CYBER
THREAT
ANALYSIS

Recorded Future®

Insikt Group®

February 12, 2026

2026 State of Security

How Global Fragmentation Is Redefining Conflict Across Cyber, Crime, and Influence

Foreword

Uncertainty is not a phase or a trope. It is the operating environment. And this year, fragmentation is driving it.

As long-established norms unwind, fragmentation is paradoxically enabling greater interoperability across domains that were once distinct. As modern power struggles threaten institutions (such as international law), risk is moving across domains where there have historically been clearer boundaries (such as in cybercrime). State objectives, criminal capability, and private-sector technology increasingly reinforce one another in an interconnected environment. That convergence creates uncertainty, compresses warning time, and expands plausible deniability.

We saw this trend gain momentum in 2025. Kinetic conflict in Ukraine continued to generate digital spillover, influence activity, and criminal-enabling behavior that moved well beyond the battlefield. Regional escalation involving Israel and Iran showed how cyber operations, influence campaigns, and commercial surveillance tools can operate alongside military force. In Venezuela, state action blurred legal, political, and cyber boundaries, challenging assumptions about sovereignty and accountability.

In the digital domain, risk is moving to the edges. Insikt Group's reporting on RedMike highlighted disciplined pre-positioning in telecommunications infrastructure: access built selectively and held quietly for intelligence value by threat actors ready to pivot quickly when timing and pressure align. Cybercrime groups and mercenary spyware also aligned with national strategic objectives, with mercenary spyware pursuing the same persistent-access goals by embedding itself where oversight was weakest and adapting under pressure.

2025 was not a breakout year for AI-driven cyber operations. To separate hype from signal, we developed AIM3, our framework for assessing AI malware maturity. It shows that most observed use remains at an early stage of development. The immediate risk is not autonomous attacks, but verification failure at scale, where deception becomes faster, cheaper, and more convincing as AI is embedded into decision workflows.

Looking ahead to 2026, diplomatic friction, selective enforcement of norms, and accelerating technology adoption will continue to widen the gap between how risk is assumed to behave and how it actually behaves.

Intelligence does not eliminate uncertainty. It makes uncertainty manageable. This State of Security is our assessment of the year behind us and the threats ahead, written to help leaders reduce surprise, prioritize effectively, and act with confidence.

Levi Gundert
Chief Security & Intelligence Officer

Executive Summary

Fragmentation defined the global threat landscape in 2025, as selective enforcement of diplomatic norms and greater risk tolerance contributed to a volatile international environment.

Geopolitical fracturing was most evident in the conduct of major powers. The United States (US) adopted a more transactional approach to power, prioritizing dominance in the West over multilateral cohesion and further eroding long-standing security frameworks. This shift strained transatlantic relations and limited coordinated responses to crises, including support for Ukraine. In the Middle East, decisive US and Israeli military operations disrupted Iran's military capabilities and regional proxy network, while domestic unrest exposed the regime to an existential threat. Across other regions, renewed interstate violence illustrated how loss of confidence in diplomatic mechanisms can increase states' willingness to use force to settle long-standing disputes.

These geopolitical dynamics directly shaped state behavior in cyberspace. In 2025, Insikt Group tracked how cyber activity shifted from a primary focus on espionage toward increased use of cyber capabilities for signaling, coercion, and disruption in both kinetic conflicts and gray-zone scenarios. Securing access to identity systems, cloud environments, and edge infrastructure emerged as a central feature of interstate competition, reflecting the growing strategic value of persistent digital access and pre-positioning.

Disruption was equally visible in the information environment. Insikt Group observed hacktivist groups, patriotic volunteers, and influence networks playing a growing role in conflicts involving Israel–Iran, India–Pakistan, Thailand–Cambodia, and Russia–Ukraine. These threat actors operated with varying degrees of state alignment, but consistently contributed to a threat landscape in which genuine intrusions, exaggerated claims, and disinformation reinforced one another.

In the cybercriminal realm, sustained law enforcement pressure fractured large criminal enterprises without eliminating them, resulting in a more decentralized, modular, and resilient criminal environment. At the same time, large-scale scam operations in Southeast Asia demonstrated how geopolitical fragmentation and weak governance can create permissive environments for industrialized cybercrime.

Technological change further shaped the risk landscape, as advances in artificial intelligence accelerated automation and lowered barriers to entry for both state and criminal threat actors, while expanding attack surfaces related to identity, data integrity, and human–machine interaction. At a strategic level, increasing competition to develop advanced models is setting the scene for future fragmentation as the US and China race for AI dominance in military technology and international market share.

Looking ahead, the trends observed in 2025 point to a 2026 threat environment in which simultaneous regional crises are likely to become the norm, and cyber pre-positioning and decentralized criminal ecosystems will drive activity that deepens identity abuse and increases systemic risk from both emerging and legacy technologies. Effective risk management in the year ahead will depend on resilience, adaptability, and the ability to operate amid persistent uncertainty.

Key Findings

- **The fragmentation of the international order contributed to the escalation of conflict.** Weakening international institutions and alliances led states to take riskier actions — up to kinetic strikes — to advance their objectives against geopolitical rivals. Supporting activity played out in cyberspace as states expanded espionage targeting and established persistence in critical infrastructure networks.
- **Russian APT targeting of the US and Canada increased compared to 2024.** While activity continued targeting Ukraine, the Baltics, and non-NATO Eastern Europe, Russia expanded operations into the Western hemisphere. From a tradecraft perspective, Russian threat actors shifted to techniques optimized for stealth, deniability, and durability.
- **Influence operators and hacktivists created feedback loops amplifying favorable conflict narratives.** As military conflicts escalated, hacktivists claimed credit for disruptive attacks against adversary nations. These claims were amplified by influence operations, alongside other narratives promoting their side's version of the conflict.
- **Insikt Group identified 289 new ransomware variants this year, a 33% increase from the previous year.** The majority of these new variants originated from leaked source code and builders for existing ransomware families. Despite the increase in variants, overall ransomware payments declined.
- **Threat actors introduced three new malicious large language models tailored for cyber operations.** While the newer models reflect operational maturity in presentation and usability, they improve efficiency and accessibility of existing techniques rather than introduce novel AI-driven tradecraft.

Table of Contents

Section I: Geopolitical Fragmentation and the Emerging Global Disorder

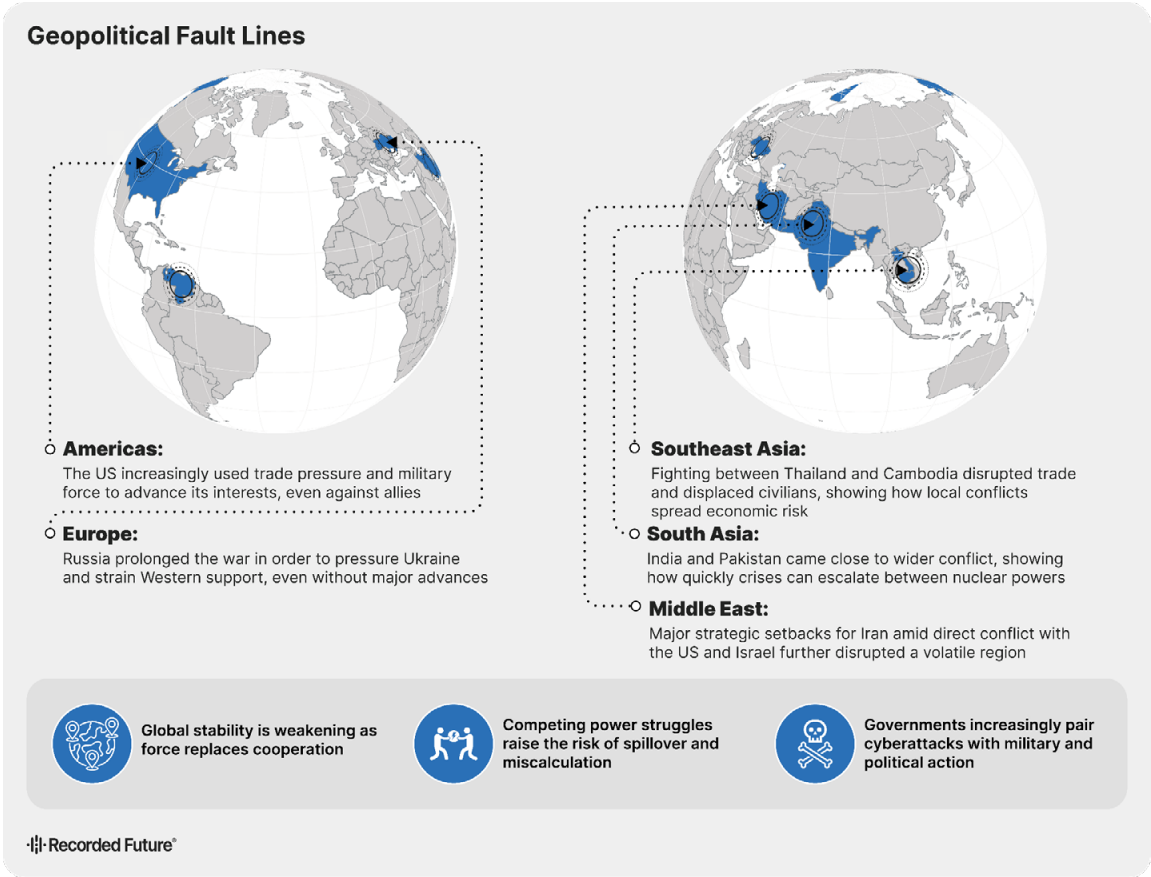


Figure 1: *2025 redefined international relations (Source: Recorded Future)*

The international geopolitical order fragmented in 2025, as hard-power competition, transactional diplomacy, and more frequent testing of geopolitical red lines became defining features of state behavior. Protracted conflicts such as Russia's war in Ukraine and the Israel–Iran confrontation underscore how sustained hostilities are increasingly being used to manage escalation, enable hybrid activity, and shape long-term strategic positioning. Renewed crises also demonstrated an increased willingness to exploit perceived gaps in US regional crisis management.

Across these flashpoints, cyber operations increasingly became an integral part of kinetic conflict. States deployed cyber capabilities to collect intelligence ahead of military action, pressure political leadership, intimidate civilian populations, and shape how events were interpreted by domestic and international audiences. Cyber reconnaissance and pre-positioning activity increasingly blurred the line between preparation and attack, increasing the risk of miscalculation during crises.

As a result, 2025 marked a structural shift away from deterrence-based stability toward an international system in which preemptive action, hybrid coercion, and escalation below the threshold of war became normalized. This shift increases the likelihood that geopolitical crises will spill over into corporate networks, supply chains, regulatory environments, and digital infrastructure with limited warning. Organizations that anticipate this risk and invest in operational resilience against short-notice disruption, degraded connectivity, and third-party failure will be better positioned to sustain operations in an increasingly volatile global environment.

Ongoing Conflicts: Protracted Wars and Escalation Management

Russia Holds Strategic Advantage in War with Ukraine, Despite Battlefield Struggles

In 2025, Russia entered the fourth year of its full-scale war against Ukraine, with Moscow likely maintaining a strategic advantage despite minimal territorial gains. The Institute for the Study of War (ISW) assesses that Russian forces only seized about 4,669 square kilometers (just over 1,800 square miles) over the year. The Kremlin appears confident that holding occupied territory and sustaining active hostilities effectively blocks Ukraine's path to NATO accession. Moscow's maximalist negotiating terms repeatedly stalled peace talks, almost certainly reflecting a strategy of using prolonged pressure to weaken Ukraine while testing Western unity and alliance resolve over time.

Russia continued to rely on long-range strike campaigns, with drone attacks central to sustaining pressure across Ukrainian cities and logistics hubs. These strikes often coincided with high-level diplomatic engagements, such as the London Summit on Ukraine in March, and direct talks between Ukrainian and Russian officials in July as part of the US-facilitated negotiations, very likely intended to signal that Moscow retains control of the battlefield.

In parallel, Russian state-sponsored cyber threat actors maintained persistent pressure on Ukrainian and NATO-aligned critical infrastructure, particularly in the energy, logistics, and communications sectors, to collect intelligence, map networks, and position themselves for potential disruptive action. This approach allowed Russia to impose costs well beyond the physical front line, extending the conflict's pressure into civilian life, allied infrastructure, and European security planning.

Russia is likely to remain focused on consolidating control over Ukraine, especially the remaining parts of the Donbas. However, Russia's limited territorial gains suggest its forces likely lack the capability to seize and hold significantly more ground in the near term. As a result, Moscow will likely intensify coercive measures short of decisive battlefield breakthroughs, including disruptive cyber operations against Ukrainian critical infrastructure, drone strikes on its civilian centers, and efforts to stoke unrest, to pressure Kyiv and extend influence deeper into western Ukraine. Russia is also highly likely to step up its hybrid warfare activities across Europe, reinforcing its ability to impose costs well beyond the physical front line while managing escalation risk.

Preventive Strikes and the Israel–Iran Power Shift

While Russia's war in Ukraine illustrates how prolonged conflict is used to impose sustained pressure without decisive escalation, events in the Middle East in 2025 revealed a contrasting trend: the increasing normalization of preventive military action to manage long-term strategic risk.

Hostilities between Israel and Iran ramped up significantly in June, culminating in a twelve-day conflict that altered regional security dynamics and upended strategic deterrence calculations for the rest of the year. The escalation followed the International Atomic Energy Agency's determination on June 12 that Iran was non-compliant with its nuclear obligations, after which Tehran announced new enrichment activities. Israel's Operation Rising Lion, launched on the following day, reflected long-standing efforts to constrain Iran's future military and nuclear capabilities through the use of force under deteriorating diplomatic conditions. The campaign, supported by US airstrikes on facilities at Fordow, Natanz, and Isfahan, killed Islamic Revolutionary Guard Corps (IRGC) commander Hossein Salami and several other senior

officers and nuclear scientists. It also damaged key elements of Iran's nuclear infrastructure, air defenses, and missile forces, likely delaying program timelines while complicating Tehran's ability to coordinate military or proxy operations in the short term.

The incident marked the first direct US attack on Iranian territory and the first US strike against another state's nuclear program. While Iran's long-term nuclear ambitions likely remain unchanged, the attacks reinforced a shift toward decisive force to forestall future threats. Additionally, the lack of a kinetic response from Iran's regional proxies, with the exception of the Houthis, underscored the deeply weakened position of Iran's proxy networks and a key pillar of its asymmetric warfare doctrine. Tehran's decision to fire at the US's Al-Udeid Air Base in Qatar, the largest American base in the region, reflected the widening regional implications for the deeply entrenched Iran–Israel hostilities.

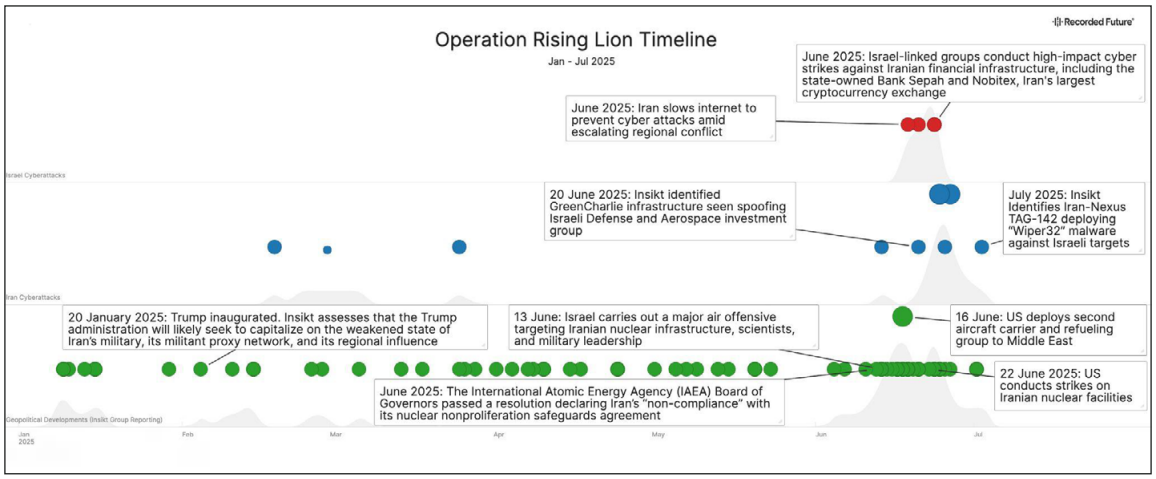


Figure 2: *Recorded Future Intelligence Operations Platform timeline showing key events leading up to Operation Rising Lion, including notable cyberattacks that Insikt Group tracked and reported on (Source: Recorded Future)*

Iran is now seeking to address exposed vulnerabilities by acquiring new air defense systems and reorganizing elements of its security apparatus, though recovery will likely be slowed by renewed snapback sanctions and international isolation.

Domestic instability is further constraining Iran's recovery. On December 28, 2025, mass protests erupted amid a deepening economic crisis and growing dissatisfaction with the regime, marking its most serious internal challenge since 2022–2023. Anger is increasingly directed at Supreme Leader Ali Khamenei, whose regional influence and alliance network have eroded. Even if the regime reasserts control, setbacks to Iran's nuclear program and the fragmentation of its proxy network — aligned non-state actors Tehran uses to project power — have shifted the regional balance of power away from Iran, increasing uncertainty as emerging powers compete for influence and the US selectively projects force.

Emerging and Reignited Conflicts

Geopolitical Tensions Boil Over in South Asia

Tensions between India and Pakistan reignited in May 2025 following the killing of 26 tourists near Pahalgam in Indian-controlled Kashmir, amid a broader rise in violence by Pakistan-backed insurgents. The attack triggered a sharper escalation than the 2019 Pulwama incident and reflected a growing willingness on both sides to act preventively based on perceived intent rather than imminent threat, increasing escalation risk between two nuclear-armed states.

On May 7, India launched Operation Sindoor, striking what it described as terrorist infrastructure across Pakistan, including sites in Punjab Province. Pakistan responded with drone and missile strikes the next day, escalating rapidly over 48 hours to include Pakistani ballistic missile launches against Indian military sites and Indian strikes on multiple Pakistani air bases, including one near Islamabad.

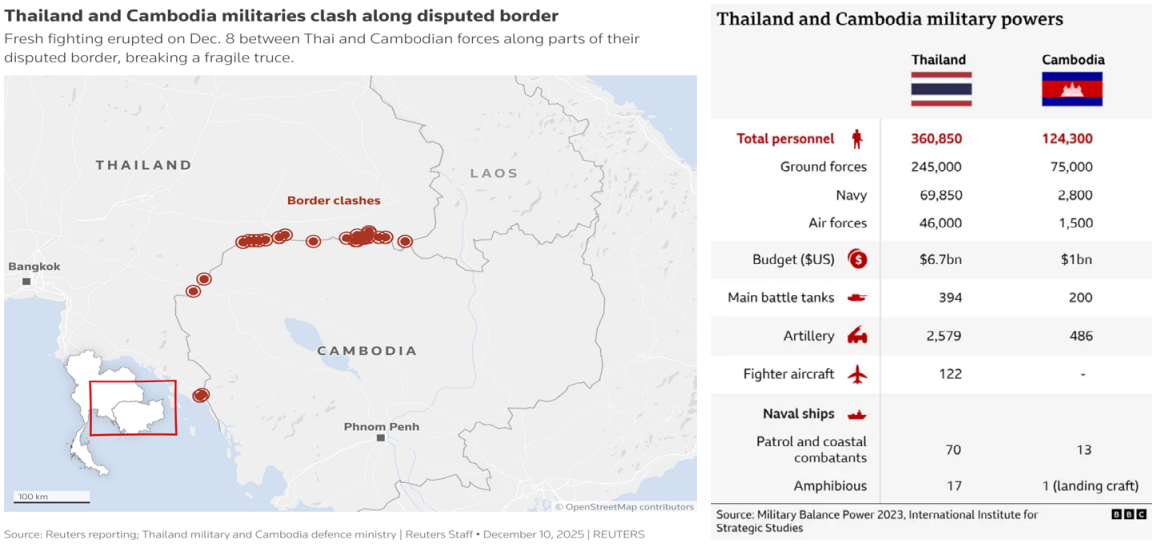
Pakistan's decision on May 10 to convene its National Command Authority, a clear nuclear signal, helped prompt intensified diplomacy and a subsequent US-brokered ceasefire. Inconsistent public messaging from Washington during the early stages of the crisis likely contributed to miscalculation and later strained US–India relations.

