CYBER THREAT INTELLIGENCE

CRITICAL**START®** Threat Research

TLP WHITE // [CS-TR-26-0101] Geo-Political Tensions Exploited for Cyberattacks

Executive Summary

Geo-political events increasingly shape the cyber threat landscape. State and non-state actors capitalize on periods of political tension to advance strategic objectives through cyber operations, often targeting governments, critical infrastructure, private enterprises, and civil society. Threat actors pursue agendas such as espionage, intellectual property theft, operational disruption, persistence, and influence campaigns, often intended to create leverage or prepare the environment for future physical, economic, or strategic action. In practice, these malicious agenda are actualized through malware deployments, technical vulnerability exploits, phishing emails or fraudulent communications that may reference current events, or security incidents to increase credibility and urgency. Government officials, corporate executives, journalists, policy analysts, and employees in strategically relevant industries are frequent targets due to their access and influence. Recognizing how geo-political events fuel both the agenda and influence the techniques of cyber threat actors is essential for anticipating adversary behavior, assessing organizational risk, and enhancing organizational resilience in an environment where political disputes routinely spill into cyberspace.

Introduction

Geo-political events increase both the likelihood, impact and complexity of cyberattacks on organizations. During periods of political or physical conflict, organizations in applicable critical sectors face sudden operational changes, compressed decision-making timelines, and exposed dependencies such as supply chains, third-party services, and critical IT or operational systems. These conditions create vulnerabilities that attackers exploit and make it harder to determine the intent, capability, and scope of malicious activity.

Cyber operations in this environment rarely occur in isolation. Reconnaissance, credential harvesting, and network intrusion may appear routine but are often strategically timed to take advantage of systemic vulnerabilities exposed by tension. Attribution becomes more difficult as overlapping campaigns and opportunistic attacks blur the lines between state-aligned, ideologically motivated, and financially motivated actors. Threat activity that seems low-impact may in fact signal pre-operational positioning or intelligence gathering, with consequences that extend beyond immediate technical compromise. A concrete example highlights this dynamic. According to Amazon's security team Iran-linked actors known as Imperial Kitten, also called Tortoiseshell, conducted reconnaissance on a commercial vessel by compromising its Automatic Identification System and onboard CCTV. Days later in 2024, Iranian-backed Houthi militants attempted a missile strike against the same ship. The key insight is that the cyber activity provided actionable intelligence that subsequently informed operational decisions. While this example involves a physical maritime attack, it illustrates a broader reality that cyberattacks during international events or conflicts can advance broader strategic objectives in ways not immediately visible.

For organizations, this means incidents that appear isolated or exploratory during periods of geo-political strain can carry outsized operational significance. Recognizing how attackers exploit human, technical, and procedural weaknesses under these conditions is critical. This sets the stage for examining access vectors, with social engineering emerging as a dominant method for gaining entry and exploiting organizational vulnerabilities during geo-political events.

Social Engineering as a Primary Attack Vector

Geopolitical tension creates conditions that significantly increase the effectiveness of social engineering cyberattacks against both individuals and organizations. Heightened attention to political events, rapid information sharing, and uncertainty surrounding unfolding situations reduce skepticism and increase engagement with unsolicited or emotionally charged messages. Threat actors exploit this environment by targeting users in spaces where geo-political discussions are already occurring, applying watering-hole-style tactics across social media platforms, forums, email, and messaging channels. Within these environments, attackers introduce weaponized content themed around sanctions, military activity, protests, or diplomatic developments. This content is delivered in familiar formats such as PDFs, documents, URLs, emails, or SMS messages and is designed to appear legitimate and time-sensitive. Interaction with such malicious content often result in credential harvesting, malware execution, payload delivery, or unauthorized access.

In addition to broad user-focused campaigns, attackers increasingly target organizations directly. Business email compromise (BEC) and similar tactics leverage geo-political pretexts to exploit organizational workflows, authority structures, and operational processes. Threat actors may impersonate government agencies, partners, vendors, or internal leadership, sending messages related to sanctions compliance, supply-chain disruptions, regulatory changes, or diplomatic developments. These messages can request urgent payments, credential verification, document review, or process approvals. Even in the absence of malware, such campaigns can yield unauthorized access, sensitive information, or operational disruption. Compromised endpoints, stolen credentials, or exploited workflows provide attackers with footholds for post-compromise activity, including lateral movement, persistence, intelligence collection, or influence operations.

