GLOBAL
GUARDIAN

WORLDWIDE THREAT ASSESSMENT

MARCH 2025

GLOBALGUARDIAN.COM 703.566.9463 INFO@GLOBALGUARDIAN.COM

TABLE OF CONTENTS

> "International business is used to a privileged 'spectator' role in geopolitics. That neutrality is now over, and firms need to adjust to the fact that they are players on the field."

Dale Buckner,
CEO and President, Global Guardian

The post-World War II period is officially over. This new reality comes amid global economic stagnation, rising inflation, uneven post-COVID recovery, and geopolitical shocks, including the Russia-Ukraine war. Trade disruptions, supply chain challenges, and mounting debt burdens in developing nations have fueled domestic instability, intensified competition for resources, and driven a shift toward protectionist policies. As debt-servicing costs mount, geopolitical influence is increasingly tied to financial resilience. Economically stable nations are leveraging their strength to expand their reach, while weaker economies face heightened vulnerability to both internal unrest and external pressures. In this increasingly fluid international environment, corporations face elevated physical, social, and cyber risks from state, non-state, and individual actors. Global Guardian's intelligence analysts assess that the next half-decade will fundamentally alter how international business is conducted. In a multipolar era with expanding geostrategic tensions, global issues—intensifying geopolitical competition, economic distress, climate change, and transnational crime—will exacerbate local risks and vice versa.

Global Guardian's 2025 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 impacts on safety and security. To this end, the 2025 Threat Assessment delves into the issues of state-backed threats to firms in the Western world, the novel threat posed by commercial drones, new business risks in the United States' regional sphere that we dub "the Amerisphere," and the Middle East's current inflection point and the associated risks. It is our hope that this document provides thought-provoking insights that promote action to protect investments, assets, and, most importantly, the safety and well-being of your colleagues and family members.

All graphics and figures contained in this report were produced by Global Guardian unless otherwise noted.

COLLATERAL DAMAGE:
IRREGULAR WARFARE & THE PRIVATE SECTOR

An irregular warfare campaign is being waged against Western societies and the corporate sector is lagging in countering this pressing threat. Adversarial nation-states have dramatically increased their efforts to harm Western firms in the aftermath of Russia's 2022 invasion of Ukraine. To mitigate the short-to-medium-term physical, logistical, cyber, and financial risks, the business community must take proactive steps now.

> "China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if or when China decides the time has come to strike."
>
>
>
> **Christopher Wray,**
> **Former Director, Federal Bureau of Investigation**

On 31 January 2024, FBI Director Christopher Wray warned congress that Chinese hackers are penetrating United States (U.S.) cyber systems in preparation for possible attacks on critical infrastructure. In a similar reckoning, six U.S. intelligence agencies—including the National Counterintelligence and Security Center (NCSC), the FBI, the Defense Counterintelligence and Security Agency, and U.S. Army Counterintelligence Command—issued a warning to the defense industrial base (DIB) on 21 November 2024 regarding Russian sabotage operations.

SCOPE OF THE THREAT

Russia, China, and Iran engage in a whole of society approach to war against all of Western societies, including the private sector. The Russians call this overarching theory of conflict "New Generation Warfare," the Chinese call it "Unrestricted Warfare," and generally in the West, it is called "Hybrid Warfare." According to the European Centre of Excellence for Countering Hybrid Threats, hybrid warfare consists of "coordinated and synchronized actions that deliberately aim at systemic vulnerabilities of democratic states and institutions" via a combination of political, economic, military, civil, and information tools. In irregular warfare, opacity is a feature, not a bug. Here, traditional dichotomies of war/peace, friend/enemy, state/non-state, and covert/overt are blurred by design. While irregular warfare is less violent than traditional war, in many ways, the irregular warfare campaign being waged against the West is transforming the homefront into the front line.

While everyone is threatened by irregular warfare, the risks are not distributed equally across the private sector. The defense industrial base, defense contractors, and their subcontractors—which in the U.S. alone consists of over 100,000 companies—face the most acute threat; however, the technology, manufacturing, chemicals, transportation, extractive, energy, utilities, logistics, and agriculture sectors also face growing direct threats. Indirectly, the entire business community is liable to—unknowingly—become collateral damage in a conflict to which they are not a party [figure 1].

THE THREE ARENAS OF MALIGN STATE ACTIVITY

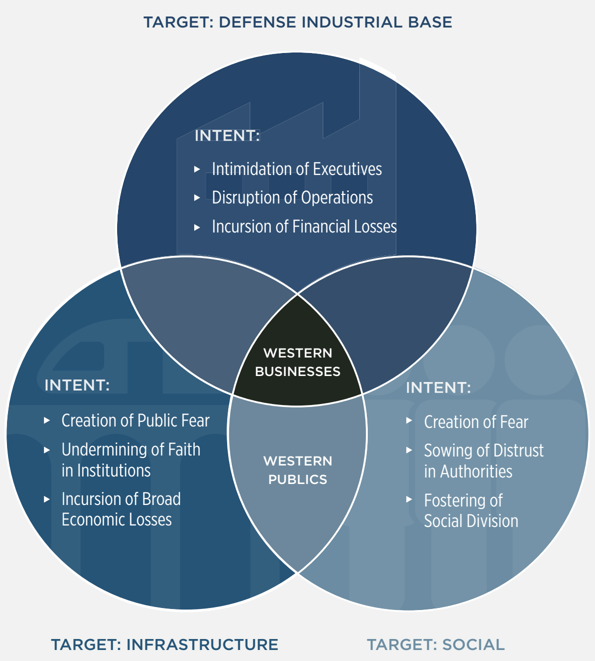

TARGET: DEFENSE INDUSTRIAL BASE
INTENT:
Intimidation of Executives
Disruption of Operations
Incursion of Financial Losses
WESTERN BUSINESSES
INTENT:
Creation of Public Fear
Undermining of Faith in Institutions
Incursion of Broad Economic Losses
WESTERN PUBLICS
INTENT:
Creation of Fear
Sowing of Distrust in Authorities
Fostering of Social Division
TARGET: INFRASTRUCTURE
TARGET: SOCIAL

Figure 1

ESCALATING TEMPO

In the last year alone, Russia is believed to be responsible for up to 100 "suspicious incidents" in Europe. These attacks have varied dramatically in their levels of sophistication and the scope of their impact. Malign states' recent escalations have included arson, assassination, attacks on critical infrastructure, ransomware, and cyber infiltration.

ARSON: In terms of return on investment, attribution difficulty, and ease of success, arson attacks have been the most expedient method for malign state actors to advance their irregular warfare on the nations of the West. For Russia, the Western DIB has been a prime target with a string of highly conspicuous fires at arms production facilities in the United Kingdom (UK), Germany, Poland, Bulgaria, and the United States [figure 2].

Russian agents have been leveraging Telegram and other platforms to recruit —sometimes unwitting—individuals to conduct acts of sabotage and terror. Suspicious fires at businesses unrelated to the Ukrainian war effort, including a local business in London, UK, an Ikea (Vilnius, Lithuania), a shopping center in Warsaw, Poland, a disrupted plot targeting a home improvement store in Paris, France, and fires at Novo Nordisk offices and production plants in Denmark. These attacks on the public are designed to instill enough fear to soften their respective government's stances on Russia.

ASSASSINATION: In early 2024, German police uncovered a Russian plot to kill Armin Papperger, the CEO of Rheinmetall, a major German industrial that manufacturers arms and automotive parts. This was only the most mature plot reported in a series of plans to eliminate other CEOs involved in the Western defense industrial base. Authorities have not publicly revealed the targets of Russia's other assassination plots, but firms directly involved in Ukraine's defense, especially those with production, sit atop Russia's list of targets.

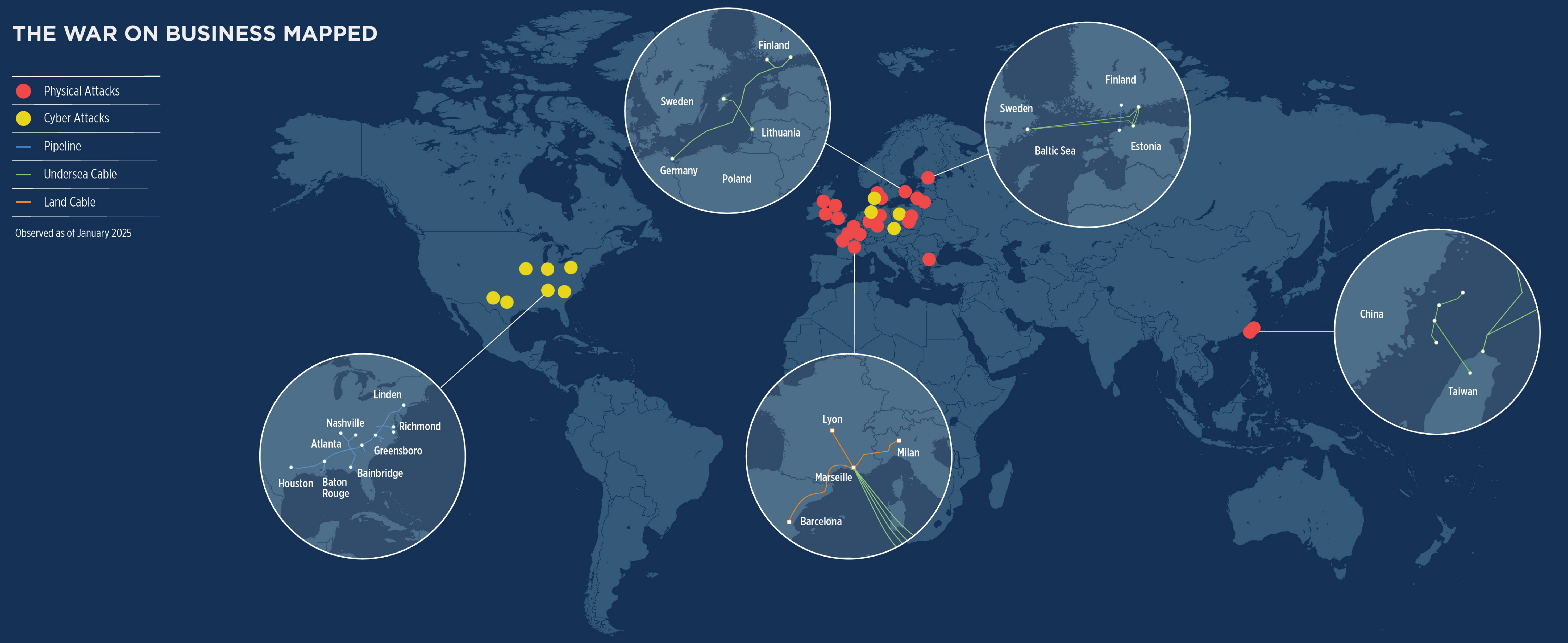
RANSOMWARE: In June 2024, Russian advanced persistent threat (APT) hacktivist group Qilin conducted a major attack on the UK's National Healthcare Service (NHS). Qilin attacked Synnovis, a pathology testing provider, affecting at least seven hospitals and dozens of general practitioners across South London. The encryption of patient test data disrupted organ transplants and blood transfusions, amongst other critical care operations. In this case, the attackers demanded USD $50 million, and when the deadline for payment expired, they subsequently published 400GB of stolen data. Hospitals are frequently targeted for ransomware attacks as access to patient data creates a life-and-death urgency for ransom payments. But hospitals are not the sole target of ransomware attacks; the 2019 Colonial Pipeline hack severely impacted American consumers and airlines along the East Coast [figure 2]. The Cyber Threat Intelligence Integration Center (CTIIC) assesses that in 2024 there were 5,289 ransomware attacks globally.

INFRASTRUCTURE ATTACKS: In July 2024, France faced a series of sophisticated sabotage attacks targeting critical infrastructure during the Paris Olympics, severely disrupting rail travel on the opening day [figure 2]. The infrastructure damaged during the 2024 Paris Olympics was far from the only suspected sabotage on land and at sea in the last 48 months. Malicious actors using a mix of both physical and cyber sabotage have temporarily shuttered rail networks in Czechia (April 2023), Denmark (October 2023), Lithuania (June 2022), Germany (October 2022 and October 2024), Poland (August 2023), and Israel (September 2023).

Undersea telecommunication cables have been dredged in the Baltic Sea on two occasions (October 2023 and November 2024) and twice in Taiwan's waters (April 2023 and January 2025); an electricity cable connecting the Swedish and Estonian grids and a Baltic gas pipeline were also damaged in November and December 2024 respectively. While information cable systems often have redundancies (pipelines do not), simultaneous and well-executed attacks on these vital conduits could severely limit internet speeds or even disconnect entire regions from the internet for an extended period.