Cyber operations expanded alongside kinetic escalation. Following the Pahalgam attack, Pakistan-linked APT36 (Transparent Tribe) conducted sustained espionage against Indian government and defense personnel, likely as preparatory activity to collect sensitive information and establish access during heightened tensions. Concurrently, the India-linked SideWinder group conducted targeted espionage across South Asia, focusing on government, defense, and financial institutions in Pakistan, Sri Lanka, and Bangladesh, with activity observed throughout the first half of 2025 and notable spikes in January, February, and April. Based on the timing and scope of both campaigns, Insikt Group assesses that cyber operations were likely embedded as preparatory and enabling mechanisms alongside the emerging conflict.

Thai-Cambodian Border Crisis Drives Violence, Threatens Regional Stability

Tensions between Thailand and Cambodia rose sharply in mid-2025 as long-standing border disputes flared into open conflict, reflecting a broader shift toward coercive, preventive action over dispute resolution. A fatal clash near Chong Bok on May 28 derailed bilateral talks and contributed to the political collapse of Thai Prime Minister Paetongtarn Shinawatra. On July 24, both militaries exchanged fire at multiple points along the border, triggering the most intense fighting in nearly fifteen years. The brief conflict left at least 48 dead and displaced hundreds of thousands before a ceasefire took hold on July 28. Subsequent incidents in November, including a reported mine explosion that injured a Thai soldier, exposed the fragility of the truce and reinforced incentives on both sides to maintain forward-deployed forces as a deterrent.

Hostilities resumed in early December with expanded scope and intensity, driving further civilian casualties and displacement. A second ceasefire on December 27 halted military operations and froze troop movements. However, confidence-building measures, including Thailand's release of eighteen Cambodian soldiers captured during the July fighting, failed to address the underlying territorial dispute, leaving the crisis unresolved as the year ended.



Figures 3 and 4: *Border clash flashpoints between Thailand and Cambodia in December 2025 (left) (Source: Reuters) Comparisons between Thai and Cambodian armed forces (right) (Source: BBC)*

Both Thailand and Cambodia signaled intent to abandon the Joint Boundary Commission, the main dispute resolution mechanism since 2000, raising the likelihood that future crises will be managed through force, economic pressure, and signaling rather than negotiation.

The economic fallout, particularly for Cambodia, was severe. Thailand's closure of border checkpoints caused Cambodia's cross-border trade to collapse by 99%, falling from 92.1 billion baht ($2.83 billion USD) in the first seven months of 2025 to just 10 million baht ($319,000 USD) in August. Cambodia, which relies heavily on Thai tourism and remittances from its workers in Thailand, faced deepening financial strain as an estimated 800,000 Cambodian laborers returned home. The crisis demonstrated how localized conflicts in a fragmenting regional order can rapidly generate humanitarian, trade, and cyber risk, particularly to border management systems, financial institutions, and critical infrastructure.

Strategic Realignment Beyond Conflict Zones

America Reasserts Dominance in the Western Hemisphere

Throughout 2025, the US adopted a more primacy-focused approach toward the Western Hemisphere, prioritizing territorial control, resource security, and unilateral enforcement over alliance coordination and consensus. President Trump repeatedly framed the annexation of Greenland, a Danish territory, as a strategic priority, explicitly declining to rule out the use of force. This rhetoric was reinforced by a March visit by Vice President JD Vance to a US military base in Greenland, a trip cut short amid protests from Greenlandic and Danish officials. Similar assertions directed at Canadian territory, combined with coercive US trade policy, drove relations with Ottawa to historic lows. While these disputes remained mostly rhetorical, the assertion of territorial claims over NATO allies marked an unprecedented departure from post-WWII alliance norms and signaled a willingness to pressure partners to advance US strategic objectives.

US policy toward Latin America has been even more dynamic. In August, the president signed a classified order designating major drug cartels as foreign terrorist organizations, expanding the legal basis for direct military action beyond traditional law-enforcement frameworks. Since then, US forces have conducted more than two dozen kinetic strikes against

suspected drug-trafficking vessels in the Caribbean and Eastern Pacific, resulting in over 100 fatalities. Legal ambiguity surrounding these operations prompted several US partners, including the United Kingdom (UK), to restrict intelligence sharing to avoid potential complicity, straining long-established security relationships.

The US also escalated pressure on Venezuela through aggressive sanctions enforcement, including the seizure of multiple oil tankers accused of sanctions evasion, and President Trump made multiple comments threatening military action in Venezuela due to the Maduro regime's alleged role in supporting drug traffickers, culminating in the operation in January 2026 to capture and extract Venezuelan President Nicolás Maduro to face drug trafficking charges in court. Together, these actions demonstrated a readiness to deploy unprecedented US military operations in pursuit of hemispheric dominance, even at the expense of diplomatic and intelligence cooperation.

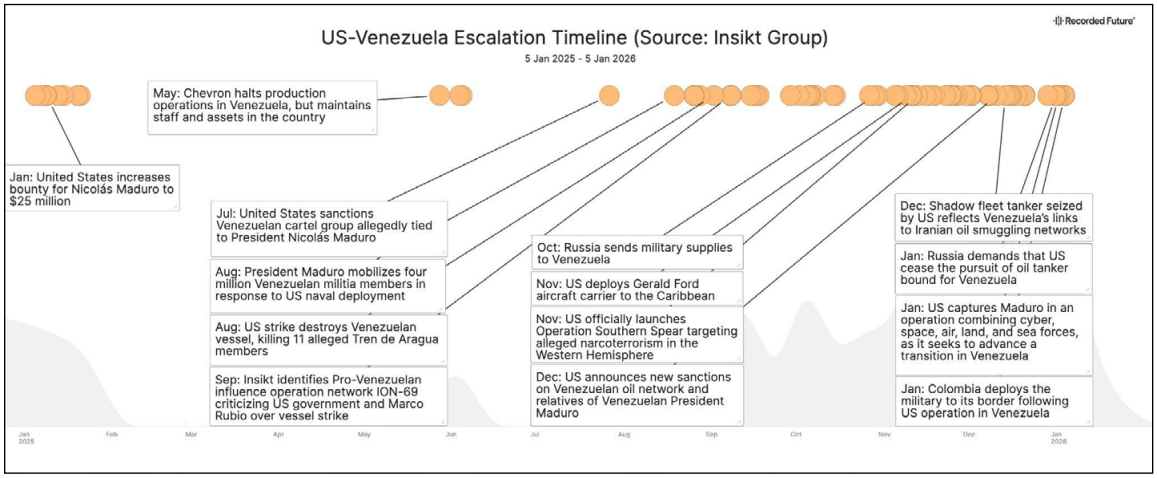


Figure 5: *Timeline showing Insikt Group reporting on key events in 2025, leading up to the capture of Venezuelan President Nicolás Maduro (Source: Recorded Future)*

Collectively, US actions in 2025 placed the greatest strain to date on the post-WWII alliance system among Western democracies. This shift was codified in the US National Security Strategy, which explicitly reframed US security priorities around hemispheric control while omitting prior emphasis on democracy promotion. The combination of coercive trade policy, unilateral military action, and reduced reliance on multilateral mechanisms increased geopolitical volatility across the hemisphere and elevated second-order risks, including diminished intelligence-sharing, legal uncertainty for partners, and increased exposure to cyber operations targeting energy infrastructure, maritime trade, sanctions enforcement systems, and migration networks.

Looking Ahead

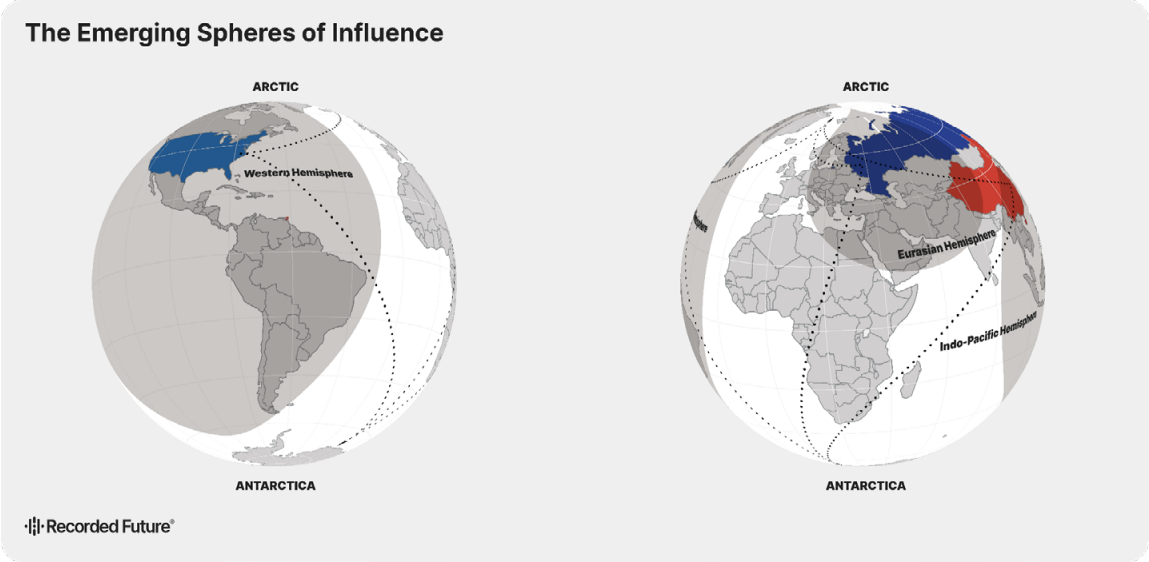


Figure 6: *Summary of emerging global disorder focused on spheres of influence (Source: Recorded Future)*

Looking ahead, the geopolitical dynamics observed in 2025 point toward a more fragmented and risk-tolerant international system defined by competing spheres of influence, declining restraint, and fewer effective guardrails.

The US 2025 National Security Strategy formalized a shift toward hemispheric priorities and narrower strategic objectives, reducing the predictability of security guarantees and weakening the stabilizing role of alliances and multilateral institutions.

Other powers have adjusted accordingly. China increasingly relies on coercion short of war, combining cyber espionage, economic leverage, legal claims, and gray-zone military activity to advance interests while managing escalation risk, simultaneously framing this approach as that of a stabilizing, responsible power in an increasingly fragmented world. Russia continues to pursue protracted conflict and hybrid warfare to impose sustained costs beyond the battlefield. Regionally, states such as Israel, India, and Pakistan have demonstrated a greater willingness to act preventively, reflecting declining confidence in diplomacy and crisis mediation.

This diffusion of power has increased systemic complexity. Risk is now driven less by coordinated expansion from a small number of threat actors and more by simultaneous, often uncoordinated actions across multiple regions. Parallel militarization trends in Europe, Canada, Japan, and South Korea further crowd the security environment, increasing the likelihood of miscalculation, spillover, and unintended escalation.

Across these dynamics, cyber operations and economic instruments, sanctions, tariffs, trade disruption, and asset seizures have become routine tools of geopolitical competition. This dynamic is already visible in regions such as Central Asia, where Russian and Chinese interests are beginning to collide. At the same time, the US, China, and Russia are accelerating their presence in the Arctic and Antarctica, regions rich in critical minerals and strategically important shipping channels essential to emerging technologies and global trade. The cumulative effect is an international system with higher tolerance for risk and fewer constraints on escalation. For governments and businesses alike, resilience rather than stability is now the baseline operating assumption.

Section II: State-Sponsored Cyber Operations amid Geopolitical Fragmentation

Figure 7: *Summary of 2025 state-sponsored cyber activity (Source: Recorded Future)*

While kinetic conflicts dominated headlines in 2025, some of the year's most consequential state-sponsored activity unfolded in digital environments. Rather than relying on destructive attacks, the four most capable and consistently active hostile state cyber threat actors tracked by Insikt Group — China, Russia, Iran, and North Korea — focused on the covert accumulation of access to identities, networks, and edge infrastructure. This allowed them to blend into normal operations while preserving options for sustained intelligence collection and rapid disruption should geopolitical tensions escalate.

State-sponsored cyber risk was not confined to these major powers, however. The continued proliferation of commercial spyware further lowered barriers to entry, enabling states with less mature cyber programs to conduct sophisticated surveillance and intelligence operations targeting end-user devices rather than enterprise networks.

This activity occurred amid the accelerating geopolitical fragmentation described in the previous section. As international norms weakened, alliances strained, and red lines became less clear, incentives for restraint in cyberspace continued to erode. For organizations, the primary risk is no longer a single, large-scale cyber incident, but sustained pre-positioning that enables persistent espionage in peacetime and creates latent capacity for disruption during periods of crisis. The sections that follow examine how individual state-sponsored threat actors operationalized this approach over the past year.

China

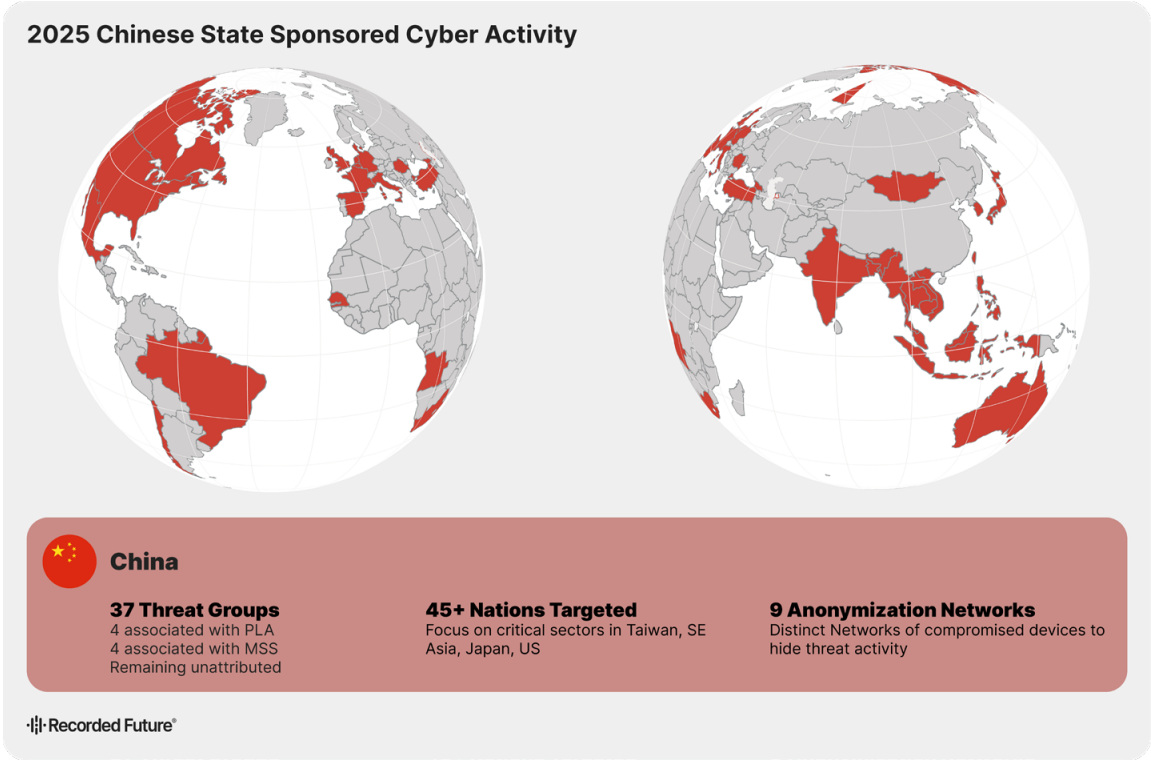


Figure 8: *Data from Recorded Future's Network Intelligence showing countries targeted by China in 2025 (Source: Recorded Future)*

In 2025, Chinese state-sponsored cyber activity continued to prioritize long-term access and strategic positioning over immediate disruption. Chinese threat actors consistently targeted infrastructure that provides durable vantage points, particularly telecommunications networks and public-facing perimeter systems.

Recorded Future data indicates that network devices and VPN appliances, including those from Fortinet, Ivanti, Cisco, Citrix, and Palo Alto, have become primary targets for exploitation, reflecting a broader shift toward edge infrastructure as organizations harden their endpoints and migrate workloads to the cloud.

In early 2025, Insikt Group identified a campaign exploiting unpatched Cisco IOS XE devices linked to telecommunications providers worldwide. Tracked as RedMike (also publicly reported as Salt Typhoon), the campaign targeted more than 1,000 devices across more than 100 countries. However, this represented only about 8% of exposed Cisco devices, indicating deliberate targeting of high-value assets rather than indiscriminate scanning.

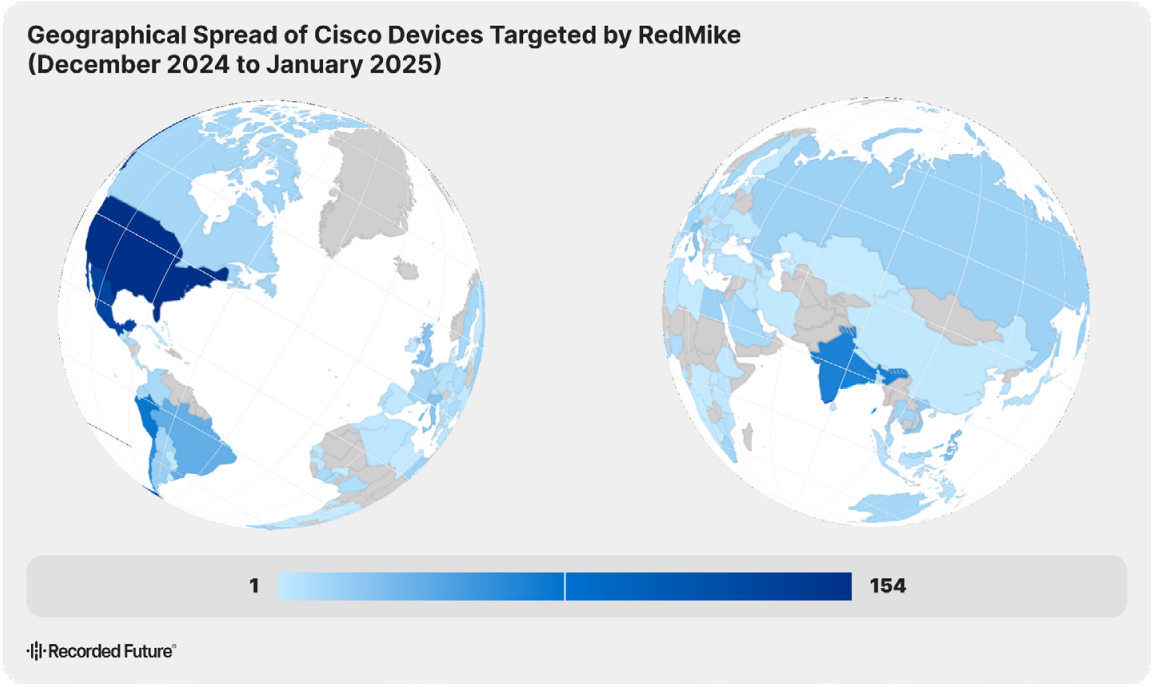


Figure 9: *Geographical spread of Cisco devices targeted by RedMike, as identified by Insikt Group in December 2024 and January 2025 (Source: Recorded Future)*

Poorly monitored and slow-to-update perimeter systems continue to provide reliable entry points for attackers. Chinese operators consistently focus on identifying and exploiting vulnerabilities in network gateways and access infrastructure, with new edge-device flaws often exposed after their likely use in China-linked campaigns. Gaining control of network gateways and access infrastructure allows Chinese operators to maintain hidden access, limit an organization's visibility into its own networks, and retain the ability to collect intelligence or disrupt operations if geopolitical tensions escalate. This strategy reflects a deliberate effort by Beijing to quietly position itself inside critical infrastructure while reducing the risk of detection and avoiding overt activity that could trigger political or military escalation.

In 2025, targeting patterns increasingly mirrored national policy priorities. Manufacturing and semiconductor companies were targeted more frequently, aligning with China's drive for technological self-sufficiency and its efforts to counter US-led export controls. Government agencies and departments — especially those with links to economic development and foreign policy — as well as think tanks and independent research organizations, remained familiar targets, and law firms and financial institutions were also in focus, indicating an interest in regulatory, legal, and policy insight that can be leveraged to shape economic strategy and strengthen China's position in international negotiations.

