U.S. House Committee on Homeland Security

Adam Meyers
Sr. Vice President, Counter Adversary Operations
CrowdStrike

"Unconstrained Actors: Assessing Global Cyber Threats to the Homeland"
January 22nd, 2025

Chairman Green, Ranking Member Thompson, members of the Committee, thank you for the opportunity to testify today. My name is Adam Meyers, and I serve as Sr. Vice President for Counter Adversary Operations at CrowdStrike. For over a decade, I've led the company's practice area on monitoring and disrupting cyber threats. The overwhelming majority of attention during that time, and in particular over recent months, has focused on the People's Republic China (PRC).[1] So I'll focus my remarks today on threats from that country and discuss other threats at a high-level.

As a leading U.S. cybersecurity company, CrowdStrike has a useful and often quite textured vantage point on malicious activities in cyberspace. Protecting organizations with our cybersecurity technology, threat intelligence, and incident response services, we confront a full range of cyber threats. We defend many components of the U.S. Federal government and serve as a commercial cybersecurity provider for major technology companies, 8 of the top 10 financial services firms, thousands of small- and medium-sized businesses, as well as all manner of critical infrastructure entities and many foreign companies. China-nexus adversaries target each of these sectors heavily, as do threat actors affiliated with other nations.

As I've noted in a recent testimony, we started CrowdStrike in large part due to the growing impact of unchecked cyber threats–frequently from China–and the inability of existing security tools to meet this challenge. In 2011, it wasn't uncommon to see Chinese campaigns spanning scores of victims, with a multi-year duration, using extremely basic tactics, techniques, and procedures (TTPs). At that time, cybersecurity was focused on preventing the most prevalent threats, rather than the most impactful ones. Moreover, it was considered impolite, or even counter to one's economic interests, to call out this activity directly. I'm proud of the work our team–and the cybersecurity community more broadly–has done over the intervening years to change this perception. Still, there's clearly more work to be done.

[1] This testimony draws in part from a previous one I delivered on "Big Hacks & Big Tech: China's Cybersecurity Threat," before the U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law on November 19th, 2024. https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/2024-11-19pm-testimony-meyers.pdf.

At CrowdStrike, we utilize a cryptonym-based naming convention to characterize adversaries. This has become a best practice, as it permits researchers the flexibility to update attribution, account for reorganizations, and manage multiple actors with the same institutional affiliation. We assign a cryptonym once we achieve a reasonably robust confidence level in our attribution, and designate China-based adversaries as "PANDAs."[2] At present, we track 64 distinct PANDA adversaries, 20 of which have been recently observed, as well as a large number of other "activity clusters" with likely ties to China, but lower attribution fidelity.

Key Threat: People's Republic of China

After over a decade of investing in programs to strengthen China's cybersecurity ecosystem, China's cyber capabilities have matured to achieve at least parity with those of world cyber powers. Chinese threat actors operate complex, sophisticated, meaningfully obfuscated, and often highly effective offensive cyber operations targeting every region and every industry vertical. Recent campaigns demonstrate the ability to compromise large, well-resourced, and well-defended enterprises operating as providers for the rest of the technology ecosystem. From an intelligence perspective, these examples highlight a growing emphasis within Chinese operations on "upstream" or "bulk" collection, which is notable for its efficiency, scale, and potential for impact. Other campaigns are suggestive of pre-positioning capabilities relevant for disruptive and destructive cyber attacks.

Over the past year, China-nexus intrusions increased 150 percent across all sectors on average compared to 2023. These increases were most significant in the financial services, media, manufacturing, and industrials and engineering sectors, which all experienced between 200- and 300-percent increases in observed China-nexus intrusions compared to previous years. Even among the top three sectors China-nexus adversaries most commonly target—government, technology, and telecommunications—intrusion activity from China increased 50 percent in 2024 compared to 2023. Suspected China-nexus cloud intrusions increased six percent in 2024 across multiple commercial cloud services providers. Another marker of maturation in general is the complexity of successfully exploited systems.[3]

Here is a brief overview of a few recent and notable campaigns:

---

[2] These names generally take the form of a community- or researcher-derived codeword with some significance, followed by an animal type determined by the actor's geography or motivation. This name scheme is designed to be somewhat more descriptive than others, and can simplify communication and information sharing with government and industry counterparts, as well as assist clients' threat modeling process. For more detail, see: "Global Threat Landscape," https://www.crowdstrike.com/adversaries/.

