GLOBAL GUARDIAN

WORLDWIDE THREAT ASSESSMENT

MARCH 2026

GLOBALGUARDIAN.COM 703.566.9463 INFO@GLOBALGUARDIAN.COM

TABLE OF CONTENTS

THREATS IN FOCUS

THREATS IN BRIEF

The 2026 global landscape will be marked by deep uncertainty and volatility as major shifts in global power present implications for multinational organizations and their people.

Global Guardian's 2026 Worldwide Threat Assessment aims to disambiguate the global security landscape and shed light on the current trends impacting international business and travel. This forward-looking report evaluates emerging risks and their impact on safety and security. To this end, the 2026 Threat Assessment examines the physical security issues of a new pattern in mass unrest, the two main drivers of the security landscape in Latin America, and the business risks associated with the trend of resource nationalism. This report also covers novel risks emanating from the digital space that include attacks on crypto holders, AI-enabled cyberattacks, and insider threats from North Korean remote workers. These insights are meant to inspire action to protect investments, assets, and, most importantly, the safety and well-being of your colleagues and family members.

LATAM'S CRIMINAL REVOLUTION AND THE BUKELE BLUEPRINT

INDUSTRY IMPACT: Energy, Materials, Industrials, Consumer Staples **RISK TYPES:** Kidnap and Ransom, Organized Crime, Political/Regulatory, Terrorism

Criminal organizations and non-state armed groups in Latin America are becoming more diversified, better resourced, and more sophisticated, creating insecurity that leaves businesses and travelers more exposed to threats. President Nayib Bukele's crackdown on El Salvador's gangs is increasingly being viewed by regional populations and their leaders as a crime fighting model to replicate at home. Despite the success of the Bukele Model in El Salvador, its application elsewhere risks increasing the levels of violence in the short term. Colombia—of all the countries considering the model—is where it could fail most catastrophically.

ECONOMIC DIVERSIFICATION

Throughout much of the 20th century and early 2000s, Latin America's criminal economy was primarily dominated by Colombian and Mexican groups that produced and distributed cocaine, marijuana, and heroin. Today, drug trafficking represents only one component of a far broader and more diversified illicit portfolio, whereby criminal groups extract income from virtually any individual, business, or state entity that they can exploit. Mexican organizations have expanded into migrant smuggling and fuel theft; Brazilian gangs traffic natural resources and run sophisticated cyber-fraud schemes; and Ecuadorian mega-gangs combine cocaine trafficking with illegal gold mining.

As criminal groups diversify, they increasingly draw legitimate businesses into the criminal economy. Through extortion, cargo theft, fuel siphoning, cyber fraud, and coerced money laundering, they now target retailers, transport companies, construction firms, energy providers, and exporters—turning them into criminal assets. Once embedded in local economies, these organizations punish non-compliance with violence, sabotage, or regulatory harassment via corrupt officials [figure 1].

RISING CRIMINAL SOPHISTICATION

Economic diversification has produced wealthier, more resilient, and more adaptable criminal actors. Criminal groups now have the resources to procure military-grade weaponry and specialized support networks such as lawyers and money launderers, and to penetrate state institutions through the corruption of police, military officials, and politicians.

In the early 2000s, countries such as Guatemala, Ecuador, and Honduras were largely dominated by street gangs like MS-13 and Barrio 18, whose activities centered on localized extortion, micro-trafficking, and turf rivalries. However, over the past two decades, these groups have evolved into more structured organizations, developing prison-based hierarchies, formalized extortion systems, and operational ties to Mexican and Colombian cartels—marking a qualitative shift in the scale and complexity of the criminal threat facing Latin American states.

Public security forces designed to prevent crime from small gangs and petty criminals are being outmatched by better-funded and better-armed opponents. This overmatch has emboldened criminal organizations, leading to increased turf battles and clashes with law enforcement, leaving more businesses and bystanders caught in the crossfire. Ecuador illustrates this transformation most starkly.

ECUADOR CASE STUDY

A decade ago, Ecuador was considered a regional success story for its handling of gang crime. Between 2011 and 2017 its homicide rate fell from approximately 18 to 6 deaths per 100,000 people. But today, Ecuador is experiencing its most severe security crisis in its modern history, reporting a record homicide rate of approximately 50 per 100,000 people in 2025. Cocaine seizures have shattered previous records, reflecting Ecuador's transformation into a key transit and logistics hub for South American drug trafficking routes supplying the United States and Europe.

Since 2018, confrontations between criminal groups have led to a steady rise in violence. The uptick has been driven by the evolution of Ecuador's criminal groups from street gangs to sophisticated criminal networks with ties to international criminal organizations from Mexico. The nation's dominant criminal factions, Los Choneros and Los Lobos, have emerged as local proxies for the Sinaloa Cartel and the Jalisco New Generation Cartel (CJNG). In exchange for firearms and cash, the Ecuadorian gangs run local operations for the cartels by securing control of drug routes, protecting shipments, and punishing rivals. Ecuador's gangs do not just work for the Mexican cartels—they have begun to act like them.

Ecuador's criminal organizations have adopted Mexican cartel tactics, including the use of heavy weaponry, systematic extortion, contract killings, corruption of public officials, and public displays of extreme violence. They are also increasingly challenging the state itself. Judges, prosecutors, politicians, and journalists have become direct targets, mirroring the intimidation strategies used by Mexican cartels to erode state authority. The 2023 gang-ordered assassination of presidential candidate Fernando Villavicencio, days before the election, underscores how deeply organized crime has penetrated Ecuadorian political life.

INCREASED EXPOSURE TO THREATS

Figure 1

Sources: Global Guardian

THE BUKELE MODEL EXPLAINED & REGIONAL ADOPTION

STRATEGIC COMMUNICATION AND NARRATIVE CONTROL:

Use of social media platforms to sustain public support by showcasing mass arrests, prison transfers, and low homicide rates, while labeling critics as gang defenders.

NATIONAL POLICE AND MILITARY FORCE DEPLOYMENT:

Territorial control operations to dismantle gangs involving mass arrests, neighborhood sieges, road checkpoints, and raids.