Taken together, Chinese cyber activity in 2025 reflected a strategy focused on the quiet accumulation of strategic advantage across critical sectors and infrastructure, a posture designed for long-term competition rather than short-term impact.

Russia

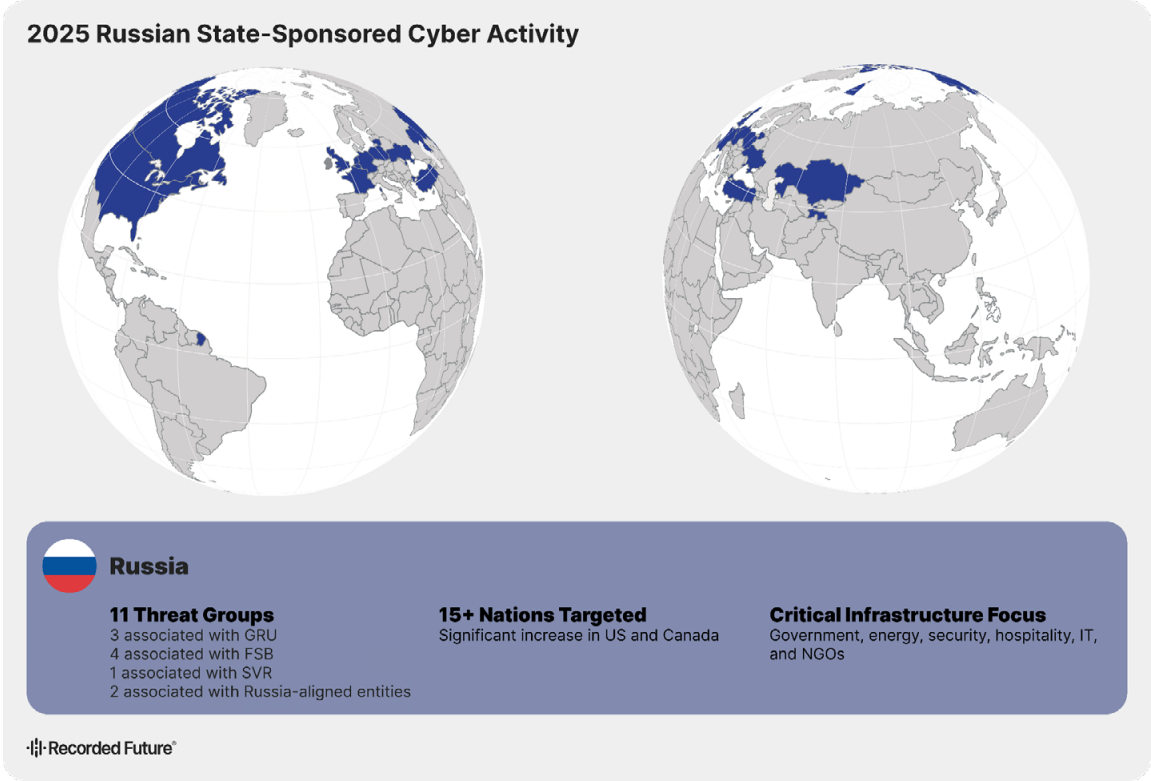


Figure 10: *Data from Recorded Future's Network Intelligence showing countries targeted by Russia in 2025 (Source: Recorded Future)*

In 2025, Russian state-sponsored cyber activity followed an access-first approach similar to that of other major powers, but with a stronger emphasis on maintaining readiness for disruption. Email and collaboration platforms, including Roundcube, Zimbra, and Microsoft Exchange, remained dominant targets due to their access to sensitive communications and credentials. At the same time, exploitation of network perimeter devices (such as Fortinet, Citrix, and Cisco) and enterprise middleware (including JetBrains TeamCity, ConnectWise, and Openfire) expanded, signaling a broader strategy aimed at initial access, lateral movement, and long-term persistence.

GRU-linked clusters, including BlueDelta and Sandworm, intensified operations against critical national infrastructure (CNI) in Ukraine and NATO member states, reflecting a strategy that prioritizes future operational flexibility over immediate impact.

- **BlueDelta** sustained large-scale credential harvesting against governments, defense institutions, energy researchers, and IT providers, enabling continuous intelligence collection.
- **Sandworm** maintained its focus on operational technology (OT), targeting energy, water, and heating providers in Ukraine and allied states, while expanding into supply-chain and logistics-linked sectors.

By stealing credentials and maintaining persistent access to cloud, email, enterprise, and critical infrastructure networks, Russian threat actors have positioned themselves to shift quickly from intelligence-gathering to operational disruption with little additional effort. This approach is also comparatively low-cost and agile, relying on disposable credential-harvesting infrastructure rather than bespoke malware that is expensive to develop, short-lived, and more

easily attributed once deployed. As a result, warning timelines are significantly shortened, attribution and response are complicated, and cyber operations become a more effective coercive tool, particularly amid the war in Ukraine and elevated tensions with NATO.

Beyond these core clusters, Insikt Group recorded eleven distinct groups, such as BlueAlpha and BlueEcho, that actively target North America, Ukraine, Central Asia, the Baltics, Europe, Japan, and Australia. Victimology spanned governments, CNI, NGOs, local authorities, and higher education and IT sectors, reflecting a broader effort to undermine NATO and European Union (EU) cohesion. Compared to 2024, Russian activity increased against North America, with heightened focus on the US and Canada, alongside sustained targeting of Ukraine, the Baltics, and non-NATO Eastern Europe.

From a tradecraft perspective, Russian threat actors optimized for stealth, deniability, and durability while retaining familiar access and execution techniques. Recorded Future data showed an approximately 70% year-over-year increase in the use of application layer protocol and web protocols, indicating a growing reliance on encrypted, web-native command-and-control channels. Core techniques such as phishing and social engineering remained stable, while abuse of command and scripting interpreters increased by roughly 27%, reflecting continued reliance on scripting for post-compromise automation and persistence.

Taken together, Russian cyber activity in 2025 reflects a shift from isolated, high-profile attacks to persistent, low-visibility access. In a more fragmented and crisis-prone security environment, this approach likely reduces warning time for potential disruptive operations against critical national infrastructure and could complicate containment by enabling rapid activation from pre-positioned access and increasing the risk of cascading effects across interconnected systems.

Iran

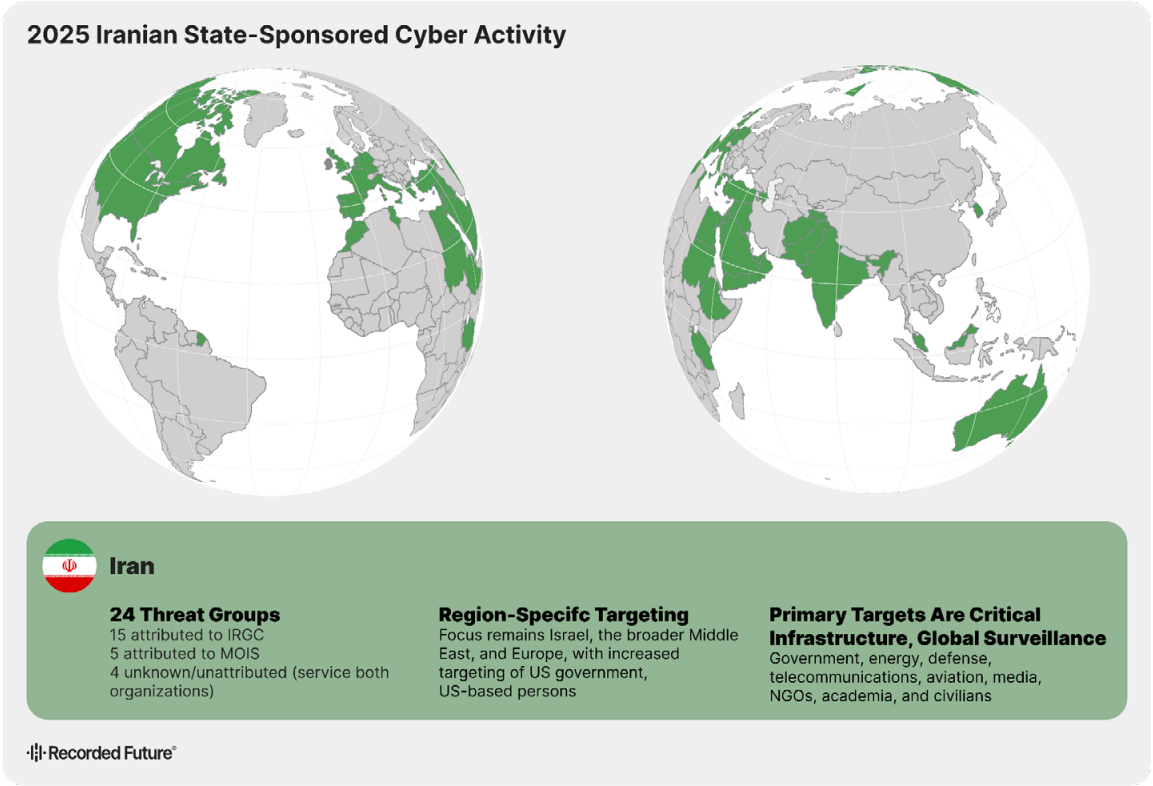


Figure 11: *Data from Recorded Future's Network Intelligence showing countries targeted by Iran in 2025 (Source: Recorded Future)*

In 2025, Iranian state-linked operations also focused on stealth, identity-driven access, and low-visibility tradecraft, but remained firmly shaped by Tehran's regional priorities. Israel was the central focus, although Iranian threat actors also targeted governments, telecommunications providers, and policy organizations across Europe, North America, and parts of Africa and Asia.

Iran relied on a combination of state-sponsored cyber groups, proxy groups, and semi-autonomous hacktivist fronts to conduct espionage, hack-and-leak operations, intimidation, and influence campaigns. Iran-aligned fronts such as Handala and Cyber Toufan publicly claimed data thefts and system compromises against Israeli entities, pairing selective disclosures with coordinated media campaigns to maximize psychological and reputational impact while maintaining a plausible distance from the Iranian state (see Section III for more detail).

Activity targeting Israel combined disruption and influence operations with recurring claims of CNI compromise. IRGC-affiliated Cyber Av3ngers repeatedly asserted access to Israeli industrial control systems (ICS) and programmable logic controllers (PLCs), often citing Israeli-made or Modbus-exposed assets. These claims coincided with seasonal #OpIsrael campaigns, sustained distributed denial-of-service (DDoS) activity, and website defacements, reinforcing a continuous pressure environment below the threshold of open conflict.

This ecosystem was reinforced by lesser-known hacktivist brands such as UNIT 1948, which circulated claims of attacks against industrial and fuel-monitoring systems via social media. These narratives often relied on imagery generated during scanning or probing activity using publicly available tools, creating the appearance of operational impact without confirmed compromise. Although several referenced technologies had known vulnerabilities, independent corroboration of exploitation remained limited as of late 2025. Observers should therefore distinguish between high-volume, low-impact public claims and verifiable, material intrusions when assessing Iranian cyber operations.

Iranian cyber operations shifted away from broad reconnaissance and the reuse of stolen credentials toward more targeted, web-based intrusions. These operations relied on link-based lures, web-native payloads, and lightweight scripting to establish access and control, enabling faster execution with less infrastructure and lower visibility. The result is a more efficient operating model that sustains tempo while reducing cost, exposure, and the risk of attribution.

North Korea

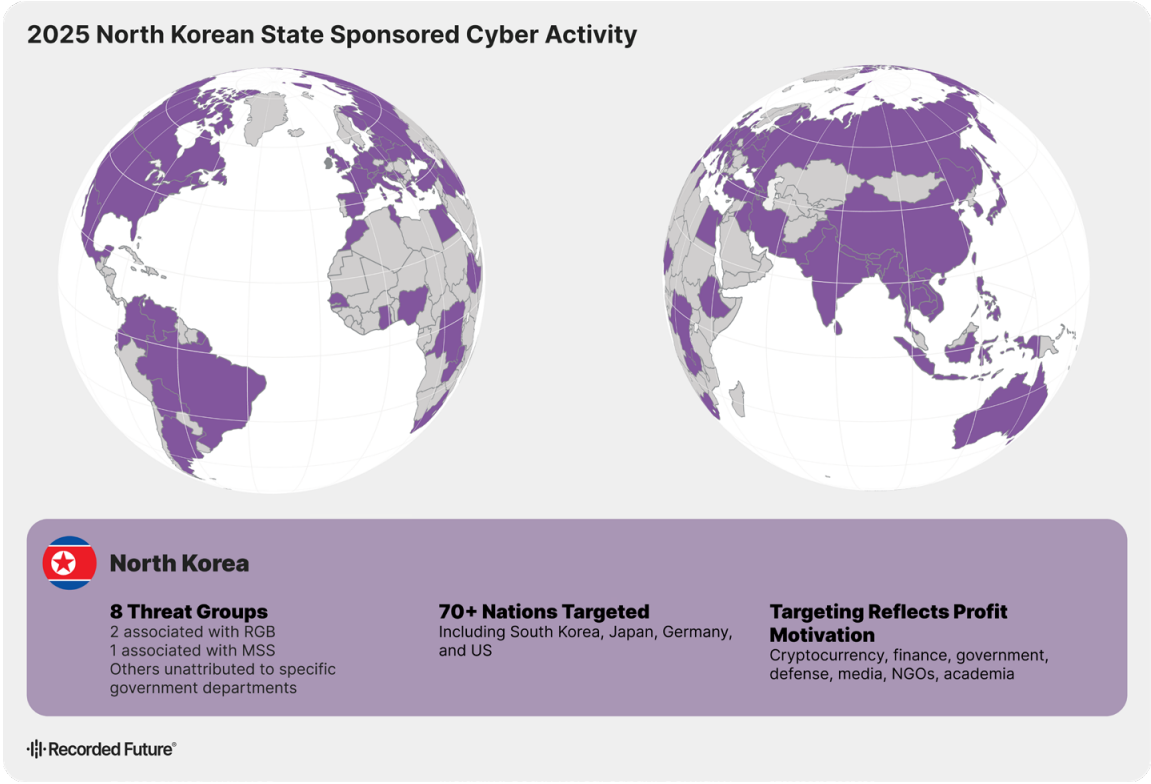


Figure 12: *Data from Recorded Future's Network Intelligence showing countries targeted by North Korea in 2025 (Source: Recorded Future)*

In 2025, North Korea's cyber activity remained focused on revenue generation while increasingly integrating espionage objectives. Recorded Future identified six active North Korean threat groups conducting global operations, primarily targeting South Korea, Japan, Pakistan, India, the US, and Europe.

Cryptocurrency theft remained the most consistent activity, with eighteen recorded incidents, almost certainly intended to offset the economic constraints imposed by prolonged international sanctions. At the same time, intrusions against government, defense, and IT providers expanded compared to 2024, indicating that financially motivated operations increasingly operated alongside traditional espionage.

This convergence was reflected in the targeting of manufacturing, energy, and telecommunications organizations in Japan, Taiwan, and the US, signaling growing interest in industrial and strategic intelligence beyond immediate monetary gain.

Espionage activity remained closely aligned with geopolitical priorities, including the sustained targeting of diplomatic missions, government agencies, and policy stakeholders in South Korea, as well as expanded operations in Central Asia, particularly in Uzbekistan.

A defining feature of North Korea's activity was its continued reliance on fraudulent remote IT worker schemes. Operatives obtained employment at foreign companies under false identities, turning hiring and contractor processes into an access vector. Once embedded, threat actors used stolen credentials, often harvested from password stores, to maintain persistence, exfiltrate data, generate revenue, and conduct espionage. Campaigns such as "Contagious Interview," attributed to the PurpleBravo cluster, exemplified this model, using

social engineering, fake job offers, and trojanized development tools to deploy malware across Windows, macOS, and Linux environments. This approach reduced reliance on conventional intrusion pathways while complicating detection and attribution.

Overall, North Korea's cyber program remains uniquely resilient because it treats access as both an intelligence asset and a revenue stream. This dual-use model enables the DPRK to sustain operations despite sanctions, law enforcement pressure, and infrastructure disruptions.

Commercial Spyware

Consistent with the access-first model discussed above, governments are increasingly augmenting their cyber capabilities with commercial spyware, with as many as 80 governments worldwide having reportedly purchased such tools. While these products are marketed for legitimate law enforcement and national security purposes, their use outside those frameworks is broadly viewed as illegitimate and has persisted despite sanctions, export controls, and public scrutiny. In response to law enforcement pressure, established vendors adapted their business models, while new providers entered the market, contributing to a more fragmented and less regulated commercial spyware ecosystem, suggesting that the potential for abuse of sophisticated commercial spyware tools is likely to persist.

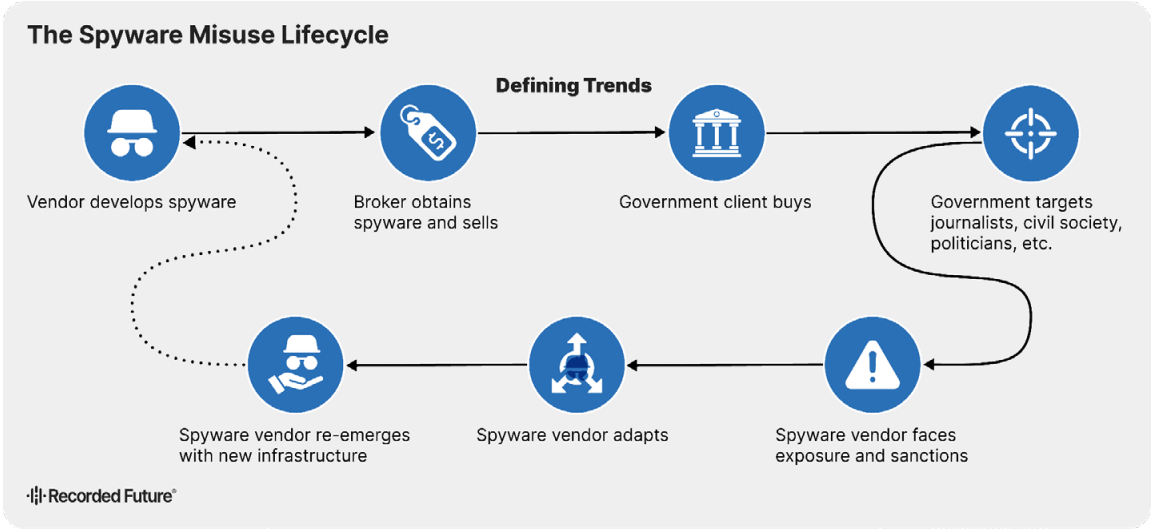


Figure 13: *Summary of spyware lifecycle (Source: Recorded Future)*

Following high-profile disclosures and US sanctions against the Intellexa consortium, activity linked to its Predator spyware initially declined, suggesting short-term disruption. However, Predator did not disappear. By mid-2025, Insikt Group observed renewed activity, including a newly identified government client in Mozambique, marking the first Predator-linked deployment associated with that country. Similarly, Israel-based Candiru, the developer of the DevilsTongue malware, maintained an active operational footprint despite being added to the US Commerce Department's Entity List. Insikt Group identified a significant number of Candiru-linked infrastructure clusters, many of which are likely still active across multiple regions.

Spyware vendors relied on techniques observed in 2024, designing their technical architectures to evade detection and takedown. Predator deployments, for example, continued to route command-and-control traffic through content delivery networks such as Cloudflare, masking origin infrastructure and complicating attribution and network-based blocking. DevilsTongue similarly employed layered infrastructure, including intermediary servers and region-specific routing paths, to obscure operator locations and reduce forensic traceability.

New vendors entered the market, filling gaps left by sanctioned providers. Israeli firm Paragon Solutions emerged as a notable competitor, with researchers confirming the first forensic cases of its Graphite spyware being used in the wild in April 2025. Paragon's emergence reinforced the notion that sanctions and exposure reshaped the market, but did not reduce demand; instead, they accelerated fragmentation and vendor churn.

Despite vendor claims of lawful use, abuse remained widespread. Graphite's use was confirmed in attacks against European journalists, including cases tied to zero-click iMessage exploit attempts. Amnesty International documented continued misuse of Pegasus spyware against journalists and activists in Serbia, marking the third known instance of such abuse. Predator activity was likewise linked to political surveillance across Europe, Africa, and the Middle East, while Candiru-linked infrastructure appeared to support campaigns targeting dissidents in Saudi Arabia and Azerbaijan.

