Beyond the Battlefield: Recalibrating Enterprise Cyber Risk in an Era of Geopolitical Escalation

Information Governance

Technology, Privacy, and eCommerce

Banner artwork by BlackWhiteMouse Design / *Shutterstock.com*

Cheat Sheet:

- **Identify parties at risk.** Critical infrastructure operators, defense contractors, supply chain vendors, academic institutions, and government agencies often face elevated cyber exposure during periods of geopolitical escalation.
- **Anticipate retaliation patterns.** Historical precedent suggests that kinetic or sanctions-based escalation between nation-states is frequently accompanied by increased cyber activity targeting civilian enterprises. Treat these events as enterprise-level risk triggers.
- **Recalibrate short-term defenses.** Organizations should validate monitoring, strengthen identity controls (including MFA), review incident response plans, and confirm insurance coverage when threat levels rise. These actions better align security with enterprise risk tolerances.
- **Strengthen long-term resilience.** Boards and executive leaders should embed geopolitical risk into governance oversight and continuous risk assessment to align risk exposure with enterprise decision-making.

Periods of geopolitical escalation are not merely political events; they are risk triggers for organizations across the private and public sectors. They require executive leaders and operational professionals to reassess whether their cybersecurity posture reflects the evolving threat environment.

Introduction

When geopolitical tensions escalate, cyber risks to civilian enterprises and public agencies often rise in parallel. Within hours of military strikes, sanctions, or other high-level confrontations, organizations frequently report elevated intrusion attempts, credential harvesting campaigns, distributed denial-of-service attacks, reconnaissance activity, and other malicious probing. In extreme cases, these attacks can cripple even highly-resourced global organizations (Reuters, “Saudi Arabia says cyber-attack aimed to disrupt oil, gas flow”).

Recent developments between the United States, Israel, and Iran illustrate this recurring pattern. Several days ago in February 2026, the United States and Israel engaged in military strikes targeting Iranian facilities, following months of intermittent escalation that began with the United States’ 2025 destruction of several Iranian nuclear enrichment sites (AP, “US and Israel launch a major attack on Iran”; CSIS, “What Operation Midnight Hammer Means for the Future of Iran’s Nuclear Ambitions"). While operational details continue to unfold, history suggests that kinetic events between nation-states are often followed by heightened cyber activity against non-military targets located outside military theaters.

For executive leaders and boards, the implication is immediate: Geopolitical conflicts do not remain confined to physical battlefields. Instead, they extend across cyberspace to affect faraway civilian enterprises and public institutions. While tensions involving Iran illustrate this dynamic, the underlying logic is not country-specific. Other nation-state actors — including Russia and China — have demonstrated similar cyber patterns in connection with geopolitical escalation (*e.g.*, CISA, “Nation-State Threats”). The question is not whether conflict will generate cyber risk, but whether an organization’s defenses are calibrated to withstand it.

This article identifies who faces heightened risk; explains why retaliation is foreseeable; and outlines both immediate and long-term measures organizations may consider during periods of geopolitical escalation.

Part 1: Identifying parties at risk

In times of heightened geopolitical tensions, certain organizations face elevated risk of attack and should consider temporarily elevating their defensive posture.

Based on recurring patterns discussed later in this article, the following organizations fall into the foreseeable “zone of fire.” They include those that are strategically significant, operationally adjacent to critical infrastructure, or are symbolically attractive targets:

- **Critical infrastructure sectors and defense contractors.** Iran has previously, and continues to, target defense contractors and critical infrastructure sectors such as energy, finance, telecommunications, and water (*e.g.*, CISA, “Cybersecurity Advisory”). These are highly favored targets due to their national importance (US Intelligence Community, “Annual Threat Assessment”).

- **Vendors and supply chains.** In addition to directly attacking defense contractors and critical infrastructure providers, Iran has also targeted organizations providing services to them. For example, in 2023, the Iranian-linked threat actor, “CyberAv3ngers,” exploited vulnerabilities in Israeli-made equipment used in US water systems (NPR, “Iran-linked cyberattacks threaten equipment used in U.S. water systems”). Academic institutions conducting federally funded research or supporting critical infrastructure initiatives may also face elevated exposure (USDOJ, “Nine Iranians Charged With Conducting Massive Cyber Theft Campaign”).
- **Government agencies.** Retaliation extends beyond the private sector and also impacts civilian government agencies. Following the 2020 death of Iranian General Qasem Soleimani by US forces, cyber attackers traced to Iranian IP addresses accelerated cyber-attacks against US federal, state, and local governments. According to Cloudflare, government agencies reported a 50-percent increase in attacks. Officials in Texas even reported encountering up to 10,000 intrusive scans per minute within hours of the strike (GovTech, “State & Local Governments Face Iranian Hacking Threats”).