Figure 2

THE WAR ON BUSINESS MAPPED



UNITED STATES

Eastern U.S. | May 2019
Russia-affiliated hackers conduct ransomware attack on Colonial Pipeline

Texas, Illinois, Gerogia, South Carolina, West Virginia, Pennsylvania | Nov 2023
Iran-affiliated hackers access programmable logic controllers in water and wastewater systems

Texas & Indiana | Jan 2024
Russian-affilated hackers manipulate control systems within five water and wastewater systems and two dairies

UNITED KINGDOM

London | Apr 2024
Fire at Ukrainian-linked business

Wales | Apr 2024
Fire at BAE Systems munitions facility

Birmingham | Jul 2024
DHL warehouse Fire

Barrow-in-Furness | Oct 2024
Major fire at BAE Systems shipyard

CZECHIA

Nationwide | Apr 2023
Russia-affilated hackers disrupt signaling systems and networks of the Czech national railway operator

POLAND

Nationwide | Aug 2023
Russian-affliated actors halt more than 20 trains across Poland

Warsaw | May 2024
Fire destroys Warsaw's largest mall

Skarzysko-Kamienna | Aug 2023
Fire at Mesko arms plant

BULGARIA

Karnobat | July 2023
Major fire at EMKO (arms company) wearhouse

FRANCE

Croisilles, Courtalain, Metz | Jul 2024
Electrical cables and train signal boxes destroyed on three SNCF rail lines hours before the 2024 Olympics

Paris & Southern France | Jul 2024
Fiber optic cables damaged in six locations disrupting SFR, Free, and Alphalink fixed-line and mobile users

TAIWAN

Connecting Matsu Islands & Taiwan | Feb 2023
TPKM3 undersea cable damaged by China-affiliated ship

Connecting Taiwan & Northeast Asia | Jan 2025
Trans-Pacific Express damaged by China-affiliated ship

DENMARK

Bagsvaerd & Copenhagen | May 2023
Fires at two Novo Nordisk sites

Copenhagen | Jun 2024
Fire at Novo Nordisk building

Nationwide | Oct 2023
Russia-affiliated hackers shut down Danish State Railways' (DSB) network

LITHUANIA

Vilnus | May 2024
Fire at IKEA warehouse

Vilnus | Nov 2024
DHL cargo plane crashes under suspicious circumstances

BALTIC SEA

Connecting Finland, Estonia, Sweden Oct 2024
Baltic Sea Submarine Cable, Finland-Estonia Connection Cable & Baltic-Connector gas pipeline damaged

Connecting Finland & Germany, Connecting Sweden & Lithuania | Nov 2024
C-Lion1 & BCS East-West Interlink undersea communications cables damaged

Connecting Finland & Estonia | Dec 2024
Estlink-2 electricity cable is damaged by a Russia-affiliated ship

GERMANY

Berlin | Jun 2024
Fire at Diehl Metall factory

Düsseldorf | Jul 2024
Russian plot to assassinate Rheinmetall CEO foiled

Leipzig | Jul 2024
Fire at DHL warehouse

Lower Saxony, Bremen, Hamburg and Schleswig-Holstein | Oct 2024
Communication cables cut in two locations, halting rail traffic across northern Germany

THE "TYPHOON HACKS"

China's recent state-sponsored Volt Typhoon and Salt Typhoon hacks—unmatched in scale—have changed the digital threats paradigm. The scope of these ongoing attacks is still unknown, and many victims have yet to be notified.

VOLT TYPHOON: Publicly identified by Microsoft in May 2023, Volt Typhoon's infiltration compromised thousands of devices worldwide, primarily targeting critical infrastructure within the communications, transportation, water, and energy sectors on the U.S. West Coast and in Guam. The Volt Typhoon hack exploited weak admin passwords, factory default logins, and unpatched vulnerabilities to compromise thousands of devices and establish botnets for future attacks. According to former National Security Advisor Jake Sullivan, the hackers were able to "...shut down dozens of U.S. ports, power grids, and other infrastructure targets at will."

SALT TYPHOON: Reported in September 2024, Salt Typhoon compromised the American telecommunications network in the most sophisticated known cyberattack in history. The group infiltrated nine U.S. telecommunications companies, gaining access to real-time communications and compromising the backdoors ("wiretaps") that telephone companies provide to law enforcement. Hackers were even able to tap the phones of top U.S. political figures, including now-President Trump. Salt Typhoon allowed Chinese officials to obtain vast records (mainly in the Washington D.C. area) detailing where, when, and with whom specific individuals communicated. In some cases, the hackers accessed the contents of phone calls and text messages. The full scope of this likely ongoing hack is still unknown.

> "According to former National Security Advisor, Jake Sullivan, the [Chinese] hackers were able to '...shut down dozens of U.S. ports, power grids, and other infrastructure targets at will.'"

Until the revelation of the extent of the Typhoon breaches, China's *modus operandi* for its cyber campaign against the West mainly promoted its economic and commercial interests. But taken together, these attacks suggest that Beijing is laying the digital groundwork for a potential invasion of Taiwan. The hackers' prepositioning and intelligence collection appear poised to prevent the U.S. from quickly projecting power eastward and creating chaos domestically to slow a military response to a possible Chinese invasion.

FUTURE THREATS

With the Axis of Disorder—comprised of Russia, China, Iran, and North Korea—digging in, there are no signs that their irregular war on the West will abate, *ceteris paribus*. Indeed, it is set to intensify. There are several "gray rhinos"—threats that we see now but ignore—on the horizon: parcel bombings, "astroturfing," automobile hacks, environmental terrorism, and blockshipping.

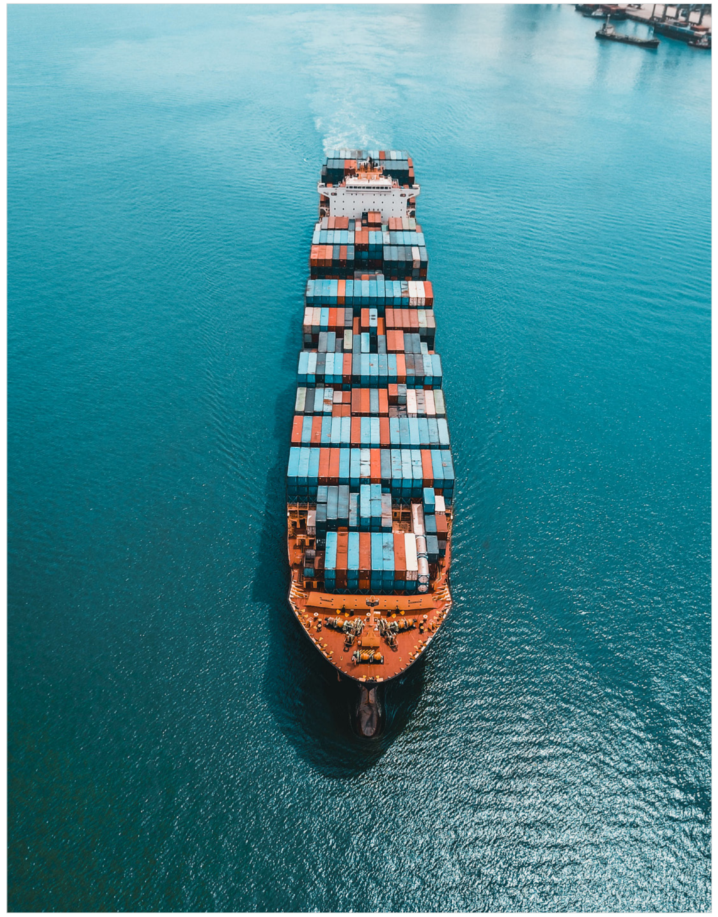
PARCEL BOMBINGS: A possible future state-sponsored threat vector is a new adaption to an old tactic: parcel bombing. On 15 January 2024, Polish Prime Minister Donald Tusk accused Russia of plotting terror attacks involving aircraft, citing recent incidents involving mailing parcels with incendiary devices. On 11 July 2023, a package ignited at a DHL facility in Leipzig, Germany and sparked a fire, with similar and concurrent incidents at DHL warehouses in Birmingham, UK, and Jablonow, Poland [figure 2]. A fourth event in November 2024 resulted in a DHL plane crashing in Vilnius, Lithuania. Polish prosecutors apprehended individuals allegedly linked to an international sabotage group sending explosive parcels to Europe with plans to target the U.S. and Canada, a claim corroborated by U.S. intelligence which has intercepted communications from Russian military intelligence discussing these plots. As Russia's war on the West persists, the threat of parcel bombs will continue, posing direct risks to logistics firms and second-order risks of increased insurance and security premiums, as well as shipping delays.

"ASTROTURFING" EXECUTIVES: Future threats against the lives of prominent individuals and executives can also be expected through novel means. Astroturfing is the practice of artificially creating the impression of a grassroots movement through paid "activists," bots, and trolls. Russian intelligence frequently uses astroturfing to exacerbate its adversaries' existing political and social divisions. Hostile state actors could easily redirect astroturfing campaigns to incite violence via third parties against specific targets, including companies and their executives. The popular support for the alleged perpetrator of the December 2024 assassination of UnitedHealthcare (UHC) CEO Brian Thompson demonstrated a public appetite for violence. State actors could exploit this environment of discontent to incite violence, both against specific individuals, and to generally corrode the social fabric.

COMPROMISED CARS: Modern vehicles collect and share immense sensitive data on their users, opening new channels for sabotage and cybercrime. Real-time access to a vehicle's data stream is particularly troubling when considered alongside the digitization of critical vehicle functions. A car infected with ransomware could force its owner to pay to unlock it or access the brakes. Ford has already patented self-repossession technology for its vehicles, presaging the possibility that hackers repossess a company's fleet of delivery vehicles—or a hospital's fleet of electric ambulances—until payment. Worse, a state actor or non-state actor could facilitate terror attacks, remotely turning cars into ramming weapons, causing hundreds of simultaneous lithium fires, or overloading the draw on EV charging stations, potentially crashing the grid.

NOT-SO-WILDFIRES: In dry and windy regions, including parts of California, Australia, the Mediterranean basin, and others, high fire risk conditions are open knowledge. Hostile state actors may use local governments' fire safety warnings to efficaciously instruct local surrogates (criminal organizations or lone individuals) to start fires. Indeed, between 85% and 90% of all wildfires are anthropogenic, with a highly conservative estimate of 10% to 15% proven as arson. Further, copycat arsonists emerge during nearly every major wildfire, serving as force multipliers. Preliminary estimates of the total damage and economic loss from the early 2025 Los Angeles-area fires are between USD $250 billion and USD $275 billion. With rising temperatures, longer fire seasons, and harsher droughts, the conditions for intentionally set fires are improving.

BLOCKSHIPPING: The use of "blockships" is an age-old naval warfare method whereby a ship is sunk in a narrow waterway to impede the movement of an adversary. In the last decade, ships have blocked off three narrow strategic maritime corridors. In 2014, Russia trapped Ukraine's naval fleet by sinking two ships. In 2021, extreme weather conditions contributed to the accidental grounding of the *Ever Given*, obstructing all Suez Canal traffic for six days. In another incident, the cargo ship *Dali* struck one of the Baltimore Francis Scott Key Bridge piers in March 2024, collapsing the bridge. Having observed several recent proofs of concept, hostile state actors may leverage blockships via sabotage or hijacking to disrupt vital maritime arteries in the West. The economic implications of a vital waterway obstruction would be untold. Since ship clearing is challenging and time-intensive, a blockship incident could take weeks to remedy.



TIME TO STEP UP

In an increasingly interconnected world where the distinction between war and peace has all but disappeared, it is imperative for decision-makers to recognize that business is downstream of geopolitics. While the risks from hostile state actors exist on a continuum, exceedingly few businesses are immune from the irregular war currently being waged on the private sector. Certain risks, including those from supply chains and infrastructure, may not be mitigatable internally; however, there are steps all organizations can take to help insulate themselves from malicious state actors and their affiliates.

Following the Salt Typhoon campaign, it should now be assumed that all non-encrypted telecommunications are insecure. The FBI and CISA's new cybersecurity guidelines advise the public to adopt end-to-end encryption for communications. Similarly, it is now recommended that app-based multi-factor authentication methods be used solely. Across the Western world, tense political landscapes are producing environments where boycotts and protests of private companies occur frequently and escalate quickly. In light of the levels of sympathy expressed for the alleged killer of UHC CEO Brian Thompson and the framing of the alleged murder as part of a class war, the threat of similar violence directed at business leaders is real.