International efforts to restrain abuse intensified but produced uneven results. The Pall Mall Code of Practice (CoP), launched by the UK and France in 2024, emerged as the primary multilateral effort to establish norms regarding the use of spyware. By September 2025, 26 countries had signed on, committing to transparency, oversight, and human rights safeguards. The framework remains non-binding and excludes many of the states most implicated in spyware abuse, limiting its immediate effect and sustaining a parallel market beyond regulatory reach. Notably, in late 2025, the US Department of the Treasury (USDT) removed sanctions on three executives previously targeted for their roles in Intellexa-related spyware activities, a reversal that may influence future enforcement.

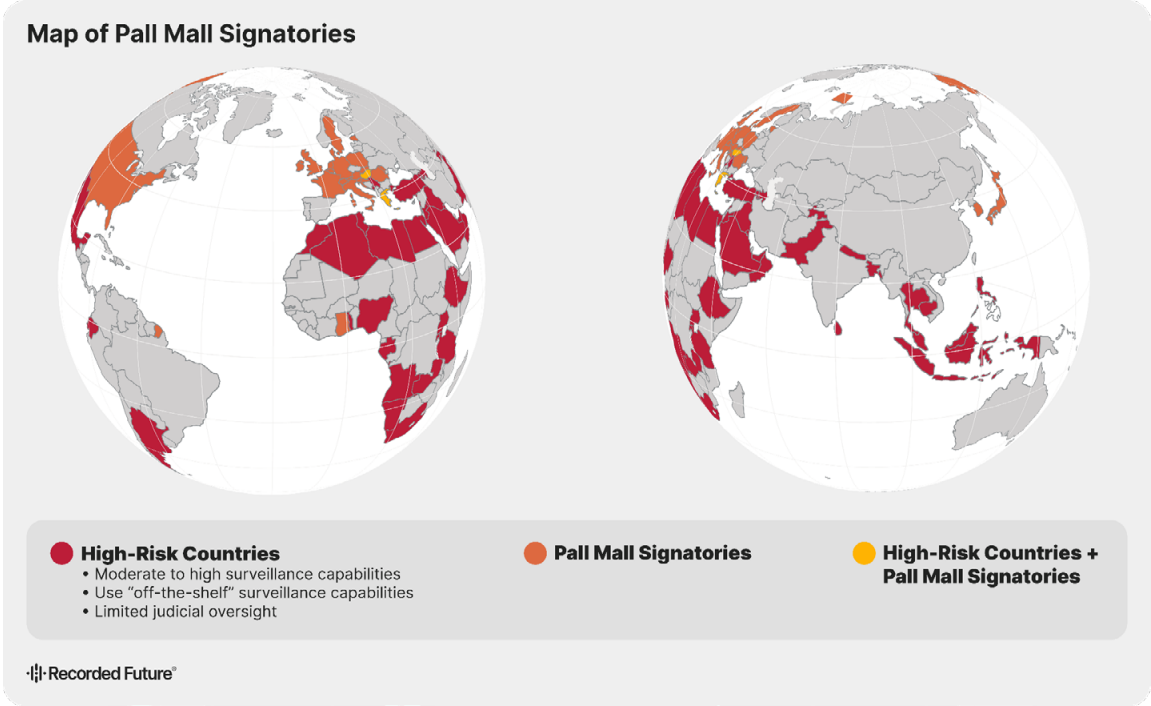


Figure 14: *The commercial offensive cyber capability industry will likely split to serve either Pall Mall signatories (in dark blue) or markets at high risk of abusing commercial surveillance tools (in red) (Source: Recorded Future)*

Technical and platform-level defenses showed some promise, particularly for high-risk users. Features such as Apple's Lockdown Mode demonstrated that hardened configurations can disrupt certain spyware vectors, including zero-click exploits. However, these protections require opt-in adoption and impose usability trade-offs, limiting their impact at scale.

Overall, the 2025 commercial spyware landscape highlighted both the impact and limits of global countermeasures. Sanctions and scrutiny forced vendors to adapt rather than exit, while new entrants sustained demand for offensive surveillance capabilities.

Looking Ahead

Looking ahead to 2026, state-sponsored cyber activity is likely to further consolidate around access-first, low-visibility operations designed to shape the strategic environment well in advance of overt conflict. Rather than prioritizing disruptive attacks, leading threat actors will continue to focus on persistent access, influence, and optionality.

Chinese state-sponsored threat actors are expected to expand beyond data exfiltration into AI-enabled narrative flooding aimed at shaping digital information environments. Beijing has advanced doctrines centered on AI-driven psychographic targeting, designed to erode adversary resolve through emotionally tailored influence operations that complement ongoing infrastructure-focused intrusions.

Russian state-sponsored threat actors are likely to continue moving away from malware-heavy campaigns in favor of credential-based intrusions and the abuse of legitimate services, particularly identity and single sign-on (SSO) platforms. This approach enables rapid escalation from espionage to disruption while preserving deniability and complicating detection.

Iranian cyber activity is expected to remain regionally focused and influence-centric, relying on hacktivist proxies to amplify messaging and apply sustained pressure below the threshold of armed conflict. While more disruptive operations cannot be ruled out, especially in the context of regional escalation, there is limited evidence to suggest a near-term expansion into widespread, high-impact operations outside the Middle East.

North Korean cyber operations are likely to further integrate workforce infiltration and supply-chain manipulation, using fraudulent hires, shell companies, and insider access to manipulate codebases, suppress patches, exfiltrate data, and generate revenue across SaaS, DevOps, and software supply-chain environments. The scale and aggressiveness of this activity will continue to be shaped by sanctions pressure and access to foreign technology.

Beyond the activity of these “Big Four” threat actors, commercial spyware will remain a key enabler of state-sponsored cyber risk. In the absence of binding international controls, misuse against journalists, activists, and political opponents is likely to persist, with the market continuing to fragment as vendors reposition to serve customers operating outside emerging regulatory frameworks.

How Recorded Future Can Help

State-Sponsored Threats

To counter state-sponsored targeting, organizations need continuous visibility into evolving state-nexus campaigns and the ability to connect threat actor behavior to defensive priorities.

- **Geopolitical Intelligence** provides country and facility risk monitoring through risk scoring across five categories and automated alerts when risk events occur near monitored facilities. (See **video**.)
- **Threat Intelligence** tracks state-sponsored APT groups in real time, surfacing targeting patterns, TTPs, and infrastructure for proactive threat anticipation. (Take a **tour**.)
- **Malicious Traffic Analysis** detects communication between your infrastructure and known command-and-control (C2) IPs. (Take a **tour**.)
- **Attack Surface Intelligence** identifies which network devices and VPN appliances are internet-facing, helping organizations remediate high-impact exposures before they are exploited. (Take a **tour**.)

Section III: Hacktivism and Influence Operations in Modern Conflict

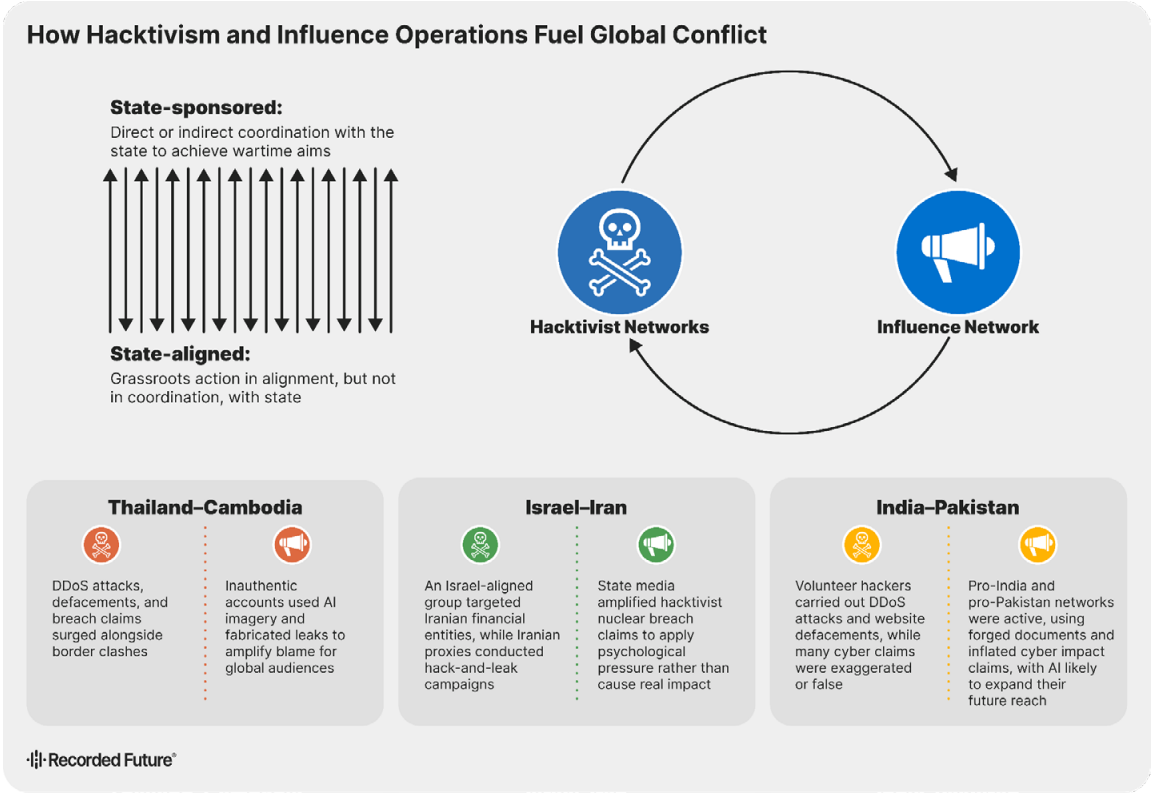


Figure 15: *Summary of hacktivism and influence operations (Source: Recorded Future)*

Amid the geopolitical fragmentation described in Section I, hacktivists and influence campaigns played an active role in amplifying discord. The outbreak of conflict was frequently accompanied by supporting (and in some cases, very likely coordinated) online campaigns. The level of state involvement in these campaigns likely varies, even within the same conflict. Some "hacktivist" groups are highly sophisticated and likely operate in coordination with the state. Other groups advance their countries' interests over their adversaries, but are neither coordinated nor sophisticated, and are likely to have closer links to other hacktivist or criminal groups than to the government.

While hacktivist and influence operations rarely have a significant impact on conflict outcomes, these strategies still provide advantages to the state they are supporting. First, hacktivists can carry out more aggressive hacking operations on a state's behalf, such as stealing sensitive data or launching disruptive attacks. Hacktivists provide deniability to the state, potentially limiting both retaliation and constraints under the law of armed conflict. Second, hacktivists and influence operations increase the perception of grassroots public support, helping one cause portray itself as more popular than the other. Finally, relying on patriotic volunteers is a relatively low-cost and resource-effective approach.

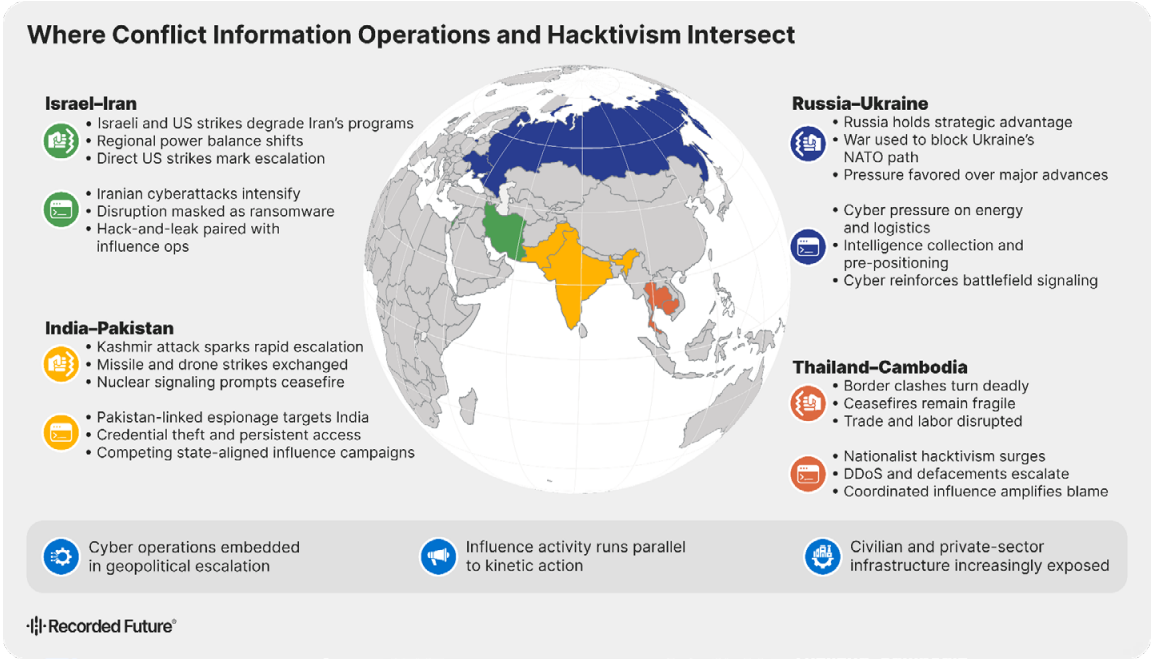


Figure 16: *2025 map of global conflicts with overlapping hacktivism and influence operations (Source: Recorded Future)*

Israel–Iran Cyber Warfare Expands Beyond the Twelve-Day War

The Israel–Iran conflict illustrated the growing synchronization of state-sponsored cyber, hacktivist, and influence operations to project strength, undermine the adversary, and shape perceptions beyond the battlefield. Predatory Sparrow, a cyber threat group aligned with Israeli government national security objectives, conducted cyber operations targeting the Iranian financial sector in an effort to disrupt funding for the IRGC. These attacks occurred during the June 2025 conflict between Israel and Iran alongside an escalation in hacktivist activity on both sides. Predatory Sparrow has been linked to other disruptive attacks in Iran in the past, often in retaliation for Iranian cyberattacks or proxy threat activity. The group is suspected to operate under the direction of the Israeli government, though there has not been definitive proof of the connection.

The hack-and-leak arm of Iran's hybrid cyber operations front has been highly active throughout 2025, as witnessed by multiple anti-Israel and anti-US campaigns involving claims of theft of sensitive data, its manipulation or selective exposure, and public distribution through aligned media channels to maximize reputational or political damage. For example, after a hacktivist group claimed to have stolen thousands of documents from Israeli nuclear facilities in 2024, similar claims were repeated in 2025 by Iranian state media and later Iranian intelligence services. The alleged breaches of high-value nuclear sites were used to promote narratives of Iranian technical superiority and to undermine Israeli security, and blurred the lines between state-driven intelligence operations and hacktivist exposure campaigns.

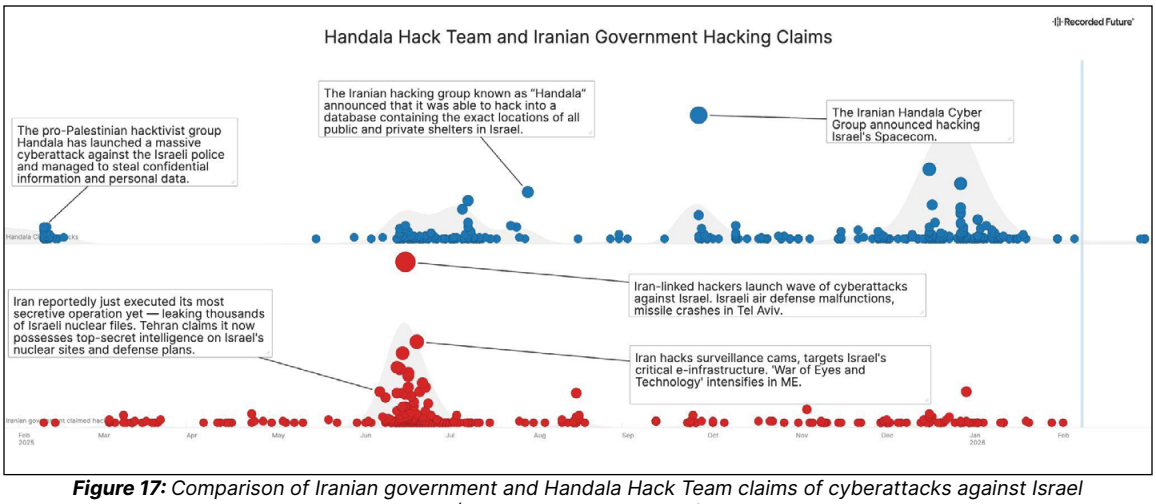


Figure 17: *Comparison of Iranian government and Handala Hack Team claims of cyberattacks against Israel (Source: Recorded Future)*

In addition to hack-and-leak operations, Iranian security services used proxy groups to conduct targeted, disruptive, and destructive attacks against public and private organizations in Israel. Multiple groups linked to Iran's Ministry of Intelligence (MOIS) and the IRGC set up fronts to carry out targeted, disruptive, and destructive operations against public and private organizations. While an overwhelming share of victims are in Israel, various other states seen as cooperating with anti-regime actors were also impacted, such as the Mujahideen-e-Khalq (MEK) in Albania.

New instances of covert activities aimed at manipulating Israeli society by amplifying ideological divisions and diminishing trust in the Israeli government emerged in conjunction with the June 2025 conflict between Israel and Iran. These campaigns almost certainly sought to sow confusion about Iranian attacks on Israel, exacerbate political tension among Israeli citizens, bolster international support for Iran, and collect intelligence from Arab-Israeli and Palestinian citizens. Researchers also revealed influence operations linked to Israeli right-wing activists, which sought to build public support among Israeli citizens for regime change in Tehran.

Influence Operations Amplify Hacker Claims in India–Pakistan Conflict

Hacktivists and influence operators in South Asia pursued similar tactics as the conflict escalated between India and Pakistan in May 2025. Insikt Group documented two large-scale, state-aligned influence networks active during the April–May 2025 conflict between India and Pakistan: Hidden Charkha (pro-India) and Khyber Defender (pro-Pakistan). Both networks — almost certainly aligned with their governments' policy goals — operated across the escalation window from the April 22 Pahalgam attack through the May 10 ceasefire. The influence networks used coordinated narratives and familiar TTPs in an attempt to control attribution and public framing of the conflict.

During this time, large volunteer hacktivist communities on both sides conducted disruptive attacks, primarily DDoS and website defacements, which were often amplified by influence networks. In one instance, Pakistani social media accounts spread false claims that hackers brought down 70% of India's electric grid. Indian energy officials later reported extensive "cyber attacks" on the country's power grid, which were blocked from having an impact on electricity operations.

Both Hidden Charkha and Khyber Defender sought to portray their side as technologically, morally, and militarily superior; undermine the adversary's credibility by amplifying forged military documents and overstating cyber impacts; and pressure opposing officials while rallying domestic and diplomatic support for limited kinetic actions.