Successful social engineering cyberattacks provides the initial access necessary to support a range of post-compromise objectives. Compromised user accounts or organizational systems enable attackers to operate within trusted environments, bypass perimeter defenses, and delay detection. This access may support data exfiltration, operational disruption, or further targeting of additional users and organizational processes. In geo-politically themed campaigns, social engineering functions not merely as an entry tactic, but as a strategic tool that facilitates access, persistence, influence, and disruption simultaneously. Threats may affect individual users, organizational decision-making, or operational continuity, making social engineering a critical concern for both personal and enterprise security in the context of geo-political events.

Targeted Sectors and Victim Profiles

Target selection in geo-politically influenced cyber activity is driven by strategic relevance, operational leverage, and downstream access. Targets are chosen based on how compromise, disruption, or exposure advances broader political or ideological objectives, rather than on ease of exploitation alone.

Public Sector Organizations

Organizations operating in critical sectors are consistently prioritized due to their systemic importance. Government institutions and defense contractors are targeted for their role in policy execution, military capability, and national security coordination. Energy and telecommunications providers are selected because disruption or surveillance within these sectors can directly affect economic stability, emergency response, and public confidence. Financial services and manufacturing entities are targeted for their economic influence, supply chain connectivity, and proximity to regulated or defense-linked ecosystems.

Private Sector Organizations

Private sector organizations are frequently targeted as intermediaries rather than end goals. Many attacks focus on service providers, suppliers, or technology partners that maintain trusted connections to higher-value networks.

Individuals within these organizations, including executives, engineers, administrators, analysts, and journalists, are targeted based on access, influence, or information exposure. In this model, victims are selected not for visibility, but for the position they occupy within interconnected political, economic, and operational systems.

Individuals of Interest

Victim profiles therefore extend across both organizations and individuals, but for different reasons. State-aligned actors often target individuals as access points, such as executives, engineers, analysts, or government employees whose credentials or communications enable deeper network penetration. Hacktivists are more likely to target individuals or organizations that represent symbolic value or public alignment with a geo-political position. Understanding these distinctions is critical for accurately evaluating threat intent, likely impact, and appropriate defensive response.

Distinguishing Cyber Threat Actors Based on Capability, Intent, and Opportunity

Geo-political tensions attract a diverse set of cyber threat actors with varying motivations and capabilities. Assessing their intent, technical skill, and the opportunities available to them is essential for predicting threat behavior, anticipating targets, and implementing effective defenses. The success and impact of cyber operations exploiting geo-political events depend on how an actor's capability, intent, and opportunity shape their choice of targets, methods, and the potential scale of disruption.

The capability-intent-opportunity framework allows a more precise understanding of risk. Capability determines the technical depth and scale of potential operations. Intent dictates the type of targets, tactics, and expected outcomes. Opportunity highlights when and where actors are most likely to strike. In combination, these factors explain not only the likelihood of attack but also its potential sophistication, persistence, and downstream impact. During periods of geo-political tension, this analytical lens helps differentiate between long-term strategic campaigns, ideologically motivated disruption, and opportunistic criminal activity, enabling defenders to tailor mitigation strategies according to actor profiles rather than assuming a uniform threat landscape.

Advanced persistent threats (APTs)

Advanced persistent threats are state-aligned actors with high capability, deliberate intent, and the patience to exploit vulnerabilities over extended periods. They are often backed, or strategically ignored, by their supporting governments to advance national objectives. APTs leverage sophisticated tools, social engineering, supply chain infiltration, and network persistence to maintain persistent access, prioritizing strategic positioning over immediate disruption. Reconnaissance for trade secret theft or business email compromise campaigns aimed at corporate takeover and infiltration are common tactics used to convert their resources into actionable intelligence or influence.

The 2025 leak of internal documents from the Chinese cybersecurity contractor KnownSec illustrates these dynamics. The materials show that KnownSec functions as a state-aligned cyber espionage entity, maintaining global reconnaissance systems, large datasets for precise targeting, and offensive tools for network and credential exploitation. This case highlights how modern APTs operate within vertically integrated ecosystems, combining technical capability, intelligence collection, and strategic awareness to advance state objectives globally. Overall, APTs demonstrate the convergence of capability, intent, and opportunity in geo-politically driven cyber operations, using careful planning and extensive resources to achieve long-term access and strategic advantage.