Figure 3

PHYSICAL THREATS	CYBER THREATS
AUDIT	**AUDIT**
Conduct a Physical Security Risk Assessment on both sites and executives	Conduct a Cybersecurity Risk Assessment
ADJUST	**ADJUST**
Conduct 24/7 social media threat detection and monitoring Install independent security camera systems with 24/7 GSOC monitoring Establish robust executive protection program Enforce robust access control measures	Conduct 24/7 cyber threat detection and monitoring Reduce exposure to the public-facing internet Enforce user access controls and multifactor authentication for remote access Install independent cybersecurity systems Back up Industrial Control Systems (ICS) regularly
PREPARE	**PREPARE**
Develop and exercise security incident response plans	Develop and exercise cybersecurity incident and recovery plans Conduct regular cybersecurity awareness training

Integrate cyber and physical incident response, mitigation, and recovery plans

AUDIT

Following a dramatic change in the corporate security landscape, reassessing your firm's position within the new paradigm is paramount—self or third-party assessment is key. The following are good questions to begin:

- Are there physical security gaps that may make a location more vulnerable to arson, sabotage, or other violent acts?
- How difficult is it to ascertain the whereabouts of your executive team?
- Is your company in the public eye, and is there public ire (real or manufactured) directed at your firm?
- How secure are your internet and telecommunication systems (hardware and software)?
- Are there systems in place to monitor for inside threats?
- Do any of your systems run on hardware from companies the U.S. government is investigating, including Huawei, ZTE, Baicells, and TP-Link?

ADJUST

Once vulnerabilities are identified, prioritization and prompt action are required. There is no one-size-fits-all solution. But generally, most firms can enhance physical and digital access control. Companies in the public spotlight need to be extra vigilant in detecting and monitoring social discourse to identify when to heighten the security posture of an executive or a location. Firms with remote work policies also must enforce robust multi-factor authentication to prevent employee residences from becoming staging grounds for cyberattacks. In the manufacturing and industrial space, industrial control systems (ICS) must be updated and backed up regularly [figure 3].

Making these adjustments is a serious undertaking involving capital expenditure, though efficiencies can be found through integration, specifically by adopting an in-house or remote global security operations center (GSOC) to tackle physical and digital threats.

PREPARE

If one fails to prepare, one prepares to fail. People are always the weakest link in any defense. User error, emotional reasoning, and buckling under pressure are all things to be expected. However, human nature—a natural liability—can be turned into an asset by reducing uncertainty through repetition and awareness. Complex and distributed threats require a layered and distributed defense, and every employee can help fortify their team by being more mindful and less robotic.

Consider running table-top exercises to test your firm's response to various scenarios such as unauthorized intrusions (to networks, offices, server rooms, manufacturing sites, and other critical areas), arson, workplace violence, and doxxing of executives. Learn from these exercises and implement needed changes based on your team's unique findings.

KEY TAKEAWAYS

Today, wars are no longer confined to battlefields. China, Russia, and Iran employ an irregular warfare doctrine that places Western societies as a whole in their crosshairs. While the defense industrial base is a primary target, arson, sabotage, information warfare, attacks on transportation and infrastructure, and cyber intrusion all have the potential to adversely impact businesses, regardless of size or sector.

UNMANNED AERIAL SYSTEMS:
CORPORATE ESPIONAGE TAKES NEW HEIGHTS

The expanding use of drones in corporate espionage is materializing as a major threat to companies in 2025 and beyond. Organizations are highly vulnerable to drone-assisted espionage as drone countermeasures continue to lag novel implementations of unmanned aerial systems (UAS). To prevent both state and non-state actors from compromising decision-making, assets, and intellectual property (IP), companies must implement counterintelligence and detection measures while carefully navigating the compliance risk of an anachronistic regulatory space.

Inexpensive drones that are easy to replace and hard to stop are redefining the modern battlefield. In combat, they are widely employed both for intelligence and as guided munitions, showing impressive results. However, the ubiquity of drones extends far beyond the military realm. UAS are increasingly appearing in a myriad of commercial sectors and in places that they are not supposed to. Last year in the United States (U.S.), there were nearly 1.2 million unauthorized UAS violations, with drones illegally flying over events and venues 12,624 times (8% YoY increase), power plants 13,325 times (18% YoY increase), and correctional facilities 14,499 times (42% YoY increase).

Consumer drones present attractive vehicles for various bad actors engaged in activities from terror attacks to corporate espionage. It is exceedingly easy for an individual to buy a drone and fly it over a military base, as was the case at Vandenberg Air Force Base in November 2024. Even for the military, shooting that drone down proved to be difficult. While recent progress is being made, advanced militaries and law enforcement still cannot reliably counter drones. At this stage, it is nearly impossible for private citizens or companies to counter the threat posed by drones legally. Without a clear solution, there is little disincentive for state and non-state actors alike to continue using drones for malicious ends, including corporate espionage.

UAS IN CORPORATE ESPIONAGE

While the most acute threat posed by drones to any organization remains physical attacks, the next drone threat is corporate espionage. Bad actors can use aerial systems not only to conduct direct surveillance of residential, commercial, or industrial sites, but also to coerce decision-makers through intimidation by surveillance. In addition, drones can be used for infiltration, using "nearest neighbor" cyberattacks, where physical proximity to a digital network can be exploited to attack weak points in a firm's cyber defenses.

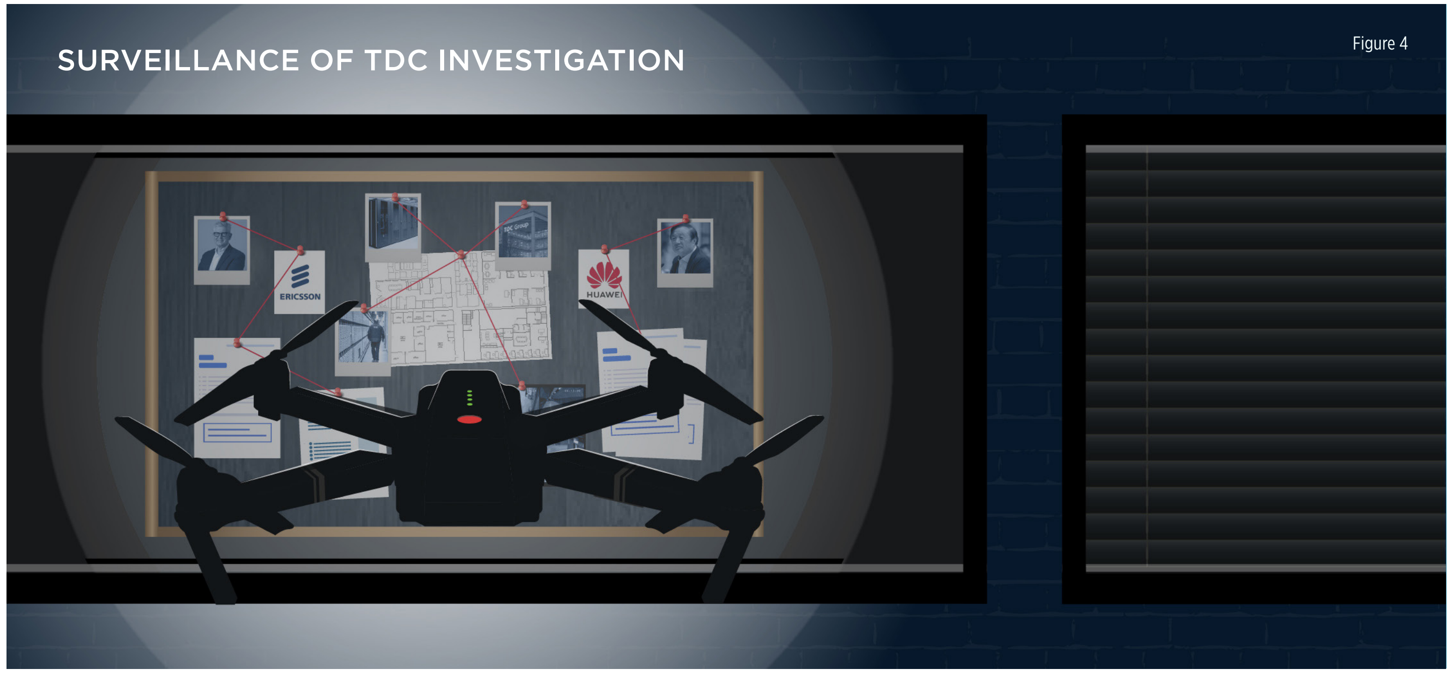
SURVEILLANCE AND COERCION: In 2019, China's Huawei and Sweden's Ericsson were in close competition over a EUR €200 million contract for Denmark's TDC to upgrade its telecommunication network to 5G. As part of a multipronged espionage effort, Huawei used drones on at least two occasions to surveil and intimidate TDC staff.

Huawei had worked with TDC since 2013, supplying and servicing equipment for prior 3G and 4G networks. In 2019, however, Ericsson made a substantially lower final bid. Before TDC's executives reached a decision, Huawei beat Ericsson's bid in an eleventh-hour revision to their offer. The timing of the revision and the similarity of Huawei's new figure to Ericsson's bid set off an internal investigation at TDC. Ericsson's bid was confidential information only known to about a dozen high-ranking personnel at TDC. The security team suspected an insider threat, hacking, eavesdropping, or a combination thereof. The investigation quickly confirmed two of their suspicions. Huawei had used cultivated insiders to ascertain Ericsson's bid information and was also eavesdropping on the TDC investigation itself through microphones built into a boardroom's teleconference system.

Finding its own offices compromised, TDC moved its investigation to a conference room belonging to Plesner, one of TDC's legal partners. Plesner's office came under an effective distributed denial-of-service (DDoS) attack the same day. The night following the investigation's relocation, a security guard observed a large drone illuminating the investigation room, where a whiteboard with the investigation's timeline and key figures of interest had been left uncovered.

SURVEILLANCE OF TDC INVESTIGATION

Figure 4



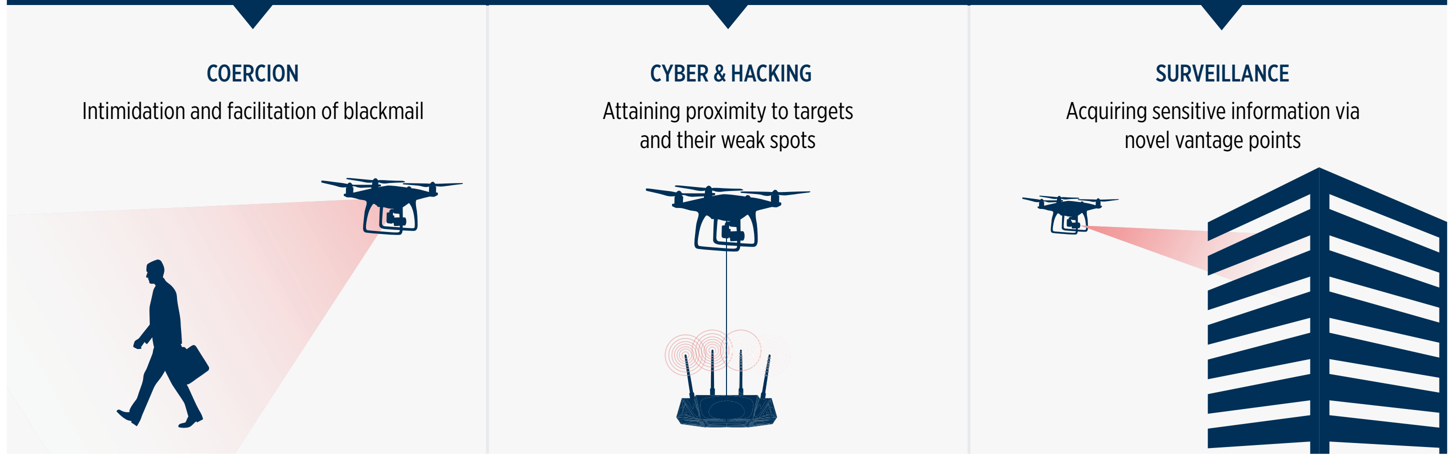
In addition to gathering information, Huawei pressured TDC's executive staff and the Danish government, including a letter to the Danish Prime Minister threatening to withhold or withdraw other Chinese investment in Denmark if Huawei lost the TDC contract. Multiple security team members reported suspicions that they were being followed and surveilled during the investigation by both people and drones. While celebrating the end of the investigation, the firm's CEO and security team were observed by a large drone on the 17th floor of the Silo Hotel in Copenhagen before the drone descended to a white van which retrieved it and sped away.

While Ericsson was ultimately awarded the contract, and Huawei's capabilities exceed those of most competitors, the TDC incident illustrates how drones are used on multiple levels to unduly influence major financial decision-making. In the TDC affair, the watchful eye of a UAS was pernicious on two levels. First, the drone's operators observed confidential information they should not have. Second, simply watching the investigators fostered harmful distrust and paranoia within the upper echelons of TDC.