MEGA-PRISON CONSTRUCTION:

In 2023, El Salvador opened the Terrorism Confinement Center (CECOT), a 40,000-capacity mega-prison for high-risk gang and terrorism suspects.

TERRORIST DESIGNATION/SECURITIZATION:

Designation of criminal groups as terrorist organizations, allowing government to justify prolonged emergency powers, mass detentions without due process, and facilities like CECOT under a terrorism legal framework.

MASS ARRESTS AND INCARCERATION:

Arrest of 94,000 individuals since 2022, pushing the prison population above 110,000 (~4% of male population).

STATE OF EMERGENCY:

Since March 2022, President Nayib Bukele has repeatedly extended a nationwide state of emergency, thereby, suspending due process, arbitrary arrest protections, and warrant requirements.

Figure 2

Sources: Global Guardian

THE SALVADORAN SOLUTION

Populations across Central and South America have become increasingly frustrated by the rising insecurity and the dominance of organized crime. In 2025, polls consistently showed crime and public security as the dominant concern, overshadowing longstanding regional problems like economic inflation, poor job prospects, and government corruption. Therefore, regional politicians and electorates alike see the political and public safety successes of El Salvador's President Nayib Bukele and view him as a model to be emulated.

Nayib Bukele was elected president on a promise to address insecurity. After gangs killed 62 people on 26 March 2022, he declared a 30-day state of emergency, suspending due-process rights and launching a sweeping crackdown with legislative approval. The emergency has since been extended 46 times, with security forces arresting suspects en masse and holding them in the CECOT mega-prison [figure 2].

Under Bukele, El Salvador's homicide rate fell from about 53.1 per 100,000 people in 2018 (the year before Bukele took office) to 1.9 per 100,000 in 2024, a decline of over 96%. Even his political opponents acknowledge that gangs no longer operate openly in El Salvador. President Bukele's security achievements have made him extraordinarily popular both at home and abroad. Over six years in office, his support has never fallen below 80%, a rare achievement in Latin America's volatile political landscape. A region-wide poll of Latin Americans found that Nayib Bukele was the highest rated leader. Latin Americans are clamoring for the implementation of the "Bukele Model" of public security.

Indeed, a key component of the right-wing sweep of the region's 2025 elections was insecurity at the forefront of Latin American voters' minds. In April 2025, Ecuador's Daniel Noboa won re-election by promising to answer rising criminal violence with Bukele-style militarized crackdowns and mega-prisons; in October 2025, Bolivia's Rodrigo Paz ended nearly two decades of MAS rule by tapping into intertwined economic and security frustrations; in November 2025, Honduras' Nasry Asfura narrowly won on pledges of stronger security measures and United States support; and in December 2025, Chile elected far-right José Antonio Kast, whose tough-on-crime stance resonated amid gang violence fears.

Not only have candidates run on Bukelismo—elected leaders have also started to implement elements of the Bukele security model [figure 2]. But the Bukele model is not universally transferable. The success of this security model will vary in each nation, depending on many factors, including the level of criminal capability and the existing state power.

In smaller states like El Salvador with relatively unsophisticated criminal threats, heavy-handed security campaigns have yielded results. Bukele's crackdown succeeded partly because Salvadoran gangs lacked the firepower, organization, and resources for sustained resistance. But in larger countries with more sophisticated and capable criminal groups, adopting the Bukele approach could exacerbate, rather than solve security issues raising the risks to business and travelers in the area.

RISKS OF THE BUKELE MODEL

Government crackdowns on crime groups in Latin America often carry the risk of retaliatory violence. When states deploy mass arrests, emergency powers, and militarized policing, criminal groups respond with targeted assassinations of police and prosecutors, prison riots coordinated from inside jails, car bombings, extortion surges, and attacks on symbolic or "soft" targets. Retaliation serves both as punishment and deterrence, signaling that state pressure will be met with disruption and fear.

Business Risks: Supply chains become vulnerable to roadblocks, arson, sabotage, and sudden "security taxes," while labor shortages emerge as workers avoid dangerous areas. Foreign companies may face higher kidnapping risk, reputational exposure, and rising insurance and security costs.

Travel Risks: Retaliatory violence is often indiscriminate in timing and location, occurring near police stations, transit hubs, shopping areas, or nightlife districts. Shootouts, explosive attacks, and gang roadblocks can trap civilians with little warning. As crackdowns escalate into cycles of action and reprisal, unpredictability increases, raising the likelihood that businesses and travelers become collateral victims in conflicts not directed at them, but unfolding around them.

> Criminal groups under pressure intensify extortion of transport firms, retailers, construction sites, and energy or mining operations to replace disrupted revenue streams.

Ecuador's adoption of Bukele-style tactics in 2025 coincided with its most violent year on record. But in no place is the risk of massive retaliatory violence greater than in Colombia.

A SECURITY "GRAY RHINO"

Abelardo de la Espriella, an admirer of Nayib Bukele, is currently second in the polls for Colombia's May 2026 presidential election in a race where security is the top voter concern. De la Espriella is campaigning on Bukele-style measures, including emergency decrees, mass arrests, zero-tolerance policing, and mega-prisons. If he wins, Colombia will test the Bukele model against a far more complex threat landscape. Even if center-right candidate, Palemo Valencia, is elected, some hardline security policies would be expected.

Colombia hosts Revolutionary Armed Forces of Colombia (FARC) dissidents, the National Liberation Army (ELN), and the Clan del Golfo, who are all well-resourced and heavily armed and have successfully resisted the state for decades. These groups do not hesitate to use acts of terror, often using explosives to target security forces, rivals, or civilians. An adoption of these policies risks overwhelming security forces already stretched across vast rural and border territories, provoking retaliatory drone bombings or territorial battles.

KEY TAKEAWAYS

Latin America's criminal landscape has undergone a structural transformation. Street gangs have matured into diversified, well-resourced organizations capable of outmatching state security forces and embedding themselves in legitimate economies—exposing businesses to extortion, supply chain disruption, and reputational risk. The region's most popular remedy, Bukelismo, may compound these dangers: Heavy-handed crackdowns that succeeded against El Salvador's unsophisticated gangs risk provoking retaliatory violence from more capable adversaries.

