ORION FORUM

Cyber Espionage and U.S. Policy Responses

OCTOBER 7, 2025

Introduction

Between September 1986 and June 1987, a group of German hackers conducted the first recorded act of cyber espionage, breaching US civil and military organizations and selling stolen data to the Soviet KGB. Since then, cyber espionage has become an evolving threat and state-sponsored campaigns targeting sensitive government and corporate data. In May 2025 alone, the UK National Cyber Security Center attributed several breaches of the Electoral Commission and Members of Parliament to China, while Russian hackers conducted a cyber espionage operation using an HTML application to implant file-based malware into Tajikistan's educational and government entities. Chinese cyber operations alone have increased by 150%, with espionage accounting for 11% of all global cyberattacks. Maryland University reported in 2023 that over 1,200 cyber attacks aimed at information theft. A recent US Department of Justice indictment on March 5, 2025, accused 12 Chinese nationals, employees of both the PRC government, state-actor hacker groups, and private companies, of email hacking and information espionage. For adversaries like China and Russia, cyber espionage increasingly serves as a low-cost, high-impact alternative to and part of a conventional warfare. This research brief examines the evolution of cyber espionage, compares Chinese and Russian tactics, evaluates US responses, and provides policy recommendations.

Overview of Cyber Espionage

Often referred to as cyber spying, the US Cybersecurity and Infrastructure Security Agency (CISA) defines cyber espionage as "a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage, or political reasons." Cyber espionage is a covert, long-term, and

intelligence-driven practice of leveraging the Internet and digital technologies, typically carried out on behalf of a foreign government or an organized group with strategic intent. National Counterintelligence and Security Center also identified economic and industrial espionage involving the theft, communication, or possession of proprietary information. Few espionage hacks are motivated by monetary gain to the perpetrator, and the majority are deployed to gain political, economic, military, strategic, or diplomatic advantage by acquiring sensitive strategic information or stealing intellectual property. Those attacks usually involve political interests as the driving force for hacktivism. Cyber espionage might also be deployed in conjunction with military operations to gather timely information on troop movements, defense strategies, and weapon innovations. Cyber espionage attacks typically target large corporations, government agencies, academic and research institutions, prominent individuals, and organizations that possess valuable IP and technical data crucial for information gathering. These types of operations often utilize numerous hacking tools from zero-day vulnerabilities, exploits previously unknown by the manufacturers that can be used to bypass firewalls and infiltrate systems, and implants, backdoor portals, used to gain unauthorized remote access. Attackers often employ open-source intelligence (OSINT) reconnaissance for mapping target environments and designing phishing campaigns. After gaining initial system access through spear-phishing, credential theft, zero-day exploits, or compromising third-party vendors, attackers move laterally within systems, escalate privileges, and exfiltrate data incrementally, often using encryption or tunneling techniques to evade detection.

The majority of cyber espionage attacks can be classified as sophisticated and long-term operations or Advanced Persistent Threats (APT), establishing an undetected presence in the network over an extended period of time. Another tactic commonly used in cyber espionage is social engineering, or the manipulation of human psychology through pretexting, baiting, and quid pro quo, focused on obtaining information from the target to advance an incoming attack. Hackers employ spear-phishing attempts, targeting specific individuals with fraudulent emails from seemingly trusted entities filled with malicious links and infected attachments designed to steal login credentials, sensitive data, and install malware. According to the FBI's IC-3 2024 report, social engineering tactics, such as phishing/spoofing, extortion, and data breaches, accounted for 83% of information losses. Hackers also infect legitimate websites frequently

visited by the victims to compromise the user in a tactic known as a “watering hole.” Malicious actors leverage zero-day exploits, security vulnerabilities, and software flaws to infect the target’s systems with malware and spyware, to secretly gather sensitive information by tracking browsing habits, login credentials, and keystroke entries, and various kinds of malware, including viruses, trojans, and worms.