Although the foregoing organizations are amongst those most targeted by Iran during periods of escalation, other nation-states have also prioritized these targets. Still, there are variations. Organizations seeking more tailored insight may consult a number of credible resources that summarize nation-specific threat patterns, including CISA’s nation-state threat advisories and the US Intelligence Community’s Annual Threat Assessment. These materials can help leadership evaluate whether their sector falls within a historically targeted profile (CISA, “Nation-State Threats”; US Intelligence Community, “Annual Threat Assessment”).

Part 2: Understanding why cyber retaliation is foreseeable

Nation-state cyber operations are not random acts of disruption. They are strategic tools used to project power, deter adversaries, preserve regime stability, and respond to perceived external aggression. This strategic logic explains why enterprise leaders should anticipate, and prepare for, retaliation during periods of global escalation. Put differently: Understanding the geopolitical context behind cyber-attacks enables enterprise stakeholders to become more effective risk predictors.

With that, the recent conflict between the United States and the Islamic Republic of Iran fits within a long-standing cycle of provocation and reprisal. Current events stem from the United States’ 2025 destruction of Iranian nuclear facilities, after which cyberattacks against private-sector organizations soon followed (AP News, “Iranian-backed hackers go to work after U.S. strikes”). This, itself, was a repeat of Iranian cyber retaliation after US forces killed Iran’s General Soleimani in 2020 (GovTech, “State & Local Governments Face Iranian Hacking Threats”).

But while modern cyber operations between nation-states command attention today, they represent the latest iteration of a broader, decades-long cycle of geopolitical escalation — an enduring dynamic that enterprise defenders should recognize and factor into their security and risk management programs (American Military University, “US-Iran Relations”).

> Understanding the geopolitical context behind cyber-attacks enables enterprise stakeholders to become more effective risk predictors.

Finally, the differences between the US and Iranian militaries play a role in explaining why that nation engages regularly in cyber activity. Historically, escalated conflicts between the two nations have been accompanied by heightened cyber activity as a form of “asymmetric warfare” — also called “irregular warfare” — a strategy in which combatants use unconventional tools to compete against stronger opponents (CSIS, “U.S. Adversaries and the Growth of Irregular Warfare”; Carnegie Russia Eurasia Center, “Iran’s Cyber Threat”). When direct military conflict poses unacceptable risk to a combatant, the use of cyber-attacks offers them a lower-cost alternative. Using proxies, such as criminals or hackers-for-hire, also offers the attacking nation a measure of plausible deniability.

With that in mind, anticipating that Iran may launch cyber-attacks in reprisal for the February 2026 attack is not speculation; it is history.

In cyber warfare, common options include:

- Credential harvesting and password spraying
- Website defacements or data leaks
- Distributed denial-of-service (DDoS) attacks
- “Wiper” data destruction malware
- Ransomware
- Supply chain compromise

Retaliation may also unfold over years. In 2012, a destructive “wiper” virus crippled 30,000 workstations at Saudi Aramco for weeks — an attack widely attributed to Iran and often linked to earlier Western cyber operations against its nuclear program (e.g., Congressional Research Service, “Iranian Offensive Cyberattack Capabilities”; CSIS, “Iran’s Threat to Saudi Critical Infrastructure”). In other cases, actors preposition malware that remains dormant until strategically activated (*e.g.,* CISA, “Countering Chinese State-Sponsored Actors Compromise of Networks”). Both models of delayed sabotage heighten uncertainty and complicate enterprise risk planning.

These multi-pronged strategies are not confined to any nation. Various geopolitical rivals have implemented comparable long-term cyber engagement strategies, reinforcing that escalation-driven digital activity is a structural feature of modern statecraft rather than a country-specific anomaly (US Intelligence Community, “Annual Threat Assessment”).