While Huawei combined the threat vectors of cyber, eavesdropping, insider threat, and drones, an unsophisticated actor could use drones alone to facilitate blackmail, virtual kidnapping, harassment, or simply to surveil executives. All a would-be attacker needs to harm a company is access to a drone and time.

COMBINED ARMS OF ESPIONAGE

Figure 5


COERCION
Intimidation and facilitation of blackmail
CYBER & HACKING
Attaining proximity to targets and their weak spots
SURVEILLANCE
Acquiring sensitive information via novel vantage points

NEAREST NEIGHBOR HACKS: A "nearest neighbor" hack is a cyberattack that relies on physical proximity to a targeted network. Conventionally, attackers need to be physically near their target. But drones negate the risks involved in attaining the requisite proximity for a nearest neighbor attack. A van parked outside an office can be picked up on CCTV or even interdicted by law enforcement. UAS allow attackers to maintain distance while pursuing this threat vector, lowering the risk and, in turn, making these attacks even more attractive.

In 2022, a financial company's internal network was partially penetrated through a drone-assisted nearest neighbor attack. The firm discovered unusual activity on its internal network. It traced the activity to a device using a remote employee's network credentials to access the company's Wi-Fi. However, the employee in question worked remotely, and their credentials were simultaneously used on a device at their home several miles away.

The security team followed the imposter signal to the roof using Wi-Fi detection equipment. There, the team found two commercially available DJI drones—a Phantom and a Matrice—modified to carry a Wi-Fi penetration tool (Wi-Fi Pineapple), a small laptop, batteries, and other devices [figure 5].

The investigators found that one of the drones had been used days before to obtain the employee's credentials from their home before being used to access the office's internal network. The attack was successful in gaining partial access to the company's Wi-Fi. The company's security team believe the attackers were attempting to retrieve the drones when one was damaged, and the effort was abandoned.

If the attack had been conducted at a different time of day, or if the drones had been successfully recovered for another attack, the infiltration could have been much worse. This nearest neighbor attack demonstrates that the modifications that turn drones into kinetic weapons on the battlefield can just as easily be used to turn drones into weapons in cyberspace.

MILITARY-CIVIL FUSION

The magnitude of the drone threat is partially due to the dual-usage crossover between civilian and military applications. Civilian demand for drones sustains a commercial UAS industry complete with research and development (R&D), manufacturing infrastructure, and private capital. Military demand for drones supercharges the commercial development cycle by directing and coordinating between multiple firms, creating reliable, long-term demand, and providing public funding. A virtuous cycle of economies of scale and rapid development follows.

The Chinese Communist Party (CCP) employs what is called "military-civil fusion" (MCF). MCF is the CCP's strategy to develop the People's Liberation Army (PLA) into a "world class military" by 2049. Under MCF, the CCP is systematically reorganizing Chinese industry to ensure that new innovations simultaneously advance economic and military development.

> "The CCP is systematically reorganizing Chinese industry to ensure that new innovations simultaneously advance economic and military development."

A prime example of MCF is China's growing light shows, where over 10,000 light-bearing drones have been coordinated through a single network. These spectacular aerial displays rely on precisely the same network of enterprises and engineers developing military drone swarms for the PLA. The drone light show market in China alone was worth USD $363.72 million in 2024 and is projected to grow. Chinese drone companies—including DJI—have close state ties and dominate the commercial UAS space. DJI alone controls 80% of the U.S. market and 70% of global drone market.

THE DRONE THREAT OF TOMORROW

The first use of quadcopters to drop munitions was likely conducted by Islamic State forces in 2016. Other actors in the region quickly adopted weaponized commercial drones, often using 3D-printed mechanisms to carry and drop ordinance. It took malicious actors at most six years to adapt this same practice but for cyberattacks.

Today, the cutting edge of drone development includes fully automated AI-directed UAS, drones disguised to look and fly like birds, and microdrones that can fit in the palm of one's hand. AI-piloted drones offer actors the ability to automate attacks, greatly increasing the scale of the threat. Drones that look inconspicuous —like birds—could bypass and negate awareness and sensor systems. Microdrones are small enough to potentially gain access to a secure site by tailgating.

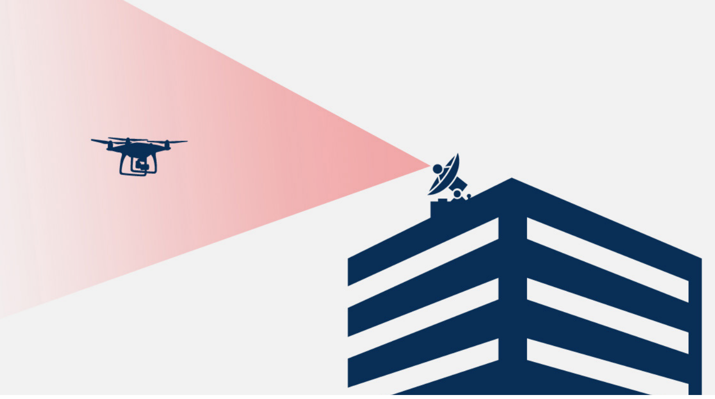
COUNTERING THE THREAT

The use of UAS in corporate espionage is likely to increase in the absence of adequate civilian countermeasures. Until effective counter unmanned aerial systems (C-UAS) measures are developed and widely adopted, malicious actors have much to gain and little to lose in exploiting the efficacity gap between UAS and C-UAS. Closing this gap requires action at three levels: legal, technological, and organizational. Given the current pace of drone technological development, companies can expect to contend with some form of these threats by 2030.

Since drones are considered aircraft by the Federal Aviation Authority (FAA) in the U.S., downing them is a federal offense. Private citizens or organizations are not allowed to shoot down drones. The only U.S. entities permitted to intercept commercial drones are the Department of Homeland Security (DHS) and the Department of Justice (DOJ). Similar legal barriers are near-universally present in other jurisdictions. Drone jamming is also illegal due to air safety concerns. While many agencies are capable of catching small drones, their capacities are mostly concentrated on counter-terror operations. Realistically, companies facing a drone threat have only two options in the legal realm: alert law enforcement or appeal to elected representatives.

UAS DETECTION

Figure 6



Other than reporting suspicious or illegal drone activity to local police and the FAA, there are steps organizations can take that fall short of "hard" or "soft" kill options. Fostering awareness of malicious UAS activity is something that private organizations can actively pursue. This can be done through drone monitoring services or by procuring on-site detection arrays. Remote warning systems monitor drone communication signals to identify and log data on drones within an area. On-site arrays use a combination of signals monitoring, cameras, and radar to track drones in the vicinity of the site in question [figure 6].

Drones are most dangerous when used in conjunction with other attack vectors. Attempts by bad actors to penetrate corporate defenses are most successful when taking a "combined arms" [figure 5] approach that pairs cyber or traditional espionage with UAS assistance. Maintaining strong cyber, physical, and human security systems is the best approach to mitigating the threat presented by drones.

KEY TAKEAWAYS

The gap between drone capabilities and counter-drone measures leaves companies vulnerable to various drone-augmented threats. In addition to new vectors of attack that rely wholly on drones, unmanned aerial systems also act as a force multiplier for cyberattacks, insider threats, conventional surveillance, and coercion. Firms must adopt and implement effective technological solutions to the novel threats of drones and other modern threat vectors.

THE AMERISPHERE:
LOOMING BUSINESS RISKS IN MEXICO

The Trump administration's approach to international affairs marks a divergence from the post-World War II United States (U.S.) foreign policy establishment. The shift to transactionality and the tactical use of trade barriers within the "Amerisphere"—America's near abroad—poses top-line, bottom-line, and physical risks to multinational businesses, especially in Mexico, America's largest trading partner.

The priorities and execution of U.S. foreign policy is akin to a nineteenth-century Victorian approach to international affairs. In Victorian diplomacy, relationships were transactional and great powers endeavored to control trade in their perceived spheres of influence. The Trump administration sees American economic and military preeminence as untapped national assets rather than global commons, as was the case since in the post-World War II era.

In its opening days, the administration has dropped normative internationalist obligations and begun levying tariffs. The U.S. is now leveraging market access as both a carrot and a stick to solidify regional hegemony in America's "backyard," portending significant risks to multinationals.

THE AMERISPHERE

Spheres of influence are regions a great power perceives as essential to its interests. Interests are both derived from potential opportunities and threats. A shared border with a friendly state is an economic and security benefit. A shared border with a hostile state is a vulnerability—road networks do not discriminate between trucks and tanks. Friction arises when great powers have overlapping spheres of influence or a smaller country contests its subordination to a more powerful actor. This dynamic is evident today in Ukraine (Russia's sphere), Taiwan (China's sphere), and Mexico (America's sphere).

Indeed, Mexico is a keystone country in the "Amerisphere" as the U.S.'s neighbor and top trade partner.. Mexico is also fundamental to President Trump's domestic agenda of securing U.S. borders and curtailing human and narcotics trafficking. Of all Latin American nations, Mexico is particularly at risk of destabilization due to its centrality in the U.S. sphere, the permeation of organized crime in all facets of society, significant Chinese influence, and historical U.S. grievances.

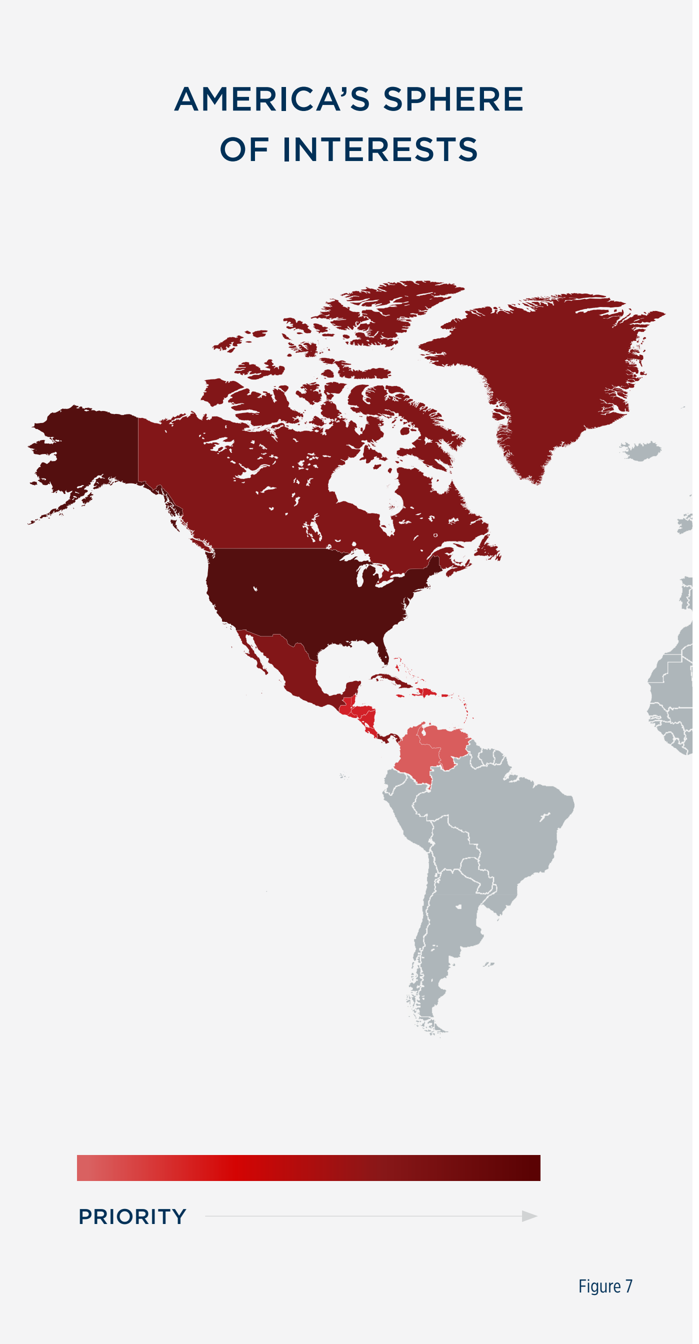


Figure 7

REDEFINING "FAIR"

Since 1945, the overarching American foreign policy position centered on upholding the international system of rules and norms. Free trade, free markets, and the legal resolution of trade disputes were pillars of the post-World War II order and viewed as ends unto themselves. For the U.S., this entailed balancing roles as both star player and referee—simultaneously competing and delineating the acceptable bounds of competition.