The tactics used for cyber espionage can also come from within. Hackers can convince insider threat actors to share or sell access to unauthorized users, bypassing traditional cybersecurity defenses. Often motivated by financial gain, personal grievances, or coercion, insider threat actors are hard to detect and mitigate. Lastly, cyber espionage hackers sometimes opt to conduct supply chain attacks that target less secure elements of an organization’s supply chain to ultimately gain access to a more extensive network. Malicious actors can compromise software update mechanisms and implant malicious components into hardware supplies, allowing attackers to infiltrate multiple organizations through a single weak point. While espionage as a form of acquiring state secrets has existed for quite some time, with statutes like the Economic Espionage Act of 1996 that criminalized theft of trade secrets and intellectual property, a similar framework has yet to exist within the cyber domain to address cyber espionage attacks. The Biden Administration signed Executive Order 14117 in 2024 that allows the DOJ to prohibit certain transactions of bulk sensitive personal data and US government-related data, instructing CISA to put forward transaction requirements.

Individuals, groups, or organizations without territorial sovereignty, also known as non-state actors in the cyber domain, operate either independently or in coordination with nation-states. These actors include state-sponsored hacker groups, cyber mercenaries, and freelancers who offer their services for financial gain. Some of these groups typically engage in Crimes-as-a-service (CaaS), providing clients a range of illicit services like hacking in exchange for payment, commercializing, and commodifying cybercriminal activities. While some of the most prominent state-affiliated hacker groups include Chinese Volt Typhoon (also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious Taurus),”), specializing in critical infrastructure attacks, Salt Typhoon (also known as Earth Estries, Ghost Emperor, or UNC2286), accused of engaging in espionage and North Korean APT 37 targeting

telecommunications and technology sectors, cyber mercenaries include groups like LockBit, specializing in ransomware attacks in exchange for payment, and RansomHub that targets global infrastructure.

Unlike politically motivated groups, cyber mercenaries present unique risks due to their lack of allegiance to a client, often resulting in unpredictable behavior. The anonymity of cyberspace enables states to employ such actors while maintaining plausible deniability, complicating the attribution of cyberattacks. For smaller states, leveraging non-state actors can enhance national cyber capabilities, as exemplified by Ukraine's IT Army, allowing them to challenge cyber-advanced adversaries. While many nations engage in cyber espionage, targeting the West; China, Russia, Iran, and North Korea remain the most prominent sponsors, with the most advanced operations typically executed by well-resourced, state-backed hacker teams.

In recent years, the distinction between nation-state actors and non-state cybercriminals which are financially motivated has become increasingly blurred. According to Microsoft's *Digital Defense Report 2024*, state-sponsored groups collaborate more frequently with independent hackers to further political and military goals at relatively low cost. While traditional cyber espionage was primarily focused on intelligence collection, modern campaigns have become more destructive. For example, there has been a notable rise in attacks targeting third-party software providers, allowing attackers to compromise multiple organizations simultaneously through a single point of entry.

Chinese-linked Cyber Espionage Case Studies

While Chinese cyber operations have evolved throughout the last two decades, there no single operational characteristic that may indicate or typify the Chinese model. Rather, these operations involve a mix of tactics and targets and involve heterogeneous actors, blending "components of espionage and entrepreneurship and capitalizing on China's pervasiveness in the international economy." The overall structure of China-linked cyber espionage includes " using contracted hacking teams" that make money out of engaging in criminal activities and work for the Chinese intelligence agencies. Such contractual relationships enable the Ministry of State Security (MSS) to work diverse cadre of hacker groups. According to the US Department of Justice, the Chinese government, through its Ministry of State Security (MSS),

employs “intelligence officers, contractor hackers, and support personnel” to engage in hacking and cyber espionage campaigns. The CISA’s joint advisory on China’s state-sponsored also states that these actors “are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.” As mentioned before, the report specifically refers to Volt Typhoon, which “has been pre-positioning themselves on U.S. critical infrastructure organizations’ networks to enable disruption or destruction of critical services in the event of increased geopolitical tensions and/or military conflict with the United States and its allies.”

China’s cyber espionage strategy involves the simultaneous targeting of diverse industries through sophisticated cyber operations. Since 2000, Chinese state-sponsored actors have been linked to approximately 90 cyber espionage campaigns. A 2013 Mandiant report revealed that groups employed ransomware during operations to obscure their true intent of cyber espionage from security researchers. The report specifically linked APT1 to the People’s Liberation Army Unit 61398. APT1 engages in widespread intelligence gathering across numerous sectors, with a particular focus on US-based systems, aiming to exfiltrate intellectual property. China’s organized and far-reaching cyber-espionage efforts are part of a broader strategic objective of laying the groundwork for future, large-scale cyber operations.