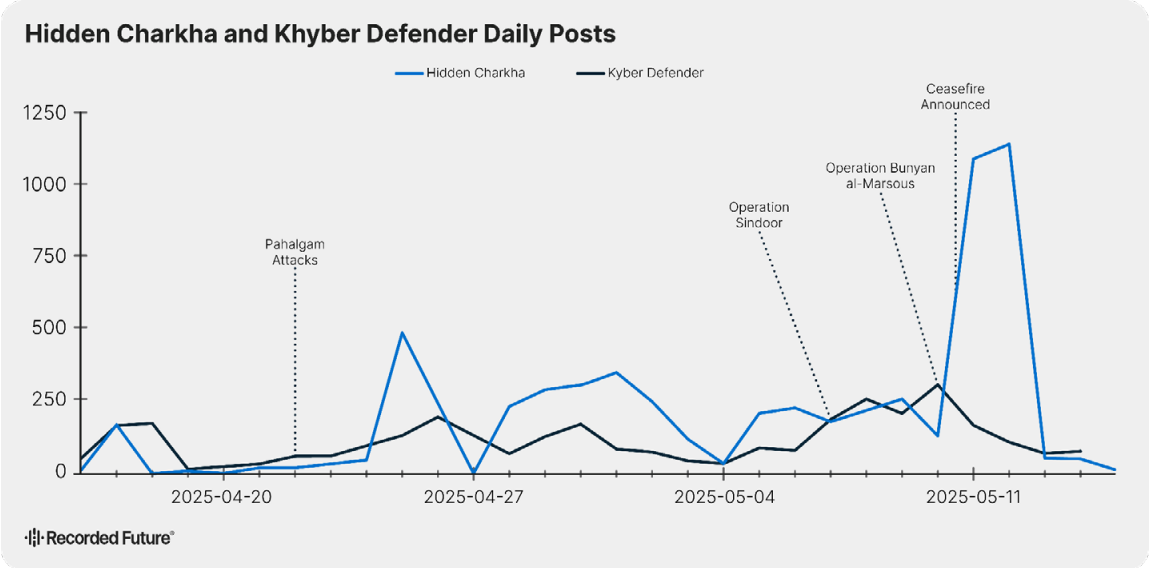


Figure 18: *Hidden Charkha and Khyber Defender daily posting since January 2024 (Source: Recorded Future)*

Insikt Group assesses that Hidden Charkha and Khyber Defender will almost certainly continue operating in alignment with the domestic and foreign policy objectives of the Indian and Pakistani governments, respectively, driven largely by patriotic sentiment even if not under direct state control. Should a new kinetic conflict arise, these networks will almost certainly replicate previous TTPs by amplifying state media narratives, government messaging, and disinformation from hacktivist and social media sources. As generative AI lowers the cost of content production, similar influence networks are likely to achieve greater volume, linguistic reach, and persistence, even if the narratives themselves have low credibility.

Hacktivists Fuel Tensions Between Thailand and Cambodia

Thai–Cambodian border clashes triggered a surge in hacktivist-led cyber activity. Groups associated with both nations engaged in defacements, DDoS attacks, and influence operations that persisted despite truce talks. Cyberattack campaigns were reactive to kinetic flashpoints, and while most had limited operational impact, they amplified nationalist narratives through coordinated influence operations.

For example, between May and June, the group AnonSecKh claimed responsibility for approximately 73 DDoS incidents that primarily targeted Thai government, financial, and manufacturing portals. Screenshots of service disruptions were circulated across social media to amplify the perceived impact and generate public attention. Concurrently, defacement operations emerged, with websites from both sides vandalized using nationalist propaganda and slogans. Threat actors used social media hashtags such as #YourAnonSRVN to share attack tradecraft, enabling sympathizers and copycats to replicate the techniques.

The cyber campaigns extended beyond direct disruptions; the pro-Thailand collective known as KH Nightmare claimed to have exfiltrated hundreds of gigabytes from the Cambodian government. However, many of the so-called leaks consisted of repackaged or partially fabricated datasets. Despite this, the perception of significant breaches contributed to a slew of influence operations and mutual accusations of digital sabotage.

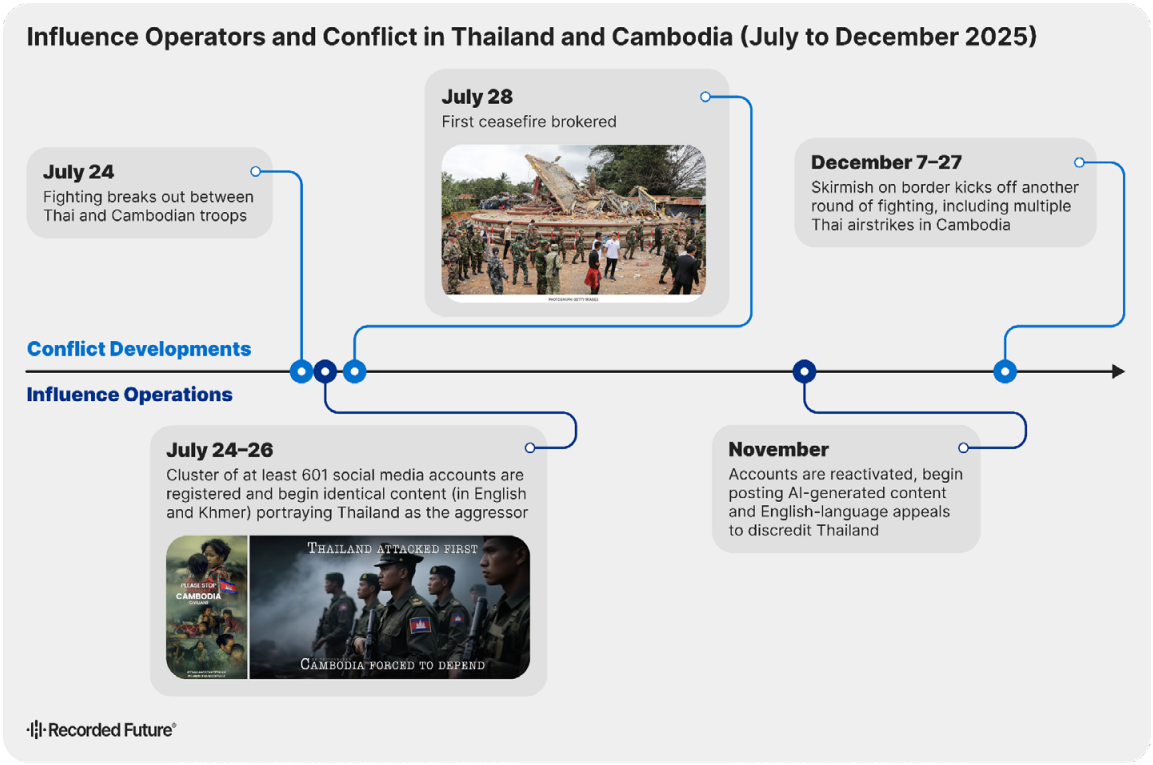


Figure 19: *Insikt Group has observed a significant overlap in kinetic activities and pro-Cambodian influence operations, beginning in late July 2025 and re-emerging as border clashes flared up in November (Source: Recorded Future)*

Insikt Group assesses that sustained hybrid and hacktivist operations blending genuine cyberattacks with propaganda amplification are likely to transpire alongside future hostilities or tensions (see Section I for more analysis). This will likely include new DDoS bursts coordinated with border tensions or protest events, new defacement campaigns leveraging recycled exploits, and continued circulation of mixed-authenticity leaks to maintain narrative dominance. The November pivot by Cambodian influence networks to engage with Western news outlets' English-language accounts emphasizes the role of external mediators like the US in the conflict and is likely an effort to secure more favorable terms in future negotiations.

Russian Hacktivists Target NATO in Asymmetric Campaigns

States leverage hacktivists and covert influence operators to advance their objectives outside of armed conflict. Russian-aligned hacktivists have targeted Ukraine and NATO-aligned countries since the 2022 invasion, largely through coordinated DDoS campaigns. Although these groups present themselves as independent "hacktivists," investigations highlight that portions of this ecosystem function as "faketivist" fronts supporting Russian state objectives. A recent US Department of Justice indictment attributed NoName057(16) activity to individuals tied to the Russian Center for the Study and Network Monitoring of the Youth Environment (CISM) and the Russian Main Intelligence Directorate (GRU).

Similarly, Russia-aligned influence networks have actively intervened in European elections and around issues of strategic importance to the Kremlin. The influence operations and corresponding networks tracked by Recorded Future — including Doppelgänger, Operation Overload, CopyCop, Operation Undercut, and the Russia-based Foundation to Battle Injustice — are longstanding and at least partially Kremlin-funded. While most influence campaigns fail to gain significant traction, some have gained mainstream media attention.

Russia's combined cyber and influence efforts are part of a long-running campaign to not only reduce NATO's support for Ukraine but also weaken the integrity of the alliance altogether. Online efforts are mirrored in real-world sabotage, such as arson and undersea cable-cutting. Using hacktivist, influence, or criminal proxies provides a low-cost and deniable means to impose pressure on NATO while avoiding thresholds that could trigger an Article 5 defense response.

Looking Ahead

Greater geopolitical instability is likely to translate into increased disorder in cyberspace, as genuine partisans and criminal opportunists alike take advantage of the confusion to advance their objectives. Websites and databases with poor cyber hygiene, such as default admin passwords, are likely to remain frequent targets for defacement, data theft, and hack-and-leak activity. For organizations, this means geopolitical crises are increasingly likely to manifest as reputational risk, data exposure, service disruption, or regulatory pressure, often driven by threat actors with limited capability but high visibility.

The persistence of influence operations alongside both cyber and kinetic operations demonstrates that narrative control remains a core objective of modern conflict. Even where influence operations fail to persuade, their continued use reflects a strategic emphasis on confusion, uncertainty, and narrative disruption. Finally, while rare, inauthentic content that receives mainstream attention, such as the false claim that USAID paid celebrities to support Ukraine, likely justifies the continued investment in these operations. Advances in artificial intelligence are already lowering the barriers to producing multilingual, high-volume, and visually compelling content, a trend that will almost certainly increase the scale and persistence of inauthentic information in future conflicts.

Section IV: Cybercrime in Transition

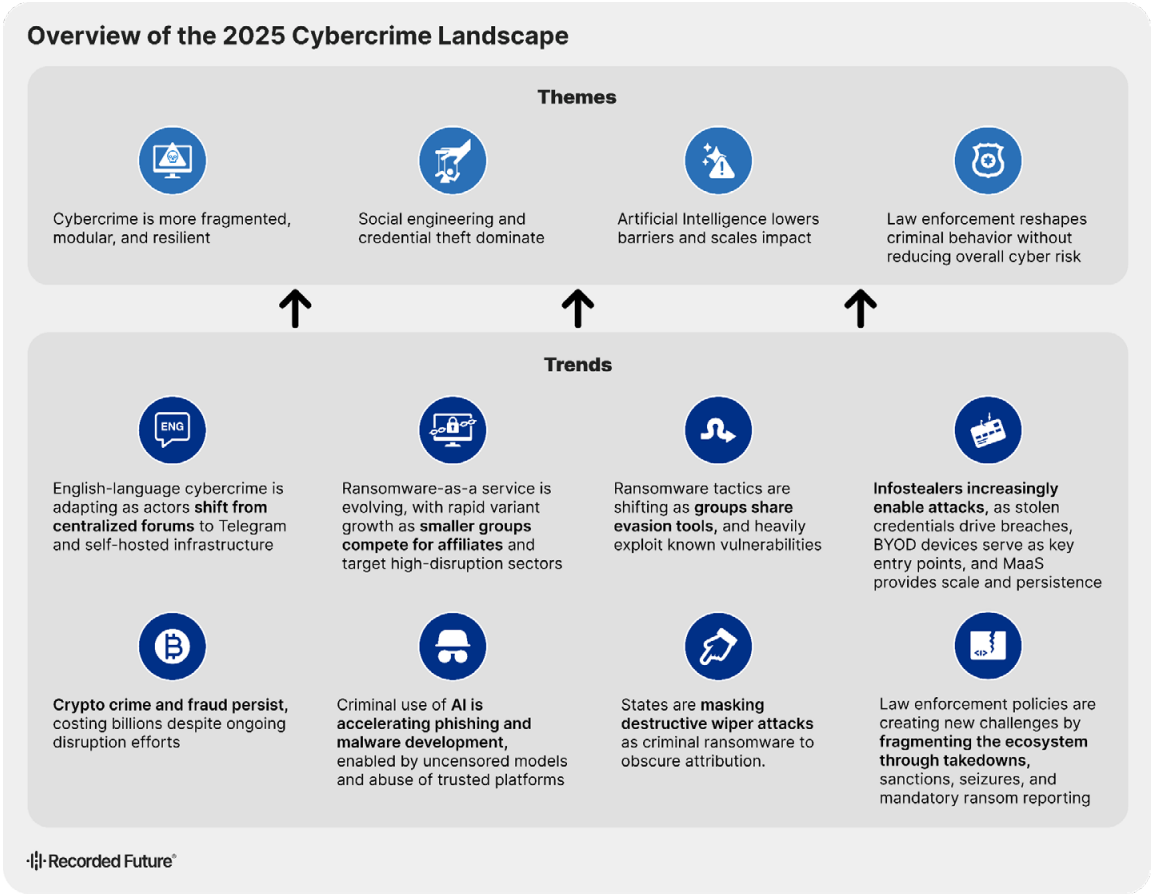


Figure 20: *High-level overview of cybercriminal activity observed by Insikt Group in 2025 (Source: Recorded Future)*

The cybercriminal ecosystem in 2025 adapted to sustained law enforcement pressure by fragmenting rather than contracting. While this reflects partial success in disrupting large-scale criminal infrastructure, it has produced a more decentralized and less predictable threat environment. Criminal groups increasingly rely on smaller collaborations, modular tooling, and platform abuse, complicating detection and response. This section examines how cybercrime evolved in 2025 and the implications for defenders.

English-Speaking Cybercriminals: Stealing the Spotlight through High-Profile Breaches

English-speaking criminal threat actors are distinctive for their loose organizational structure, visibility-seeking behavior, and reliance on social engineering tactics to conduct extortion campaigns. These characteristics create a constantly adapting threat, as influential threat actors recruit opportunistically and refine social engineering tactics targeting help desk or support employees, as well as others who could provide network access. These groups actively court public attention for their activity to build notoriety and amplify extortion pressure.

In January 2025, law enforcement seized several high-profile, English-language cybercriminal forums and arrested individuals involved in running them. In the past, these forums have either recovered by rebranding, or they have been replaced by another, newer forum as the trusted outlet.

However, the January 2025 operations catalyzed two major shifts that would characterize a spree of high-profile incidents carried out by English-speaking cybercriminals throughout the year:

- The formation of new hacking collectives
- The shift from centralized forums to Telegram and privately hosted infrastructure

New Hacking Collectives, Same Hacking Tactics

Some of this year's most publicized cyberattacks, notably the extortion campaigns against Salesforce, Jaguar Land Rover (JLR), and Salesloft Drift, were claimed by a group calling itself Scattered LAPSUS$ Hunters (SLSH). SLSH (also stylized Shinysp1d3r and Sp1d3rHunters) is a self-proclaimed merger of the threat groups Scattered Spider, LAPSUS$, and ShinyHunters. Insikt Group assesses that the effort is likely led by ShinyHunters, and we note that no known members of LAPSUS$ or Scattered Spider have claimed or acknowledged their involvement. The collaboration announcements may be an effort to attract public attention by playing on the name recognition of notorious groups, as well as an attempt to troll researchers who track these groups.

English-speaking cybercriminal threat actors rely on low-cost, high-impact social engineering techniques, particularly help desk impersonation, to carry out extortion campaigns. This approach bypasses multi-factor authentication (MFA) by convincing customer support staff to reset passwords or grant access to privileged accounts. These techniques were likely used in the compromise of British retailers Marks & Spencer (M&S) and Co-op, which were targeted in a highly publicized ransomware campaign in spring 2025. Using social engineering tactics, such as impersonating internal help desk personnel, threat actors were able to request password resets and pivot into the retailers' environments. This also illustrates how compromising a single third party can provide access to multiple downstream enterprises, amplifying both the scale and impact of extortion operations. The Salesloft Drift exploit similarly exemplifies this "one-to-many" approach, as more than 200 companies were breached via compromised authentication tokens.

Telegram and Private Infrastructure

In the aftermath of the takedowns of forums like BreachForums 2, Nulled, and Cracked, English-language groups shifted to Telegram, a messaging platform, and set up their own infrastructure for hosting data leak sites. For instance, SLSH launched numerous Telegram channels to promote its involvement in extortion campaigns targeting Salesforce, Jaguar Land Rover (JLR), and other organizations. The Telegram channels enabled the group to establish a trusted communication network outside of the traditional centralized forums. It also introduced its exploits to a broader audience. However, the platform's openness introduced new challenges, such as SLSH impersonation accounts and bans on users for terms-of-service violations.

The forum takedowns also meant that threat actors no longer had a reliable place to host and share stolen data. As a result, SLSH established its own data leak site in October 2025 to host the Salesforce data. This represents a shift away from centralized forums where multiple threat actors control the forum and post data breach claims. Attempts to recreate the forums

following the takedowns were largely unsuccessful, as newer forums lacked the same level of trust and security. The move to independently hosted forums can reduce risk by limiting the number of individuals involved in controlling or maintaining a forum, as well as reducing the source's overall exposure and notoriety.

Groups like SLSH have had a significant impact on the cyber threat landscape in 2025, despite their low-tech tactics and persistent law enforcement actions against them. This perception is due at least in part to the groups' ability to grab and hold public attention, using the "hacking spree" narrative to their advantage to maximize chaos. Educating employees to identify social engineering tactics, along with a well-managed incident response plan, can help mitigate these improvisational extortion tactics.

Increased Competition Accelerates Innovation in Ransomware-as-a-Service

Unlike the loosely organized English-speaking criminal ecosystem, Russian-speaking ransomware syndicates operate more like structured businesses and are therefore highly responsive to market pressures. The ransomware-as-a-service environment became increasingly competitive in 2025, driven by the continued proliferation of new ransomware variants. Insikt Group identified 289 new variants this year, a 33% increase from the previous year. The majority of these new variants originated from leaked source code and builders for existing ransomware families, including LockBit, Chaos, Makop, and Dharma, among others.

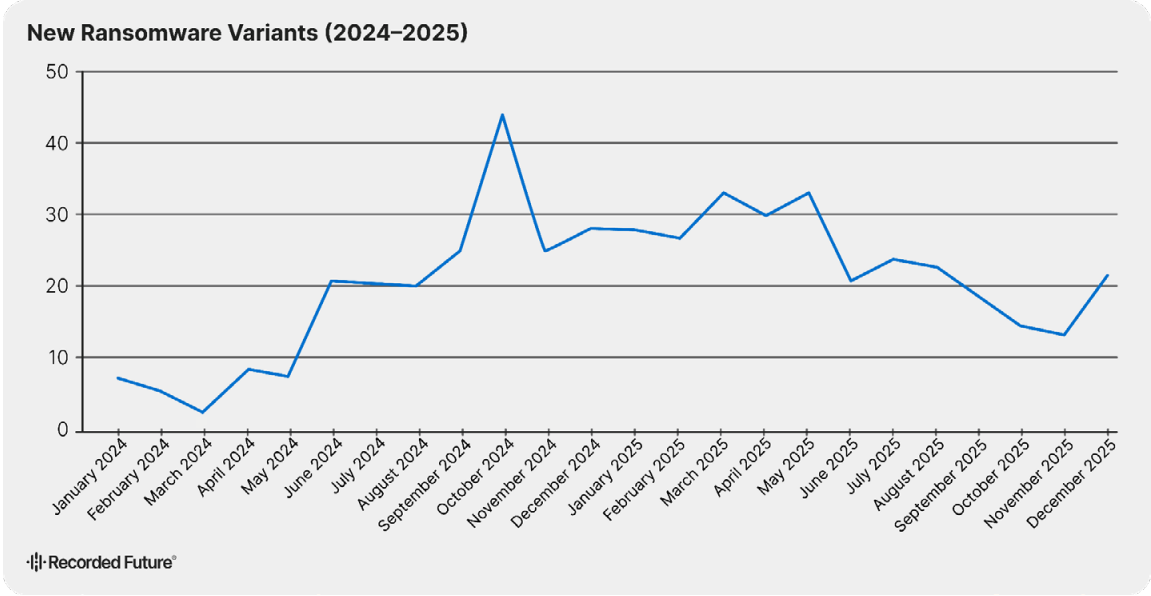


Figure 21: *Leaked source code and builders likely drove an acceleration in new variants that spiked in October 2024 and remained high throughout 2025 (Source: Recorded Future)*

Despite the increase in variants, 2025 has seen a steady decline in ransomware payments, as reported by the USDT's Financial Crimes Enforcement Network (FinCEN), from a 2023 peak. This trend may put increased pressure on RaaS developers to continue evolving their product to remain profitable in an increasingly competitive environment.

Insikt Group has observed several novel features of RaaS programs that emerged in 2025, helping them differentiate from the competition. These improvements fall into one of two categories:

- **Greater flexibility in operations:** Multiple groups have begun offering affiliates the option to choose between deploying ransomware, exfiltrating data, or providing "extortion" services only.
- **New features:** Since the takedowns of major RaaS programs such as LockBit and ALPHV, smaller groups are vying to entice affiliates with attractive business models. In May, for example, the Qilin ransomware group introduced a "call lawyer" option, which claimed to include a "legal assessment" of the value of compromised data, potential lawsuits resulting from the breach, classification of violations based on the attack jurisdiction, and consultation regarding how to threaten maximum damage to victims who refuse to cooperate.