This is no longer the case. The United States' foreign policy revision calls into question not only American's role as a global referee but also the legitimacy of the liberal international order itself. The administration views intergovernmental organizations—the United Nations, World Trade Organization, International Criminal Court (ICC), and others—as bodies that, at best, take advantage of the U.S. and, at worse, undermine American interests. Secretary of State Marco Rubio articulated this worldview during his confirmation hearing, stating that "the post-war global order is not only obsolete, it is now a weapon being used against us." The re-examination of bilateral relations based on reciprocity and benefit rather than "values" will shake the foundations of globalized business. Precepts taken for granted in the Western world, such as market access and enforceable contracts, come into question when they are factored into a geopolitical balance sheet. In deal-making diplomacy, nothing is off the table.

In practical terms, new U.S. foreign policy in action will leverage tariffs to pressure the governments of Mexico, Canada, and elsewhere to achieve policy objectives. These include, aggressively reducing illegal immigration and establishing favorable trade and defense agreements with countries within the U.S. sphere of influence to the exclusion of other powers, particularly China. The transition to this style of relationship carries major concerns for American enterprises—particularly those operating in Mexico—in the forms of trade barriers, compliance, and coercion.

TRADE

The principal instrument to rebalance U.S. relationships within its orbit is America's tremendous economic gravity. The U.S. accounts for more than 80% of Mexico's exports, and over a quarter of Mexican jobs rely on cross-border trade with the United States and Canada. Restrictions to that access, while it could hurt the U.S.—costing as many as 400,000 American jobs—could cripple the Mexican economy. By threatening 25% tariffs, Trump is presenting Mexican president Claudia Sheinbaum with the choice: call the bluff, and possibly face economic catastrophe, or agree to U.S. demands, and in so doing, alienate China and antagonize the cartels. To this end, the Mexican government has taken swift action to address U.S. demands on border security, repatriation, and curtailing Chinese commercial access. Reciprocal sanction plans have been established, putting "Chekhov's gun" on the table.

FTO AND COMPLIANCE

The classification of cartels as foreign terrorist organizations (FTOs) carries dramatic implications for firms that conduct business in Mexico. The FTO designation—at its most maximalist prosecution—allows Washington to take unilateral military action in Mexico. In the first two weeks of February, the U.S. conducted at least 18 surveillance flights along the border with Mexico, and in international airspace around Baja California. Prior, the U.S. typically conducted an average of one surveillance flight a month. On the ground, U.S. Customs and Border Patrol (CBP) districts have issued at least two memos warning of possible cartel violence against CBP agents and U.S. military personnel. In the first memo, issued 01 February 2025, the El Paso Sector Intelligence and Operations Center warned agents that cartel leadership had potentially greenlit the use of weaponized drones against U.S. security forces. The second memo, issued 07 February 2025 suggested a cartel group operating out of Matamoros planned to frame Mexican authorities for the shooting of a U.S. Border Patrol agent or soldier. CBP agents have been instructed to wear body armor, carry rifles, and to operate in groups. The killing of a U.S. soldier or agent would have highly destabilizing consequences, and probably result in more direct kinetic U.S. action inside Mexico.

The FTO designation also grants the U.S. government the capability to prosecute people and organizations not directly involved in the drug trade who provide material support or services—including financial services—to cartels. If agglomerated, the Mexican cartels are the fifth largest employer in Mexico. While their principal revenue comes from drugs and trafficking, they are also involved in an increasingly diverse set of legal economic activities. Cartels control or are involved in logistics networks, transportation companies, the agricultural sector (namely, avocado and corn tortilla production), wide swathes of the tourism industry, and a host of other enterprises touching nearly every sector of the Mexican economy. Depending on how wide a net the U.S. government casts, nearly everyone with assets and personnel in Mexico could be liable for supporting terror. Purchasing from, selling to, hiring, or providing services to these cartel-linked companies could expose firms to terror charges under the FTO designation.

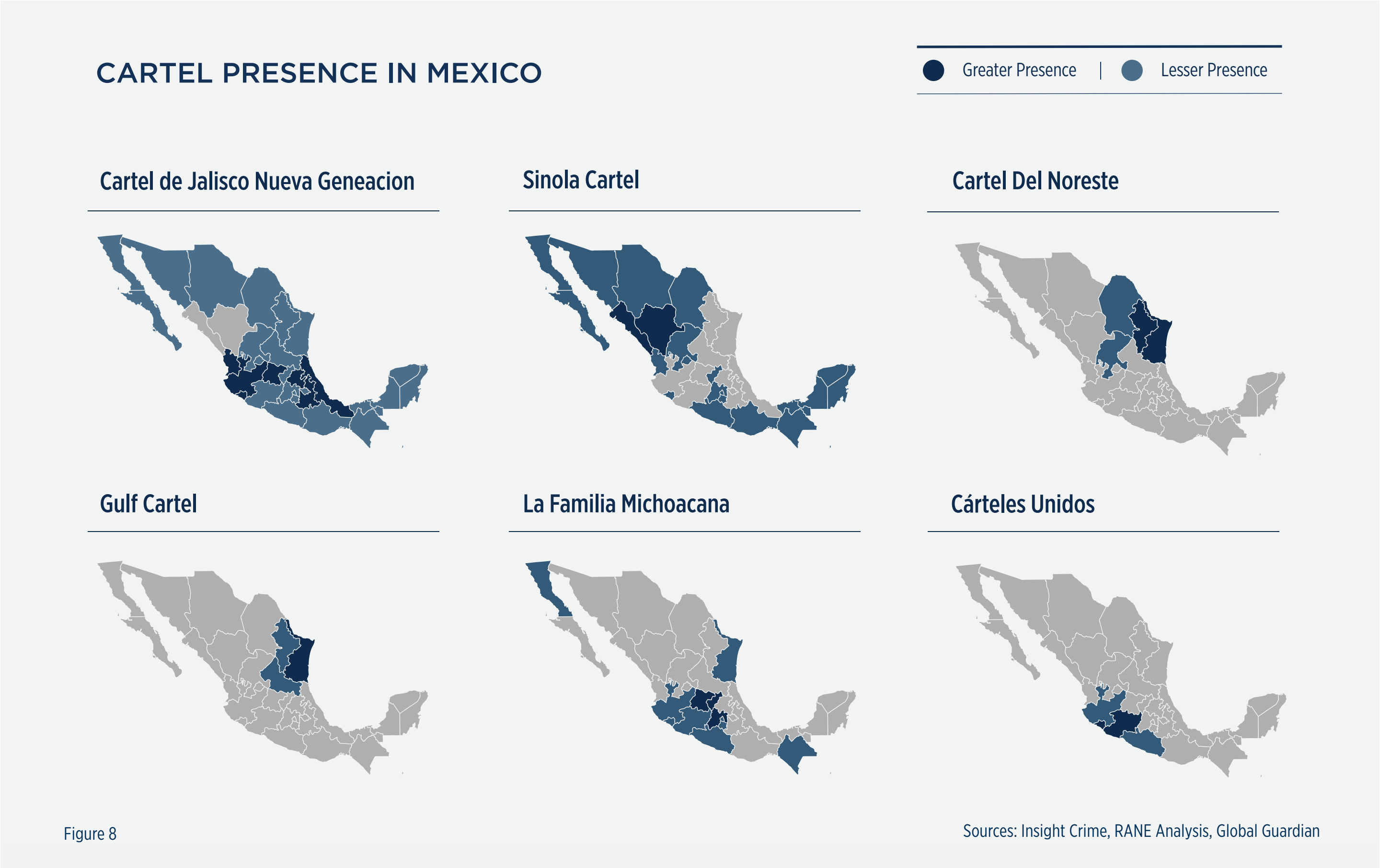

CARTEL PRESENCE IN MEXICO

Figure 8

Sources: Insight Crime, RANE Analysis, Global Guardian

Doing due diligence on these companies will be daunting, given their proprietors' resources and inclination for opaque business practices. But these entities are less problematic than the vast array of mostly U.S.-based shell companies and money laundering mechanisms cartels use to legitimize their revenue. The secrecy and obfuscation inherent to money laundering make avoiding business with these entities challenging. The Sinaloa Cartel, Jalisco New Generation Cartel, the Northeast Cartel, the Michoacán Family, the United Cartels and the Gulf Cartel, as well as the El Salvadorian Maras Salvatruchas and Venezuelan Tren de Aragua, have so far received this designation. The legal framework presents compliance risks for firms with operations in a designated group's territory [figure 8].

COERCION

The United States' new approach to transnational organized criminal elements within the "Amerisphere" risks increasing physical threats to U.S. firms and the approximate two million U.S. citizens living and working in Mexico.

According to a survey from the American Chamber of Commerce in Mexico, roughly 12% of American firms in Mexico have had organized criminal groups "take partial control of the sales, distribution, and/or pricing of their goods," 45% reported receiving extortionate demands for payment or ransoms, and 50% of the respondents said their delivery vehicles had been attacked. Yet American firms tend to be targeted less than local firms. The disproportionate amount of police and media attention that violence against Americans draws has led cartels to avoid American victims. In March of 2023, an element of the Gulf Cartel killed three U.S. citizens in the Mexican border town of Matamoros in a probable case of mistaken identity. The incident garnered widespread coverage and significant pressure from both the U.S. and Mexican governments. The cartel quickly turned in the five "guilty" members, along with a letter of apology. This contrition is not extended to Mexican victims.

But if the U.S. adopts a maximum pressure campaign that achieves its goal of meaningfully reducing drug inflows, then it would have little room to escalate with the cartels short of unilateral or joint military action (with Mexican forces). In essence, the U.S. buys the safety of American citizens with the threat of pressure—the pressure itself holds little currency with the cartels. In this maximum pressure scenario, the cost-benefit analysis for the cartels changes. Currently, violence against Americans is more trouble than its worth. But if the trouble can no longer be avoided, cartels will seek to increase its worth.

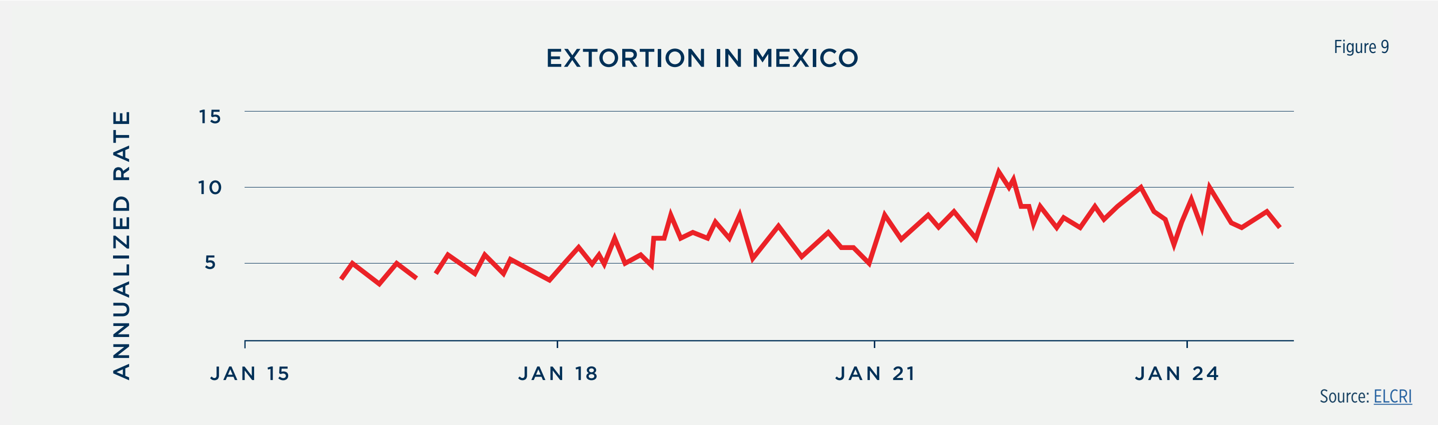

EXTORTION IN MEXICO

Figure 9

Source: ELCRI

Cartel extortion of Mexican businesses has expanded in both scope and the size of their targets, portending a possible future for American firms [figure 9]. In July 2024, extortion led Mexico's largest convenience store chain, Oxxo, to close all 191 of its locations in the border town of Nuevo Laredo. In addition to traditional protection payments, Oxxo stores were forced by the Northeast Cartel to purchase gasoline from Northeast-affiliated suppliers, and at least two Oxxo employees were kidnapped and forced to work as informants for the cartel under threat of violence. The Nuevo Laredo closures are just one piece of a broader picture of ambitious extortion.