The following four case studies, involving Chinese cyber espionage groups, illustrate the diverse targeting strategy. The report delves into the October 2024 hacking and cyber espionage incident carried out by Salt Typhoon, PRC-associated cyber actors; the 2021 Microsoft Exchange espionage hack conducted by the Chinese cyber espionage group, Hafnium, linked to MSS, the Operation CuckooBees perpetrated by APT41, known as Barium or Winnti, a Chinese state-sponsored cyber espionage group linked to the Chinese government’s MSS, and the espionage hacks of APT1, also known as the Comment Crew or the Shanghai Group, with links to China’s People’s Liberation Army (PLA) Unit 61398 outlined in the Mandiant report.

In October 2024, Salt Typhoon breached at least nine U.S. telecommunications providers.

Perpetrator: Salt Typhoon, PRC-associated cyber actors

Target: Telecommunication companies, including AT&T and Verizon

Tactics: Hacking into telecommunication companies.

As stated before, Salt Typhoon is particularly focused on specializing in cyber espionage, which also included gaining access to America's telecommunication companies, including AT&T and Verizon. The attack also involved targeting telecom providers in more than twenty other countries, as part of a wide-ranging espionage and intelligence collection campaign. The attack also involved stealing customer call data and law enforcement surveillance request data and compromising individuals' private communications that involved in government or political activity. The nature of this attack is particularly worrisome due to its extensive targeting, the compromise of telecommunication networks, and the high-value intelligence the attack enabled the attackers to obtain. Echoing this concern, Sen. Mark Warner, D-Va, who was a former telecommunications executive, described the attack as "the most serious telecom hack in our nation's history."

The 2021 Microsoft Exchange Hack is one of the largest and fastest-spreading cyber espionage campaigns to date, compromising tens of thousands of servers worldwide

Perpetrator: Hafnium, a state-sponsored cyber-espionage group linked to China's Ministry of State Security (MSS)
Target: Range of US entities, including private businesses, government agencies, defense contractors, law firms, and academic institutions

Tactics: Exploited four zero-day vulnerabilities in Microsoft Exchange Server software, installing web shells that provided persistent remote access to targeted systems

In response to the breach, the Biden administration issued a joint condemnation with key allies, the European Union, NATO, and the United Kingdom, marking the first time the US government publicly attributed a major cyber operation to China. Although the US Department of Justice did not indict individuals specifically for the Microsoft Exchange hack, it did charge four Chinese nationals affiliated with the MSS for broader cyberespionage activities. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-02, mandating federal agencies to patch or disconnect vulnerable Exchange

servers. In May 2021, the White House issued Executive Order 14028 to enhance national cybersecurity, and in April 2021, the FBI obtained court approval to conduct a mass remote operation to delete malicious web shells from privately owned Exchange servers without prior individual consent.

The Chinese government denied any involvement in the operation or the existence of Hafnium as a state-backed entity. Beijing accused the US of politicizing cybersecurity and called for the presentation of concrete technical evidence before making credible attributions. Chinese officials also deflected criticism by referencing the NSA's global surveillance operations revealed through the PRISM program and Edward Snowden's leaks. Hafnium itself did not issue any public statements and remained out of the media spotlight. The group's name, "Hafnium," was determined by Microsoft's Threat Intelligence Center (MSTIC), further obscuring the group's identity and raising questions about its potential affiliation with China's People's Liberation Army (PLA).

Operation CuckooBees was one of the most impactful intellectual property (IP) theft campaigns between 2019 and 2022.

Perpetrator: APT41, Barium or Winnti, linked to the Ministry of State Security (MSS)

Target: US and European defense, aerospace, energy, pharmaceutical, and manufacturing sectors

Tactics: Multi-stage infection chains, custom malware, and covert data exfiltration techniques

The stolen data is believed to have contributed to the advancement of China's industrial base and military capabilities. Before the operation was publicly exposed by cybersecurity firm Cybereason in 2022, one in five US corporations had experienced IP theft. In response, the US Department of Justice indicted five Chinese nationals affiliated with APT41 and placed several Chinese technology firms on the Commerce Department's Entity List, restricting their access to US technologies. The US government also issued public warnings and advisories, including alerts from the Cybersecurity and Infrastructure Security Agency (CISA), detailing Chinese cyber espionage tactics and mitigation strategies. In March 2023, the Biden administration released a new National Cybersecurity Strategy, explicitly addressing state-sponsored IP theft

and supply chain vulnerabilities, with repeated references to persistent threats from Chinese actors like APT41.