In addition to improving services for affiliates, ransomware operators are actively investing in novel methods to enhance their product through initial access, defense evasion, and payload delivery.

- **Use and abuse of AI:** Insikt Group observed several ransomware campaigns that integrate AI into their attack chains. The discovery of PromptLock in August marks the first known AI-powered ransomware, which uses a large language model (LLM) to generate malicious scripts in real-time. Furthermore, new research has uncovered the use of ClickFix in AI summarization tools, which weaponizes legitimate AI services to deliver ransomware payloads.
- **Shared defense evasion tools:** A shared antivirus (AV) killer tool is being deployed across at least eight different ransomware groups to systematically terminate security processes, indicating a new level of tool-sharing and collaboration.
- **Diversified loaders and access tools:** Ransomware families are incorporating new loaders, diversifying initial access tools and techniques to make early detection more difficult. Multiple ransomware groups have also used the stealthy malware Skitnet in phishing campaigns, leveraging it as an all-in-one utility across multiple stages of the attack chain, making it especially attractive to ransomware operators.

The pace of change and reuse of shared tools exemplifies ransomware operators' broader shift toward modular, interchangeable delivery ecosystems that lower development costs, speed up operations, and allow affiliates to combine and reuse components across campaigns. Threat actors are likely doing this to strengthen defense evasion and resiliency. This type of adaptation ensures competitiveness against rival RaaS groups and minimizes the risk of exposure to law enforcement.

Ransomware groups continued to exploit critical vulnerabilities to gain access to target networks throughout 2025. Although several campaigns did involve zero-day vulnerabilities, most ransomware operations in 2025 continued to rely on already disclosed vulnerabilities, capitalizing on patching fatigue across multiple industries. For example, while CL0P successfully conducted mass targeting of organizations via a zero-day vulnerability in Oracle E-Business Suite, some of the most frequently exploited CVEs were much older, such as exploits of Atlassian Confluence Server and Data Center, as well as the recurring abuse of the ProxyShell exploit chain in Microsoft Exchange Server. These demonstrate the importance of prioritizing patching or other mitigation of known vulnerabilities to avoid opportunistic exploitation.

Broadly speaking, ransomware victimology trends have remained relatively consistent with those of the previous year: ransomware groups have continued to primarily target sectors with high business continuity demands, such as manufacturing, healthcare, and critical infrastructure, as well as sectors rich in valuable data, including finance, law, and retail. The majority of victims have remained concentrated in Western, high-GDP nations; however, Insikt Group has observed a rise in targeting of Asian countries in 2025, with India rising to join the top ten targeted countries in multiple months throughout 2025.

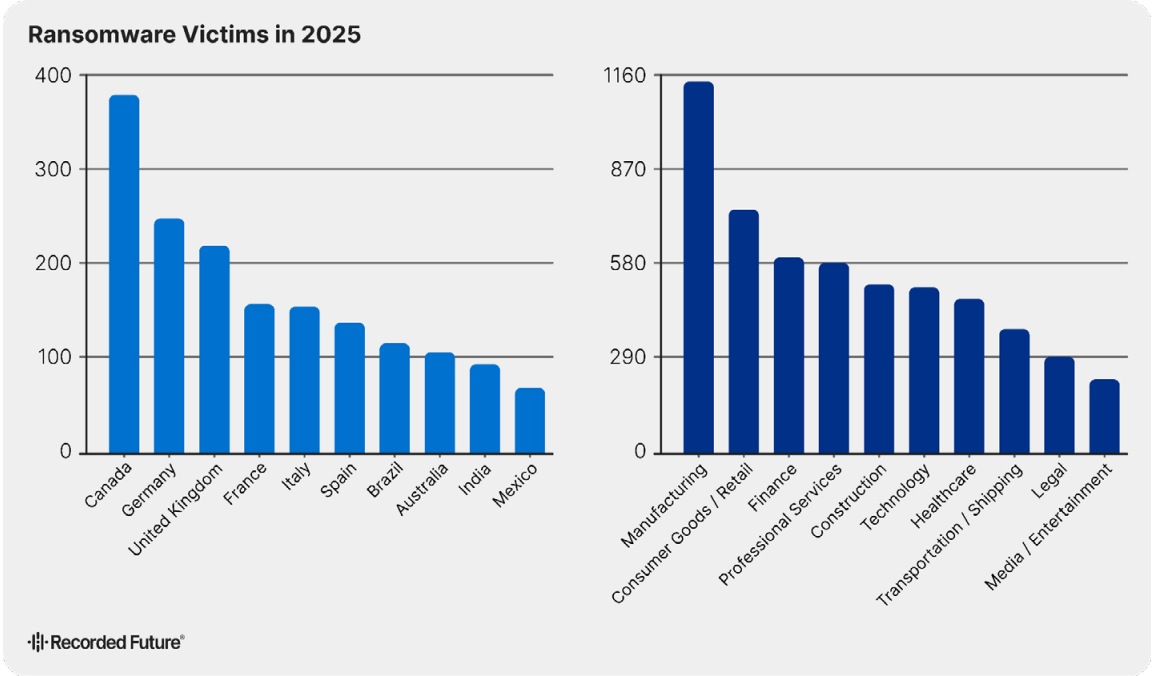


Figure 22: *Extortion claims by country and industry (Note: excludes the US, which was the most targeted country at 3,617 claims) (Source: Recorded Future)*

Organized Crime in Southeast Asia Industrializes Fraud

While ransomware payments may be decreasing, cryptocurrency-based scams are on the rise. These crimes resulted in nearly $10 billion in losses in 2024, driven by large-scale scam operations run by Chinese-speaking transnational criminal organizations (TCOs). These groups set up call center compounds in Cambodia and Myanmar, using coerced labor augmented by AI-driven automation and impersonation tools to carry out scams at an industrial scale. The TCOs took advantage of political instability in Myanmar to operate largely unimpeded by law enforcement; however, following public outcry in China over scams and trafficking of Chinese citizens, the Chinese government put pressure on Myanmar to shut down the compounds and extradite the leaders, some of whom now face the death penalty for their involvement. Despite this pressure, many scam compounds remain in operation, and it is likely they will pivot to targeting wealthy Western countries to avoid further interference.

The Southeast Asian scam ecosystem depended on Huione Guarantee, a Telegram-based marketplace for fraud tools, and Huione Pay, which openly supported money laundering. Both were part of the Huione Group, a Cambodian financial conglomerate with government ties. In addition to tools for carrying out scams, such as deepfake face-swapping capabilities, Huione Guarantee and other marketplaces also deal in malware-as-a-service and supplies needed for other types of crimes. Insikt Group tracked the growing prevalence of "ghost-tapping" on these marketplaces. Ghost-tapping is an attack vector to commit retail fraud by using stolen payment

card details linked to mobile payment services. Huione Guarantee supported ghost-tapping by selling phones pre-loaded with stolen payment details, and provided a marketplace for reselling stolen goods (often luxury products) purchased with those phones.

In March 2025, Cambodia's central bank revoked Huione Pay's license. Two months later, the USDT designated Huione Guarantee as a primary money-laundering concern, cutting it off from the US financial system. These actions forced Huione Guarantee to shut down and led to the removal of thousands of related Telegram channels. Despite this disruption, alternative "Guarantee" services such as Tudou quickly emerged, underscoring the resilience of the crypto-scam ecosystem.

Infostealers: The Hidden Threat Enabling Ransomware and Extortion

Infostealers are delivered via malware-as-a-service kits sold or rented to a wide market of customers. These kits enable lower-skilled criminals to conduct cyber exploits, contributing to the prevalence of infostealers.

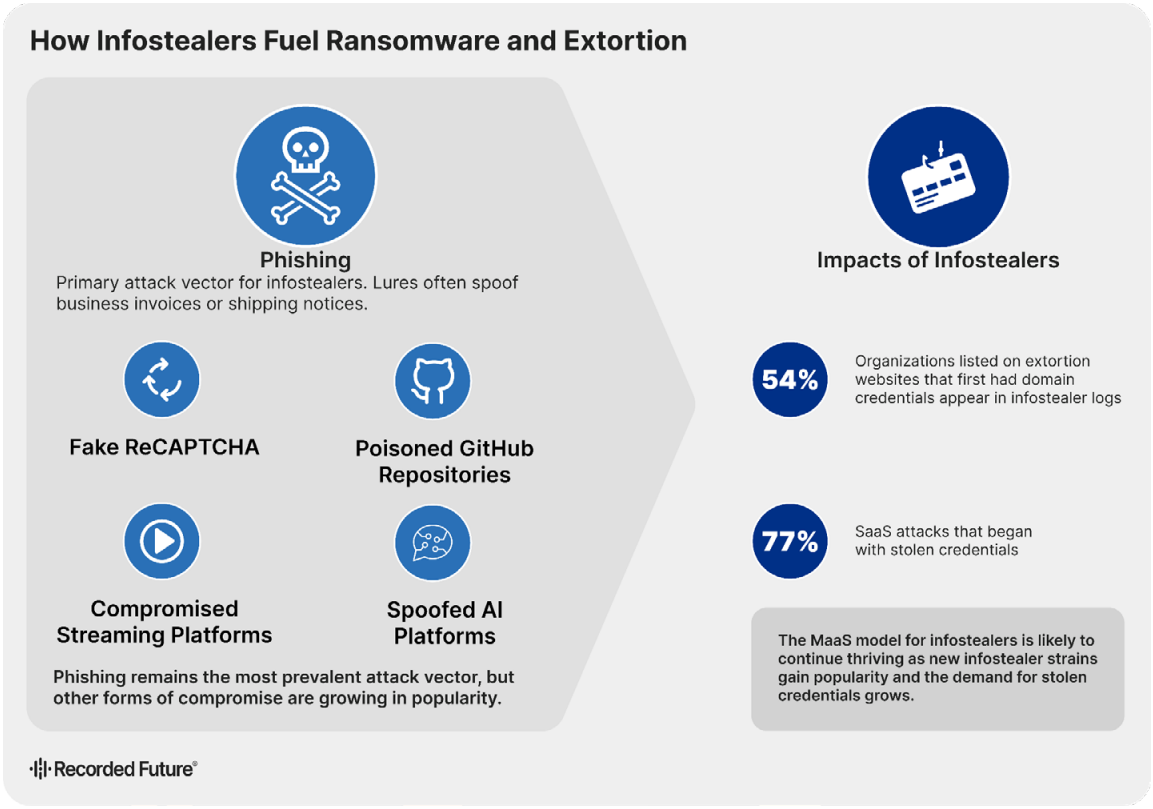


Figure 23: *Continued evolution in the infostealer malware-as-a-service marketplace is fueling other cybercrimes, including extortion and ransomware (Source: Recorded Future)*

Criminals Experiment with AI to Support Social Engineering, Malware Development

Throughout 2025, threat actors experimented with malicious AI models tailored for cyber operations, introducing three new varieties: Nytheon AI, Xanthorox AI, and GhostGPT. Compared to earlier offerings, such as WormGPT, FraudGPT, and DarkBARD, many of which were short-lived, fraudulent, or basic jailbreak frontends, these newer models reflect operational maturity in presentation and usability. Nytheon and Xanthorox feature modular designs, multimodal capabilities, SaaS-style delivery, and reputational shields, including ethical

disclaimers and public GitHub repositories intended to reduce scrutiny. Despite developer claims, these models do not provide unique operational capabilities that could not also be achieved by evading safety guardrails on commercial or open-weight models.

Throughout 2025, threat actors integrated generative AI across the malware development cycle. In most cases, generative AI served as an efficiency and capability multiplier rather than a source of fundamentally new techniques, but the breadth of use meaningfully expands what lower-skilled threat actors can achieve. Beyond malware development, threat actors in 2025 continued using commercial and open-source LLMs to enhance phishing operations. Phishing-as-a-service (PhaaS) offerings also integrated AI, further democratizing access to advanced phishing operations.

Threat actors targeted AI platforms and tools themselves, experimenting with new attack vectors and techniques unique to LLMs:

- Abuse of trusted, AI-powered platforms and widely used software development services by threat actors; this technique, known as "living-off-trusted-sites" (LOTS), exploits user trust and, in the case of AI platforms, enables tailored lures and scalable operations
- Manipulating AI-enabled tools through prompt injection, where threat actors deliver prompts to "trick" AI models into carrying out malicious operations
- Repurposing commercial AI platforms and tooling as operational infrastructure

These developments reflect a persistent interest in using AI to enhance criminal operations. However, criminals face the same challenges as legitimate users in configuring reliable autonomous operations. We anticipate that threat actors will continue to adapt AI tools to scale up specific tasks, as full automation remains out of reach. (See Section V for more on offensive uses of AI.)

Law Enforcement Takes a Multifaceted Approach to Cybercrime

Figure 24: *Law enforcement operations had a measurable impact against cybercrime, although criminals persisted by adapting their tactics (Source: Recorded Future)*

Law enforcement conducted extensive, multinational disruptive efforts against cybercriminal forums and ransomware groups, resulting in takedowns, arrests, and asset seizures. Operation Endgame, the multinational effort hosted at Europol, continued targeting various malware loaders and initial access services through a combination of law enforcement actions and videos meant to amplify the operation. These actions targeted not only technical infrastructure but also trust among cybercriminals by highlighting law enforcement infiltration of previously trusted forums.

Government authorities have also addressed cryptocurrency scams with a multi-pronged approach, including seizures, sanctions on supporting entities, and raids. The actions have fractured the underground economy, leading to threat actor decentralization and pressuring enabling services, such as those involved in money laundering.

Private industry also contributed to disruption efforts in 2025, sometimes in collaboration with law enforcement. The success of these disruption operations was significantly amplified by partnerships, including with governments, international organizations, and across the private sector.

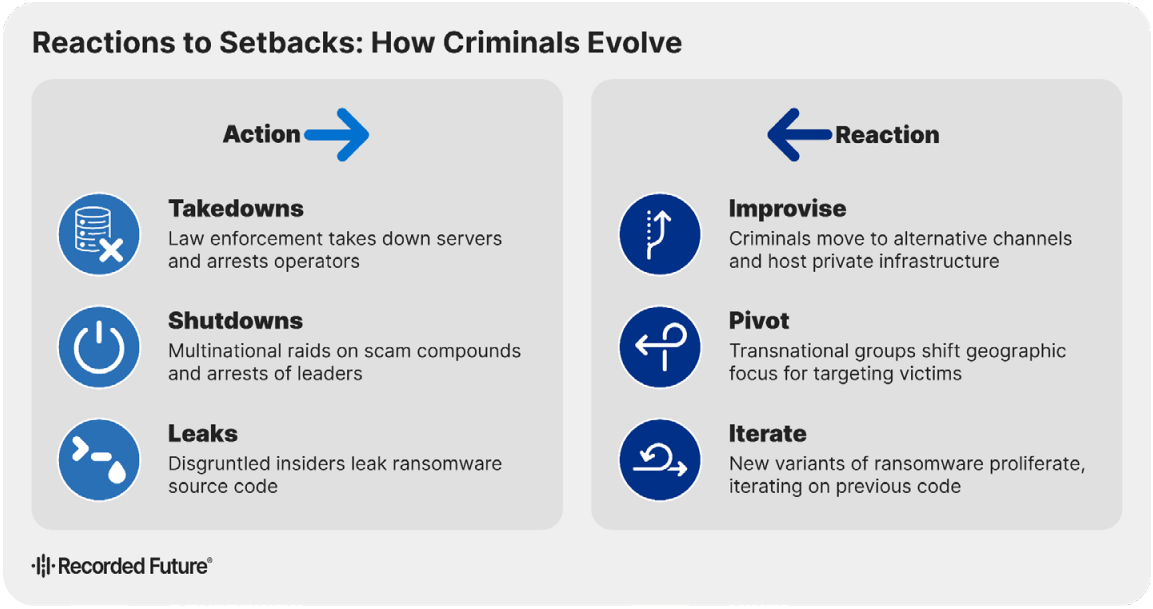


Figure 25: *Criminals evolve their tactics and targeting in reaction to setbacks caused by law enforcement or by other criminals (Source: Recorded Future)*

Despite these efforts, criminal groups have remained resilient, continually adapting their tactics and infrastructure. Recognizing the limitations of reactive countermeasures alone, governments are taking proactive measures to reduce the number of victims who choose to pay ransoms, hoping to cut off criminals' revenue. For example, Australia and the UK recently enacted mandatory reporting requirements for organizations that pay ransoms, and the US has implemented a reporting requirement for critical infrastructure entities, although enforcement has been delayed pending the finalization of rulemaking. While it is unclear whether reporting requirements will successfully reduce payouts, they will have the advantage of improving law enforcement visibility into the prevalence of ransomware and extortion, which may contribute to improving deterrence and mitigation efforts.

Crossover Focus: State-Sponsored Ransomware

Not all ransomware is motivated by profit. Recorded Future identified ransomware groups receiving direct tasking from Russian state security services, validating a long-held suspicion of coordination between the Russian government and cybercriminals. The Russian government very likely benefits from criminal activity that disrupts critical infrastructure in NATO-allied countries by maintaining a degree of separation and deniability from these attacks. If linked to the Russian government, attacks on hospitals or critical manufacturing risk being interpreted as an act of war, triggering an Article 5 response. This type of activity aligns with other "gray war" acts of sabotage, which are both disruptive and deniable.

Similarly, Iran-based groups such as BlackShadow/Agrius/Apostle have also masked deliberate wiper attacks against Israeli targets as ransomware. The FBI accused state-aligned threat actors of collaborating with or coordinating with ransomware groups, including NoEscape, RansomHouse, and ALPHV. These activities advance similar disruptive objectives against adversary targets, with the additional incentive of profit for both the hacker and the government.

Looking Ahead

We anticipate that the trends of fragmentation, modularization, and adaptation will continue to accelerate, driven by advances in AI technology and persistent global instability. AI is already making certain types of cybercrime, particularly social engineering, significantly easier for a broader range of potential threat actors. Consistent improvements in AI coding capabilities will make developing sophisticated malware similarly more accessible.

Geopolitically, cybercrime is enabled by weak or corrupt governments that exploit criminal activity for their own gain. Russia's relationship with cybercriminals has been long documented and is even written into ransomware code. We expect other countries to follow a similar playbook, leveraging criminal networks to advance their objectives. Furthermore, the erosion of international institutions may make international law enforcement cooperation more difficult, providing greater impunity to cybercriminals who can exploit leniency in one country as long as they target that country's adversaries.

Section V: AI Developments in 2025

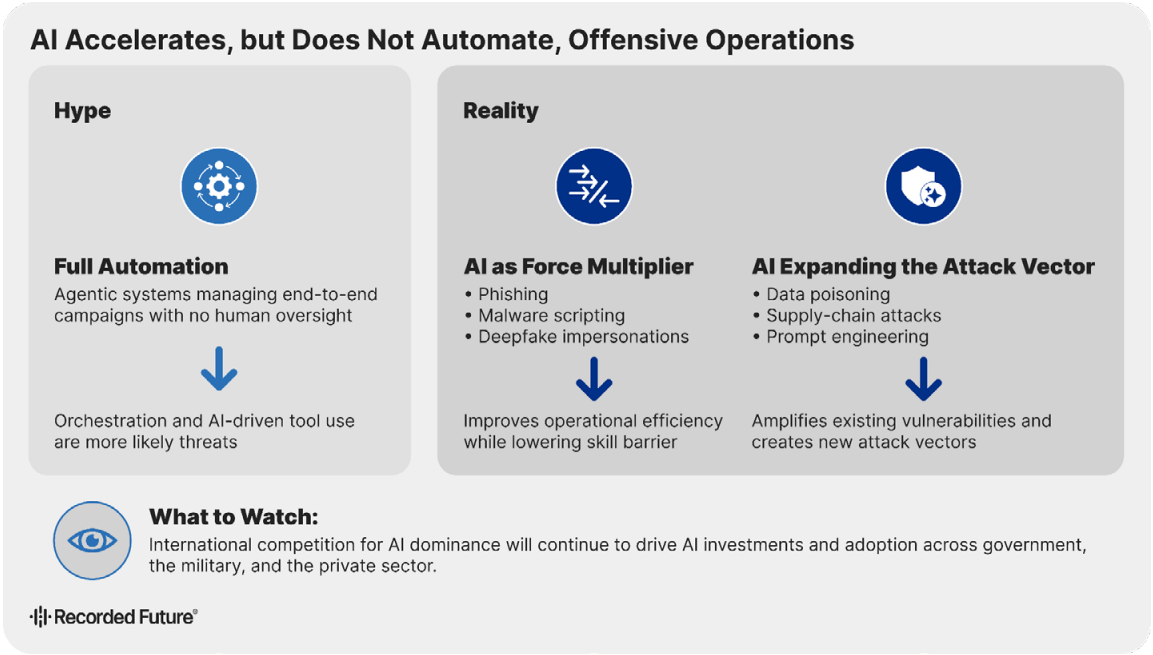


Figure 26: *Offensive uses of AI (Source: Recorded Future)*

Artificial intelligence, particularly large language models (LLMs) such as ChatGPT, Claude, and their peers, continued to advance in 2025, with measurable improvements in reasoning, multimodal processing, and task automation. These developments coincided with AI's growing macroeconomic importance. In 2025, AI was a major driver of the US economy, accounting for 37% of year-over-year growth in the first nine months. Despite these gains, the structural limitations of the LLMs underpinning this growth have become clearer, and threat actors are increasingly learning how to exploit them. This persistent gap between capability growth and real-world reliability has fueled growing skepticism about whether the scale of global AI investment will produce the transformative returns many expect.