CRITICAL MINERALS AND RESOURCE NATIONALISM

INDUSTRY IMPACT: Materials, Industrials **RISK TYPES:** Activism, Political/Regulatory, Supply Chain, Unrest

Critical minerals are the building blocks of the 21st century economy. From the components of the green transition to the chips fueling the AI revolution, from consumer electronics to hypersonic missiles—critical minerals are ubiquitous in today's economy. As their name implies, critical minerals are also strategically essential. Yet, in an age defined by deglobalization and the weaponization of trade, access to these critical resources is limited, not only by their geographic distribution, but by a rising wave of resource nationalism.

RESOURCE NATIONALISM

Resource nationalism is not entirely novel. In the 1960s and 1970s, a sense of growing nationalism in the wake of colonial independence drove a wave of outright industrial nationalizations, the most famous of which related to oil and incurred extensive geopolitical ramifications. The contemporary wave of resource nationalism offers a broader range of options to resource rich countries seeking to exercise more control over their resources. At the less muscular end of the spectrum, countries seeking to benefit more from extractive industries can levy taxes. Countries including the Democratic Republic of Congo (DRC) and Zambia have instituted substantial levies on the mining industry to fund critical infrastructure projects.

More forcefully, countries can institute export controls or full export bans like the one Malaysia instituted on rare earth exports in 2023. Export bans are designed to increase the share of a commodity value chain located in the country where the raw resource is extracted by requiring companies to facilitate refinement and production as well as extraction. At the most heavy-handed end of the resource nationalism spectrum, countries can still resort to outright nationalization, as Mexico did for the country's lithium sector in February of 2023. But this response carries the risk of backlash. Mexico's cancellation of nine lithium mining concessions held by Chinese mining companies resulted in a lawsuit against Mexico in international court. There are now a range of options open to resource-rich nations, all with benefits and drawbacks.

THE INDONESIAN MODEL

Most countries engaging in resource nationalism have instituted some combination of measures from across the spectrum. Indonesia—the world's largest nickel producer—pioneered the implementation of a set of resource nationalist measures that have become a model for other resource rich

countries. Indonesia's turn toward resource nationalism began in 2009 with a law requiring greater state control over natural resources. In 2013, Indonesia mandated state ownership of 51% of foreign mining enterprises after 10 years of operation. In 2014, Jakarta fully banned the export of unprocessed nickel ore, which required foreign investors engaged in nickel extraction to dedicate funding to downstream smelting and refinement facilities. As a result, Indonesia is now the world's second largest producer of stainless steel, a production chain that involves a large amount of nickel, and the value of Indonesia's nickel exports has increased ten-fold from 2013 to 2022. Moving forward, Indonesia seeks to position itself as a competitive manufacturer of electric vehicles (EVs), another industry that relies heavily on nickel for battery components. This model—where a state increases ownership over a resource, places controls on its export, and develops increasingly valuable downstream industries—has been replicated by at least a dozen countries across Asia, Africa, and Latin America [figure 3].

NATIONAL RESOURCE DILEMMA

Despite Indonesia's success, resource nationalism is not without drawbacks. Countries endowed with vital resources must play a game of balance. Instituting low or no controls is likely to incur domestic backlash as impoverished populations see the country's resources extracted without feeling any of the benefits. This "hypo-nationalist" scenario is exemplified by protests that ultimately shut down a foreign-owned mining project in Panama. On the other hand, implementing stringent resource controls can similarly shutter valuable projects, as foreign companies with critical mining capacities are shown the door before domestic miners can replace them. This "hyper-nationalist" scenario is explored through Burundi, where a valuable rare-earths mine has yet to reopen following Burundi's nationalization of the sector.

CRITICAL MINERALS AND RESOURCE NATIONALISM

Figure 3

Sources: U.S. Geological Survey (USGS), International Energy Agency, Organization for Economic Co-operation and Development (OECD), Global Guardian

HYPO-NATIONALISM | PANAMA

Situation: The Cobre mine in Panama is one of the world's largest copper mines. The terms of the original 1997 contract gave the mine's foreign proprietors exemptions from environmental regulations, the right to effectively seize private property for critical infrastructure, and allowed them to charge Panama fees for its use. This arrangement was deeply unpopular with most Panamanians.

Result: In 2022, more than 150,000 Panamanians took to the streets to protest the mining contract. Protesters objected to the flat yearly payment of USD $375 million, amounting to only a third of the mine's gross revenue, as well as the mine's negative environmental and social impacts. In response to popular pressure, Panama's government was forced to shutter the mine in 2023 and put a moratorium on all new mining projects. Negotiations to reopen the mine are ongoing. At the time of its closing, the Cobre project constituted 5% of Panama's GDP and accounted for 75% of the country's exports. By failing to distribute the benefits of foreign extractive investment, Panama lost a least USD $1 billion in direct revenue and the development of a key national economic asset.

HYPER-NATIONALISM | BURUNDI

Situation: Burundi holds small, but high-grade rare earth deposits. Rainbow Rare Earths, a British company, began mining and processing rare earths at the Gakara mine in 2018, with the Burundi government holding a 10% stake. In 2021, Burundi was the world's 11th largest producer of rare earths at 200 tons a year. That year, Burundi's president Évariste Ndayishimiye suspended all foreign mining operations and created a national company with exclusive mining rights.

Result: In 2023, this full nationalization effort was walked back to allow for foreign mining under strict government oversight with a minimum 15% government stake that increases by 5% upon each contract renewal. But stringent government terms and a continued lack of transparency left foreign mining companies wary of reinvestment. Today, the Gakara mine remains effectively shuttered on caretaker status while Burundi and Rainbow Rare Earths continue to negotiate the possible resumption of operations. In October of 2025, Burundi made its first official export of minerals since the suspension of foreign operations. Officially, the country has produced no rare earths since 2021, representing tens of millions of dollars in lost revenue.

IMPLICATIONS FOR BUSINESS

UPSTREAM AND MIDSTREAM

The most direct implications for businesses primarily affect firms engaged in the actual extraction of critical minerals and strategic resources. In both the Panamanian and Burundian cases, a rapid change in the government's national resource policy resulted in mining companies prevented from mining. In addition to the revenue lost while their operations are suspended, these companies are also exposed to the costs of maintaining their mining sites as well as the cost of legal battles and negotiations.