Beijing categorically denied involvement in the cyberattacks and stated that no credible evidence emerged linking Chinese state actors to the perpetrators. This approach marked a contrast with Russia's typical denials, which often dispute involvement broadly without directly addressing ties to specific APT groups. Chinese officials turned the accusations back on the US, citing Washington's own global surveillance programs, revealed in the Snowden leaks, and accusing the US of offensive cyber operations. Chinese state-run media outlets like Global Times, Xinhua, and CGTN framed the indictments as politically motivated attempts to curb China's technological rise and infringe upon its cyber sovereignty. APT41 did not issue any public statements in the wake of the disclosures. However, cybersecurity analysts observed marked shifts in the group's behavior, including changes to malware toolsets, command-and-control (C2) infrastructure, and domain replacement strategies, suggesting operational adaptation in response to public exposure. Despite the indictments, none of the five named individuals have been arrested or extradited.

APT1 was one of the earliest and most notable groups publicly and credibly tied to a foreign military unit.

Perpetrator: APT1, linked to the Chinese government (PLA Unit 61398)

Target: Between the mid-2000s and early 2013, APT1 targeted more than 140 companies across over 20 industries, focusing primarily on the US and English-speaking countries.

Tactics: Deployment of Remote Access Trojans (RATs), credential harvesting, and extensive data exfiltration

The 2013 Mandiant report that exposed APT1's ties to the PLA revealed that the group maintained persistent access to some networks for extended periods, from several months to years, suggesting a systematic campaign of intellectual property theft. In 2014, the US Department of Justice indicted five officers from Unit 61398 for cyber-enabled theft of trade secrets. Diplomatically, the US responded with public condemnations while engaging in dialogue, resulting in the 2015 US–China Cyber Agreement. This agreement included a pledge

to refrain from engaging in cyber-enabled commercial espionage, though its enforceability remains questionable.

China, in turn, denied all involvement in the cyberattack and the existence of Unit 61398. Chinese officials deflected blame by pointing to US cyber operations exposed in the Snowden leaks and dismissed the Mandiant report as a politically motivated work of amateurs. Although APT1 did not issue a public response, the group's activity decreased sharply following the report's publication, suggesting that they either disbanded or restructured to evade future detection. Analysts believe that APT1 was split into multiple operational units within China's broader cyber espionage apparatus.

When comparing cyber operations originating from Russia and China, it becomes clear that the US has largely relied on diplomatic and legal tools such as sanctions and indictments, whose mechanisms often lack enforceability. In contrast to its approach with Russian cyber actors, Washington imposed relatively few sanctions in response to Chinese-backed hacks. This restraint may reflect the deep economic interdependence between the two nations, potentially encouraging Chinese threat actors to conclude that the strategic benefits of cyberespionage outweigh the limited diplomatic consequences.

US Framework and Policy Discussion

On November 27, 2024, the UN General Assembly adopted the Cybercrime Convention or the Convention on Cybercrime: Strengthening International Cooperation to Combat Crimes Committed Through ICT Systems, which became the first international criminal justice treaty in over 20 years. The convention aims to make responses to cybercrime quicker and better coordinated, establishing a global framework and providing capacity-building to countries with limited resources. The Convention will be open to signatures and ratification in 2025 in Hanoi, Vietnam, where countries will have to recognize the text as international law that domestic jurisdictions have to conform to. The Economic World Forum has pushed for the creation of an International Cybercrime Coordination Authority (ICCA) to coordinate enforcement and responses to cybercrimes across nations, as well as establishing extradition laws to enforce national indictments. None of these efforts, however, have produced a regulated approach to which the 5 Permanent Members of the Security Council (US, UK, China, France, and Russia)

could subscribe, indicating a lack of enforceability of the efforts to establish an international framework for cyber espionage.

