime.** Gangs and drug and arms trafficking influence ports, customs, and some public bodies, creating insider and corruption risk.
- **Ransomware and fraud.** Government bodies, utilities, and banks face ransomware, and business email compromise is common.
- **Energy sector.** Operators and contractors hold valuable data and face espionage and fraud.
- **Regulation.** Trinidad and Tobago has a data protection act and a cybercrime act.
- **Employees based in country.** Employees face violent crime risk, card fraud, and possible extortion. Vet drivers and avoid movements at night.
- **Vendor and supply chain risk.** Logistics, security, and port vendors operate near organized-crime networks, and insider risk is elevated. Vet vendor staff, limit shared personal data, and verify payment changes out of band.

The TIDE team does not currently track actors that list Trinidad and Tobago among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Violent crime.** Robbery, carjacking, and murder are common, and tourists have been victims.
- **Phishing and card fraud.** Bank impersonation and card skimming are common.
- **Express kidnapping.** Criminals target travelers using taxis and ride-hailing.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Trinidad and Tobago.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Trinidad and Tobago Level 3, Reconsider Travel, citing crime, terrorism, health. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Violent crime and extortion risk, express kidnapping, organized-crime insider risk, and the State Department's Level 3 advisory drive the rating.
- **What would change this rating.** Raise to Level 4 if violence or Venezuela-related hostilities escalate. Lower to Level 2 as crime declines.

Public Wi-Fi

- Trinidad and Tobago faces high organized-crime activity and insider risk in port and financial sectors, with criminals actively targeting travelers for fraud and express kidnapping. Use a corporate VPN on any public network and avoid public Wi-Fi in areas frequented by the tourism industry without security review.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Use hotel-arranged transport, avoid walking at night, and avoid areas flagged in the advisory.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

TUNISIA

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Tunis

GOVERNMENT
Presidential republic

LANGUAGE
Arabic (French widely used)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued May 21, 2026)

Risk indicators: Terrorism, unrest, crime

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Speech laws used against critics, state monitoring, phishing and card fraud, and border-area risk.

Country Overview

Tunisia is the northernmost country in Africa and was the home of ancient Carthage. Phoenician, Roman, Arab, and Ottoman rule shaped it, and France made it a protectorate in 1881. It became independent in 1956 under Habib Bourguiba.

A 2010 to 2011 uprising, which began after a street vendor's self-immolation, ousted Zine El Abidine Ben Ali and started the Arab Spring. Tunisia had the region's most promising democratic transition until President Kais Saied suspended parliament in 2021 and rewrote the constitution. It has about 12 million people and a struggling economy.

Geopolitical Landscape

- **Authoritarian turn.** Saied has jailed opponents, journalists, and lawyers, including in mass trials in 2025, and won a second term in October 2024 with about 90 percent of the vote on low turnout.
- **Economic strain.** High debt, shortages, and a stalled IMF program drive discontent and migration to Europe.
- **Migration.** Tunisia is a main departure point for migrants crossing to Italy, and Europe has funded border control.

- **Regional position.** Relations with Libya and Algeria shape security and trade.

Cyber Threats | Organizations

- **Speech and cybercrime law.** Decree 54 of 2022 criminalizes spreading false news and has been used to jail critics, journalists, and lawyers.
- **State monitoring.** Security services monitor communications, and contacts with foreign actors can bring charges.
- **Banks and telecoms.** Institutions face phishing and account takeover with limited resources.
- **Hacktivism.** Regional hacktivist groups periodically target Tunisian sites.
- **Employees based in country.** Employees should assume communications can be monitored, avoid political commentary, and expect phishing and card fraud. Staff linked to civil society or foreign-funded groups face elevated risk.
- **Vendor and supply chain risk.** Telecoms and local IT vendors operate under state oversight and can be compelled to share data. Segment vendor access and verify payment changes out of band.

The TIDE team tracks 4 threat actors that list Tunisia among their targets. By attributed nexus, they break down as 2 cybercriminal, 1 unattributed or other, and 1 Iran-nexus. The most frequently targeted sectors are government (2), industrial and manufacturing (2), civil society and activism (1), diplomatic and foreign affairs (1), and energy (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Social media posts critical of the president can lead to prosecution.
- **Phishing and card fraud.** Bank impersonation and card skimming occur.
- **Phone theft.** Snatch theft occurs in Tunis.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Tunisia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Tunisia Level 2, Exercise Increased Caution, citing terrorism, unrest, crime. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Speech laws used against critics, state monitoring, phishing and card fraud, and border-area risk drive the rating.
- **What would change this rating.** Raise to Level 3 if detentions of foreigners or unrest increase. Lower to Level 1 if the legal environment eases.

Public Wi-Fi

- Given the state monitoring of communications and phishing campaigns targeting financial institutions, avoid public Wi-Fi, as eavesdropping could expose both work and personal sessions to compromise. If a public network is unavoidable, connect through a corporate VPN first.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations and the Algerian and Libyan border areas flagged in the advisory.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

TURKEY

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2

CAPITAL
Ankara

GOVERNMENT
Presidential republic

LANGUAGE
Turkish

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued June 9, 2026)

Risk indicators: Terrorism, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: State monitoring and legal risk for speech, social media throttling during unrest, and role-based targeting of media and civil society.

Country Overview

Turkey straddles Europe and Asia and was the center of the Ottoman Empire, which ruled much of the Middle East, North Africa, and the Balkans for six centuries. After defeat in the First World War, Mustafa Kemal Ataturk led a war of independence and founded the secular republic in 1923.

Turkey joined NATO in 1952 and has been an EU candidate since 1999, though accession talks are frozen. It has about 86 million people and a large industrial economy. Recep Tayyip Erdogan has led the country since 2003, first as prime minister and since 2014 as president, and a 2017 referendum created a powerful presidency.

Geopolitical Landscape

- **Opposition crackdown.** The March 2025 arrest of Istanbul mayor Ekrem Imamoglu, Erdogan's main rival, triggered the largest protests in a decade and a wave of prosecutions of opposition politicians.
- **Kurdish peace process.** The PKK announced its dissolution in May 2025 and began disarming, opening a fragile process on Kurdish rights.
- **Syria and regional role.** Turkey backs Syria's new government and competes with Israel for influence there, and it mediates in Ukraine and the Middle East.

- **Economy.** High inflation and a weak lira have eased but still strain households.

Cyber Threats | Organizations

- **Platform throttling.** Authorities have throttled social media and messaging services during protests and crises, including in March and September 2025.
- **State-linked operations.** Turkey-nexus actors target Kurdish, Greek, and regional government and media networks, and domestic surveillance law is broad.
- **Ransomware and leaks.** Banks, retailers, and public bodies have suffered breaches, including leaks of citizen data.
- **Regulation.** The KVKK data law and a 2022 disinformation law shape duties and speech risk.
- **Employees based in country.** Employees should assume communications can be monitored, avoid political commentary, and expect throttling of social media during unrest. Staff in media and civil society face elevated risk.
- **Vendor and supply chain risk.** Telecoms and local IT vendors operate under state oversight and can be compelled to share data. Segment vendor access, review data location, and verify payment changes out of band.

The TIDE team tracks 46 threat actors that list Turkey among their targets. By attributed nexus, they break down as 12 Iran-nexus, 11 cybercriminal, 7 China-nexus, 7 unattributed or other, 3 Russia-nexus, 3 Turkey-nexus, 2 India-nexus, and 1 Lebanon-nexus. The most frequently targeted sectors are government (24), telecommunications (12), banking and financial services (12), healthcare and pharmaceuticals (11), and civil society and activism (11). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Social media posts critical of the president or government can lead to prosecution, including for foreigners.
- **Phishing and card fraud.** Bank and courier impersonation circulates in Turkish.
- **Tourist scams.** Overcharging and fake-police scams occur in Istanbul.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Turkey.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Turkey Level 2, Exercise Increased Caution, citing terrorism, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** State monitoring and legal risk for speech, social media throttling during unrest, and role-based targeting of media and civil society drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest escalates with shutdowns or detentions of foreigners. Lower to Level 1 as political tension eases.

Public Wi-Fi

- Turkish authorities have throttled social media and messaging services during unrest, and state monitoring of communications is routine, making public Wi-Fi an elevated risk for both data exposure and surveillance. Connect through a corporate VPN if a public network is unavoidable.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, and avoid the Syrian and Iraqi border areas flagged in the advisory.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

TURKMENISTAN

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 3



CAPITAL
Ashgabat

GOVERNMENT
Presidential republic (authoritarian)

LANGUAGE
Turkmen (Russian widely used)

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued August 21, 2026)

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Near-total state control of the internet, VPN restrictions, pervasive monitoring, and device inspection risk.

Country Overview

Turkmenistan is a Central Asian country that is about 70 percent Karakum Desert, long on the Silk Road. Russia absorbed it in the nineteenth century, and it became a Soviet republic and then independent in 1991.

Saparmurat Niyazov ruled as a personality-cult dictator until 2006, followed by Gurbanguly Berdimuhamedov, who handed power to his son Serdar in 2022. Turkmenistan has about 7 million people and the world's fourth-largest natural gas reserves, with exports going largely to China. It is among the most closed countries in the world.

Geopolitical Landscape

- **Hereditary authoritarianism.** Power is concentrated in the Berdimuhamedov family, with Gurbanguly retaining a senior role, and independent institutions do not exist.
- **Gas and China.** Almost all gas exports go to China, which makes the country dependent on one buyer, and it explores new routes.
- **Neutrality.** Turkmenistan maintains a declared permanent neutrality and avoids alliances.