In cases where production is not shut down, but continued operation requires investment in in-country processing—such as Indonesia and Malaysia—both extractive and processing firms are exposed to risks and costs. Extractive firms can no longer rely on their old supply chains which, for rare earths, mostly entailed shipping to Chinese processing enterprises. Processing firms either must relocate to the country of extraction or see their market share decline as competing processing industries are established nearer to the mines.

DOWNSTREAM

Firms that depend on reliable access to critical minerals in either their raw or refined states will also be subjected to the insecurity of international competition. The overwhelming majority of downstream enterprises will experience growing resource nationalism in the form of an uncomfortable choice: Increased risk or increased cost. Previously reliable supply chains will become more susceptible to disruption as resource rich countries turn increasingly to nationalist resource policies. Firms can guard against potential disruptions by diversifying their input sources, developing redundant supply chains, and stockpiling critical materials. However, all these measures impose costs. Diversified inputs reduce the benefits of economies of scale. Redundant supply chains entail some degree of overspending. And stockpiling requires increased overhead through storage and maintenance. Downstream enterprises are thus faced with two suboptimal options: Be exposed to potentially disastrous disruption or pay a premium to avoid the supply risk.

KEY TAKEAWAYS

Driven by soaring commodity prices, the global race for critical minerals and growing awareness of it are creating mounting pressure on resource-rich nations to capture greater value from their natural wealth. Mining firms now face increased operating and investment costs. In countries that still have favorable business environments, activist and protest risks are increasing. The rise of resource nationalism confronts manufacturers with a thrift or shift dilemma: Maintain efficient supply chains and just-in-time inventory for materials and face possible disruptions or diversify suppliers and shift from just-in-time to just-in-case inventory management at great cost.

GENERATION DISCONTENT

INDUSTRY IMPACT: Consumer Discretionary, Consumer Staples, Industrials, Materials

RISK TYPES: Activism, Unrest, Civil Conflict, Regime Instability

In 2025, youth-led protests toppled governments and stirred unrest across South Asia and Africa. Young people took their disillusionment to the streets in movements characterized by online mobilization, social discontent, and references to anime. This social media-savvy cohort—aggrieved by inequality, corruption, and poor governance—has taken inspiration and symbolism from one protest to the next with a momentum that will make the "Gen Z Protest" one of the defining trends of 2026.

The first Gen Z protests took place in Bangladesh in the summer of 2024 following the rollback of a jobs reform package. Young people mobilized across the capital of Dhaka and successfully ousted the government. The speed with which Bangladeshi youth toppled a seemingly entrenched government inspired emulation across the region in Indonesia, Mongolia, Malaysia, and nearby Nepal where the government was also overthrown. By the time of Nepal's revolution in September of 2025, the protests adopted the moniker of Gen Z protests. The movement then spread through South Asia to Timor-Leste, the Maldives, and across the Indian Ocean to Madagascar—where another government fell. By winter of 2025, images of young people toppling their governments had spread unrest to Latin America and the Balkan Peninsula with Gen Z protests in Paraguay, Mexico, and Bulgaria. Even other protest movements, such as the student-led protests in Serbia and the anti-government unrest in Georgia, adopted Gen Z language and symbolism, retroactively affiliating with the global wave.

DEFINING GEN Z PROTESTS

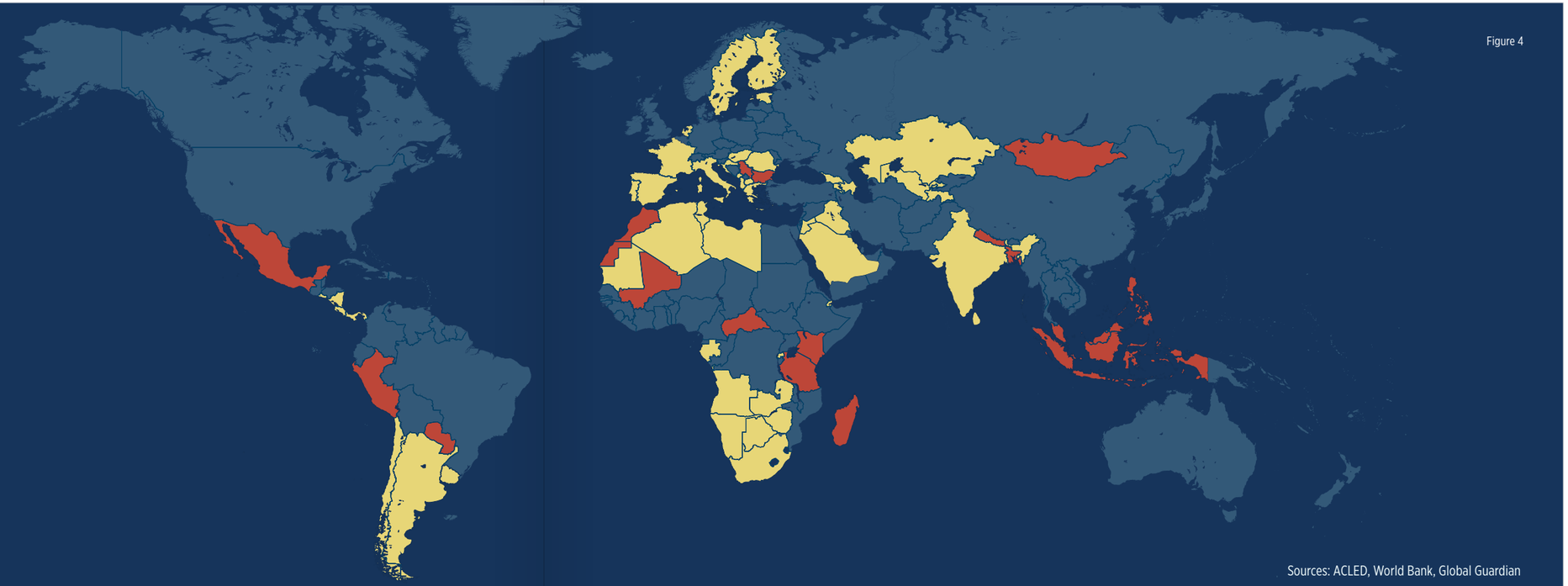
While most protests are youth-led, Gen Z protests are distinguished by a set of common factors. These movements share similar grievances and consciously self-identify—through memes—as belonging to a global protest movement. The core grievances are corruption, inequality, and the failure of essential government services. Gen Z protests are oriented around a perception that young people are being shut out of opportunities—mainly economic, but also political—either through corruption or through the mismanagement of a country's resources. The clearest indication that a protest is part of the Gen Z movement is that participants explicitly call themselves members of a Gen Z protest.