Hacktivists

Hacktivists are ideologically driven actors with high intent but generally more limited technical capability than APTs. Their objectives focus on symbolic impact, disruption, or influence rather than sustained access or intelligence collection. Geo-political crises amplify their opportunities by creating emotionally-charged narratives, highly visible platforms, and social tension that can be leveraged for attention and amplification. While hacktivists may lack tools for deep network penetration, they exploit open systems, social media, and public-facing infrastructure to disrupt operations, influence perception, or challenge targeted organizations.

Success is measured by visibility, reputational impact, and the amplification of a political message rather than stealth or persistence. A prominent example is Handala, a pro-Palestinian hacktivist group with a nationally symbolic name. The group targets Israeli organizations through phishing, data theft, extortion, and destructive malware attacks, often using multi-stage loaders and custom wiper malware for both Windows and Linux environments. Public disclosure through data leak sites amplifies their ideological message, though some claims are disputed by targeted organizations.

Hacktivists have also conducted highly visible, symbolic operations. Iran's state-run TV broadcast was temporarily hijacked via the Badr satellite on January 18, 2026, airing anti-regime messages from exiled figures, with a similar incident reported in June 2025. These cases demonstrate the ability of hacktivists to leverage crises and public attention; weaponizing cyberattacks for political messaging rather than long-term access or technical dominance. Overall, hacktivists operate at the intersection of high intent, opportunistic timing, and social leverage, exploiting periods of geo-political tension to maximize visibility and reputational impact.

Cybercriminals

Cybercriminals are opportunistic actors with variable technical capability, typically motivated by financial gain rather than political or strategic objectives. Their activity can intersect with geo-political events, incidentally, taking advantage of uncertainty, weakened defenses, and periods of operational disruption. Crises create opportunities through gaps in oversight, rushed digital transitions, and unmonitored communication channels, allowing cybercriminals to conduct ransomware, fraud, credential theft, and other financially-driven cyberattacks. While their operations are transactional, cybercriminal activity can still significantly disrupt critical sectors, especially when attacks coincide with periods of geo-political tension.

Large-scale criminal platforms illustrate the efficiency and reach of modern cybercrime. For example, RedVDS, a global cybercrime subscription service, enabled criminals to rent disposable virtual computers for as little as $24 per month, facilitating scalable and difficult-to-trace fraud campaigns. Coordinated legal action by Microsoft, in partnership with Europol, German authorities, and other international partners, disrupted RedVDS, which had been linked to approximately $40 million in U.S. fraud losses since March 2025, including high-profile cases against a pharmaceutical company and a real estate firm. This example highlights how cybercriminal infrastructure has become commoditized, enabling opportunistic actors to exploit systemic vulnerabilities for financial gain. Unlike APTs or hacktivists, success is measured in monetary terms rather than strategic or symbolic impact, but the consequences for organizations can be substantial.

While the capability-intent-opportunity framework gives a starting point of analysis, these categories are not absolute. Actors may shift behavior due to operational errors, last-minute strategic decisions, false-flag operations, or evolving political priorities. Motivations can overlap, with hacktivists and criminal groups occasionally advancing objectives that align with state interests, or APTs engaging in disruptive operations for signaling rather than intelligence.

Recent Geo-politically themed Threat Activity in the Last 6 Months

Over the past six months, geo-political tensions involving the United States and nations such as Venezuela, Iran, and Russia have intersected with cyber threat activity, highlighting how digital operations are increasingly tied to international conflict dynamics. Adversaries including Iran, China, and Russia remain among the most reported sources of cyberattacks targeting U.S. interests and allies. These activities often leverage real-world events to craft phishing campaigns, espionage operations, or influence efforts that exploit the confusion and urgency of evolving crises.