While identifying patterns and techniques the United States employs in response to cyber espionage by Russian and Chinese state actors is essential, it is equally important to understand the broader principles that shape US responses to cyberattacks. The legal framework governing cyber espionage in the U.S. is primarily grounded in two key statutes: the Espionage Act and the Computer Fraud and Abuse Act (CFAA). The US employs a dual approach of deterrence by denial and deterrence by cost imposition. Deterrence by denial aims to prevent adversaries from achieving their objectives, often through defensive measures such as network segmentation, deception tactics, and cyber resilience. Its effectiveness is often measured by the absence of successful malicious activity. In contrast, deterrence by cost imposition seeks to raise the perceived costs and risks for adversaries, using offensive cyber capabilities, legal actions, and the credible threat of retaliation to discourage hostile actions.

In practice, the US response to cyber espionage includes a range of tools and measures, which form a comprehensive approach that combines legal, diplomatic, economic, and technological measures to defend against and respond to cyber espionage.

- Diplomatic Measures: These include official condemnations, joint public statements with allies, and coalition-building efforts aimed at isolating or pressuring the perpetrator
- Legal and Economic Measures, including court-authorized cyber operations, like the FBI's action following the Microsoft Exchange hack, indictments by the Department of Justice (DOJ), and asset forfeiture to hold attackers accountable. Economic measures come in the form of sanctions, trade restrictions, and export controls. Due to the autocratic nature of the international system, the lack of an enforceable international body means that indictments and sanctions lack enforcement and are dismissed by adversaries as symbolic. A more structured sanctions framework can make these measures more effective in deterring malign behaviors.
    - There have been successful attempts to enforce the indictments, however. At the request of the US authorities, the Italian authorities took a Chinese national, Xu Zewei,

into custody in Milan in July 2025, for his involvement in espionage between February 2020 and June 2021 and participation in the HAFNIUM campaign described earlier. While Xu Zewei awaits extradition to the US, this case is one of the first instances of an enforceable indictment for cyber espionage, giving hope that future legal efforts can produce tangible results.

- Private Sector Collaboration: The government frequently partners with private companies to issue public guidance, mitigation frameworks, and threat intelligence. The US, however, should involve private companies from the beginning steps of any investigation, as their expertise and first-hand experience with hacker groups can prove effective in attack mitigation and response frameworks.
- Offensive Cyber Capabilities: Initiatives like the Defend Forward strategy and actions authorized through Presidential Policy Directives enable the US to proactively disrupt cybersecurity operations.
- Policy and Strategy Development: Long-term cybersecurity engagement is guided by national strategies and policies such as the National Cybersecurity Strategy, Executive Order 14028, and the Cyber Defense Policy.
- Interagency Cooperation: National Cyber Investigative Joint Task Force (NCIJTF), established in 2008, connects over 30 partnering agencies to share information in response to cyber-attacks. Yet, as agencies like the FBI focus on domestic threats and have an enforcement function, while the CIA collects foreign intelligence, the federal government should establish a comprehensive collaborative initiative to encourage information sharing to enable a broader understanding of cyber hackers and their domestic targets.
- Multilateral Cooperation: At the 2014 NATO Summit in Wales, member states formally recognized cyber defense as a core component of collective defense. However, ambiguity remains over what constitutes a cyberattack severe enough to trigger Article 5, a principle that an attack on one is an attack on all. Since most cyber incidents to date have fallen below this threshold, the US must work with its NATO allies to establish a comprehensive response framework as well as cyber network security requirements for NATO membership.

Beyond polishing existing measures, the recent changes in CISA and CYBERCOM funding are bound to impact these policy initiatives as government agencies shift resources and capacity while maintaining the defense and security of networks. The bill includes an increase of $2 million for CISA to implement the Cyber Incident Reporting for Critical Infrastructure Act and a $3.2 million increase for the CISA cybersecurity division's critical infrastructure program, while the overall funding will decrease by $134 million to become $2.7 billion in 2026, rather than by almost $500 million as proposed by President Trump earlier. The Bill also allocated $250 million for Cyber Command for "artificial intelligence" and another $20 million toward cybersecurity programs at the Defense Advanced Research Projects Agency. Through the current shifts in funding and staffing, the federal government must ensure that federal agencies like CISA and CYBERCOM can combat incoming cyber espionage attacks and provide timely and effective responses to the adversaries and perpetrators.