Cyber Threats | Organizations

- **Extreme internet control.** The state controls internet access, blocks most foreign platforms, and has restricted VPNs.
- **State surveillance.** Security services monitor communications, and users face penalties for accessing blocked content.
- **Gas sector.** Foreign operators and contractors operate under tight state control.
- **Foreign presence.** Foreign organizations are few and heavily scrutinized.
- **Employees based in country.** Employees should assume all communications and devices are monitored, expect blocked platforms, and carry minimal data. Remove company access from personal devices before any entry.
- **Vendor and supply chain risk.** Local telecoms and vendors operate under state control and can be compelled to share data. Avoid storing sensitive data locally and segment vendor access.

The TIDE team tracks 1 threat actor that lists Turkmenistan among their targets. By attributed nexus, they break down as 1 Russia-nexus. The most frequently targeted sectors are defense and defense industrial base (1), diplomatic and foreign affairs (1), government (1), industrial and manufacturing (1), and politics and political organizations (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Blocked platforms and VPNs.** Most foreign websites and messaging apps are blocked, and VPN use is risky.
- **Monitoring and detention.** Authorities monitor and detain people for online activity.
- **Device checks.** Border officials may inspect devices.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Turkmenistan.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Turkmenistan Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Near-total state control of the internet, restrictions on VPNs, pervasive monitoring, and device inspection risk drive the rating.
- **What would change this rating.** Raise to Level 4 if detentions of foreigners increase. Lower to Level 2 if internet controls ease.

Public Wi-Fi

- The state exercises near-total control of internet access and has restricted VPNs, so public Wi-Fi is both a surveillance and a legal risk. Do not use public Wi-Fi. Rely instead on approved devices and the authorized connectivity plan.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Expect limited connectivity and blocked services, and carry offline copies of key documents.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

TUVALU

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Funafuti

GOVERNMENT
Parliamentary constitutional monarchy (Commonwealth realm)

LANGUAGE
Tuvaluan and English

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued December 2, 2024)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Very limited connectivity and low crime; government staff may draw external interest.

Country Overview

Tuvalu is a Polynesian nation of nine low-lying coral islands in the central Pacific with about 11,000 people, one of the world's smallest and most climate-vulnerable countries. It was part of the British Gilbert and Ellice Islands colony and became independent in 1978.

Tuvalu earns revenue from fishing licenses, remittances, and the sale of its .tv internet domain. It recognizes Taiwan. Feleti Teo became prime minister in February 2024. Rising seas threaten its habitability.

Geopolitical Landscape

- **Climate and migration.** The 2023 Falepili Union treaty with Australia provides defense guarantees and a special mobility pathway for Tuvaluans in exchange for security coordination.
- **Taiwan recognition.** Tuvalu is among the few states that recognize Taiwan, which exposes it to pressure from Beijing.
- **Digital preservation.** Tuvalu has begun creating a digital twin of its territory and records to preserve sovereignty if land is lost.

Cyber Threats | Organizations

- **Minimal digital footprint.** Connectivity depends on limited cable and satellite links, and local security capacity is extremely limited.
- **Domain revenue.** The .tv domain is operated through a foreign partner and is a valuable national asset and target.
- **Regional diplomatic targeting.** Government networks draw external espionage interest.
- **Employees based in country.** Employees face very limited connectivity and basic phishing risk. Government and diplomatic staff may draw external interest.
- **Vendor and supply chain risk.** A single set of cable and satellite providers and the .tv registry partner carry concentrated exposure. Plan for offline operation.

The TIDE team does not currently track actors that list Tuvalu among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Limited connectivity.** Internet is slow and costly.
- **Basic phishing.** Social media and messaging scams exist.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Tuvalu.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Tuvalu Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity is very limited and crime is low. Government staff may draw external interest.
- **What would change this rating.** Raise to Level 2 if great-power competition increases targeting of Tuvaluan systems.

Public Wi-Fi

- While government and diplomatic staff may draw external espionage interest, connectivity on the island is generally limited and crime is low. Standard cyber hygiene applies: avoid public Wi-Fi, and use a corporate VPN if one becomes unavoidable.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Carry offline copies of key documents, since connectivity is limited.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

UGANDA

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 3

CAPITAL
Kampala

GOVERNMENT
Presidential republic (dominant-party)

LANGUAGE
English and Swahili (with Luganda and others)

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued June 4, 2026)

Risk indicators: Unrest, crime, terrorism, health

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Nationwide internet shutdown precedent, state surveillance and spyware, mobile-money fraud, and a U.S. Level 4 advisory.

Country Overview

Uganda is a landlocked country in East Africa at the source of the Nile, home to the historic Buganda kingdom. Britain made it a protectorate in 1894, and it became independent in 1962. Idi Amin's military dictatorship from 1971 to 1979 killed an estimated 300,000 people.

Yoweri Museveni took power in 1986 after a guerrilla war and has been president since, removing term and age limits. Uganda has about 45.9 million people, hosts one of Africa's largest refugee populations, and is developing oil reserves with a pipeline to Tanzania. Museveni won a seventh term in the January 2026 election, which was held under a nationwide internet shutdown.

Geopolitical Landscape

- **January 2026 election.** The electoral commission declared Museveni the winner of the January 15, 2026 election with 71.65 percent of the vote against 24.72 percent for Bobi Wine, who rejected the result and alleged fraud. The campaign saw heavy military deployment, arrests, and a nationwide internet shutdown that lasted from January 13 until it was partly restored late on January 17, with social media still blocked. A joint African Union and regional observer mission criticized the shutdown and the military's role.

- **Succession.** Museveni's son, army chief Muhoozi Kainerugaba, is widely viewed as a likely successor, which concentrates power in the family.
- **Regional security.** Ugandan forces operate in eastern DRC and Somalia, and ADF attacks in western Uganda and the DRC remain a threat.
- **Oil and pipeline.** The East African Crude Oil Pipeline project draws financing and environmental scrutiny.

Cyber Threats | Organizations

- **Internet shutdowns and social media blocks.** The Uganda Communications Commission ordered providers to suspend internet access from January 13 to January 17, 2026 and has blocked Facebook since 2021.
- **State surveillance.** Security services monitor communications.
- **Mobile money fraud.** MTN MoMo and Airtel Money face large fraud, and insiders have been involved in major thefts.
- **Oil and mining sectors.** Operators and contractors hold valuable data and face espionage and fraud.
- **Employees based in country.** Employees face possible nationwide internet shutdowns, monitoring, mobile-money fraud, and phone snatching in Kampala. Avoid political content, and keep offline access to key contacts.
- **Vendor and supply chain risk.** Telecoms, fintech, and oil-sector contractors operate under state oversight and can be ordered to shut down or share data. Plan for sudden loss of connectivity, segment vendor access, and verify payment changes out of band.

The TIDE team tracks 1 threat actor that lists Uganda among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), and telecommunications (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and arrest.** Online criticism of the president or his family can lead to arrest under computer misuse laws.
- **Mobile money fraud.** Fake agent and fake reversal scams are common.
- **Phone theft.** Snatch theft by motorcycle occurs in Kampala.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Uganda.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Uganda Level 4, Do Not Travel, citing unrest, crime, terrorism, health. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** A nationwide internet shutdown around the January 2026 election, state surveillance and spyware, mobile-money fraud, and the State Department's Level 4 advisory drive the rating.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require an end to election-period shutdowns and a lower State Department advisory level.

Public Wi-Fi

- Uganda has a precedent of nationwide internet shutdowns during election disputes and state monitoring of communications, so public Wi-Fi poses both availability and surveillance risks. If a public network is necessary, connect through a corporate VPN first.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid demonstrations and the eastern border and northern areas flagged in the advisory.

Return protocol

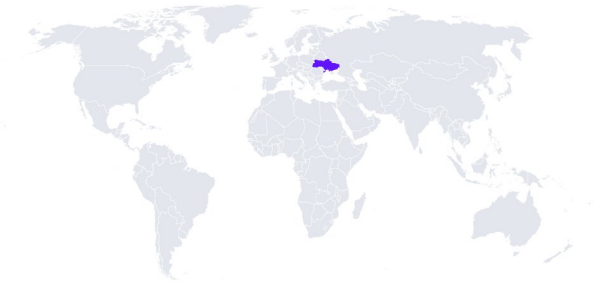
- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

UKRAINE

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Kyiv

GOVERNMENT
Semi-presidential republic

LANGUAGE
Ukrainian

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued August 28, 2026)

Risk indicators: Other, unrest

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Active war with missile and drone strikes, power and connectivity loss, targeted Russian state cyber operations, and a U.S. Level 4 advisory.

Country Overview

Ukraine is the second-largest country in Europe by area and was the heartland of Kievan Rus', the medieval state from which Ukrainian, Russian, and Belarusian identities derive. Poland, Lithuania, the Russian Empire, and Austria-Hungary ruled its lands, and a short-lived independent state emerged after 1917. Ukraine became a Soviet republic, endured the 1932 to 1933 Holodomor famine, and declared independence in August 1991.

The 2004 Orange Revolution and the 2014 Maidan revolution moved Ukraine toward the West. Russia annexed Crimea and backed separatists in Donbas in 2014 and launched a full-scale invasion in February 2022. Ukraine had about 41 million people before the war, and millions have fled or been displaced. Volodymyr Zelensky has been president since 2019.

Geopolitical Landscape

- **War.** As of an October 9, 2026 update from the Council on Foreign Relations, Russia occupies roughly 20 percent of Ukraine, and U.S.-mediated talks have not produced a ceasefire.