In Morocco, for example, the protest organizers labeled their movement "Gen Z 212" using the country telephone code 212 to denote their franchise status within a larger movement (reminiscent of the 2011 Occupy Wall Street movement). Another identifier is the use of common symbols, the most prevalent being the Straw Hat Jolly Roger from the popular anime One Piece. While the use of memes in civil unrest may not be new, the extent to which the Gen Z protest movement is defined by memes is. The use of the Straw Hat Jolly Roger simultaneously points to a common generational culture and is also a conscious invocation of one of the major themes of the show: Youth resistance to a tyrannical world government. Indeed, the novel extent to which the Gen Z movement is itself a meme is useful in tracking the trend and differentiating Gen Z protests from other youth-led unrest.

The central role played by memes and social media in the 2025 revolution in Nepal makes it the best conceptual illustration of the Gen Z protest. Nepal has a large youth population—21% are aged 15–24—and high youth unemployment also at around 21%. In Kathmandu, latent resentment against the nation's elite had been building for years. Social media focused this resentment on the opulent lifestyles of the children of these wealthy elites with netizens taking to TikTok and Facebook to criticize the ostentatious displays of wealth by "nepo babies." The Nepalese government then banned 26 major social media platforms on 04 September to defuse the situation. The ban ignited mass protest instead. Security forces killed 19 people, but the crackdown backfired. The government collapsed and several ministers fled the country as angry crowds ransacked government residences while waving pirate flags from One Piece.

GLOBAL GEN Z PROTESTS

Figure 4



THE NEXT GEN Z PROTESTS

The countries most likely to experience Gen Z protests in 2026 are clustered throughout the Global South. Going forward, Gen Z protests are most likely to materialize in regions with young populations, high rates of social media usage, and high youth unemployment. The following regions are at highest risk of expanding Gen Z unrest [figure 4].

SOUTHERN AFRICA:

South Africa, Botswana, Eswatini, Namibia, and Angola all exhibit many of the features necessary to facilitate a wave of youth-driven unrest. South Africa in particular has a high proportion of both young people relative to its general population (16%) and youth unemployment (60%). Along with persistent energy and corruption issues, these demographic features contribute to a social environment that could quickly turn an inciting event into a significant wave of unrest. From 2000 to the mid-2010s, South Africa's GDP per capita skyrocketed, and the country was hailed as an economic model for the continent. But within Gen Z's living memory, that growth has faded into stagnation, fueling discontent and resentment.

BALKANS:

The Balkans present the highest regional risks outside the Global South with Serbia, Bosnia and Herzegovina, North Macedonia, Albania, and Greece all exhibiting strong indicators of future Gen Z unrest. In fact, Serbia has been experiencing persistent youth-driven protests since late 2024 that exhibit all the characteristics of a Gen Z protest. The grievances of the Serbian anti-corruption movement included a lack of government transparency and education spending and were spurred by a fatal roof collapse in November 2024 that was perceived as a major government failure. Though the protests began prior to the development of the Gen Z protest label, young people in Serbia have since adopted the moniker and symbols, including the Straw Hat Jolly Roger, as part of their movement.

The risk of youth unrest in the Balkans is particularly acute given the regions history of violent ethno-nationalist confrontation. Faced with mass unrest, populist politicians could try to steer discontent into war rather than face a loss of power.

CENTRAL ASIA:

Central Asia, more than most regions, is increasingly defined by generational divides. The leaders that govern in Kazakhstan, Tajikistan, Turkmenistan, Kyrgyzstan, and Uzbekistan have been in power since the dissolution of the Soviet Union. This cohort of politicians were adults when their countries became independent. The populations of these countries, however, are largely made up of young adults born in the late 1990s and early 2000s with no memory of socialism. In some Central Asian countries, these young people have grown up with relatively liberal access to social media. Kazakhstan has already experienced several bouts of youth-led unrest and is prone to further outbreaks in the coming years. Possible triggers include price shocks and cultural resistance to a growing economic reliance on China.

INCREASED VOLATILITY

The risk of Gen Z driven unrest is not equally distributed across the world, nor is it equally distributed across the Global South. International firms a with assets, operations, and personnel need to take proactive measures to mitigate the rapid onset of unrest when Gen Z-driven protests occur in their reas of operation, including active Global Security Operations Center (GSOC) monitoring of local events and social media trends.

KEY TAKEAWAYS

Young people across the Global South, and in parts of the rest of the world, are increasingly exposed via social media to images of their contemporaries using protest to express their discontent, overturn unpopular policies, and in some cases, overthrow regimes. Social media, in addition to providing inspiration for Gen Z protest movements, is also facilitating their organization. Sharing symbolism from one protest to the next allows the movement to carry momentum internationally. In 2026, the regions most likely to experience Gen Z protests are Southern Africa, the Balkans, and Central Asia. The success and safety of firms will increasingly rely, in part, on being able to understand local youth culture, its references, and its modes of communication.

Threats in Brief

Threats in Brief is designed to surface fast-moving risks that may not yet appear on the radar of security planners but carry significant near-term implications for corporations and high-net worth individuals. Each entry distills complex threat dynamics into actionable intelligence, pairing key findings with practical implications that security professionals can incorporate directly into existing risk frameworks, duty of care programs, and advisory workflows.