Offensive Uses of AI

See also Criminals Experiment with AI to Support Social Engineering, Malware Development

AI shaped the cybersecurity landscape across three interconnected dimensions. Its widespread integration expanded the attack surface, introducing new classes of vulnerabilities that traditional security controls were not designed to mitigate. At the same time, more and more security teams incorporated AI to enhance and automate cyber capabilities, such as detection, incident response, and high-volume analytical workflows. Meanwhile, adversaries continued experimenting with AI to increase the scale, speed, sophistication, and precision of their operations, enabling more automated exploitation and highly targeted social engineering campaigns.

Threat Actors Are Hacking LLMs

Adversaries are expanding their attack vector arsenal by targeting weaknesses unique to LLMs. For example, malicious prompts can be embedded in shared text, video, or image files, such as emails or calendar invites, to hijack LLM-based assistants into carrying out the attacker's objectives. Similarly, data poisoning techniques are becoming more operational, with threat actors exploiting "generative search optimization" to prompt AI search engines to surface malicious content in their results. These techniques demonstrate the unique vulnerabilities of LLMs that are likely to become the new entry point for malicious operations. As AI becomes empowered to take more real-world actions, such as through agentic commerce that manages transactions, the attack surface for fraud and cybercrime will expand.

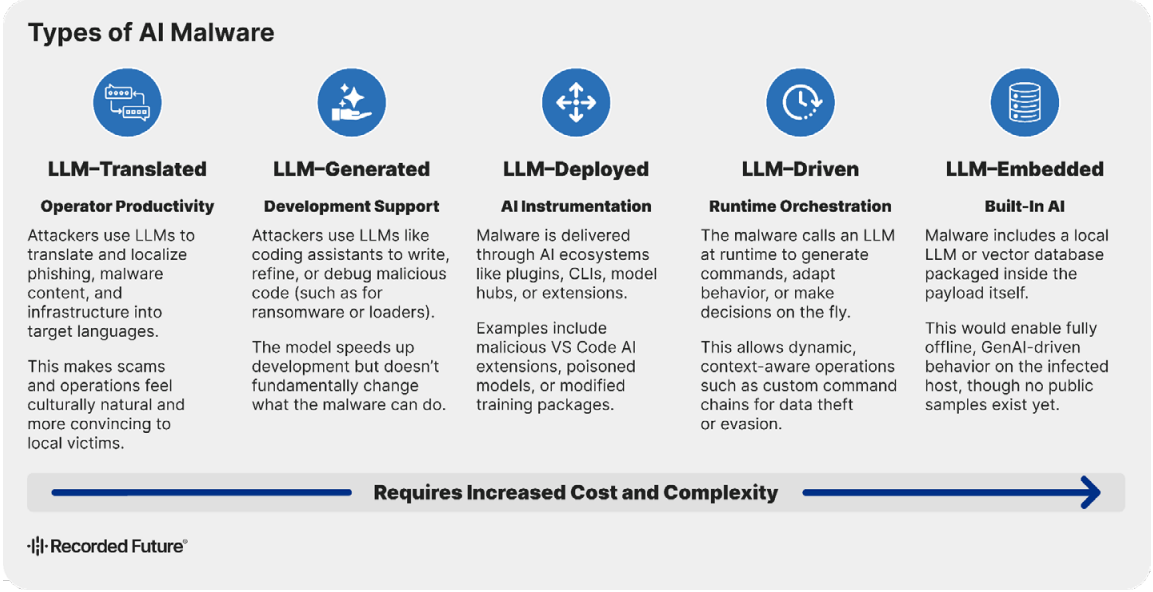


Figure 27: *Summary of the different types of AI malware (Source: Recorded Future)*

AI-Powered Malware Is Still Largely Experimental

Beyond enabling new attack vectors, AI is also being used by threat actors to incrementally enhance traditional cyber operations, though with mixed results. Despite frequent warnings about "AI-powered malware," observed real-world activity remains far less advanced than the surrounding hype suggests. Most threat actor use of AI is limited to experimentation or marginal efficiency gains — such as assistance with code generation, reconnaissance, or evasion — rather than fully autonomous attack execution.

When mapped to Recorded Future's AI Malware Maturity Model (AIM3), the vast majority of known examples fall within Levels 1–3, often reflecting proofs-of-concept, research artifacts, or AI-assisted variants of existing tools. While one widely cited case has been described as Level 4 (Transforming), that assessment remains contested and still requires meaningful human oversight. To date, no threat actor has credibly demonstrated a truly AI-orchestrated cyber operation. In practice, AI is enhancing attacker efficiency at the margins, but fully autonomous AI-driven attacks remain theoretical rather than operational.

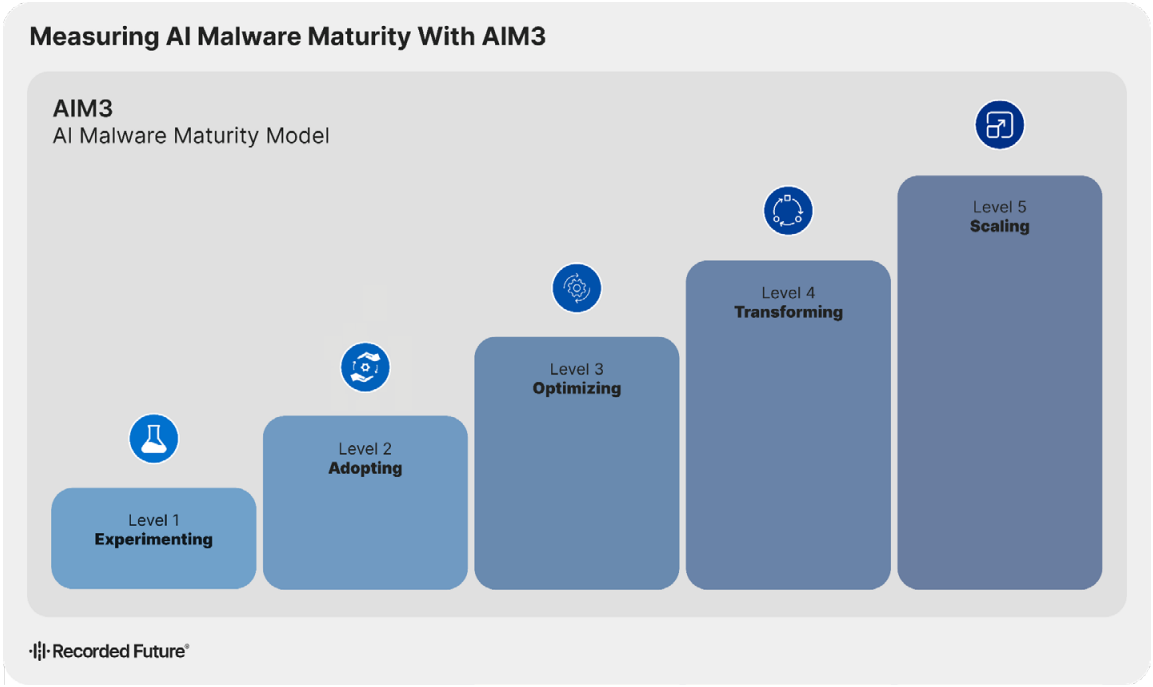


Figure 28: *Levels of Recorded Future's AI Malware Maturity Model (AIM3)(Source: Recorded Future)*

Deepfakes and Synthetic Identity Fraud Rising

AI has accelerated social engineering and fraud by enabling the production of inauthentic voices, images, and videos at scale. Synthetic identity fraud, or using inauthentic personas to open fraudulent accounts, has significantly expanded alongside the introduction of advanced AI capabilities. In Q1 2025 alone, synthetic identity document fraud rose by 300%, while deepfake-enabled fraud has increased more than tenfold since the start of 2024. The growing inability to distinguish between real and artificial content, accounts, or personas will make fraud detection increasingly difficult, potentially limiting the transactions that can occur in a virtual-only setting.

The US–China AI Gap

At the strategic level, many governments view AI adoption as a national security imperative. The US is currently leading global development efforts, though China remains in close competition. The US has remained focused on pursuing artificial general intelligence (AGI), systems capable of matching or surpassing human performance across most tasks, and continues to lead in private-sector investment. Until recently, US policy has also sought to constrain China's progress by restricting access to advanced computing chips required to train and operate frontier models.

China, however, appears to be pursuing a different approach centered on AI diffusion rather than outright capability leadership. The January 2025 launch of DeepSeek's then-leading reasoning model, R1, accelerated AI adoption not only within China but globally. Notably, open-source developers are increasingly building on Chinese models: fine-tuned or modified Alibaba models shared on Hugging Face now outnumber those derived from Google, Meta, Microsoft, and OpenAI combined. Embedding Chinese LLMs into the global software ecosystem may represent an alternative, and potentially more scalable, path to AI dominance.

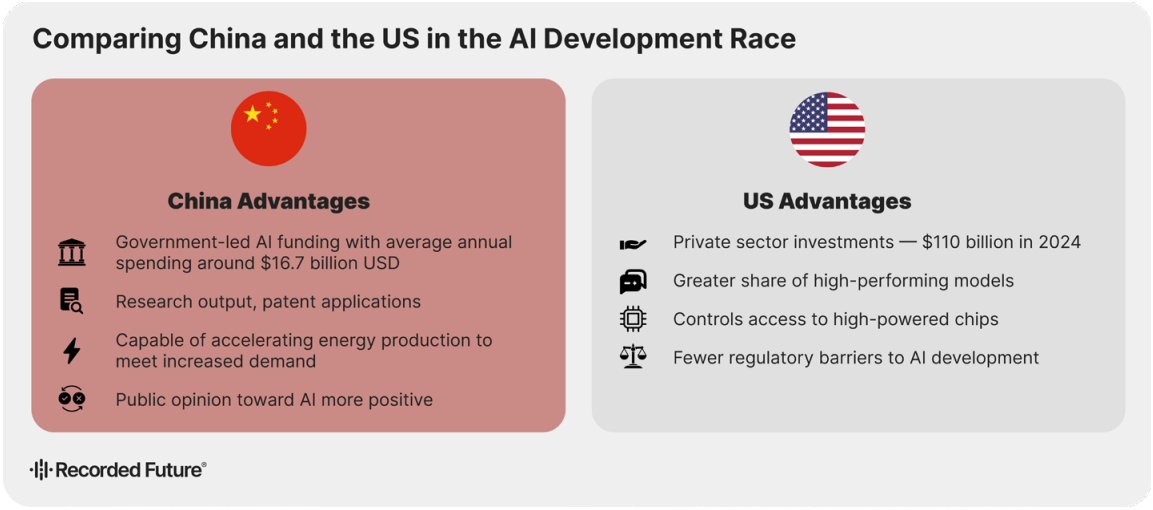


Figure 29: *The US currently leads the global AI race, but China is pursuing an aggressive strategy for AI development (Source: Recorded Future)*

Looking Ahead

The rapid disruption caused by generative AI since 2023 provides a useful reference for how other emerging technologies may evolve as they mature. Competition over quantum computing, advanced robotics, and space systems will extend beyond commercial markets into sustained geopolitical rivalry. As adoption accelerates, these technologies are likely to reinforce existing fragmentation across technological, economic, and security domains.

Generative AI has already demonstrated how emerging technologies can lower barriers for malicious activity and amplify cyber capabilities at scale. Similar dynamics are likely to accompany future innovations. Without proactive mitigation, technologies that drive productivity and growth may also introduce systemic vulnerabilities.

At the strategic level, early adopters stand to gain disproportionate economic and military advantages, reshaping global power dynamics. While historical comparisons provide context, they understate the defining characteristic of the current era: the speed of change. For decision-makers, the challenge is not only anticipating breakthroughs but preparing for the cascading security, economic, and geopolitical consequences that follow.

How Recorded Future Can Help

Emerging Technology Risks

As AI and autonomous systems reshape the threat landscape, organizations need intelligence that keeps pace with adversary adoption of new capabilities.

- **Autonomous Threat Operations** unlocks AI-driven intelligence operations with automated threat hunting, response orchestration, and continuous risk assessment, enabling teams to defend at machine speed. (Take a **tour**.)
- **AI Insights** generates summaries across searches, alerts, and Intelligence Cards for risk-scored entities, malware, and threat actors.
- **AI Sessions** enables natural-language queries, letting analysts ask conversational questions instead of building complex searches. AI also powers automated report generation using templates or custom formats. (See **video**.)

Section VI: Lessons from 2025 and Outlook for 2026

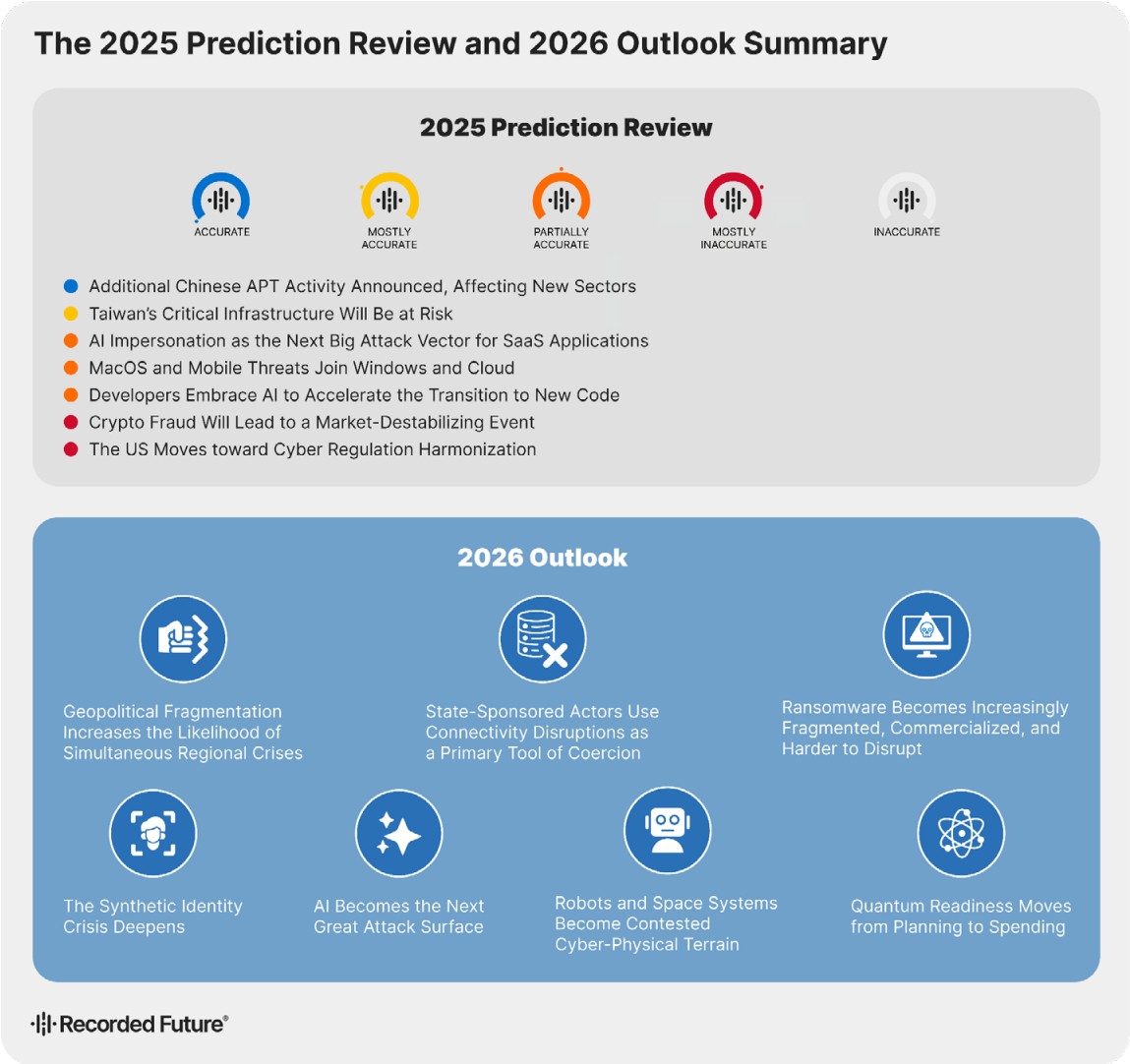


Figure 30: *Summary of 2025 predictions and 2026 outlook (Source: Recorded Future)*

This section evaluates key predictions from the previous year's report against developments observed in 2025. Those outcomes inform six strategic forecasts for 2026, aligned to the core themes of this report: geopolitical fragmentation, persistent state-sponsored cyber activity, criminal adaptation, and the growing security impact of emerging technologies.

Lessons from 2025

Prediction for 2025: AI Impersonation Will Be the Next Big Attack Vector for SaaS Applications

Insikt Group expected that a major breach would very likely result from one of two AI-related factors: implementation of generative AI into enterprise workflows or abuse of AI for effective impersonation. In either case, we assessed that an SaaS application was likely to play a role in initial access or data exposure. Companies like OpenAI (with SORA), Meta (with MovieGen), and Google (with Veo 2) had released models that make incredibly realistic fake videos and images, tools that would make it much easier for scammers to carry out existing scams in more convincing ways, such as by making video calls to IT help desks in order to trick their way into gaining access to sensitive data and systems.

2025 Outcome: AI Exploits and SaaS Exploits Have Not Yet Meaningfully Merged

Threat actors are using AI and exploiting SaaS, but these activities have not fully merged. This may be because AI is more useful for other exploits, or because exploiting SaaS with only human intelligence is still very effective.

Threat actors are using AI to carry out fraud, with criminals promoting "near-real time" deepfake capabilities. North Korean state-sponsored threat actors have used deepfake technology to steal identities and pose as legitimate IT workers, demonstrating the capability to gain legitimate credentials to access a network through AI-enabled fraud.

Prediction for 2025: Additional Chinese APT Activity Will Be Announced, Affecting New Sectors

Despite major revelations in 2024 of intrusions into US critical infrastructure by Chinese-linked advanced persistent threat (APT) groups, Insikt Group believed that additional high-profile breaches of critical infrastructure by Chinese APTs would be disclosed in 2025. We predicted that other industries beyond the energy and telecommunications sectors would disclose breaches attributed to Chinese APTs, likely conducted with the goal of pre-positioning for disruptive operations.

2025 Outcome: Chinese Espionage Activity Was Extensive and Indiscriminate

In September 2025, the US and allies released a joint statement indicating that Chinese espionage activity impacted organizations in over 80 countries, targeting not only telecommunications but also government, transportation, lodging, and military infrastructure. The wide-ranging collections activity likely impacted "nearly every American," according to US government officials.

As discussed, we have observed RedMike continuing to compromise edge device networks and target telecom companies worldwide, demonstrating that exposure is no longer a deterrent to persistent espionage operations. While the US and China have clashed on AI, chips, rare earth minerals, and tariffs, the public US response to Chinese cyberattacks has been limited to sanctions on Chinese hackers in January 2025.

Prediction for 2025: MacOS and Mobile Threats Will Join Windows and Cloud

In malware and vulnerability trends, Insikt Group predicted that one of the high-impact cyber incidents of 2025 would likely involve either macOS malware or mobile malware and that this would result from certain environmental factors reaching breaking points, such as higher attention to macOS targets and increased access to sensitive corporate and financial data via mobile devices.