- **Energy strikes.** On October 11, 2026, President Trump announced that Russia and Ukraine had agreed to stop striking each other's energy infrastructure, but neither confirmed it and Ukraine reported Russian strikes on six energy facilities the next day.
- **Long-range strikes on Russia.** Ukrainian long-range drones have knocked out up to 40 percent of Russian refining capacity, according to the Council on Foreign Relations, and have also struck Russian data centers.
- **EU path and politics.** Ukraine is an EU candidate, and wartime rules postpone elections, with martial law renewed repeatedly.

Cyber Threats | Organizations

- **Russian state cyber operations.** Sandworm and other GRU, SVR, and FSB groups target energy, telecoms, government, and logistics with destructive and espionage operations, and attacks coordinate with kinetic strikes.
- **Power and telecom disruption.** Missile and drone strikes cause outages, and operations depend on generators and satellite links.
- **Hacktivism and cybercrime.** Pro-Russia and pro-Ukraine volunteer groups launch DDoS and data theft, and ransomware crews exploit the war.
- **Compelled mobilization and staffing.** Conscription affects the availability of staff and contractors.
- **Employees based in country.** The TIDE team does not recommend travel to Ukraine for company staff. Employees and contractors in country face missile and drone attacks, power and connectivity loss, and targeted Russian cyber operations.
- **Vendor and supply chain risk.** Ukrainian vendors, especially developers and IT outsourcers, face outages, mobilization, and targeting by Russian state actors, and compromise of one can affect many clients. Verify continuity plans, segment vendor access, and require incident notification.

The TIDE team tracks 32 threat actors that list Ukraine among their targets. By attributed nexus, they break down as 15 Russia-nexus, 6 cybercriminal, 3 North Korea-nexus, 3 unattributed or other, 2 Belarus-nexus, 2 China-nexus, and 1 hacktivist. The most frequently targeted sectors are government (25), defense and defense industrial base (9), banking and financial services (9), diplomatic and foreign affairs (8), and military (7). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Air alerts and strikes.** Missile and drone attacks threaten cities, including Kyiv and Odesa, with little warning.
- **GPS interference and device targeting.** Jamming is widespread, and phones and apps can reveal location to adversaries.
- **Phishing and disinformation.** Impersonation of officials and aid groups and false narratives are common.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Ukraine.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Ukraine Level 4, Do Not Travel, citing other, unrest. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has very limited ability to assist, and armed conflict is ongoing.

TIDE Risk Level Rationale

- **Drivers.** Missile and drone strikes, power and connectivity loss, targeted Russian state cyber operations, and a U.S. Level 4 advisory drive the rating.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable ceasefire and restored infrastructure.

Public Wi-Fi

- Ongoing military conflict, missile and drone strikes, and targeted Russian state cyber operations against networks make public Wi-Fi a high-risk vector for both military targeting and intelligence gathering. Do not use public Wi-Fi; if travel is authorized, rely on approved devices only.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

UNITED ARAB EMIRATES

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3

CAPITAL
Abu Dhabi

GOVERNMENT
Federation of seven absolute monarchies

LANGUAGE
Arabic (English widely used)

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued August 29, 2026)

Risk indicators: Terrorism, other

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: Iranian missile and drone attacks on UAE territory during the 2026 war, airport and airspace disruption, state monitoring, and a U.S. Level 3 advisory.

Country Overview

The United Arab Emirates is a federation of seven emirates on the southeastern Arabian Peninsula: Abu Dhabi, Dubai, Sharjah, Ajman, Umm al-Quwain, Ras al-Khaimah, and Fujairah. Pearl diving and trade shaped the Trucial States under British protection until the federation formed in 1971.

The UAE has about 11.3 million people, about 90 percent of them foreign nationals, and one of the world's most diversified Gulf economies, anchored by oil in Abu Dhabi and trade, finance, aviation, and tourism in Dubai. Sheikh Mohamed bin Zayed Al Nahyan has been president since 2022.

Geopolitical Landscape

- **Iranian attacks in the 2026 war.** After the United States and Israel struck Iran on February 28, 2026, Iran fired 438 ballistic missiles, 2,012 drones, and 19 cruise missiles at the UAE by April 1, according to the UAE Ministry of Defence. Strikes hit Dubai International Airport, Zayed International Airport in Abu Dhabi, the Palm Jumeirah, the Burj Al Arab, Jebel Ali port, and an Emirates Global Aluminium facility. The UAE and neighboring states closed their airspace for about a week. A ceasefire took effect on April 8, but later

exchanges between the United States and Iran have continued to threaten Gulf states. The State Department rates the UAE Level 3.

- **Aviation and economic hit.** Middle Eastern airlines are projected to lose billions in 2026, and Dubai's airport and port generate a large share of the emirate's revenue.
- **Regional role.** The UAE hosts U.S. and French forces, backs actors in Sudan and Libya, and has deepened ties with Israel under the Abraham Accords.
- **Foreign policy balancing.** The UAE is also investing heavily in AI and technology partnerships with the United States and China.

Cyber Threats | Organizations

- **Iran-linked and regional targeting.** Iran-nexus actors target energy, government, finance, aviation, and logistics, and escalations raise destructive and hack-and-leak risk.
- **Critical infrastructure and aviation.** Airports, ports, and desalination plants have been physically struck and are priority cyber targets.
- **State surveillance and spyware.** Authorities monitor communications and online speech, restrict VoIP, and have used commercial spyware against dissidents, and cybercrime law punishes criticism.
- **Financial and data center hub.** Banks, exchanges, and a growing data center and AI sector hold concentrated data and draw ransomware and espionage.
- **Fraud.** Investment, job, and impersonation scams target residents and visitors.
- **Employees based in country.** Employees should expect regional escalation to disrupt flights and airspace, assume monitoring of communications, and avoid political content online. Finance, energy, aviation, and government staff face elevated Iran-linked targeting.
- **Vendor and supply chain risk.** Gulf-wide telecoms, cloud and data center providers, and logistics vendors can be disrupted during Iran-related escalations and may be compelled to share data. Segment vendor access, plan for airspace and connectivity disruption, and screen vendors for compelled-access risk.

The TIDE team tracks 53 threat actors that list United Arab Emirates among their targets. By attributed nexus, they break down as 19 Iran-nexus, 14 cybercriminal, 7 China-nexus, 6 unattributed or other, 3 North Korea-nexus, 1 India-nexus, 1 Lebanon-nexus, 1 Turkey-nexus, and 1 hacktivist. The most frequently targeted sectors are government (33), banking and financial services (16), telecommunications (16), energy (15), and healthcare and pharmaceuticals (15). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and legal risk.** Social media posts critical of the government, rulers, or religion can lead to prosecution, including for visitors.
- **VoIP and VPN limits.** Some voice-over-IP services are blocked, and using VPNs to access them can be illegal.
- **Missile and drone alerts.** Alerts and airspace closures can disrupt travel with little warning.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to United Arab Emirates.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates United Arab Emirates Level 3, Reconsider Travel, citing terrorism, other. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Iranian missile and drone attacks hit the UAE during the 2026 war, airport and airspace disruption occurred, authorities monitor speech, and the State Department rates the UAE Level 3.
- **What would change this rating.** Raise to Level 4 if attacks on the UAE resume at scale or airspace closes. Lower to Level 2 if U.S.-Iran de-escalation holds.

Public Wi-Fi

- Iran-linked threat actors target the UAE's aviation, energy, and financial sectors with espionage and destructive operations, and authorities monitor communications and restrict VoIP. Avoid public Wi-Fi entirely; if unavoidable, use a corporate VPN first.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Confirm airline and evacuation arrangements before travel, since airspace closures and airport damage occurred during the conflict.
- Follow official alert guidance and shelter instructions.

Return protocol

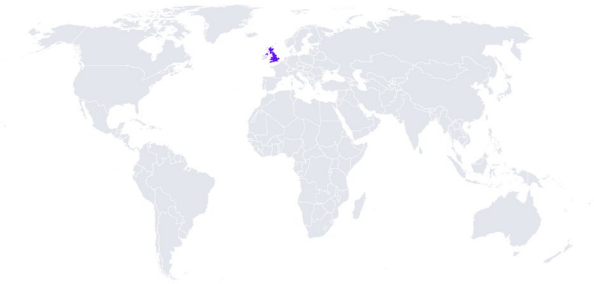
- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

UNITED KINGDOM

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
London

GOVERNMENT
Parliamentary constitutional monarchy

LANGUAGE
English (with Welsh, Scottish Gaelic, and Irish in parts)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 9, 2026)

Risk indicators: Terrorism, unrest, crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Stable and well-regulated; exposure is phishing, phone snatching, and role-based state-linked targeting.

Country Overview

The United Kingdom comprises England, Scotland, Wales, and Northern Ireland. England unified under Anglo-Saxon and then Norman rule, and the kingdoms of England and Scotland merged in 1707 to form Great Britain. The British Empire became the largest in history, and the country led the Industrial Revolution.

After the Second World War the empire dissolved and the UK helped found NATO. It joined the European Community in 1973 and left the EU in January 2020 after a 2016 referendum. The UK has about 69 million people, a service-based economy centered on London's financial sector, and a nuclear deterrent. King Charles III has reigned since 2022.

Geopolitical Landscape

- **New prime minister.** Andy Burnham became prime minister on July 20, 2026, the seventh in ten years, after Keir Starmer resigned as Labour leader on June 22 following heavy losses in the May 7 elections. Burnham, a former Greater Manchester mayor, returned to Parliament in June, was elected Labour leader unopposed, and appointed John Healey as chancellor. The next general election is not required until 2029.