Absent a substantial change in Mexico's security landscape, extortion will pose an increasing threat to Western firms operating in Mexico. The net extortion rate has risen steadily over time and may be even higher due to underreporting [figure 9]. As cartels diversify their revenue streams beyond narcotics, extortion becomes a more vital component to their financial portfolios. Amid the dynamic splintering and restructuring in the Mexican cartel system, groups seeking to change momentum in the ongoing drug war may now be more inclined to extort higher-risk, higher-reward multinationals and their local suppliers. While the current extortion threat affects much of the country, the intensity of cartel extortion is unevenly distributed among Mexico's states. Mexico's current highest extortion rates are found in Nuevo Leon, the Federal District, Morelos, and Guanajuato [figure 10].

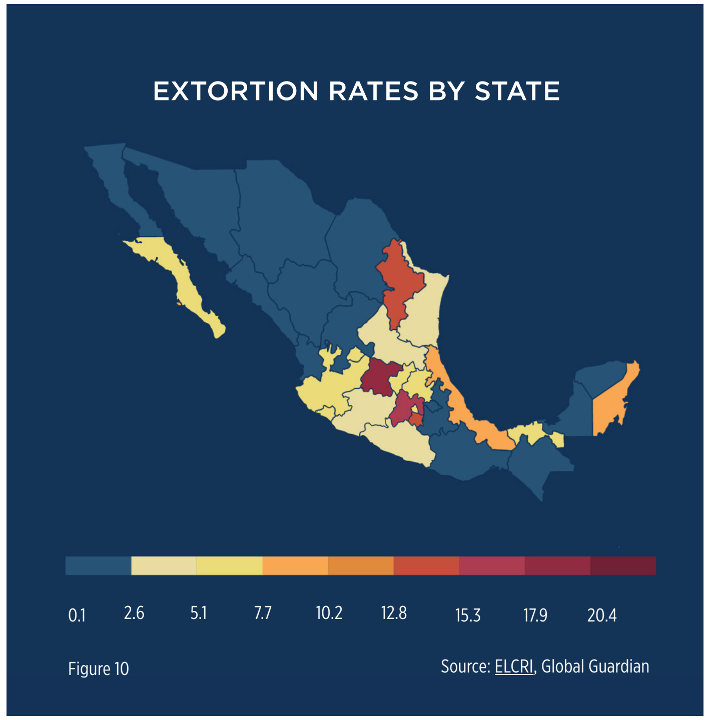

EXTORTION RATES BY STATE

Figure 10

Source: ELCRI, Global Guardian

KEY TAKEAWAYS

The Trump administration's neo-Monroe Doctrine in its sphere of influence will see an aggressive projection of American hard power, upsetting the status quo from Greenland to Panama. Counterpressure is expected and will be exercised on multinationals. In Mexico especially, multinational firms will face increased risks of violence and extortion, as well as both compliance and supply-chain uncertainties.

THE MIDDLE EAST AT A CROSSROADS

Over a century after the collapse of the Ottoman Empire, the Middle East is again reshaping following the transformative events of 2024. Iran began the year as a hegemon, demonstrating its regional might. But after the degradation of Lebanese Hezbollah and the fall of the Assad Regime in Syria, Iran has devolved into a nuclear threshold chaos actor. The region's geopolitical sea change offers both new partnership opportunities and opportunities for new rifts. The short-term outlook includes renewed fighting in Gaza and a nuclear showdown with Iran.

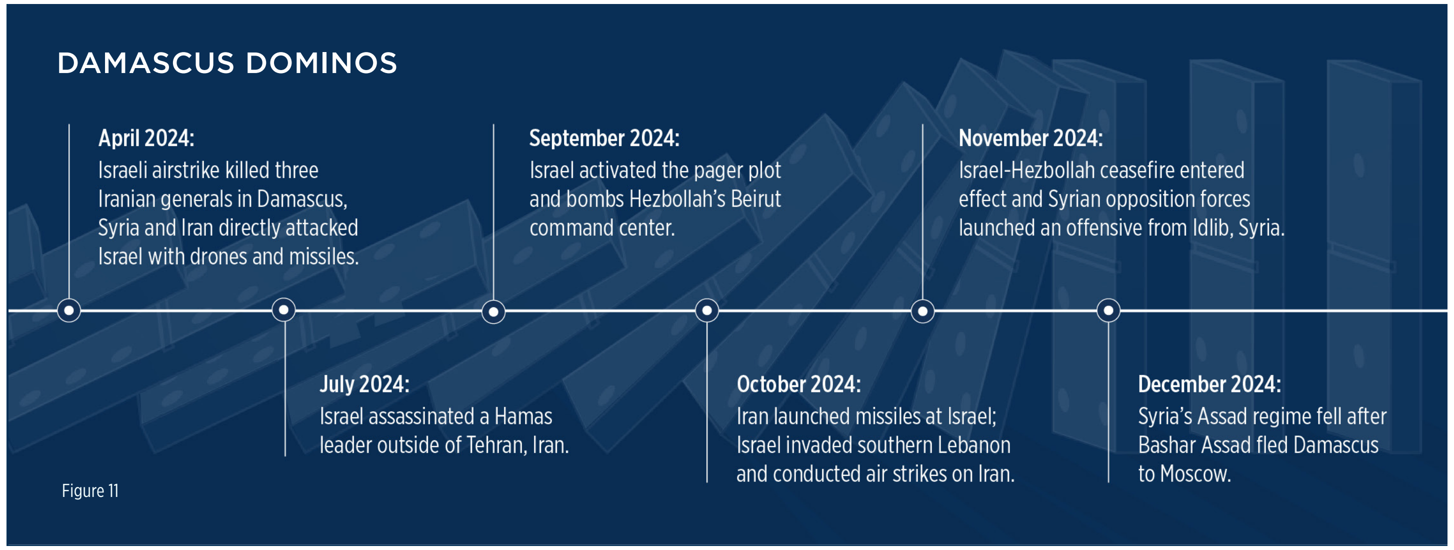
Six months after its security failure on 07 October 2023 and under diplomatic and military pressure, Israel shifted its strategic doctrine, engaging Iran and its partners head-on. Then, as soon as the Israel-Hezbollah ceasefire in Lebanon began in November 2024, the Syrian opposition—led by Hayat Tahrir al-Sham (HTS)—launched an offensive, seizing control of Syria in just 13 days, bringing an end to the 13-year Syrian Civil War. What began with an Israeli airstrike in Damascus ended in Syrian President Bashar Assad's secret escape from Damascus to Moscow some eight months later [figure 11]. With Iran's dominoes falling rapidly and a major foreign policy shift in Washington, the long-term regional outlook in the Middle East is extraordinarily opaque as jostling over the vacuum left by Iran ensues.

"AXIS OF RESISTANCE" DOWN, BUT NOT OUT

Since the brutal Iran-Iraq War (1980-1989), the Islamic Republic of Iran has sought to export its Khomeinist revolution while keeping the fight far from home. To this end, open confrontation against the regime's ideological foes (Israel, the West, and the Arab monarchies) and the perception of protecting the Middle East's Shi'a minority communities have been paramount to preserving its legitimacy.

Consequently, Iran has spent the last 30 years developing a three-pronged and mutually reinforcing strategic concept. It built a robust network of partners across the Middle East (sometimes finding common cause with Sunni Jihadists) to form the "Axis of Resistance," achieved threshold nuclear status, and domestically produced accurate and powerful standoff weapons, including medium-range ballistic missiles (MRBMs), long-range cruise missiles, and attack drones. This approach allowed Tehran to engineer two concentric "Rings of Fire" around its foes. The first ring aimed to surround Israel to make it unlivable and embroiled in an existential "forever war." The second ring aimed to pressure the Gulf Cooperation Council (GCC) monarchies—Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates—to pursue appeasement by threatening their ability to export petrochemicals and invite the necessary investment to diversify their economies away from oil.

AXIS OF RESISTANCE, THEN AND NOW: At the start of 2024, Iran stood as the preeminent Middle Eastern power backed by organizations that were physically and politically entrenched in Lebanon, Syria, Iraq, Yemen, the Gaza Strip, and the West Bank. Tehran was exporting an average of around 1.6 million barrels of oil per day and had successfully pressured Saudi Arabia and the UAE to abandon their interests in Yemen and opt for détente. At the start of 2025, the reality is very different. Iran's incremental long-term "Unity of Fronts" strategy to destroy Israel backfired: Hamas' invasion forced Iran's hand before its Lebanese partner, Hezbollah, was ready to execute its Capture the Galilee Plan —an October 7th-style invasion from Southern Lebanon.



DAMASCUS DOMINOS

April 2024:
Israeli airstrike killed three Iranian generals in Damascus, Syria and Iran directly attacked Israel with drones and missiles.

July 2024:
Israel assassinated a Hamas leader outside of Tehran, Iran.

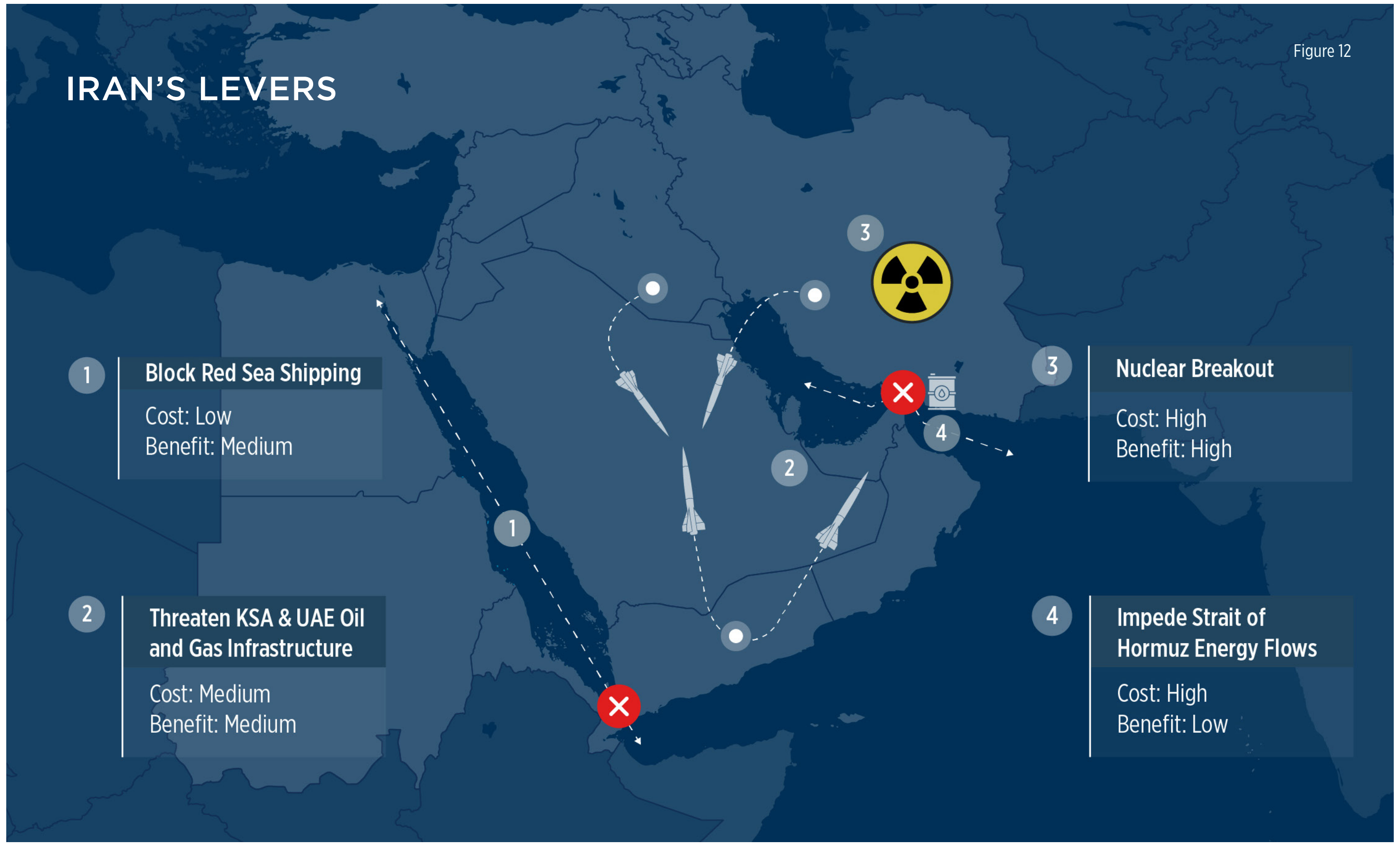
September 2024:
Israel activated the pager plot and bombs Hezbollah's Beirut command center.

October 2024:
Iran launched missiles at Israel; Israel invaded southern Lebanon and conducted air strikes on Iran.

November 2024:
Israel-Hezbollah ceasefire entered effect and Syrian opposition forces launched an offensive from Idlib, Syria.

December 2024:
Syria's Assad regime fell after Bashar Assad fled Damascus to Moscow.