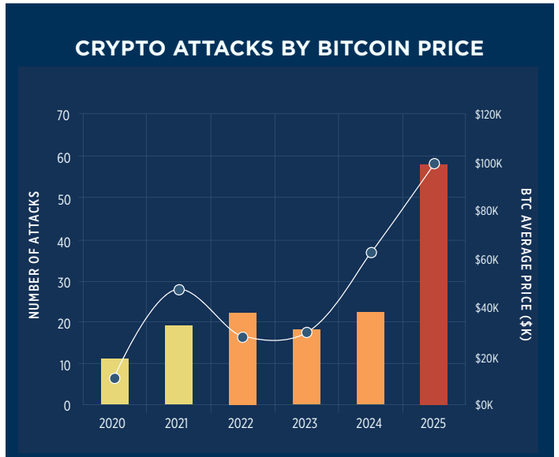
The topics in this section cover three distinct but thematically connected threats. The first examines the growing physical danger facing large cryptocurrency holders, driven by a statistically significant correlation between Bitcoin valuations and targeted violent crime. The second addresses the emergence of agentic AI as a force multiplier for malicious cyber actors—a capability that has already moved from concept to operational deployment within a six-month window. The third details North Korea's infiltration of Western companies through a coordinated fraudulent remote workforce, presenting layered risks spanning sanctions compliance, intellectual property theft, and insider threat. Together, these briefs reflect a broader pattern: digital assets, digital tools, and digital identities are increasingly generating real-world consequences that demand a physical and organizational security response.

DIGITAL WEALTH CREATES PHYSICAL RISK

INDUSTRY IMPACT: Financials **RISK TYPES:** Crime, Kidnap and Ransom

From home invasions and SIM-swap attacks to high-profile kidnappings, crypto holders are increasingly being targeted offline.

Bitcoin has undergone significant swings in price over the last five years, driven up first during the post-COVID boom where it went from less than USD $15,000/BTC in September 2020 to more than USD $60,000/BTC one year later. Bitcoin continued to rise, peaking at USD $125,000/BTC in August 2025. During those five years, attacks on crypto holders increased from 15 reported incidents in 2020 to 65 in 2025. The trend is clear—there is significant positive correlation between the price of Bitcoin and number of attacks on large crypto holders.



Sources: Chainalysis 2025 Mid-Year Report, Jameson Lopp's Physical Bitcoin Attacks Archive, Fortune, NBC News, Bloomberg

ANALYZING THE DATA REVEALS THREE KEY FINDINGS:

1. Strong positive correlation between BTC price and attacks.

2. Lag effect of 3–6 months—attacks spiking after price increases as criminals identify targets. This was most noticeable after BTC rose in fall 2024, resulting in a spike in attacks in January 2025.

3. While kidnap and ransom remain the primary attack method, home invasions are on the rise.

THE NEXT ATTACK WAVE

Crypto is no longer a retail, speculative asset class driven by supply dynamics. With institutions owning roughly 20% of holdings, it is increasingly being traded as a macro asset. In other words, it is tied to liquidity conditions, real yields (lagging inverse relationship with real interest rates) and de-dollarization. This means that the next major wave of attacks on holders will lag a few months behind sustained interest rate cuts.

IMPLICATIONS

1. Digital asset security is essential: Hardware wallets keep holdings offline and out of reach, while seed phrases must never be shared, digitized, or cloud-stored; metal backups and physical separation from devices are baseline requirements.

2. Online exposure enables targeting: Sharing wallet addresses, transaction wins, or crypto holdings on social media makes individuals identifiable, while phone-based authentication remains vulnerable to SIM swaps; authenticator apps, carrier locks, and minimal public footprint reduce risk.

3. Physical security must match digital security: Home surveillance, access controls, and professional assessments protect against home invasions, while travel demands operational discretion, and avoidance of predictable itineraries or unsecured networks.

4. Privacy is protection: LLCs, trusts, and custodial solutions obscure ownership and reduce exposure to bad actors.

5. Security is only as strong as its weakest link: family, staff, and partners require operations security (OPSEC) training and rehearsed duress scenarios.

KEY TAKEAWAYS

When Bitcoin reaches higher valuations, the economic incentives to violently target holders increase. Holders of significant amounts of Bitcoin or other cryptocurrencies should strongly consider increasing their security posture. This can include digital hygiene, camera surveillance, executive protection, secure transportation, and threat assessments.

AGENTIC ATTACKS

INDUSTRY IMPACT: Information Technology, Communication Services, Health Care, Financials, Utilities **RISK TYPES:** Cyber

Artificial Intelligence (AI) is now acting as a force multiplier for cyber threat actors in their attacks on corporations.

Advances in the sophistication and autonomy of cutting-edge AI models has enhanced their utility in executing cyberattacks. Large Language Models (LLMs) can now solve individual problems with greater reliability and creativity. Increased autonomy, or agency, has led to the proliferation of agentic models that can implement the very solutions they propose for problems. Agentic models also have unprecedented access to tools—such as web searching, coding environments, and data entry—that can be used to facilitate malicious actions. To this end, cybercriminals can now give an AI agent a target, and with minimal human feedback and direction, the agent can then conceive, orchestrate, and conduct attacks on its own.

This discovery was first reported by Anthropic. Since June 2025, Anthropic was aware that its Claude model was being prompted to write malicious code in what is known as "vibe hacking." In November 2025, however, Anthropic discovered an attack on multiple institutions where Claude didn't just write the code, it planned and conducted the attack with minimal direction from its users—a Chinese state-sponsored hacking group.