Against this backdrop, the relevant question is not whether geopolitical tension will produce cyber risk — but how organizations should respond when it does. The following steps are designed to reduce immediate exposure while strengthening ongoing operational readiness.

Part 3: Recalibrating short-term defenses

While long-term planning is ideal, taking certain immediate steps can deliver strong returns. To clarify: these suggestions are not mandatory requirements, but practical considerations for in-house professionals to align with their organization’s capabilities, resources, and priorities. Even during periods of global unrest, cybersecurity investments must be weighed against competing strategic demands.

Tier One: Validate foundational visibility and readiness

Before implementing new controls, organizations should confirm that existing safeguards are functioning as intended.

- **Confirm monitoring and logging are active.** Organizations should ensure that logging and alerting systems are enabled and reviewed. Even smaller organizations without dedicated security operations centers can confirm that alerts are being received and that notification pathways are clear.
- **Review incident response plans.** An incident response (IR) plan should define roles, escalation protocols, containment procedures, and communication pathways. Confirming that the plan reflects current personnel and reporting lines enables faster response. Similarly, identifying or pre-retaining a "breach coach" can also significantly reduce confusion during an active incident (Midwest Insurance Group, "The Role of a Data Breach Coach").
- **Review cyber insurance coverage.** Review insurance policies to determine whether incidents attributed to nation-state actors or their proxies are covered. Some policies contain "act of war" exclusions, which may limit recovery. Organizations should also determine whether they may pre-approve preferred vendors (e.g., forensics firms, crisis communications firms, breach coaches) with their carriers.

Tier Two: Address common retaliation tactics

Cyber threat actors routinely conduct reconnaissance, credential harvesting, and password spraying. Iran is no different, as seen in the U.S. Department of Justice's 2018 indictment of several Iranian nationals accused of successfully compromising over 100,000 accounts belonging to private sector organizations and government agencies (USDOJ, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign").

Because these campaigns often begin with credential abuse, organizations should determine whether there is a need to strengthen identity-based controls.

- **Strengthen password hygiene.** Confirm that your organization does not use easily guessed passwords (e.g., "February2026" or "Password123") – particularly in help desk-initiated password resets. Reset procedures should be reviewed to confirm that temporary credentials are strong and that administrative or privileged accounts receive enhanced safeguards.
- **Evaluate multi-factor authentication (MFA).** Consider whether MFA is enabled across critical systems. Implementing MFA may not be feasible in all instances due to technical or operational constraints. But farsighted leaders should make inquiries. Some legal regimes encourage, or may even eventually require, MFA (*e.g.,* EU, "NIS2 cybersecurity regulations," encouraging use of MFA "where appropriate").

Tier Three: Temporary posture elevation for mature programs

Organizations with established security operations may consider temporarily implementing further defensive measures during periods of heightened geopolitical tension. Potential options include:

- Increase monitoring cadence
- Extend log retention duration
- Validate identity governance controls
- Review IT (Information Technology) and OT (Operational Technology) segmentation

Finally, for those seeking further guidance, government agencies worldwide regularly issue threat

advisories and mitigation guidance. They may serve as useful reference points (*e.g.,* CISA, "Cybersecurity Alerts and Advisories").

> Even during periods of global unrest, cybersecurity investments must be weighed against competing strategic demands.

What to prioritize

If resource constraints require prioritization, consider focusing first on:

- **Visibility.** Confirm that monitoring and alerting systems are active
- **Prevention.** Validate critical identity controls, including password resets and MFA
- **Response.** Review incident response escalation protocols
- **Risk transfer.** Confirm cyber insurance scope for state-attributed attacks

Each organization's priorities and capabilities will differ. But these are prudent starting points spanning technical, business and legal domains.

Part 3, Continued: Recalibrating long-term defenses

Elevating risk posture in the short-term is important. But geopolitical cyber risk is not episodic; it is structural. Consider treating periods of escalation not as isolated events, but as opportunities to revisit strengthening long-term resilience.