- **Fragmented politics.** Nigel Farage's Reform UK led the English local elections, Plaid Cymru displaced Labour as Wales's leading party, and the Greens made gains in London, so some polls suggest Farage could be a future prime minister.
- **Security and Ukraine.** The UK is a leading supporter of Ukraine and is raising defense spending, and Burnham said support for Ukraine is solid.
- **Economy.** Cost of living and weak growth dominate politics, and Burnham has promised a prudent approach and a ten-year plan.

Cyber Threats | Organizations

- **Ransomware and supply chain.** Retailers Marks and Spencer and the Co-op and carmaker Jaguar Land Rover were disrupted by major attacks in 2025, and the Jaguar Land Rover incident was among the costliest in UK history. The NHS and local councils also face repeated incidents.
- **State-linked espionage.** The NCSC attributes campaigns to Russia and China, and organizations in defense, finance, and government are priority targets.
- **Hacktivism and DDoS.** Pro-Russia groups target government, transport, and local authority sites.
- **Regulation.** The Online Safety Act, UK GDPR, and a planned Cyber Security and Resilience Bill set duties for organizations.
- **Employees based in country.** Employees face phishing and phone snatching in London. Staff in finance, defense, and technology roles may draw state-linked targeting.
- **Vendor and supply chain risk.** Managed service providers, logistics, and software suppliers are common compromise paths, as the 2025 retail and automotive incidents showed. Require supplier attestations, segmentation, and incident notification.

The TIDE team tracks 198 threat actors that list the United Kingdom among their targets. By attributed nexus, they break down as 118 cybercriminal, 33 China-nexus, 15 Iran-nexus, 13 unattributed or other, 8 Russia-nexus, 8 North Korea-nexus, 1 Pakistan-nexus, 1 Lebanon-nexus, and 1 hacktivist. The most frequently targeted sectors are healthcare and pharmaceuticals (106), government (93), technology (81), industrial and manufacturing (80), and banking and financial services (70). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and impersonation.** Messages impersonating banks, delivery firms, HMRC, and police are widespread.
- **Account takeover and SIM swap.** Credential theft and SIM-swap fraud target banking and crypto accounts.
- **Phone theft.** Moped-borne snatch theft of phones is common in London.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to the United Kingdom.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates the United Kingdom Level 2, Exercise Increased Caution, citing terrorism, unrest, crime. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** The UK is stable and well-regulated. Exposure is phishing, phone snatching, and role-based targeting of finance, defense, and technology staff by state-linked actors.
- **What would change this rating.** Raise to Level 2 for staff in those sectors if state-linked targeting of travelers escalates.

Public Wi-Fi

- While the UK is stable and well-regulated, ransomware and supply-chain attacks have disrupted retailers and critical services, and state-linked actors target staff in finance, defense, and technology roles. Apply standard cyber hygiene: avoid public Wi-Fi, and use a corporate VPN if necessary.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Keep phones secured when walking near roads, where snatch theft occurs.

Return protocol

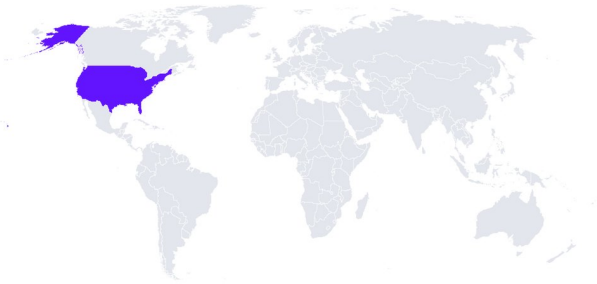
- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

UNITED STATES

U.S. STATE DEPT. N/A

TIDE CYBER RISK LEVEL 1



CAPITAL
Washington, D.C.

GOVERNMENT
Federal presidential republic

LANGUAGE
English (with no official language at the federal level)

U.S. DEPARTMENT OF STATE

Not applicable. The Department of State does not issue a Travel Advisory for the United States.

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low state-surveillance risk to visitors; exposure is border device searches, SMS fraud, public Wi-Fi, and role-based targeting by state-linked actors.

Country Overview

The United States is a federal republic of fifty states that grew from thirteen British colonies on the Atlantic coast. It declared independence in 1776, won the Revolutionary War, and adopted its Constitution in 1788. Westward expansion, the Civil War, and industrialization made it a continental power, and the country emerged from the Second World War as a global superpower.

The United States has about 340 million people and the world's largest economy, anchored by technology, finance, energy, and agriculture. Donald Trump returned to the presidency in January 2025. Midterm elections for Congress are scheduled for November 3, 2026.

Geopolitical Landscape

- **Midterm elections on November 3, 2026.** The election will decide control of Congress, and political polarization and concern about disinformation and threats to officials shape the environment.
- **Foreign policy.** The administration captured Venezuelan leader Nicolas Maduro in January 2026, launched strikes on Iran with Israel on February 28, 2026, and uses tariffs and sanctions as primary tools. President Trump said on October 8 that the United States would not resume strikes on Iran before the midterms.

- **Trade.** Tariff policy is a central instrument and continues to change through litigation and new legal authorities.
- **Domestic security.** Political violence, immigration enforcement operations, and National Guard deployments to cities have been flashpoints.

Cyber Threats | Organizations

- **State-linked intrusions.** China-linked groups Volt Typhoon and Salt Typhoon pre-positioned in critical infrastructure and compromised major telecom carriers, and Russia- and Iran-linked actors target government, energy, and elections.
- **Ransomware.** The United States is the most targeted country for ransomware, including health care, municipalities, manufacturers, and education.
- **Government capacity and policy.** Cuts to federal cyber agencies and uncertainty over the renewal of information-sharing protections have drawn concern from security leaders.
- **Supply chain and zero-days.** Widely used software, such as the SharePoint flaws exploited in 2025, can expose thousands of organizations at once.
- **Regulation.** SEC rules require public companies to disclose material incidents, and state privacy laws vary widely.
- **Employees based in country.** Foreign employees and visitors should expect device and social media scrutiny at the border, SMS fraud, and public Wi-Fi risk. Staff in technology, finance, and critical infrastructure roles are priority targets for state-linked and criminal actors.
- **Vendor and supply chain risk.** The United States hosts most large cloud, software, and managed service providers, so a single supplier compromise can affect organizations worldwide. Review concentration risk, require attestations and segmentation, and note that U.S. legal process can compel disclosure of data held by U.S. providers.

The TIDE team tracks 260 threat actors that list the United States among their targets. By attributed nexus, they break down as 139 cybercriminal, 58 China-nexus, 22 Iran-nexus, 13 unattributed or other, 12 North Korea-nexus, 10 Russia-nexus, 3 hacktivist, 1 Pakistan-nexus, 1 Lebanon-nexus, and 1 Turkey-nexus. The most frequently targeted sectors are government (133), healthcare and pharmaceuticals (128), technology (108), industrial and manufacturing (100), and banking and financial services (81). These figures count actors, not incidents.

Cyber Threats | Individuals

- **SMS toll and package scams.** Smishing impersonating tolls, delivery services, and banks is pervasive.
- **Account takeover and SIM swap.** Credential stuffing, SIM swaps, and crypto theft are common.
- **Border device searches.** U.S. Customs and Border Protection can search electronic devices at the border, including those of citizens and visitors, without a warrant.
- **Public Wi-Fi and charging.** Airports, hotels, and cafes are common places for rogue networks and juice jacking.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to the United States. The United States appears in TIDE tracking as a target.

Cyber Travel Considerations

Official guidance

The U.S. Department of State does not issue a Travel Advisory for the United States. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions, which applies to travelers entering the United States and not to U.S. residents. Check the Department of Homeland Security and Customs and Border Protection for current entry rules.

TIDE Risk Level Rationale

- **Drivers.** State surveillance of visitors is limited, but border officers can search devices, SMS and account-takeover fraud is pervasive, and staff in technology, finance, and critical infrastructure are priority targets for state-linked actors.
- **What would change this rating.** Raise to Level 2 if device searches or entry restrictions on foreign business travelers expand. This rating applies to travelers entering the United States.

Public Wi-Fi

- Rogue networks and juice jacking are common in airports, hotels, and cafes, and foreign staff should be especially cautious at border entry points where device searches are routine. Avoid public Wi-Fi, and use a corporate VPN if a public network is unavoidable.

Recommended corporate policy

- Apply standard corporate travel controls: full-disk encryption, a strong device passcode, phishing-resistant authentication, and remote wipe.
- For travelers entering the United States, carry the minimum data needed. Border officers may search devices, and policies on social media and device review for visa applicants and visitors have tightened, so confirm current entry requirements with counsel.
- Travelers in government, defense, or sensitive research roles should consider clean loaner devices.

Local practices

- Treat SMS and phone requests for payment or verification as suspect, and use official apps and numbers.
- Keep devices secured against theft in cars, hotels, and airports.

Return protocol

- Treat any device that was out of your control, for example if it was taken from you or searched, as untrusted and wipe it before re-enrolling it. Rotate credentials for accounts it touched, and report the event to your security team.

WORLDBOOK

URUGUAY

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1

CAPITAL
Montevideo

GOVERNMENT
Presidential republic

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued July 28, 2026)

Risk indicators: Crime

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Low surveillance risk; exposure is phishing, phone snatching, and thin local security capacity.

Country Overview

Uruguay is a small South American country between Argentina and Brazil, settled by Spain and contested by Spain and Portugal. It became independent in 1828 and is known as one of Latin America's most stable and secular democracies. A military dictatorship ruled from 1973 to 1985.

Uruguay has about 3.5 million people and an economy based on agriculture, forestry, and services. It was the first country to fully legalize cannabis. Yamandu Orsi of the Broad Front became president in March 2025.