IMPLICATIONS

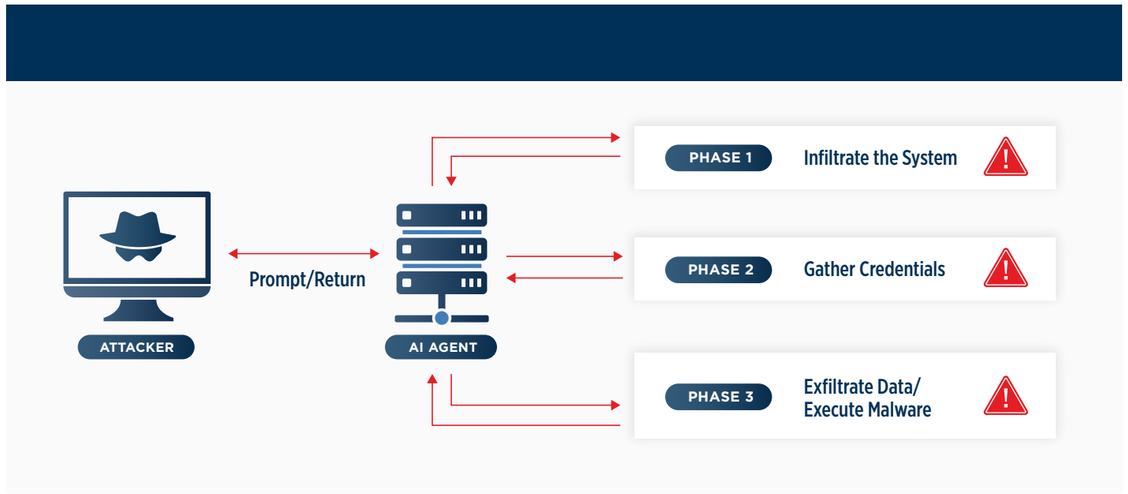
1. More threat vectors: Vibe hacking lowers the barriers to entry for cyber-attacks with coding expertise no longer serving as a prerequisite.

2. More efficient attacks: Individuals or organizations that leverage Agentic AI can direct and monitor cyber-attacks in less time and with less effort, freeing bandwidth for more attacks.

3. More sophisticated attacks: As AI models are increasingly employed to act as automated attackers, their access to specific training data and feedback on successful hacks will increase, and with it, their efficacy and sophistication.

KEY TAKEAWAYS

Just as AI is increasing workforce productivity through force multiplication, it is also increasing the productivity of bad actors through precisely the same means. It only took six months to go from the first record of vibe hacking using Claude to the first record of a Claude-conducted attack. While AI models are currently prone to hallucinations—incorrect or misleading AI-generated results—as the models improve, so too do the new tools for attack.



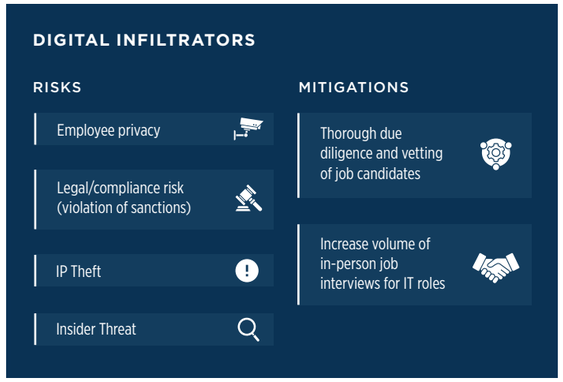
DIGITAL INFILTRATORS

INDUSTRY IMPACT: Energy, Information Technology **RISK TYPE:** Cyber, Political/Regulatory

North Korea is infiltrating Western companies with an army of remote workers to circumvent sanctions and steal sensitive information, including intellectual property and employee identities.

Pyongyang is being helped in this effort by American and European citizens, some of them unwitting, who run laptop farms and aid in the theft of identities for use by North Koreans posing as other nationalities. This operation presents both direct and indirect risks to firms that can persist even after North Korean employees are discovered. Firms that attempt to fire North Korean workers have had their intellectual property (IP) threatened, and companies that follow through on termination are often attacked with ransomware.

Under strict sanctions, the Democratic People's Republic of Korea (DPRK) became adept at acquiring foreign currency through creative means. Pyongyang has long used the manufacture and sale of illicit drugs and currency counterfeiting, but recently began taking advantage of the rise in remote employment to secure hundreds of millions of dollar- and euro-denominated salaries. Thousands of North Koreans work remotely—primarily as coders—for dedicated facilities often based in China, Russia, and Pakistan.



BANG FOR BUCK

The primary goal of this fraudulent remote work is to acquire foreign currency. As such, North Korean remote workers are concerned with maintaining gainful employment. But in addition to circumventing sanctions to gain hard currency, North Korean remote workers are directed to secure roles in sensitive industries such as energy, cybersecurity, artificial intelligence, and other dual use sectors. By acquiring useful technical capacity in and intellectual property from critical sectors, North Korea can advance its own civil and military industries, while also gaining the hard currency necessary to fund those projects. North Korea's "digital infiltrators" are an asset that provides its government with mutually reinforcing benefits.

Both the scale and the direction of the threat are significant. Amazon alone has stopped applications from more than 1,800 applicants suspected to be working from the DPRK since April of 2024. And corporations are not the only ones under threat. A recent U.S. Department of Justice (DOJ) action uncovered over 80 U.S. citizens whose identities had been used without their knowledge to help North Korean workers gain over 100 remote employment roles with firms across at least a dozen U.S. states. South Korean intelligence estimates that the headcount of North Korea's cyber corps that include its remote workforce increased by almost 25% between 2022 and 2024, indicating that this trend has yet to reach its zenith.

IMPLICATIONS

1. This discovery is the canary in the coal mine. While North Korea's state-directed operation is probably the most substantial, it is unlikely to be the only state-directed fraudulent remote work scheme.

2. Firms that fire North Korean staff are often threatened with the release of IP or attacked by North Korean hackers using ransomware.

3. Firms that pay North Korean individuals are violating the sanctions of their home country and could face civil or criminal penalties, including possible asset forfeiture.

4. The personnel at firms where North Korean workers have gained employment are susceptible to having their identities stolen and used in further fraudulent employment efforts.

KEY TAKEAWAYS

North Korean applicants are continuously attempting to gain employment at high-profile firms across North America and Europe under fraudulent pretenses. A failure to do sufficient due diligence could present significant compliance risks to firms as the fraudulent employees are using their salaries to fund illicit North Korean weapons programs. Aside from compliance, North Korean employees present risks to the security of firms' intellectual property and the identities of their employees.

OUTLOOK AND KEY TAKEAWAYS

2026 OUTLOOK

The information domain is especially contested as curated realities shape political narratives. In this environment—and amid worsening economic conditions—state and non-state actors alike are waging agitation campaigns designed to demoralize, polarize, and radicalize populations.