Institutions may benefit from making the following programmatic investments:

- **Embed executive oversight and "tone from the top."** Cybersecurity is no longer solely an IT function. Maintaining periodic briefings to boards of directors and executive leadership on relevant geopolitical threat developments may better enable them to align security decisions with enterprise strategy. Similarly, consider incorporating strategic geopolitical escalation scenarios into executive tabletop exercises.
- **Institutionalize continuous risk assessment.** Cyber risk assessments should not be episodic compliance exercises. Organizations should consider revisiting threat models and risk registers in light of geopolitical developments, particularly when operating in sectors historically targeted by nation-state actors. Where appropriate, assessments may be conducted under attorney-client privilege to preserve candid internal analysis (Corporate Counsel Now, "5 Questions Corporate Counsel Should Ask About Cyber Risk Assessments").
- **Participate in intelligence sharing.** Various industries have stood up information sharing organizations designed to collectively enhance situational awareness for evolving cyber risks. Subject to legal and operational requirements, organizations may benefit by pooling information to meet common threats (Corporate Counsel Now, "How Information Sharing Organizations Help Businesses").

Part 4: Recalibrating beyond cybersecurity

This article focuses on recalibrating enterprise-level response in connection with foreseeable cyber-attacks — those deployed by nation-state actors during periods of escalation. But cyber risk rarely operates in isolation. Organizations maintaining a physical footprint in conflicted regions will need to reevaluate risks beyond cybersecurity.

In the short term, these organizations may need to reassess travel policies and personnel safety protocols, such as whether to relocate employees during an active conflict. Beyond that, organizational leaders may need to recalibrate business decisions against evolving geographic concentration risks, including whether to alter existing supply chains or to minimize business presence.

Part 5: Why recalibration matters

Geopolitical escalation is a foreseeable enterprise-level risk trigger for organizations operating in an interconnected digital economy. When nation-states exchange strategic threats or kinetic attacks, cyber activity often follows. The threat actor's identity may change across conflicts but the underlying pattern — escalation followed by cyber activity — remains constant.

Organizations that treat these moments as decision points — by validating defensive controls, reassessing monitoring practices, and aligning cybersecurity posture with enterprise risk — better position themselves to withstand both immediate disruption and delayed intrusion. Those that do not may find that heightened tensions expose vulnerabilities that were visible but unaddressed, resulting in public and regulatory scrutiny, operational disruptions, and financial loss.

> Nation-state cyber operations are not random acts of disruption.

For executive leaders and boards, this is not a technical issue, but one squarely involving governance. These moments present boards with an opportunity to confirm that their organizations maintain reasonable systems of reporting, compliance, and risk monitoring to manage mission-critical risks — a principle reflected in longstanding oversight doctrine (Harvard Law School Forum, "2024 Caremark Developments: Has the Court's Approach Shifted?"; *see also,* NYDFS, "Consent Order on Cybersecurity and AML Regulatory Violations").

This raises a final important governance question: when should board members begin their inquiries? Although oversight is essential, directors should avoid substituting their judgment for management's operational response. Allowing established escalation processes to unfold before requesting additional reporting reflects prudent governance. Afterwards, directors may engage through targeted inquiries — for example, whether insurance policies exclude state-attributed attacks or whether incident response plans require updating.

The primary takeaway: Elevated geopolitical risk warrants deliberate oversight, disciplined inquiry, and proportional response.

Conclusion

While geopolitical developments may appear external to enterprise operations, their cyber implications are inherently governance concerns. Enterprise leaders should treat escalation risk not as episodic crisis management, but as an input into enterprise risk appetite, capital allocation, and resilience planning.

Periods of escalation are therefore not merely moments of danger, but moments of decision. Leadership teams that use them to reassess exposure, validate defensive controls, and align cybersecurity investments with geopolitical realities will strengthen enterprise resilience. Those that treat them as distant political events may find that consequences hit closer to home than anticipated.

*(**Author's Note:** For practitioners seeking additional foundational guidance, ACC's Cybersecurity Toolkit for In-house Lawyers provides practical resources developed by ACC members).*

Join ACC for more cyber risk insights!

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its authors' employers, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

Robert Kang

Adjunct Professor

Loyola Law School, Los Angeles & USC Viterbi School of Engineering

Professor Robert Kang serves as adjunct faculty at the foregoing institutions. His role includes training the next generation of attorneys, CISOs and business leaders in meeting emerging technology and national security needs. He also provides corporate training. He is also a former in-house legal executive focusing on technology, cybersecurity and national security. Robert serves as a member of the ACC Foundation's Cybersecurity Advisory Board.

Visit his LinkedIn page.