Geopolitical Landscape

- **Stable politics.** Power alternates peacefully between the center-left Broad Front and center-right parties, and the Orsi government is pursuing moderate policies.
- **Crime.** Drug trafficking and gang violence, especially in Montevideo and Rivera, are public concerns.
- **Regional trade.** Uruguay is a member of Mercosur and has sought trade deals beyond the bloc.

Cyber Threats | Organizations

- **Ransomware and fraud.** Government bodies and firms have limited security capacity and have faced ransomware and phishing.
- **Port and logistics.** Montevideo's port is a transit hub for trafficking and trade, and operators face insider and fraud risk.
- **Financial sector.** Banks and fintechs face account takeover and social engineering.
- **Regulation.** Uruguay has an EU-recognized data protection framework and a national cyber agency.
- **Employees based in country.** Employees face phishing and phone snatching in Montevideo.
- **Vendor and supply chain risk.** Local logistics and banking vendors have thin security capacity. Verify supplier controls and out-of-band payment verification.

The TIDE team tracks 1 threat actor that lists Uruguay among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are education and research (1), government (1), and healthcare and pharmaceuticals (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Phishing and wallet fraud.** Bank and wallet impersonation circulates in Spanish.
- **Phone theft.** Snatch theft occurs in Montevideo.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Uruguay.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Uruguay Level 2, Exercise Increased Caution, citing crime. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Low surveillance risk, with phishing, phone snatching, and thin local security capacity as the main exposure.
- **What would change this rating.** Raise to Level 2 if organized-crime violence or targeting of Uruguayan institutions increases.

Public Wi-Fi

- Local security capacity is thin, and phone snatching in Montevideo occurs alongside basic phishing campaigns. Avoid public Wi-Fi; connect through a corporate VPN if one is necessary.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Keep devices out of sight in Montevideo, and avoid areas flagged by local police at night.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

UZBEKISTAN

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2



CAPITAL
Tashkent

GOVERNMENT
Presidential republic (authoritarian)

LANGUAGE
Uzbek (Russian widely used)

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued January 26, 2026)

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: State monitoring of communications and speech, periodic platform blocks, and a shutdown precedent in Karakalpakstan.

Country Overview

Uzbekistan is a doubly landlocked Central Asian country and the heartland of the historic Silk Road, home to Samarkand, Bukhara, and Khiva. Russia conquered the region in the nineteenth century, and Uzbekistan became a Soviet republic and then independent in 1991.

Islam Karimov ruled until his death in 2016. Shavkat Mirziyoyev succeeded him and opened the economy and loosened some controls, while keeping tight political control. A 2023 constitutional referendum reset presidential term counts. Uzbekistan has about 39 million people and large reserves of gas and gold.

Geopolitical Landscape

- **Controlled opening.** Economic reforms and tourism have grown, but opposition and independent media remain limited.
- **Karakalpakstan.** A 2022 crackdown in the autonomous region of Karakalpakstan killed dozens and was accompanied by an internet shutdown.
- **Balancing powers.** Uzbekistan balances ties with Russia, China, the United States, and its neighbors, and it is a major source of migrant labor in Russia.
- **Afghanistan.** Tashkent engages the Taliban pragmatically on trade and transit.

Cyber Threats | Organizations

- **State monitoring.** Security services monitor communications, and authorities have blocked platforms and restricted access during unrest.
- **Platform controls.** Social media platforms have been blocked and throttled periodically.
- **Banks and fintech.** Rapid digitization has increased fraud and account takeover.
- **Limited security capacity.** Public bodies and firms have thin staffing and basic defenses.
- **Employees based in country.** Employees should assume communications can be monitored and expect occasional platform blocks. Avoid political commentary.
- **Vendor and supply chain risk.** State-linked telecoms and local IT vendors can be compelled to share data. Segment vendor access and verify payment changes out of band.

The TIDE team tracks 7 threat actors that list Uzbekistan among their targets. By attributed nexus, they break down as 4 China-nexus, 1 Iran-nexus, 1 Russia-nexus, and 1 cybercriminal. The most frequently targeted sectors are government (5), defense and defense industrial base (4), aerospace (2), healthcare and pharmaceuticals (2), and technology (2). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring.** Online criticism of the government can lead to prosecution, and bloggers have been jailed.
- **Fraud.** Phishing and wallet scams circulate in Uzbek and Russian.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Uzbekistan.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Uzbekistan Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** State monitoring of communications and speech, periodic platform blocks, and the 2022 shutdown in Karakalpakstan drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest brings shutdowns or detentions of foreigners. Lower to Level 1 if controls ease.

Public Wi-Fi

- Uzbek authorities monitor communications and have blocked platforms and restricted access during unrest, including a 2022 internet shutdown in Karakalpakstan. Avoid public Wi-Fi; if a public network must be used, connect through a corporate VPN first.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, and carry offline copies of key documents.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

VANUATU

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 1

CAPITAL
Port Vila

GOVERNMENT
Parliamentary republic

LANGUAGE
Bislama, English, and French

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued May 22, 2025)

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Very limited connectivity and low crime; a 2022 attack showed fragility of government systems.

Country Overview

Vanuatu is a Melanesian archipelago of more than eighty islands in the South Pacific with extraordinary linguistic diversity. Britain and France jointly administered it as the New Hebrides until independence in 1980.

The country has about 320,000 people and an economy based on tourism, agriculture, and offshore services, including citizenship by investment. Cyclones, earthquakes, and volcanoes are recurrent hazards, and a December 2024 earthquake caused deaths and damage in Port Vila. Jotham Napat became prime minister in early 2025.

Geopolitical Landscape

- **Political instability.** Frequent no-confidence votes and changes of government are common, and 2024 constitutional reforms aim to curb them.
- **Great-power competition.** Australia and China compete for influence, and a security and economic treaty with Australia has been stalled.
- **Climate leadership.** Vanuatu led the push for an International Court of Justice opinion on climate obligations.

Cyber Threats | Organizations

- **2022 government cyberattack.** A November 2022 attack disabled Vanuatu's government emails, websites, and systems, with only partial access restored a month later, and it showed the exposure of small states.
- **Minimal digital footprint.** Connectivity depends on limited cable and satellite links, and local security capacity is very limited.
- **Passport program.** Citizenship-by-investment agents and the program hold sensitive identity data.
- **Employees based in country.** Employees face limited connectivity and basic phishing risk, and cyclone and earthquake disruption.
- **Vendor and supply chain risk.** A few external vendors provide connectivity and IT, and the 2022 incident shows how a single compromise can disable government. Plan for offline operation and require incident notification.

The TIDE team tracks 1 threat actor that lists Vanuatu among their targets. By attributed nexus, they break down as 1 cybercriminal. The most frequently targeted sectors are banking and financial services (1), government (1), healthcare and pharmaceuticals (1), logistics, supply chain and transportation (1), and technology (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Limited connectivity.** Vodafone Vanuatu and Digicel provide mobile service, and internet is slow and costly.
- **Phishing and fraud.** Basic phishing and mobile fraud exist, including bank-impersonation messages reported by ANZ Vanuatu.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Vanuatu.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Vanuatu Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Connectivity is very limited and crime is low. The 2022 government attack showed how fragile small-state systems are.
- **What would change this rating.** Raise to Level 2 if another major attack or political crisis disrupts government and connectivity.

Public Wi-Fi

- A late-2022 ransomware attack claimed by the RansomHouse group took Vanuatu's government offline for weeks and exfiltrated a reported 3.2 terabytes of data, underscoring the fragility of small-state infrastructure;

connectivity has since improved via the Interchange Cable link to Fiji, but avoid public Wi-Fi and use a corporate VPN if a public network is unavoidable.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Cyclone season, November through April, can disrupt travel and connectivity.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

VATICAN CITY

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 1



CAPITAL
Vatican City

GOVERNMENT
Ecclesiastical absolute elective monarchy (the Holy See)

LANGUAGE
Italian and Latin

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued September 10, 2026)

Risk indicators: Terrorism

TIDE CYBER RISK LEVEL

Level 1, Exercise Normal Cyber Precautions

Guidance: Standard cyber hygiene applies.

Rationale: Tiny and low crime; exposure is pickpocketing near St. Peter's, impersonation scams, and state-linked targeting of Church communications.

Country Overview

Vatican City is the world's smallest sovereign state, an enclave of about 0.44 square kilometers inside Rome and the seat of the Catholic Church. The Lateran Treaty of 1929 with Italy established it as an independent state, ending a dispute that followed the loss of the Papal States in 1870.

About 880 people live there. The pope is head of state, and Pope Leo XIV, the first pope from the United States, was elected in May 2025. The Holy See, the Church's governing body, maintains diplomatic relations with more than 180 states and has permanent observer status at the United Nations.

Geopolitical Landscape

- **Diplomatic role.** The Holy See acts as a moral and diplomatic voice on peace, migration, and conflict, and it has offered to host talks on Ukraine and the Middle East.
- **Finance and transparency.** The Vatican has reformed its bank and finances to meet international transparency standards after past scandals.
- **Security threats.** Terrorist threats against high-profile religious events and the crowds in Rome are a concern.

Cyber Threats | Organizations

- **State-linked espionage.** Vatican networks have been targeted in the past, including by China-linked actors reported to have probed Catholic and Vatican-related targets before negotiations over bishops.
- **Sensitive communications.** Diplomatic cables, finance, and personal data of clergy and staff are high-value targets.
- **Phishing and impersonation.** Fraudsters impersonate clergy and charities, and the Vatican's name is used in scams.
- **Dependence on Italian vendors.** Utilities and connectivity depend on Italian providers.
- **Employees based in country.** Visitors face pickpocketing and ticket scams around St. Peter's, and phishing that impersonates Church officials.
- **Vendor and supply chain risk.** Italian utilities and a small set of technology providers support Vatican operations. Verify supplier controls for sensitive communications.