United States vs. Venezuela

In January 2026, researchers reported a spear-phishing campaign (T1566.001) that leveraged geo-political tensions between the United States and Venezuela to target U.S. government and policy organizations. Attackers distributed emails with a ZIP file titled "US now deciding what's next for Venezuela.zip," which contained a malicious DLL executed via DLL side-loading (T1574.002). The activity has been attributed with moderate confidence to the China-aligned threat group Mustang Panda, also tracked under names such as Earth Pret, HoneyMyte, and Twill Typhoon. The DLL installs the LOTUSLITE backdoor, a custom C++ implant capable of remote command execution, data exfiltration, persistence through Windows Registry logon keys, and other espionage functions. This campaign reflects a continued trend of geo-politically themed lures paired with reliable execution techniques to gain initial access and establish footholds in targeted environments.

Iran vs. Israel

Iran-linked threat actors have conducted operations against multiple Israeli sectors using new tooling and refined tradecraft. In a recent campaign identified by cybersecurity researchers, a backdoor known as 'MuddyViper' was deployed via a loader called 'Fooder', which disguises itself as a simple game and reflectively loads the payload into memory to avoid detection. MuddyViper enables reconnaissance, credential theft, browser data exfiltration, persistent access, and execution of arbitrary commands. This activity affected Israeli organizations across engineering, local government, manufacturing, technology, transportation, utilities, and universities, with at least one confirmed Egyptian target, and demonstrates an escalation in sophistication relative to earlier campaigns tied to the Iran-aligned MuddyWater group.

Russia vs. Ukraine

Between October and December 2025, Ukraine's defense forces were targeted in a campaign delivering the PLUGGYAPE backdoor malware. The activity was reported by the Ukrainian Computer Emergency Response Team (CERT-UA) and attributed with medium confidence to the Russia-aligned group Void Blizzard, also tracked as Laundry Bear or UAC-0190. Attackers first made contact through messaging apps such as Signal and WhatsApp, impersonating charitable organizations. They directed victims to fake websites hosting password-protected archives that contained malicious executables. Once executed, the malware installed a Python-based backdoor. It provided remote code execution, persistence via the Windows Registry (T1547.001), and communication over WebSocket and MQTT protocols (T1071). This campaign demonstrates evolving tactics in Russia-linked cyber activity. The actors combined social engineering, exploitation of trusted communication channels, and dynamic command-and-control infrastructure to enhance operational security and effectiveness.

Across these incidents, a consistent theme emerges. Threat activity closely tracks ongoing international conflicts, with adversaries exploiting real-world events to craft lures, gain access, and pursue intelligence objectives. Whether using political narratives to drive spear-phishing, novel malware to infiltrate critical sectors, or social engineering via trusted messaging platforms, recent campaigns show how quickly geo-political tensions are leveraged in cyberspace. These developments highlight the importance of anticipating threat patterns tied to evolving conflicts and adjusting defenses.

Implications for Organizations

Geo-politically driven cyber activity has significant consequences for organizations, extending beyond technical risks to operational, strategic, and reputational dimensions. Understanding these implications is essential for designing defenses that address both immediate threats and long-term exposure during periods of international tension. Organizations in critical sectors such as government, defense, energy, telecommunications, finance, and media face elevated risk because their networks, data, and influence are inherently valuable to state-aligned actors and ideologically motivated groups.

Private sector organizations outside these sectors can also be targeted indirectly through trusted connections, supply chain relationships, or digital infrastructure that provides access to higher-value entities. The nature of these attacks highlights the importance of human factors alongside technical defenses. Social engineering, phishing, and misinformation campaigns exploit trust, urgency, and routine behaviors. Employees at all levels, particularly those in strategic or operational roles, represent potential access points. Organizations must therefore invest in security awareness, verification processes, and incident response protocols that anticipate behavior-based exploitation.