Figure 11



IRAN'S LEVERS

Figure 12

1. **Block Red Sea Shipping**
Cost: Low
Benefit: Medium

2. **Threaten KSA & UAE Oil and Gas Infrastructure**
Cost: Medium
Benefit: Medium

3. **Nuclear Breakout**
Cost: High
Benefit: High

4. **Impede Strait of Hormuz Energy Flows**
Cost: High
Benefit: Low

Today, Hezbollah—the Axis of Resistance's lynchpin—sits temporarily defanged, having lost its original leadership team, its forward attack bases, roughly 80% of its short- and medium-range rockets, and a significant degree of political power in Lebanon. It is also accountable for restocking its arsenal and rebuilding the neighborhoods and villages of its own Shi'a constituency that were destroyed, reliant on a more circuitous financial pipeline from Iran. Assad's ouster in Syria, in effect, removed the Axis of Resistance's connective tissue from the land bridge it used to move Iranian military supplies and hard currency from Iran (via Iraq) to Syria and Lebanon and to traffic Syrian-produced narcotics to Jordan and the GCC.

Moreover, in its 25 October 2024 airstrike on Iran, Israel destroyed Iran's long-range air defense radars and several elements of its MRBM production chain (fuel mixing and motor making), temporarily halting the restocking of Iran's main active deterrent. However, the Islamic Republic and its Yemeni partner, Ansarullah (Houthis), still possess sufficient capabilities to threaten their GCC neighbors. With its strategic trifecta temporarily broken, Iran's Axis is now left with four coercive levers [figure 12].

GOING FORWARD:
Iraq & Syria: Iran will seek to make both Iraq and Syria ungovernable, driving wedges in already highly sectarian societies.

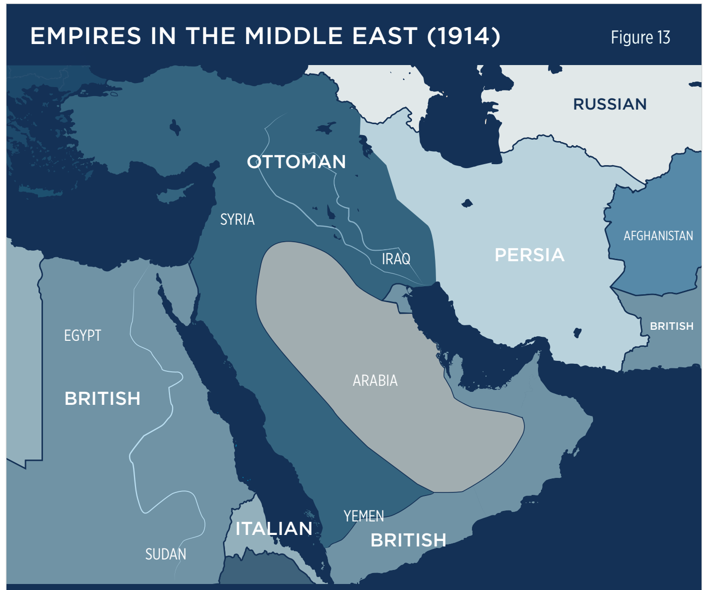
Yemen: The Houthis have renewed their threats to thwart the monarchies' attempts at economic diversification ("Vision 2030") and accused Saudi Arabia of driving Yemen's internationally recognized government toward greater economic and possibly renewed physical aggression. With their battlefield momentum continuing to build against the Yemeni government, the Houthis are poised to escalate operations around Marib and other strategic frontline areas. But early signs indicate that a more unified approach to degrade the Houthis' coercive potential may be underway, owing to a shift in U.S. and foreign aid policy toward Houthi-controlled areas and an increased appetite for anti-Iranian forces to push their current advantage.

Iran: While unlikely, a United States (U.S.)-Russia détente may open the door to a diplomatic breakthrough with Iran vis-à-vis its nuclear program. Barring this, Israel will likely capitalize on this unique strategic opportunity to set back Iran's nuclear program before Iran can reestablish its air defense network and MRBM production.

THE QUESTIONS OF PALESTINE AND SYRIA

The Middle East now sits at a crossroads after a troubled century brought about by the dissolutions of the Ottoman, British, and French Empires amid the struggles for post-colonial identity formation. The answers to the questions of Palestine and Syria will offer insights into the new epoch currently taking shape.

EMPIRES IN THE MIDDLE EAST (1914) Figure 13



Ethnic Groups: Arabs, Assyrians, Circassians, Chechens, Kurds, Turkmens, Armenians, Greeks, Africans, and Jews (Mizrachi, Ashkenazi, Yemeni)

Religious Groups: Sunni, Shi'a (Twelver, Alwite), Eastern Catholic (Syriac, Maronite), Orthodox (Greek, Syriac), Protestant, Druze, Yazidi, and Jewish

These lists are not exhaustive.

Sources: BBC Radio, Global Guardian

POST-OTTOMAN PERILS: Following the colonial divisions of the former Ottoman Empire after World War I, modern polities were created by pen stroke, cobbling together culturally, religiously, ethnically, and linguistically diverse populations into nation-states to be ruled by their favored minority communities [figure 13]. The French Mandate for Syria and Lebanon initially attempted to create a Lebanon socially dominated by the Maronite Christian elite and a confederation of ethnic statelets in Syria. But this project failed during World War II, and Lebanon and Syria became unitary republics shortly after. The British ceded the Hashemites (the historical rulers of Mecca), the kingdoms of Transjordan, Iraq, and what became Saudi Arabia. The crown's conflicting promises in Palestine resulted in the British abdicating the issue and passing it to the nascent United Nations (UN), who voted to partition it.

Issues of social heterogeneity and lack of legitimacy have since plagued the region, opening the door to outside intervention from the Europeans, Americans, Turks, Persians, and Soviets. This structural disharmony helped birth ideological answers to the dialectics of modernity-tradition and local-foreign in Pan-Arabism and Islamism.

THE PALESTINE QUESTION: The Palestinian cause remains a central force in shaping political identity and fostering social cohesion in the modern Middle East. Including the ongoing War in Gaza, there have been 15 conflicts to liberate Palestine. Israel is no closer to disappearing but also no closer to winning peace. The conflict will not stop until the underlying incentives change.

Framed as a post-colonial conflict akin to the Algerian War, the Palestinian Cause is an movement rooted in the demand for the "right of return" for 1948 Palestinian refugees and opposition to Jewish sovereignty in the Levant. Since the First Arab-Israeli War and the resulting mass displacement of Arab Palestinians and then Middle Eastern Jews, regional leaders have promoted an Israel-free vision for the Levant's future through the region's 20th-century ideologies of secular Pan-Arabism and Islamism while preventing Palestinian integration and resettlement. The cause has often been leveraged as a pressure valve to direct endogenous social ills surrounding poor governance and persisting issues of identity in heterogeneous states. When it became evident after three interstate wars (1948, 1967, 1973) that a conventional military victory over Israel was not achievable, the concept of Pan-Arabism was laid to rest. Eventually, some states reluctantly embraced the two-state solution (a Jewish and Palestinian state side by side), as military defeats repeatedly cost land and caused embarrassment. While Egypt signed a peace treaty with Israel in 1979 and Jordan in 1994, the region's Islamist factions (which include Hamas) never did [figure 14].

ANSWERS TO THE PALESTINE QUESTION

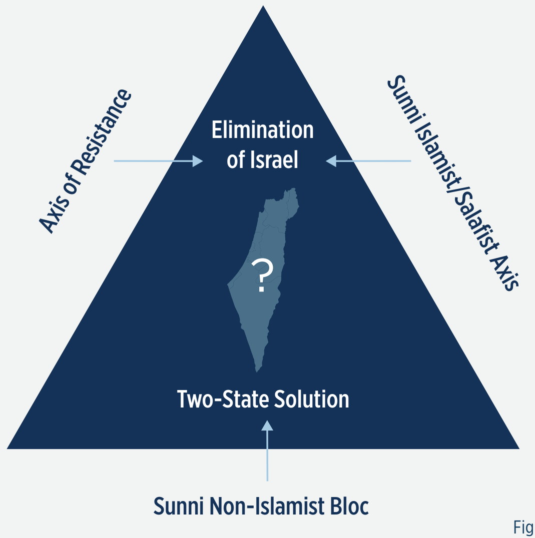


Figure 14

Israel	
Short-Term Goals	
Return hostages	
Eliminate Hamas' military capabilities	
End Hamas's rule of Gaza	
Return residents from conflict zones	
Long-Term Goals	
Thwart Existential Threats	
Regional Integration	

Hamas
Short-Term Goals
Thwart Saudi Arabia-Israel normalization
End two-state solution paradigm within Israel
Diplomatically isolate Israel
Retain control of Gaza
Long-Term Goals
Assume leadership of the Palestinian people
Eliminate Israel

Figure 15

> "Leadership on the 'Palestine Question' is, therefore, a persisting source of soft power on the Arab Street and a means of acquiring hard power."

Islamists categorically reject Israel's existence and view armed struggle to extirpate it as the only legitimate path forward. The elimination of a non-Arab Muslim state—no less that of *dhimmis*— in the geographic center of the Umma (the Islamic nation) is seen as a political precondition of Islam's restoration after centuries of humiliation by outsiders. From the Maghreb to the Malay Peninsula, civil society and religious organizations receive donations and remain relevant by supporting violence in Palestine at zero cost to themselves. Given the significant influence of Islamist movements, particularly through the clergy's hold on societies, this stance cannot be easily ignored. In some cases, it may even outweigh the formal policy positions of many governments.

While the Gulf monarchies have the resources to build legitimacy through entitlements and economic promise, the social contracts in less prosperous states are on shakier ground. Leadership on the Palestine Question is, therefore, a persisting source of soft power on the Arab Street and a means of acquiring hard power. Saudi Arabia and the other Gulf states used to support Hamas before Iran became its main patron (Qatar still does). Indeed, Hamas is the one non-Shi'a terrorist organization that Iran supports and uses to gain inroads in Arab societies in the Middle East and in the diaspora. Türkiye, the Middle East's other major non-Arab power also supports Hamas and would like to claim the ideological mantle for regional leadership.

Squaring the Circle: The success of Hamas' 07 October 2023 attack on Israel effectively put a nail in the coffin of the two-state solution, taking off the table the answer to the question of Palestine championed by the international community and the non-Islamist forces in the Middle East. Simply put, Hamas and Israel's goals are mutually exclusive [figure 15]. The Palestinian alternative to Hamas, the Palestinian Authority (PA), is weak, corrupt, unpopular, and has no succession plan for its 89-year-old President, Mahmoud Abbas. No Israeli government can accept a Hamas-controlled neighbor and no Hamas leader can accept Israel's existence. The Israeli hostages Hamas is holding and its effective control over the Gazan civilian population give Hamas the ultimate bargaining chips. Egypt's 04 March 2024 postwar proposal illustrates the paradox that the region faces. Cairo and the Arab League, by extension, cannot propose a solution that effectively sidelines Hamas without appearing to jettison the Palestinian cause.

By proposing a radical postwar plan, President Trump's answer to the question of Palestine is to stop asking it. In this vision, the United States takes over the Gaza Strip following a continuation of the war or a deal to dislodge Hamas, and many of its two million Palestinian residents voluntarily relocate. The coastal enclave would then be cleared of debris, tunnels, and unexploded ordinance, rebuilt, and commercially developed under U.S. trusteeship.

Notwithstanding the possible resumption of heavy and devastating urban combat in Gaza, this concept also engenders short-term risks in Jordan and the West Bank, where the relocation of Palestinians could destabilize their regimes entirely. A displacement of civilians from Gaza could also generate strong anti-American sentiment throughout the Middle East and around the globe.