The TIDE team tracks 1 threat actor that lists Vatican City among their targets. By attributed nexus, they break down as 1 Belarus-nexus. The most frequently targeted sectors are diplomatic and foreign affairs (1), and government (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Pilgrim and tourist scams.** Fake tickets, tours, and charity appeals target visitors, and pickpocketing is common near St. Peter's.
- **Impersonation of the Church.** Messages claiming to be from clergy or the Holy See request donations.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Vatican City.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Vatican City Level 2, Exercise Increased Caution, citing terrorism. The TIDE Cyber Risk Level is 1, Exercise Normal Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** The state is tiny and crime is low, but pickpocketing near St. Peter's, impersonation scams, and state-linked targeting of Church communications drive the rating.
- **What would change this rating.** Raise to Level 2 for staff with access to sensitive Church communications if targeting increases.

Public Wi-Fi

- Vatican networks have faced state-linked espionage targeting sensitive diplomatic and financial communications. Avoid public Wi-Fi, and connect through a corporate VPN if a public network is necessary.

Recommended controls

- Standard cyber hygiene applies: full-disk encryption, a managed profile, multi-factor authentication, remote wipe, and a corporate VPN. Avoid public USB charging, and bring personal chargers.

Local practices

- Crowds at major events attract pickpockets, so secure phones and bags.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

VENEZUELA

U.S. STATE DEPT. LEVEL 3

TIDE CYBER RISK LEVEL 3



CAPITAL
Caracas

GOVERNMENT
Interim government led by an acting president

LANGUAGE
Spanish

U.S. DEPARTMENT OF STATE

Level 3, Reconsider Travel (issued June 27, 2026)

Risk indicators: Crime, health, kidnapping or hostage-taking, terrorism, natural disaster

TIDE CYBER RISK LEVEL

Level 3, Heightened Cyber Precautions

Guidance: Exercise increased cyber hygiene. Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer.

Rationale: State monitoring and detention risk, power outages, kidnapping and extortion, sanctions uncertainty, and a U.S. Level 3 advisory.

Country Overview

Venezuela lies on the northern coast of South America and holds the world's largest proven oil reserves. Spain colonized it, Simon Bolivar led its independence movement, and it became independent from Gran Colombia in 1830. Oil discoveries in the twentieth century made it one of Latin America's richest countries.

Hugo Chavez's election in 1998 began the Bolivarian Revolution, and Nicolas Maduro succeeded him in 2013. Mismanagement, sanctions, and corruption shrank the economy by more than three quarters, and about eight million Venezuelans left. Venezuela has about 28.6 million people. On January 3, 2026, U.S. forces captured Maduro and his wife, Cilia Flores, who face narco-terrorism charges in New York.

Geopolitical Landscape

- **Post-Maduro transition.** Delcy Rodriguez, Maduro's vice president and oil minister, became acting president and is governing under heavy U.S. pressure. She passed an oil reform law to open the sector to foreign investment and pursued amnesty measures. U.S. officials, including Secretary Rubio in June, say a real transition requires free, multi-party elections, and the opposition and the Trump administration differ on how to get there.

- **Opposition.** The opposition says it won the rigged 2024 election, and its leaders have disagreed with the administration's chosen dialogue process.
- **Oil and sanctions.** U.S. control over oil sales and proceeds is a key lever, and foreign firms weigh whether Venezuela is investable while the Chavista state remains.
- **Regional effects.** Maduro's fall has affected Cuba and shifted migration and security dynamics in the Caribbean.

Cyber Threats | Organizations

- **State surveillance.** Intelligence services monitor communications, and the institutions that do so remain in place.
- **Power and connectivity instability.** Blackouts and weak infrastructure disrupt operations.
- **Sanctions and counterparties.** Residual sanctions, designated officials, and shifting U.S. licenses create significant compliance risk.
- **Oil sector.** Operators and contractors hold valuable data and face espionage and fraud.
- **Employees based in country.** Employees face state monitoring, detention risk, power outages, and kidnapping and extortion risk. Remove company access from personal devices where policy requires, and keep movements confidential.
- **Vendor and supply chain risk.** Local telecom, security, and logistics vendors operate under state oversight and sanctions uncertainty and can be compelled to share data. Screen ownership and licenses, segment vendor access, and plan for outages.

The TIDE team tracks 4 threat actors that list Venezuela among their targets. By attributed nexus, they break down as 2 unattributed or other, 1 China-nexus, and 1 cybercriminal. The most frequently targeted sectors are government (3), banking and financial services (2), energy (2), hospitality and travel (1), and military (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and detention.** People have been detained for online posts and contacts with foreigners, and the situation is evolving.
- **Kidnapping and extortion.** Criminal groups and armed actors carry out kidnapping and extortion.
- **Currency and payment fraud.** Dollarized transactions and informal payments create scam risk.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Venezuela.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Venezuela Level 3, Reconsider Travel, citing crime, health, kidnapping or hostage-taking, terrorism, natural disaster. The TIDE Cyber Risk Level is 3, Heightened Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** State monitoring and detention risk, power outages, kidnapping and extortion, sanctions uncertainty during the post-Maduro transition, and the State Department's Level 3 advisory drive the rating.
- **What would change this rating.** Raise to Level 4 if the transition breaks down, detentions of foreigners increase, or violence escalates. Lower to Level 2 as institutions normalize and sanctions clarify.

Public Wi-Fi

- State intelligence services monitor communications, power outages are frequent, and local telecom vendors operate under state oversight and sanctions uncertainty. Avoid public Wi-Fi; connect through a corporate VPN if a public network is unavoidable.

Recommended corporate policy

- Do not bring company or vendor devices or access company or vendor infrastructure unless explicitly needed and authorized by your employer. Where travel is authorized, prefer clean loaner devices for travelers in government, defense, energy, finance, or other sensitive roles.
- Use company-managed devices with full-disk encryption and phishing-resistant multi-factor authentication, a corporate VPN, and remote wipe. Assume hotel and carrier networks are monitored, and avoid public Wi-Fi and public USB charging.

Local practices

- Avoid the Colombian border areas and other regions flagged in the advisory, and use secure transport arranged by your employer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

VIETNAM

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2



CAPITAL
Hanoi

GOVERNMENT
One-party socialist republic

LANGUAGE
Vietnamese

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued June 24, 2026)

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: State monitoring and data localization, platform blocks, motorbike phone snatching, and scam exposure.

Country Overview

Vietnam lies on the eastern coast of mainland Southeast Asia and has a history of resistance to foreign rule, including a thousand years of Chinese domination ending in 938. France colonized it in the nineteenth century, and Ho Chi Minh declared independence in 1945. The wars against France and then the United States ended with the fall of Saigon in 1975 and reunification in 1976.

The Communist Party has held power since, and economic liberalization from the Doi Moi reforms of 1986 turned Vietnam into a manufacturing export hub. It has about 102 million people. To Lam leads the Communist Party and has consolidated power since 2024.

Geopolitical Landscape

- **Anti-corruption campaign and consolidation.** A sweeping purge has removed senior officials and concentrated power in To Lam, and the 2026 Party Congress set the leadership for the next five years.
- **South China Sea.** Vietnam has built up its outposts and faces Chinese pressure while avoiding open confrontation.
- **Balancing powers.** Vietnam keeps ties with China, the United States, and Russia and is a beneficiary of supply chain shifts, though U.S. tariffs weigh on exports.

Cyber Threats | Organizations

- **State monitoring and data localization.** The Cybersecurity Law requires data localization and cooperation with authorities, and Decree 147 ties social media accounts to phone numbers.
- **Platform blocks.** Authorities banned Telegram in 2025 and can order content removal and platform restrictions.
- **State-linked espionage.** APT32, tracked as Vietnam-nexus, targets governments, media, and foreign firms in the region.
- **Ransomware and fraud.** Banks, retailers, and manufacturers face ransomware and account takeover, and scam operations are active.
- **Manufacturing.** Electronics and textile plants hold intellectual property and face business email compromise.
- **Employees based in country.** Employees should assume communications can be monitored, avoid political commentary, and expect phishing and motorbike phone snatching. Staff in manufacturing, media, and government-adjacent roles face elevated targeting.
- **Vendor and supply chain risk.** Local telecoms, hosting providers, and IT vendors must comply with data localization and state access rules. Segment vendor access, review where data is stored, and verify payment changes out of band.

The TIDE team tracks 45 threat actors that list Vietnam among their targets. By attributed nexus, they break down as 34 China-nexus, 7 cybercriminal, 3 North Korea-nexus, and 1 Vietnam-nexus. The most frequently targeted sectors are government (36), technology (15), telecommunications (15), defense and defense industrial base (14), and banking and financial services (10). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Monitoring and arrest.** Online criticism of the party or leaders can lead to prosecution under national security laws.
- **Phishing and scams.** Bank, delivery, and police impersonation and investment scams are common.
- **Phone theft.** Snatch theft by motorbike occurs in Hanoi and Ho Chi Minh City.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors that carry a public government attribution to Vietnam. Security vendors track one Vietnam-nexus espionage cluster whose targeting aligns with Vietnamese state interests, but Vietnam does not acknowledge it.

GROUP	ALSO KNOWN AS	ATTRIBUTED SPONSOR	FOCUS	ACTIVE
APT32	OceanLotus, SeaLotus, APT-C-00, Cobalt Kitty	Vietnam-nexus; no government attribution	Espionage against regional governments, media, and foreign firms	2013 to 2026

The cluster has been linked by vendors to targeting of foreign automotive, media, and government organizations. This list excludes U.S. agencies by design.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Vietnam Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** State monitoring and data localization, platform blocks, motorbike phone snatching, and scam exposure drive the rating.
- **What would change this rating.** Raise to Level 3 if detentions of foreigners increase or restrictions tighten. Lower to Level 1 if controls ease.