Organizational Mitigation Strategies

Given ongoing geo-political tensions, organizations must adopt proactive, structured measures to reduce the likelihood and impact of cyber threats. Key strategies include:

- **Continuously monitor network and system activity:** Look for unusual login activity, anomalous data flows, unexpected account changes, or suspicious file behavior. Early detection is critical, as attackers often exploit rapidly evolving geo-political events to launch timely campaigns.
- **Maintain and update security policies and defenses:** Ensure endpoint protections, intrusion detection systems, and access controls reflect current threats and organizational priorities. Regular updates reduce exploitable vulnerabilities and enhance organizational resilience.
- **Educate employees on social engineering:** Human behavior remains a primary attack vector. Train staff to recognize phishing, business email compromise, fake communications, political-themed lures, and other manipulative tactics. Emphasize vigilance around critical assets, sensitive data, and operational systems, and simulate realistic attack scenarios to reinforce awareness.
- **Apply structured threat modeling:** Leverage frameworks like DAIN to identify and catalog critical assets, then map potential attack techniques, likely adversaries, and potential impacts. Factor in the organization's industry, geographic exposure, regulatory environment, and historical targeting patterns, then validate findings against threat intelligence from peers and sector-specific sources.
- **Engage in intelligence sharing through ISACs and peer networks:** Sharing indicators, observed tactics, and emerging threats with sector-specific Information Sharing and Analysis Centers improves situational awareness. Early warnings and coordinated response planning reduce blind spots and enhance resilience during periods of heightened geo-political activity.
- **Prepare incident response for multi-vector attacks:** Recognize that modern campaigns often combine social engineering, technical compromise, and operational disruption. Conduct tabletop exercises and communications drills to ensure continuity and minimize impact when attacks target multiple domains simultaneously.

Conclusion

Geo-political tensions shape the cyber threat landscape and increase risk for all organizations, particularly those in critical sectors such as government, energy, finance, telecommunications, and defense. Organizations outside formally designated critical sectors remain vulnerable because attackers exploit third-party connections, supply chain relationships, and less-defended networks to reach higher-value targets or cause collateral disruption.

Assessing exposure requires mapping assets, understanding how systems connect to partners and critical infrastructure, and evaluating how operations intersect with sector-wide risks. Threat modeling frameworks, employee training, intelligence sharing through platforms such as ISACs, and proactive defense strategies help organizations anticipate likely attack vectors and prioritize protections. Integrating these measures reduces operational impact, limits vulnerability to multi-stage campaigns, and strengthens resilience in a landscape where geo-political tensions increasingly drive cyber activity.

Further Reading

1. https://dti.domaintools.com/research/the-knownsec-leak-yet-another-leak-of-chinas-contractor-driven-cyber-espionage-ecosystem
2. https://www.welivesecurity.com/en/eset-research/muddywater-snakes-riverbank/
3. https://thehackernews.com/2026/01/lotuslite-backdoor-targets-us-policy.html
4. https://securityaffairs.com/187055/hacktivism/hacktivists-hijacked-iran-state-tv-to-broadcast-anti-regime-messages-and-reza-pahlavis-protest-appeal.html
5. https://www.cfr.org/global-conflict-tracker/conflict/confrontation-between-united-states-and-iran
6. https://www.iranintl.com/en/202506188310
7. https://thehackernews.com/2025/11/iran-linked-hackers-mapped-ship-ais.html
8. https://cybersecuritynews.com/ukraine-police-exposed-russian-hacker-group/
9. https://securityaffairs.com/186910/intelligence/cert-ua-reports-pluggyape-cyberattacks-on-defense-forces.html
10. https://www.csis.org/blogs/strategic-technologies-blog/beyond-hacktivism-irans-coordinated-cyber-threat-landscape
11. https://blogs.microsoft.com/on-the-issues/2026/01/14/microsoft-disrupts-cybercrime/
12. https://www.isaca.org/resources/news-and-trends/industry-news/2025/enhancing-asset-visibility-with-the-dain-methodology

IOCs and IOAs

PLUGGYAPE	https://cert.gov.ua/article/6286942
LOTUSLITE	https://www.acronis.com/en/tru/posts/lotuslite-targeted-espionage-leveraging-geopolitical-themes/
Handala	https://www.splunk.com/en_us/blog/security/handalas-wiper-threat-analysis-and-detections.html
KnownSec	https://dti.domaintools.com/research/the-knownsec-leak-yet-another-leak-of-chinas-contractor-driven-cyber-espionage-ecosystem
RedVDS	https://www.microsoft.com/en-us/security/blog/2026/01/14/inside-redvds-how-a-single-virtual-desktop-provider-fueled-worldwide-cybercriminal-operations/
MuddyWater/MuddyViper	https://www.welivesecurity.com/en/eset-research/muddywater-snakes-riverbank/