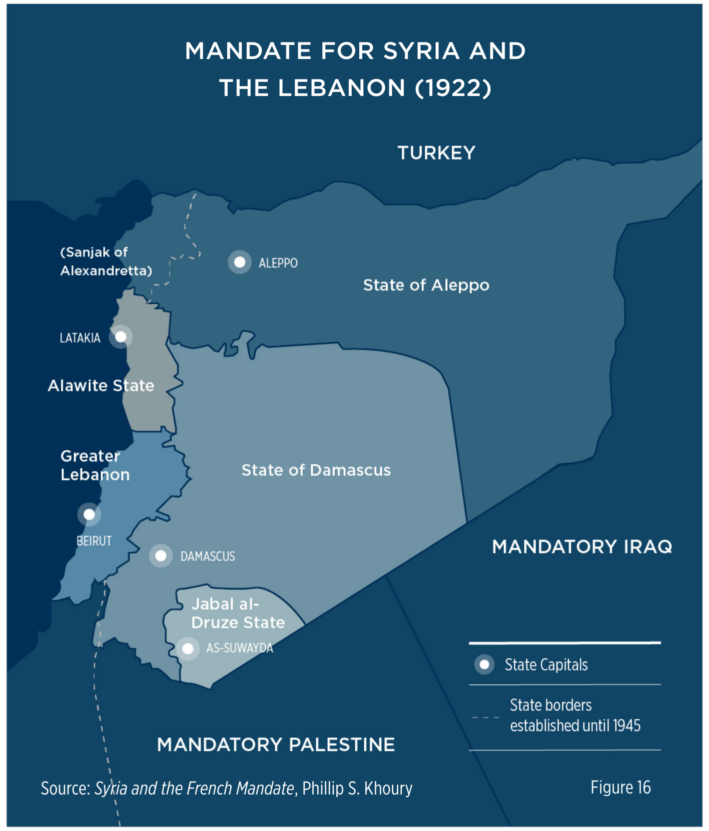
THE QUESTION OF SYRIA: While the ouster of the Assad regime in Syria presents opportunities to stabilize the Levant it also brings significant challenges. Broadly, the stability of a post-revolution state is contingent on the new regime's ability to manage security and stability, balance foreign relations, and promote economic reconstruction. Ultimately, threading the needle to create a stable and functional Syria will depend on which Syrians post-Assad Syria is for. Assad's Syria was a minoritarian state primarily privileging Syria's Alawite and the Damascus elite. Should Syria become majoritarian, outside actors will step in—as they have already begun to—and Syria could fragment along 1922 French mandate lines [figure 16].

Majoritarian Syria vs Pluralistic Syria: The new government has already begun suppressing counter-revolutionary forces and integrating rebel forces. But despite the striking of an agreement to integrate the Kurdish-led Syrian Democratic Forces (SDF) into new state, a security dilemma exists. The Syrian-Kurds need to be armed and quasi-independent to defend against the predations of Turkish-backed Syrian-Arab militias and Türkiye itself. However, having an armed Kurdish presence on its border makes Türkiye insecure. Should the Kurdish integration into state institutions fail, outside actors may enhance cooperation with Kurdish groups to balance Turkish power.

Managing relations between the new government and the coastal Alawite communities will also be vital. Iran is already exploiting opportunities to foment disorder in Syria, resulting in mass sectarian violence. In Syria's south, Israeli Prime Minister Benjamin Netanyahu has demanded demilitarization. To this effect, Israel has been systematically destroying military infrastructure in the region since Assad's fall. Israel's buffer zone along with its offer to protect the Druze community in southern Syria may soon come into friction with Damascus.

Balancing Nationalism and Islamism: Managing the ideology of the Syrian revolution itself will also be a challenge for the new regime. Hayat Tahrir al-Sham (HTS) evolved from Jabhat al-Nusra, a Syrian offshoot of al-Qaeda in Iraq (AQI). The HTS-led government must carefully balance its image in Europe and the GCC to facilitate Syria's reconstruction and reentry into international finance and trade. While HTS is rhetorically nationalist and the new government is branding itself as a pragmatic force, it still holds Salafi-Jihadist views at its core. Among many other tenets, the ideology seeks the revision of humiliation by "Crusaders" (Christians), "Zionists" (Jews), and "apostates" (Shi'a) through armed struggle.

MANDATE FOR SYRIA AND THE LEBANON (1922)



Source: *Syria and the French Mandate*, Phillip S. Khoury

Figure 16

With "apostates" and "crusaders" already being killed at home and Israeli forces within Syria, the temptations to continue its Jihadist revolution could prove to be too compelling for some members of the new regime and its allies.

Looking Ahead: Coming to a *modus vivendi* with Türkiye, Israel, Iran, Russia, and the U.S. will be a challenge. Remnants of Iran's Axis of Resistance are present and will continue to resist the new regime and its security services. While Türkiye can offer Syria security, the fledgling regime will also need Saudi and Emirati capital for reconstruction. Ankara's potential role as a defense patron for a future Syrian state suggests that Türkiye may eventually come into direct friction with Israel, which may allow Russia to reenter Syria at the behest of those seeking to balance Türkiye.

KEY TAKEAWAYS

Over the last 12 months, Iran and its Axis have been dealt strategic setbacks at the hands of Israel and the former Syrian opposition, creating a dangerous vacuum in the region. The current jostling to create a new security order will bring new frictions and form new alliances. In Syria, the new regime faces many potential traps when managing the interests of its heterogeneous population and those of outside actors. Only time will tell if the region can move past the structural issues it inherited from the dissolution of the Ottoman, British, and French empires or if its path dependency is too strong.

OUTLOOK AND KEY TAKEAWAYS

The post-World War II international order has collapsed. The emerging era resembles nineteenth-century great power rivalry, but with the added constraint of twenty-first-century weaponry, including non-interceptable nuclear devices. This fundamental shift in international dynamics, marked by de-globalization and neomercantilism, will profoundly impact global business.

So far, in this emerging geopolitical playing field, great power conflict is increasingly waged through proxies, cyber operations, and economic warfare—where private firms often serve both as frontline defenders against attacks and as tools of state power. State actors are increasingly using private firms to pursue national interests, and consequentially, adversarial states are increasingly targeting private firms. The business community now contends with the threats posed by exposure to new dimensions of state-sponsored espionage, sabotage, hacking, and violence. Risks are higher in regions of strategic competition such as Latin America, where the prospect of a renewed American hegemony threatens to upend a precarious balancing act between China, the United States, and powerful non-state actors. In the Middle East, the sudden fall of the Assad regime and a weakened Iran have primed the region for a restructuring unseen since the fall of the Ottoman Empire.

PRECARIOUS GEOPOLITICAL ERA

The current geopolitical landscape echoes both the Cold War and pre-World War II eras. Whether the Russia-Ukraine War marks the first "hot" conflict of Cold War 2.0 or the prologue to World War III remains unclear and will only be determined in hindsight. Three Cold War flashpoints strikingly mirror today's geopolitical environment. The Korean War (1950-1953) featured nuclear threats and large-scale territorial shifts before settling into static lines. Hamas's surprise October 7 attack in 2023 parallels the Yom Kippur War (1973), both occurring on religious holidays almost exactly 50 years apart. The Cuban Missile Crisis (1962) saw rival superpowers face off over an island near one's coast.

Similarly, World War II occurred in a period following a global financial crisis when the zeitgeist favored isolationism in the U.S., and pacifism in Europe. As in present times, WWII witnessed an ascendant Asian power forming a pragmatic alliance with a revisionist European power. The beginning of WWII can be traced to regional wars in Europe (Spanish Civil War, 1936-1939) and Asia (Japanese invasion of Manchuria, 1931), mirroring the ongoing War in Ukraine and the looming Third Taiwan Strait Crisis.

As the U.S. rushes to nearshore the high-end semiconductor production chain and bolster its standoff and asymmetric capabilities, the defenses of the anti-China coalition continue to strengthen. As a result, President Xi Jinping's window to successfully move on Taiwan militarily is starting to close. History's red flags presage precarious times ahead.

SPHERES OF INFLUENCE

Conflict in the post-Cold War era largely revolved around the global political and economic order. Regardless of region, actors made decisions based largely on whether the U.S.-led international community would allow those decisions to pass, using military intervention and economic sanctions as sticks and integration into global capital markets as a carrot. The new era will move away from an internationalist framework into a framework governed by spheres of influence.

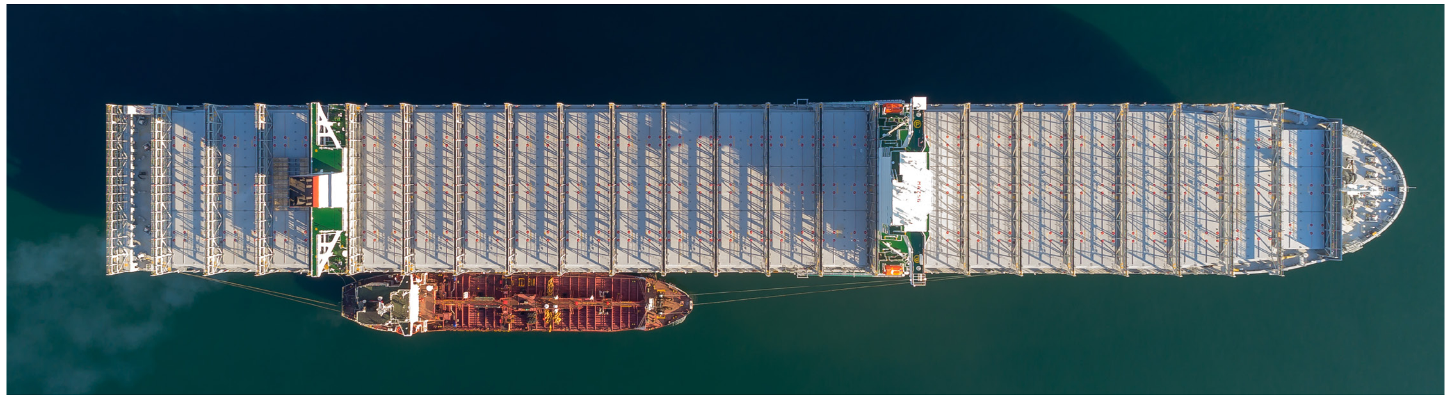
Today's geopolitical flashpoints arise from rival spheres of influence and the conflicts they generate. The Russia-Ukraine War, China's drive to assert sovereignty over Taiwan, the three-way struggle for dominance in the Middle East among Türkiye, Saudi Arabia, and Iran, and the United States' effort to assert influence in its near-abroad (Canada, Mexico, Panama, and Greenland) all exemplify this dynamic.

Understanding the new drivers of conflict is imperative to minimizing risk to assets and personnel as the patterns of insecurity shift both regionally and politically. Regions once considered stable could destabilize amid the reshuffling. Increased anti-American sentiment is likely to intensify where the aggressive pursuit of U.S. interests runs into local resistance and where leaders politically benefit from the rally 'round the flag effect.

END OF THE POST-YALTA ORDER

The United States is no longer the world's police, referee, banker, or "moral" arbiter. The intergovernmental institutions created to prevent a repeat of World War II's horrors—and their NGO partners—must now rely primarily on European funding. While structural flaws in the liberal international order have driven this shift for over a decade, the world has fully reverted to a "might is right" approach to dispute resolution, replacing the post-1945 "values-based" model.

In the post-Yalta era, weaker states are increasingly vulnerable to the ambitions of stronger nations. Great powers now have greater latitude to pursue their interests through military aggression and economic coercion, creating imbalanced relationships. This more anarchic environment incentivizes middle powers—such as Saudi Arabia, Türkiye, South Korea, Japan, and Iran—and countries neighboring great powers to prioritize "self-help" strategies. These nations are now more inclined to pursue previously taboo means of defense, including the development and use of cluster munitions, anti-personnel mines, and potentially even nuclear weapons.



DECOUPLING AND DEGLOBALIZATION

The post-Cold War neoliberal hypothesis that economic interdependence would make conflict unappetizing has been proven wrong. The West is now reversing course on economic integration at breakneck speed. Reliance on a potential adversary's economy is now an unmitigated liability, and self-reliance is a powerful asset. As such, reindustrialization and nearshoring are now high priorities.

Tariffs and trade barriers will become more prevalent as countries de-risk and great powers decouple, prioritizing sovereignty over financial growth. Supply chains are shifting from cost efficiency to geographic proximity, introducing new political and security risks. This geoeconomic shift is particularly evident in Latin America, where compliance risks are rising as drug cartels—deeply embedded in political economies—are designated as Foreign Terrorist Organizations (FTOs).

BOARDROOMS ON THE FRONTLINE

In today's conflicts, adversaries primarily target the private sector, stealing strategically important intellectual property (IP), penetrating critical infrastructure, and damaging, denying, or depleting components of the industrial base. This new landscape transforms firms into both offensive assets and defensive liabilities—acting as both sword and shield in the modern battleground.

Major economies like the U.S. and China recognize the catastrophic costs of direct conflict. This recognition drives them to seek decisive advantages that would predetermine the outcome of any potential war. They compete to secure overwhelming superiority in key strategic domains: resources, technology, industrial capacity, and military capability. Each side aims to gain such a clear edge that it overcomes its opponent's will to resist, effectively deterring conflict by making the result a foregone conclusion.

The private sector forms the foundation of a country's strategic potential, playing a crucial role in "holding ground" across key domains. Private enterprises operate critical infrastructure, extract raw materials, and conduct cutting-edge semiconductor research. In this contest of capabilities, adversaries target each other's private sectors to undermine strategic advantages. Attacking a rival's private industry has become a primary means of weakening their overall strategic position.

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