2025 Outcome: It's Still Windows and Cloud, But Mobile Malware Is Catching Up

Microsoft was the most targeted vendor in Recorded Future's H1 2025 Malware and Vulnerability Trends report. Notably, the SharePoint zero-day (which combines both Microsoft and cloud) caused extensive headaches across sectors due to widespread exploitation. That said, mobile malware is on the rise, with eleven new malware strains emerging in H1 (primarily banking trojans, RATs, spyware, and stealware).

Prediction for 2025: Crypto Fraud Will Lead to a Market-Destabilizing Event

Cryptocurrency scams were among the most common and lucrative types of investment scams, and we predicted that criminals would likely be emboldened by the crypto boom to carry out market-destabilizing scams that would at least temporarily reduce the value of cryptocurrencies, leading to calls to restrict their use.

2025 Outcome: Crypto Market Remains Stable, Though Fraud Persists

The US announced the creation of a "crypto reserve" in addition to crypto-friendly legislation. The GENIUS Act seeks to increase the legitimacy of stablecoins by addressing regulatory ambiguity around cryptocurrency. While this may increase commercial use, investment, and adoption, critics say the bill contains loopholes that could facilitate money laundering and sanctions evasion. Cryptocurrency is increasingly used for money laundering, according to Chainalysis. As a result, we may see an increase in cryptocurrency fraud and money laundering, though not a single "market-destabilizing" incident.

Prediction for 2025: Developers Will Embrace AI to Accelerate the Transition to New Code

As a result of multiple factors, including improved AI coding capabilities and new software liability rules in Europe, Insikt Group expected that both companies and threat actors would very likely rely increasingly on generative AI to accelerate the transition to modern code libraries — whether for memory-safe code in companies or for more modular code in malware.

2025 Outcome: Vibe Coding Is Here, But It May Not Be Safer

This prediction examined two trends: the increased use of AI for coding and the regulatory push away from memory-unsafe coding. For the first part, AI is getting better at coding, and more people are using it. The term "vibe coding", or creating code purely through conversations with AI chat interfaces, has now become part of the technology lexicon. However, there are serious concerns about the security of AI-generated code, regardless of whether or not it's in a memory-safe language. An analysis of over 100 LLMs revealed that only 55% of generated code was secure, a statistic that has remained constant since 2023. Developers are also five times more likely to miss errors in AI-assisted code than in non-AI-assisted code, possibly due to over-trusting the reliability of AI code.

As for the second trend, the US continues to call for memory-safe languages to reduce vulnerabilities, though this is not tied to any sort of mandate.

These two trends do not seem to have converged, likely because the transition remains arduous, even with AI assistance. The US Defense Advanced Research Projects Agency (DARPA) has announced a project to automate the translation of all C/C++ code to Rust, though this remains an area of ongoing research.

Prediction for 2025: The US Will Move toward Cyber Regulation Harmonization

Insikt Group anticipated that the new administration's deregulatory agenda, combined with a Supreme Court decision that put more pressure on Congress to clarify its regulatory implementation intentions, would likely drive support for passing the Cyber Regulatory Harmonization Act. Simplifying the US's complex cyber regulatory landscape has long enjoyed bipartisan support, and taking action to improve the nation's cybersecurity in the aftermath of major cyber incidents, such as the Salt Typhoon breaches, would be seen as an early win for Congress.

2025 Outcome: The US Moves Away from Regulations

A deregulatory agenda combined with an overall de-prioritization of cybersecurity has left US cyber policy uncertain. Congress has not made significant progress on regulatory harmonization, despite discussing the topic in both the House and Senate homeland security committees in 2025. Notably, a widely supported cybersecurity law was allowed to lapse, eliminating protections for cybersecurity information sharing, and there is currently no clear path to renewing or updating the legislation. Finally, despite the initial outrage over the Salt Typhoon breaches, there has been no significant response from Congress to improve critical infrastructure resilience or to impose costs on China.

Prediction for 2025: Taiwan's Critical Infrastructure Will Be at Risk

As China continued to pursue incremental escalation in its coercion of Taiwan short of initiating an armed conflict, a disruptive cyber campaign targeting Taiwan's energy, transportation, or financial sectors — or the disclosure of widespread pre-positioning in Taiwan networks — would be a logical next step. More generally, China would continue to use its cyber capabilities to reconnoiter the policies and preparations of Taiwan and potential partners in a conflict, such as the US and Japan.

2025 Outcome: Cyberattacks and Sabotage Disrupt Critical Infrastructure

China is continuing to use cyber and other asymmetric means to increase coercive pressure on Taiwan, very likely to erode resistance to a future invasion. Throughout 2025, Chinese vessels severed undersea cables connecting Taiwan with the rest of the world, and the Chinese military continued its coercive air and sea operations encircling Taiwan. While we have not yet seen a large-scale cyber disruption, espionage and various attacks attributed to threat actors in China against Taiwanese critical infrastructure persist and are increasing in volume compared to the previous year.

Threat Outlook for 2026

Geopolitical Fragmentation Increases the Likelihood of Simultaneous Regional Crises

We assess that interstate clashes are likely to become more frequent in 2026 as the rules-based order continues to erode and no credible replacement framework emerges. As noted in Section I, major powers are increasingly prioritizing regional access and strategic positioning over adherence to global norms, reducing the predictability of military action and response thresholds.

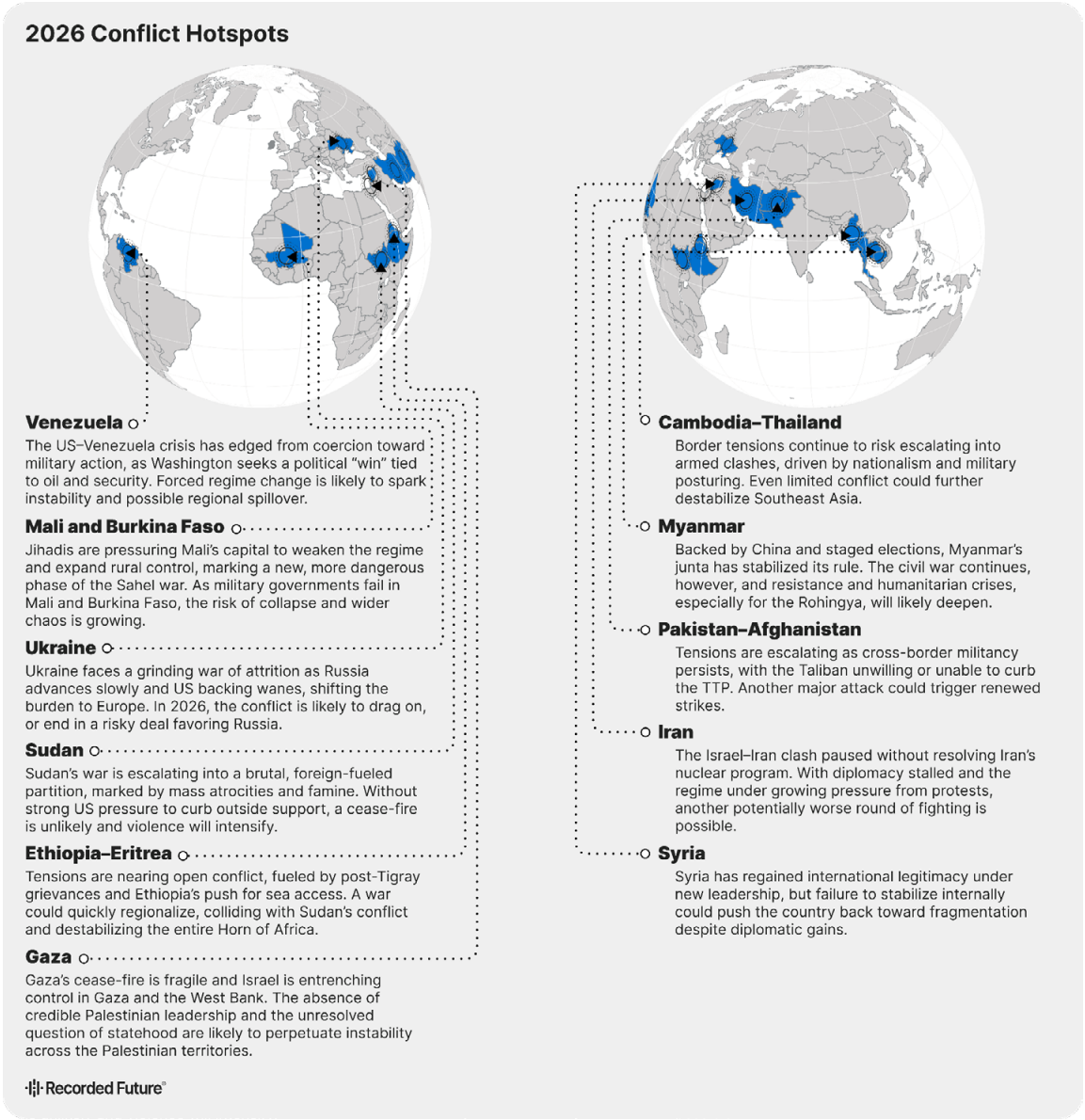


Figure 31: *Summary of 2026 potential conflict hotspots (Source: Recorded Future)*

As enforcement of established norms becomes more selective, regional and emerging powers are likely to pursue territorial, political, and economic objectives more aggressively, particularly where borders are contested or states are politically fragile. 2026 could see a heightened risk of border disputes between Pakistan and Afghanistan, along the Ethiopia-Eritrea border, and between Mali and Burkina Faso, as well as an escalation of existing tensions along the Cambodia-Thailand border.

External involvement in internal conflicts is also likely to expand, with stronger states seeking to shape outcomes or secure strategic access during periods of instability. While intervention is not new, incentives to act earlier and more assertively have increased. In contexts such as Sudan, Myanmar, and Venezuela, the absence of consistent international consequences for coercive behavior increases the likelihood of faster escalation and broader regional spillover.

Signals to Watch:

- Increased military build-up near contested borders
- Selective erosion, disregard, or enforcement of international legal and diplomatic norms
- External involvement spreads local conflicts into regional crises

Prepare:

- Validate continuity and crisis response plans for multi-region disruption scenarios
- Expand risk models to account for opportunistic intervention, escalation, and spillover effects

State-Sponsored Threat Actors Use Connectivity Disruptions as a Primary Tool of Coercion

As detailed in Section II, state-sponsored threat actors are increasingly treating cyber access as both a measure of operational readiness and a tool for espionage. While large-scale destructive cyberattacks remain unlikely in 2026, warning timelines will continue to compress as adversaries position themselves to activate preexisting access during periods of crisis.

Central to this readiness is a growing focus on connective infrastructure, including undersea cables and satellite-based positioning, navigation, and timing (PNT) systems. These assets underpin cloud services, financial transactions, emergency response, and AI-driven operations, yet remain comparatively underrepresented in cyber risk planning. Even limited cyber or physical interference can cascade across multiple critical sectors, producing outsized civilian and economic effects.

Building on operational successes observed in 2025, Chinese and Russian state-sponsored threat actors are likely to continue favoring selective, reversible disruptions to these systems. As a result, the most consequential state-sponsored activity in 2026 is likely to take the form of brief outages, degraded performance, and coordinated gray-zone operations that blur the boundaries between cyber, electronic, and physical domains.

Signals to Watch:

- Brief, localized connectivity loss, latency spikes, or timing drift affecting utilities, transport, or financial services
- Anomalous activity at telecom providers, cable landing stations, satellite ground segments, or associated service vendors
- Coordinated OT/IT anomalies or access patterns spanning multiple regions or infrastructure sectors

Prepare:

- Prioritize monitoring of telecom, satellite, and third-party provider access, including vendor and maintenance pathways
- Integrate timing- and connectivity-loss scenarios into continuity and incident-response exercises
- Treat correlated, low-level disruptions across sectors or geographies as potential rehearsal or signaling activity, not isolated faults

Ransomware Becomes Increasingly Fragmented, Commercialized, and Harder to Disrupt

Ransomware is highly likely to remain fragmented and highly adaptive through 2026. Continued law enforcement pressure will almost certainly drive major players to splinter into smaller, faster-moving groups that favor shorter attack cycles, lower ransom demands, and opportunistic targeting, marking the end of the “big-game hunting” era. The ransomware ecosystem will continue becoming more organized and commercialized, with more groups adopting subscription models, outsourcing operations, and relying on specialized laundering and negotiation services. The result will be a distributed criminal supply chain — resilient, decentralized, and increasingly difficult to track or disrupt.

Ransom payments, already down 23% in Q3 2025, are likely to decline further as more organizations refuse to pay and smaller targets yield lower financial returns. With extortion success rates declining, threat actors are likely to prioritize disruption and visibility over direct financial gain, conducting reputation-driven attacks to compel victims to engage. Established families such as LockBit, Albabat, and Nitrogen are expected to remain influential, while emerging variants merge and modularize codebases for stealth and persistence. Through 2026, adversaries will almost certainly continue to experiment with AI-assisted phishing, payload tuning, and automated ransom negotiations, sustaining innovation even as profits decline.

Signals to Watch:

- New leak sites are emerging from recycled or leaked code
- Cross-posting of identical victims across multiple leak sites
- Affiliates advertising “speed runs” or ultra-fast deployment cycles

Prepare:

- Rollback controls for storage and critical applications
- End-to-end recovery workflows: detect → isolate → restore
- Rapid communication channels for containment, coordination, and victim notification

The Synthetic Identity Crisis Deepens

Identity fraud is shifting from individuals to corporations, a trend we assess will accelerate in 2026. As outlined in Section II, state-sponsored threat actors are already using synthetic identities to secure loans, launder funds and, in the case of the North Korean IT worker scheme, embed operatives within legitimate organizations. We anticipate that other hostile states and criminal threat actors will adopt similar models, expanding beyond technical IT roles into non-technical functions such as HR, finance, supplier onboarding, and benefits administration, further eroding trust in remote identity and verification systems.

Also in 2026, AI-generated audio and video will almost certainly make business email compromise (BEC) and social engineering more convincing and scalable. Biometric and identity-verification systems will likely remain vulnerable to spoofing, replay, and cloned credentials, enabling synthetic personas to coerce payments, manipulate employees, and facilitate access handoffs to cyber operators. Governments are likely to respond by tightening identity assurance and compliance requirements, accelerating a shift from static controls toward zero-trust identity models built on behavioral signals, cryptographic provenance, and continuous authentication.

Signals to Watch:

- Reused freelance accounts or mismatched interview and work identities
- Synthetic personas appearing in HR, finance, or supplier roles
- Unexplained access sharing or overlap with known threat groups

Prepare:

- Enforce video interviews with live identity and continuity checks
- Validate identity consistency across hiring, onboarding, and access provisioning
- Monitor post-hire access for anomalies, sharing, and impossible travel indicators

AI Becomes the Next Great Attack Surface

As AI changes the way users interact with software, data, and devices, we expect more threat actors to pivot away from code-based exploits toward prompt-based manipulation, exploiting weaknesses in AI platforms and autonomous agents. Malicious prompts will increasingly replace malware as the preferred intrusion method, enabling adversaries to extract sensitive data, override guardrails, or induce harmful actions without breaching traditional defenses or even knowing how to code.

As users shift from search engines to model-generated responses, attackers will very likely move from SEO poisoning to “generated-SEO” manipulation, aiming to bias AI outputs for financial gain, influence, or misdirection. Early indicators suggest that pro-Russia influence operators are already testing these tactics, with criminal groups likely to follow suit.

Signals to Watch:

- Incident reports citing autonomous task chains or uncontrolled tool use by AI agents
- Manipulated or biased model outputs linked to coordinated influence or financial activity
- Synthetic code or content injections appearing in public AI training or retrieval sources

Prepare:

- Apply "minimum viable security" for AI systems: define clear intent boundaries, assign per-agent identities, limit tool permissions, and log data provenance

Maintain human-in-the-loop oversight for all external-facing AI actions

Monitor AI dependencies for tampering, data poisoning, or prompt manipulation

Quantum Readiness Moves from Planning to Spending

In 2026, quantum readiness will move decisively from long-term planning to sustained investment as governments and standards bodies translate post-quantum cryptography (PQC) guidance into actionable migration timelines. US initiatives such as CNSA 2.0 and the NIST standardization process are both targeting full transition by 2035, alongside parallel efforts in Europe. Although many mandates formally apply only to public-sector systems, these frameworks are increasingly establishing de facto expectations across most sectors, making PQC adoption a practical necessity for large organizations.

At the same time, the "harvest now, decrypt later" problem — threat actors stealing encrypted data under the assumption that it will be decrypted in the future using quantum computers — is narrowing the margin for delay, particularly for data with long-term confidentiality requirements. As a result, boards are beginning to allocate dedicated quantum security budgets in 2026, in some sectors approaching 5% of total cybersecurity spend, to support cryptographic inventories, vendor transitions, and agility pilots.

Beyond 2026, quantum readiness will become a strategic differentiator: organizations that act early will minimize migration risk, manage costs, and preserve customer trust as PQC standards mature.

Signals to watch:

- RFPs requiring PQC migration or roadmap commitments
- Cryptographic dependency inventories entering enterprise risk registers
- Agility pilot programs testing hybrid and upgradeable encryption

Prepare:

- Conduct a full crypto inventory to identify RSA and ECC dependencies
- Collect vendor attestations on PQC readiness and timelines
- Pilot PQC and hybrid encryption in external-facing and high-sensitivity systems
- Review key-deletion and archival practices to mitigate future decryption exposure

Robots and Space Systems Become Contested Cyber-Physical Terrain

In 2026, humanoid robots and space infrastructure will move from experimentation to operational deployment, increasing economic and strategic reliance on network-connected cyber-physical systems. Advances in LLMs have accelerated robotics readiness, while expanding satellite constellations and lunar missions are making space a foundational layer for connectivity, finance, and security. Competition among the US, China, and their partners will increasingly center on resilience, access, and control of these systems.

As scale increases, so does risk. Robots and space assets introduce broad, often immature attack surfaces dependent on remote access, default configurations, and complex supply chains. The most likely threat in 2026 is not catastrophic failure, but selective, reversible disruption. Cyber operations against robots or space systems can produce immediate safety, economic, or connectivity impacts while remaining below traditional escalation thresholds.

Signals to Watch:

- Operational deployment of humanoid robots in industrial or security settings
- Cyber activity targeting aerospace, satellite, or robotics providers
- Short-duration degradation of satellite-enabled connectivity or timing

Prepare:

- Treat robotics and space systems as critical cyber-physical risk assets
- Enforce secure-by-design controls and vendor assurance at deployment
- Exercise response plans for short, high-impact cyber-physical disruptions

Conclusion

By the end of 2025, the global threat environment had shifted toward a more fragmented and unpredictable baseline. Power was exercised with fewer constraints, alliances proved more situational, and diplomatic mechanisms were less effective at containing escalation. Rather than isolated crises, instability increasingly emerged as a pattern of overlapping pressures, with states more willing to test limits and absorb risk. This erosion of consensus reshaped not only geopolitical dynamics but also the strategic calculus behind cyber operations, which became an integral tool for shaping behavior, managing escalation, and positioning for future conflict.

Cyber and information activity reflected a broader move toward persistence and ambiguity. States and non-state threat actors alike prioritized durable access to digital ecosystems — particularly identity and cloud infrastructure — while loosely affiliated threat actors amplified disruption in ways that blurred attribution and intent. In parallel, cybercrime adapted to sustained disruption by reorganizing into smaller, more flexible networks, often flourishing where governance gaps and regional instability provided cover. Rapid advances in artificial intelligence further accelerated these trends, compressing timelines, widening participation, and increasing the scale of potential impact. Looking ahead to 2026, organizations should expect a threat landscape defined less by discrete events than by continuous pressure, where preparedness, operational resilience, and strategic foresight will matter more than reactive defenses alone.

In this environment, effective defense depends on the ability to anticipate change, not simply react to incidents. Recorded Future enables organizations to do exactly that by delivering real-time, intelligence-driven insight into geopolitical risk, cyber threats, criminal ecosystems, and emerging technologies. By integrating external intelligence into security and business decision-making, organizations can identify early warning signals, reduce exposure across identity and cloud environments, and make faster, more confident risk decisions — turning uncertainty into a strategic advantage.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®
Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®
Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.
Learn more at www.recordedfuture.com.