Public Wi-Fi

- Vietnamese authorities enforce data localization, block platforms such as Telegram, and monitor communications through decree and practice, while China-linked actors maintain active espionage against the region. Avoid public Wi-Fi; use a corporate VPN if a public network is necessary.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Keep phones secured near roads, where motorbike snatch theft occurs, and use ride-hailing apps.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

WEST BANK AND GAZA

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4

CAPITAL
Ramallah (Palestinian Authority seat in the West Bank), Gaza City

GOVERNMENT
Palestinian Authority in parts of the West Bank, Hamas in parts of Gaza, with Israeli military control in much of both

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued August 26, 2026)

Risk indicators: Unrest, health, terrorism

Note: The State Department issues separate advisories: Gaza is Level 4, Do Not Travel (unrest, health, terrorism), and the West Bank is Level 3, Reconsider Travel (unrest, terrorism). The final status of these areas is subject to negotiation under U.S. policy.

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Armed conflict and severe physical risk, Israeli and local surveillance, connectivity blackouts, and a U.S. Level 4 advisory for Gaza.

Country Overview

The West Bank and Gaza are Palestinian territories that Israel captured from Jordan and Egypt in the 1967 war. The Oslo Accords of the 1990s created the Palestinian Authority and divided the West Bank into areas under varying degrees of Palestinian and Israeli control. Israel withdrew its settlers and troops from Gaza in 2005, and Hamas took control there in 2007.

About 5.6 million Palestinians live in the West Bank and Gaza, according to Palestinian official estimates, and roughly 500,000 Israeli settlers also live in the West Bank outside East Jerusalem. Much of Gaza's population has been displaced by the war that began after Hamas's October 7, 2023 attack on Israel.

Geopolitical Landscape

- **Gaza ceasefire and the Yellow Line.** A ceasefire took effect in October 2025. Israel holds territory behind the so-called Yellow Line that analysts say covers nearly 65 percent of Gaza, and the ceasefire framework and any further Israeli withdrawal remain contested, with Israel's October 27 election complicating decisions.
- **West Bank.** Israeli military raids, settler violence, and settlement expansion continue, and the United Kingdom and others have urged Israel at the UN Security Council to halt settlement expansion.
- **Palestinian Authority.** The Authority faces a fiscal crisis, a legitimacy gap, and an unresolved succession question.
- **Humanitarian crisis.** Aid access, food insecurity, and destroyed infrastructure remain acute in Gaza.

Cyber Threats | Organizations

- **Israeli control of telecoms and spectrum.** Israel controls much of the telecom infrastructure and frequencies, and Gaza has suffered repeated connectivity blackouts.
- **Surveillance and spyware.** Israeli authorities monitor communications.
- **Damaged infrastructure.** Power, networks, and banking are heavily damaged, so operations depend on generators and satellite links.
- **Staff safety.** Leaks of staff, site, or convoy information can create direct physical risk.
- **Employees based in country.** Staff in the West Bank and Gaza face monitoring, checkpoint device searches, power and connectivity loss, and severe physical risk. Remove company access from personal devices and keep movements and location data confidential.
- **Vendor and supply chain risk.** Local telecom, banking, and logistics vendors operate under Israeli and Palestinian authority controls and can lose access abruptly. Limit shared location data, segment vendor access, and plan for sudden loss of services.

The TIDE team tracks 4 threat actors that list the West Bank and Gaza among their targets. By attributed nexus, they break down as 3 unattributed or other, and 1 China-nexus. The most frequently targeted sectors are government (4), civil society and activism (2), diplomatic and foreign affairs (2), banking and financial services (1), and politics and political organizations (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Surveillance and detention.** Palestinians and visitors face monitoring, checkpoint device searches, and administrative detention.
- **Connectivity loss.** Blackouts can cut communications for days.
- **Disinformation and fraud.** False content and fraudulent aid and donation appeals spread widely.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to a Palestinian state authority. Non-state and Hamas-aligned clusters are tracked in other categories.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Gaza Level 4, Do Not Travel, citing unrest, health, and terrorism, and the West Bank Level 3, Reconsider Travel, citing unrest and terrorism. The U.S. government has very limited ability to assist in either area. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** Armed conflict and severe physical risk, Israeli and local surveillance, connectivity blackouts, and the State Department's Level 4 advisory for Gaza drive the rating.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable ceasefire and restored access and infrastructure.

Public Wi-Fi

- Israeli control of telecom infrastructure, monitoring by multiple authorities, and recurring connectivity blackouts create severe risks. Do not use public Wi-Fi; rely only on approved devices with pre-arranged connectivity plans if travel is authorized.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices or access company or vendor infrastructure while in the West Bank or Gaza unless explicitly authorized for an essential mission, and then use clean loaner devices with minimal data.
- Remove company-linked accounts and applications from personal devices, and assume checkpoint officers may inspect devices.

Connectivity and communications

- Expect power and network outages and plan satellite or offline communications and check-in schedules that do not depend on mobile data.

Personal safety and legal exposure

- Keep movements, locations, and contact lists confidential, and avoid commentary on political or military matters.
- Identify counsel before departure and prepare an evacuation plan.

Return protocol

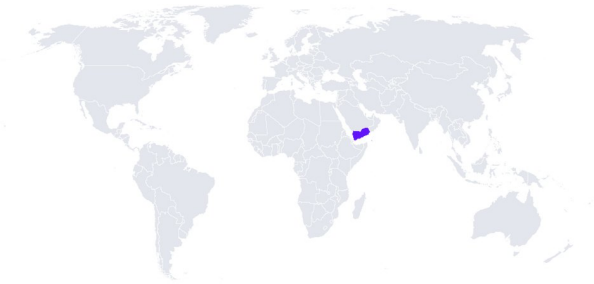
- Treat any device that traveled as untrusted and wipe it before re-enrolling it. Rotate credentials for accounts it touched from a trusted network, and hold a debrief.

WORLDBOOK

YEMEN

U.S. STATE DEPT. LEVEL 4

TIDE CYBER RISK LEVEL 4



CAPITAL
Sanaa (Houthi-controlled) and Aden (seat of the internationally recognized government)

GOVERNMENT
Divided between the Houthi movement and the internationally recognized government

LANGUAGE
Arabic

U.S. DEPARTMENT OF STATE

Level 4, Do Not Travel (issued December 19, 2025)

Risk indicators: Unrest, crime, health, kidnapping or hostage-taking, terrorism, other

TIDE CYBER RISK LEVEL

Level 4, Maximum Cyber Precautions

Guidance: Take additional preventative measures before and after travel. DO NOT bring or access company or vendor devices or infrastructure.

Rationale: Renewed war with Houthi strikes on Saudi and Yemeni airports, Houthi control of telecoms and detention of staff, kidnapping risk, and a U.S. Level 4 advisory.

Country Overview

Yemen lies at the southwestern tip of the Arabian Peninsula, an ancient crossroads of trade and the home of the historic kingdoms of Saba and Himyar. The Ottomans and later Britain, in the south, ruled parts of the territory. North and South Yemen unified in 1990 and fought a brief civil war in 1994.

Long-time president Ali Abdullah Saleh was pushed out after the 2011 uprising. The Houthi movement, backed by Iran, seized the capital Sanaa in 2014, and a Saudi-led coalition intervened in 2015. The war killed hundreds of thousands and created one of the world's worst humanitarian crises. Yemen has about 32.7 million people.

Geopolitical Landscape

- **Renewed Saudi-Houthi war.** A four-year truce has collapsed. The Houthis announced a blockade of Saudi ports in July 2026, seized Yemen's Red Sea coast from government forces in September, and struck airports in Saudi Arabia and Aden in early October. Saudi Arabia and allied Yemeni forces launched a ground and air offensive in early October and retook Mokha. President Trump said on October 10 that he is considering strikes on the Houthis.

- **Red Sea and Hormuz.** The Houthis attack Saudi-linked shipping, which threatens the Red Sea as an alternative route to the Strait of Hormuz during the Iran war.
- **Fragmented anti-Houthi camp.** Southern separatists and the government coalition have competing aims.
- **Humanitarian crisis.** Famine, cholera, and aid cuts affect most of the population.

Cyber Threats | Organizations

- **War damage and outages.** Strikes, power cuts, and damaged networks disrupt operations, and local security capacity is minimal.
- **Houthi control of telecoms.** The Houthis control telecom infrastructure in the north, monitor communications, and detain people, including UN and NGO staff.
- **Iran-linked and regional cyber activity.** Iran-aligned and Gulf-aligned actors target regional government, telecom, and shipping networks.
- **Staff safety.** Leaks of staff, site, or convoy information can create direct physical risk.
- **Employees based in country.** Do not travel. Staff in country face armed conflict, detention, kidnapping, and connectivity loss. Remove company access from personal devices and keep movements confidential.
- **Vendor and supply chain risk.** Local telecom, logistics, and security vendors operate under competing armed authorities and can lose access abruptly. Limit shared location data, segment vendor access, and plan for sudden loss of services.

The TIDE team tracks 2 threat actors that list Yemen among their targets. By attributed nexus, they break down as 2 unattributed or other. The most frequently targeted sectors are media and journalism (2), civil society and activism (1), and government (1). These figures count actors, not incidents.