While Europe has accelerated military production and coordination, it faces a crossroads: It can either reform and become an actor capable of projecting force and defending its interests and risk alienating traditional allies—or fragment. In the Middle East, the terms upon which the Third Gulf War end will dictate the regional power structure. Meanwhile, a realignment is underway with Saudi Arabia, Turkey, Pakistan, and Qatar forming a counterbalance to the Abrahamic Bloc consisting of Israel and the United Arab Emirates (UAE). The already unstable Horn of Africa is set to become the focal point for competition between these new blocs.

In the Western Hemisphere that we dub "The Amerisphere," the United States government is laser-focused on fighting narco-crime, controlling immigration, and limiting Chinese, Russian, and Iranian influence, as demonstrated by the capture of Venezuelan President Maduro in a "regime alteration" operation. While it is still unclear how Venezuela's acting president, Delcy Rodriguez will govern, what is clear is that Cuba is next in line to face economic, and possibly military, coercion.

THE YOUTH ARE NOT ALRIGHT

In the last 18 months, youth-led protests have toppled governments in Bangladesh, Nepal, and Madagascar, while stirring unrest across South Asia and Africa. Social media helped facilitate organization and spillover from country to country. This phenomenon is not confined to the Global South. Multiple concurrent studies show that satisfaction and happiness in young adults in the anglosphere are in major decline. This is translating into youth holding more extreme views. For example, while only 11% of Americans view political violence as justified, 19% of respondents aged 18-29 said that it could be.

While the specific grievances differ, there is a generational gap where youth across the globe believe that they have less social mobility than previous generations and have identified people to blame for it. In much of the Western world, youth politics resembles a horseshoe whereby the right and left fringes mirror each other. This dynamic is most acutely apparent in the swelling of antisemitism. More broadly, it is reflected in the same anti-elite sentiment that led to the murder of the UnitedHealthcare CEO in late 2024. With transformative technologies set to further disrupt economies, disaffected youth could usher in an era of extremism in the Western world and topple more governments across the Global South.

NOVEL TECHNOLOGICAL THREATS

Artificial intelligence crossed a threshold in 2025—from theoretical risk to operational threat across economic, political, and security domains. AI-driven automation eliminated an estimated 50,000–180,000 jobs in the U.S. alone, concentrated in tech, finance, logistics, consulting, and media—displacement that fuels the economic anxiety already driving political polarization. That polarization is itself a target: Deepfakes scaled to industrial deployment, with over 2,000 incidents recorded in Q3 2025 alone and 482 explicitly political fabrications designed to suppress turnout, simulate confessions, or reverse candidates' stated positions. In the financial sector, artificial executive announcements enabled stock manipulation and real-time wire fraud. North Korean operatives exploited AI-generated personas to infiltrate Western firms, then leveraged access for espionage, malware deployment, and extortion upon discovery. Meanwhile, the barrier to cybercrime collapsed: 2025 saw both the first LLM-prompted malware and the first autonomous AI-conducted cyberattack. AI is no longer a future concern—it is an active, compounding threat that simultaneously displaces workers, degrades democratic discourse, and enables fraud and infiltration at scale.

TRANS-ATLANTIC TURBULENCE

The United States and Europe are drifting apart—not toward rupture, but toward parallel systems operating under incompatible assumptions. Europe, along with Canada, continues to function within the liberal hegemonic paradigm that defined the post–Cold War order: Multilateral institutions, extensive regulation, consensus seeking, and values-based partnerships. Washington has moved on. The current U.S. administration prioritizes transactional return-on-investment over alliance maintenance, nationalism and bilateralism over multilateralism and supranationalism, and speed over consensus. The row over Greenland crystallized the divergence, but tariffs, defense burden-sharing, and tech sovereignty underlie it.

Europe (and Canada) is responding by de-risking its American dependence. Military spending is accelerating, with particular focus on replacing systems where reliance on U.S. suppliers is greatest—including cyber and defense technology. France has migrated government communications from Zoom and Teams to the domestic platform Visio. The European Union's 2026 Roadmap outlines a "Buy European" joint procurement strategy aimed at reducing the continent's 50% dependence on American arms. Meanwhile, "Sell America"—a market-driven capital flight from U.S. financial assets—reflects private-sector de-risking rather than coordinated policy. None of this portends a NATO rupture; the alliance remains intact, and American support for Ukraine continues. But the trajectory is unmistakable.

Washington has also turned toward a different set of Atlantic partners: the Gulf states. The appeal is transactional. Gulf states offer what the AI revolution requires—energy and capital—without the regulatory constraints that complicate deals in Europe. The emerging framework prioritizes equal footing, high-stakes agreements, and fewer conditions, a model that resonates with Gulf leaders and aligns with an administration that views partnerships through the lens of returns. For businesses navigating the transatlantic space, the implication is clear: the assumption of U.S.-European alignment that underwrote decades of commercial strategy can no longer be taken for granted.

ABOUT GLOBAL GUARDIAN

Global Guardian protects and delivers employees and families from political, environmental, and bad actor threats around the world.

Our team of experienced subject matter experts build tailored security programs to mitigate risk and provide real outcomes to a range of threats at home and abroad — all at the push of a button. Clients benefit from:

- **OUTCOME-ORIENTED TEAM**

  From travel emergencies to the most challenging crisis environments, client safety and security is our top priority. Our team will problem solve until a positive outcome is achieved.

- **OPERATIONAL EXCELLENCE**

  With a team comprised of highly experienced former military, special operations, and federal law enforcement personnel, our operational execution is unmatched.

- **HYPER-RESPONSIVE SUPPORT**

  With 24/7/365 Global Security Operations Centers and local response teams in over 140 countries, Global Guardian moves in minutes and hours instead of days and weeks.

- **BREADTH OF GLOBAL SERVICES**

  We offer a full range of customizable global security and medical services over 98% of the world, including travel risk management, executive protection, medical assistance and evacuation, cyber security, and video surveillance.

Learn how Global Guardian can support your business and employees.

INQUIRE HERE

Global Guardian
8280 Greensboro Dr. Suite 750
McLean, VA 22102, United States

Global Guardian London
99 Bishopsgate
London EC2M 3XD, United Kingdom

Global Guardian Asset Security
2127 Ayrsley Town Blvd. Suite 201
Charlotte, NC 28273, United States

+1.703.566.9463
info@globalguardian.com
globalguardian.com