Cyber Threats | Individuals

- **Detention and surveillance.** Houthi authorities have detained aid workers and critics, and people face monitoring of phones and social media.
- **Kidnapping.** Kidnapping for ransom and political reasons occurs, and al-Qaeda is active in parts of the south and east.
- **Connectivity loss.** Outages are frequent and prolonged.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Yemen.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Yemen Level 4, Do Not Travel, citing unrest, crime, health, kidnapping or hostage-taking, terrorism, other. The TIDE Cyber Risk Level is 4, Maximum Cyber Precautions. The U.S. government has no embassy operations in Yemen and cannot assist.

TIDE Risk Level Rationale

- **Drivers.** The renewed Saudi-Houthi war, Houthi control of telecoms and detention of staff, kidnapping risk, and a U.S. Level 4 advisory drive the rating.
- **What would change this rating.** Level 4 is the ceiling. Lowering would require a durable truce and an end to detention of aid and company staff.

Public Wi-Fi

- Houthi forces control telecom infrastructure in the north and monitor communications, while active warfare creates both surveillance and connectivity loss risks. Do not bring company devices or access company infrastructure in country. Standard VPN or public Wi-Fi use is not a workable mitigation.

Recommended corporate policy: no device, no infrastructure

- Do not bring company or vendor devices, remove all company-linked accounts and applications (including authenticator apps and password managers) from personal devices before travel, and do not log in to company or vendor infrastructure while in country.
- Block sign-ins from the country with geo-based conditional access and alert on every attempt; since a VPN may let an attacker bypass the geographic block, these alerts are the primary way to detect such an attempt.
- Approve exceptions only with a documented security plan and executive sign-off, issue clean loaner devices with minimal data and no persistent VPN or single sign-on, and reimage them on return.
- Confirm that travel medical and evacuation coverage applies and that the provider can operate there. Do not wear company apparel or discuss work, and prepare an approved cover answer.

Return protocol

- Treat any device that traveled as untrusted, wipe it before re-enrolling it, rotate credentials for accounts it touched from a trusted network, and hold a debrief. Apply heightened monitoring to traveler identities for 30 to 90 days.

WORLDBOOK

ZAMBIA

U.S. STATE DEPT. LEVEL 1

TIDE CYBER RISK LEVEL 2



CAPITAL
Lusaka

GOVERNMENT
Presidential republic

LANGUAGE
English (with Bemba, Nyanja, and other languages)

U.S. DEPARTMENT OF STATE

Level 1, Exercise Normal Precautions (issued July 31, 2023)

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: Contested 2026 election with opposition arrests, expanded state data powers, mobile-money fraud, and phone theft.

Country Overview

Zambia is a landlocked southern African country named for the Zambezi River and is home to Victoria Falls. Britain governed it as Northern Rhodesia, and it became independent in 1964 under Kenneth Kaunda, who led a one-party state until 1991.

Zambia has about 23 million people and is Africa's second-largest copper producer. It was the first African country to default in the COVID era, in 2020, and completed a debt restructuring in 2024. Every change of president since the return to multiparty politics in 1991 has come through elections.

Geopolitical Landscape

- **August 2026 election.** President Hakainde Hichilema was declared the winner on August 18, 2026 with about 60 percent of the vote against Brian Mundubile's 38 percent, avoiding a runoff. The count was suspended at one point because of violence at polling stations, opposition officials were arrested, courts were closed during the challenge period, and Mundubile and his running mate were reported to be in prison. Hichilema was inaugurated for a second term on September 1.
- **Opposition claims.** Mundubile alleged the alteration of result forms and called for an independent investigation, which the government rejected.

- **Economy and copper.** Debt restructuring and rising copper prices have helped, but power shortages after the 2024 drought and living costs weigh on households.
- **Regional role.** Zambia is a key corridor for copper exports and a partner for U.S. and Chinese mining and rail investment.

Cyber Threats | Organizations

- **Election-period restrictions.** Authorities have previously restricted social media and could do so around disputes.
- **Cyber laws.** The 2025 Cyber Security and Cyber Crimes Acts expanded state powers over data and online speech, drawing criticism from rights groups.
- **Mining sector.** Operators and contractors hold valuable data and face fraud and espionage.
- **Mobile money and banking.** Wallets and banks face SIM-swap and social engineering.
- **Employees based in country.** Employees face mobile-money fraud and phone theft, and possible connectivity restrictions and demonstrations around election disputes. Avoid political content online.
- **Vendor and supply chain risk.** Telecoms, mining contractors, and fintech vendors operate under expanded state data powers. Segment vendor access, review data location, and verify payment changes out of band.

The TIDE team does not currently track actors that list Zambia among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Speech and monitoring risk.** Online criticism of the president can lead to arrest.
- **Mobile money fraud.** SMS and wallet scams are common.
- **Phone theft.** Snatch theft occurs in Lusaka.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Zambia.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Zambia Level 1, Exercise Normal Precautions. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** The contested August 2026 election with opposition arrests, expanded state data powers, mobile-money fraud, and phone theft drive the rating.
- **What would change this rating.** Raise to Level 3 if post-election unrest brings shutdowns or detentions of foreigners. Lower to Level 1 as tension eases.

Public Wi-Fi

- Recent elections have prompted opposition arrests and connectivity restrictions; expanded state data powers and mobile-money fraud are common. Avoid public Wi-Fi, and use a corporate VPN if a public network must be used.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations around political events, and keep devices out of sight in traffic.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.

WORLDBOOK

ZIMBABWE

U.S. STATE DEPT. LEVEL 2

TIDE CYBER RISK LEVEL 2



CAPITAL
Harare

GOVERNMENT
Presidential republic (dominant-party)

LANGUAGE
English, Shona, and Ndebele (16 official languages)

U.S. DEPARTMENT OF STATE

Level 2, Exercise Increased Caution (issued June 27, 2023)

Risk indicators: Unrest, crime, other

TIDE CYBER RISK LEVEL

Level 2, Exercise Increased Cyber Precautions

Guidance: Apply enhanced controls and heightened awareness of device theft, fraud, or targeted interest.

Rationale: State monitoring and broad interception powers, a shutdown precedent, power cuts, and mobile-money fraud.

Country Overview

Zimbabwe is a landlocked southern African country named for the stone ruins of Great Zimbabwe, the capital of a medieval trading kingdom. British settlers colonized it as Rhodesia, and a white minority government declared independence in 1965. A guerrilla war ended in 1980 with independence as Zimbabwe under Robert Mugabe.

Mugabe's rule included violent land seizures and hyperinflation, and a 2017 military intervention removed him. Emmerson Mnangagwa has been president since. Zimbabwe has about 17.1 million people, large gold, lithium, and platinum resources, and a long history of currency collapse and economic crisis.

Geopolitical Landscape

- **Term-extension push.** Elements of the ruling ZANU-PF have pushed to extend Mnangagwa's rule beyond the 2028 end of his term, which has split the party and drawn opposition.
- **Repression.** Authorities have arrested opposition figures, journalists, and activists, and political gatherings are tightly controlled.
- **Economy.** The government has introduced a new gold-backed currency, but inflation, shortages, and power cuts persist, and Zimbabwe is in arrears to creditors.

- **Resources and sanctions.** Lithium and gold attract Chinese investment, and Western sanctions on certain individuals remain.

Cyber Threats | Organizations

- **State monitoring and law.** The Interception of Communications Act and a 2021 cyber and data protection law give authorities broad powers over data and online speech.
- **Connectivity restrictions.** The government shut down the internet during the January 2019 protests and could do so again.
- **Mining sector.** Operators and contractors hold valuable data and face fraud and espionage.
- **Mobile money and banking.** EcoCash and banks face SIM-swap and fraud, and informal currency markets create scam risk.
- **Employees based in country.** Employees face monitoring, possible connectivity restrictions during unrest, power cuts, and mobile-money fraud. Avoid political commentary.
- **Vendor and supply chain risk.** Telecoms and mining contractors operate under state oversight and can be compelled to share data or restricted. Segment vendor access and plan for power and connectivity outages.

The TIDE team does not currently track actors that list Zimbabwe among their targets. That reflects limited public reporting and does not indicate an absence of threat.

Cyber Threats | Individuals

- **Monitoring and arrest.** Online criticism of the government can lead to arrest, and activists have been abducted.
- **Mobile money fraud.** SMS and wallet scams are common.
- **Phone theft.** Snatch theft occurs in Harare.

State-Sponsored Cyber Threats

The TIDE team tracks no state-sponsored cyber threat actors attributed to Zimbabwe.

Cyber Travel Considerations

Official guidance

The U.S. Department of State rates Zimbabwe Level 2, Exercise Increased Caution, citing unrest, crime, other. The TIDE Cyber Risk Level is 2, Exercise Increased Cyber Precautions.

TIDE Risk Level Rationale

- **Drivers.** State monitoring and broad interception powers, a precedent of internet shutdowns, power cuts, and mobile-money fraud drive the rating.
- **What would change this rating.** Raise to Level 3 if unrest or the term-extension push triggers shutdowns or crackdowns. Lower to Level 1 as controls ease.

Public Wi-Fi

- The Interception of Communications Act grants authorities broad surveillance powers, and the government has previously shut down the internet during civil unrest. Avoid public Wi-Fi; connect through a corporate VPN if a public network is unavoidable.

Recommended controls

- Exercise increased cyber precautions: use managed devices with full-disk encryption, phishing-resistant multi-factor authentication, remote wipe, and a corporate VPN. Carry only the data the trip requires, avoid public USB charging, and bring personal chargers. Give travelers a stolen-device procedure.

Local practices

- Avoid demonstrations, and carry power banks and offline plans, since outages are frequent.

Return protocol

- Report lost or stolen devices immediately, revoke sessions and tokens, and rotate credentials if a device left your control.