[3] China-nexus adversaries continue to increase their stealthiness and knowledge of the environments they are operating in, using novel techniques to move quickly, move laterally and escalate privileges, and remain undetected. Notably, a widely-reported 2023 breach of a major software provider demonstrated the ability to manipulate encryption systems to arbitrarily mint keys to grant the threat actors access to sensitive systems. See, "Review of the Summer 2023 Microsoft Exchange Online Intrusion," Cyber Safety Review Board, March 20, 2024. https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

- Over the past year or so, **VANGUARD PANDA** (*Volt Typhoon*) drew significant attention from U.S. policymakers due to targeting critical infrastructure providers. Threat activity associated with this actor demonstrates the potential application for "preparation of the battlespace." That is, potential use of disruptive or destructive attacks preceding or coinciding with military hostilities. For initial access, the actor targeted ubiquitous unmanaged or perimeter (edge) devices and infrastructure.[4] These same edge devices that are integral to connecting networks to the internet provide a ripe attack surface for adversaries. Targeting these systems is fruitful because they are critical components for authentication and provide a pathway to compromise identities. These attacks are also relatively stealthy on account of reduced visibility from third-party security providers, minimal telemetry generated by system access and use, and limited forensic artifacts. Use of these techniques further limits the detection capabilities of defenders and the capacity to track adversary operations by researchers.
- At present, China-nexus adversaries heavily target telecommunications infrastructure likely in support of the intelligence collection goals of the PRC. **OPERATOR PANDA**[5] is one such adversary whose attacks have been widely reported. As noted above, this activity is consistent with tradecraft that we assess is designed to facilitate bulk collection and subsequently specific targeting. In some cases, the latter appears aimed at major U.S. political and national security officials.
- Other advanced adversaries such as **LIMINAL PANDA** also target the telecommunications sector and demonstrate extensive knowledge of its networks, including understanding interconnections between providers and the protocols that support mobile telecommunications.[6] Recently, this adversary compromised these networks by exploiting trust relationships between telecommunications organizations and poor security configurations, allowing them to create footholds to install multiple redundant routes of access across the affected organizations. The adversary ultimately emulated the global system for mobile communications (GSM) protocols to enable command-and-control (C2) and developed tooling to retrieve mobile subscriber information, call metadata and text messages, and facilitate data exfiltration. Actions on objectives indicated additional adversary aims of surveilling targeted individuals by gathering metadata about their cellular devices.

North Korea, Russia, Iran, and Beyond

As China's threat activity captures high-level attention, other threats continue to evolve. I'll mention a few high points here and can discuss at more length as appropriate.

---

[4] This is consistent with other China-nexus adversaries increasingly moving away from the use of low-sophistication methods for initial access like spear-phishing, weaponized USBs, and credential harvesting, instead favoring specific exploitation of vulnerabilities in edge devices like firewalls, gateways, or enterprise proxies to achieve initial access.

[5] This adversary's activity broadly aligns with previous China-nexus targeted intrusion activity tracked in industry reporting as *Salt Typhoon*.

[6] "Unveiling LIMINAL PANDA: A Closer Look at China's Cyber Threats to the Telecom Sector" CrowdStrike Blog, November 19, 2024. www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/.

- **North Korea.** Amid high-profile disruptive and destructive attacks in the mid-2010s, notably the Wannacry pseudoransomware attack and blended operation targeting Sony Pictures Entertainment, North Korea has engaged in significant financially-motivated threat activity since at least 2015. After 10 years of currency-generation campaigns, these operations have become a key lifeline to the regime while it is cut off from the international financial system due to sanctions. In addition to continuing to target banking and cryptocurrency targets, North Korea over the past few years has pivoted to campaigns placing malicious insiders in remote work positions. Beyond earning paychecks, these actors often attempt to steal intellectual property. In 2024, CrowdStrike Falcon OverWatch, our managed threat hunting service, responded to 304 incidents for a single prolific threat actor, FAMOUS CHOLLIMA, with nearly 40 percent of these representing insider threat operations.
- **Russia.** While Russia-nexus adversaries continued to focus on traditional Western targets and North Atlantic Treaty Organization (NATO) member states, the war in Ukraine continued to be the primary driver of these adversaries' 2024 operations, which were focused on intelligence collection against military, political, and diplomatic entities. A need for tactical intelligence also likely forced Russian adversaries to evolve their operations to keep pace with battlefield developments in Ukraine, as exemplified by adversaries associated with the GRU (a.k.a. GU, Main Directorate of the General Staff of the Armed Forces of the Russian Federation) heavily targeting mobile devices in Ukraine.
- **Iran.** In 2024, motivated by ongoing conflicts in the Middle East, Iran-nexus adversaries continued to extensively target Israeli entities. One threat actor, CHARMING KITTEN, collected traditional intelligence on regional policy experts, while other adversaries conducted destructive operations and information operations (IO), including targeting elections. Iran-nexus actors were also among the most notable groups over the past year leveraging generative AI support in the vulnerability landscape. Iran's government aims to use Large Language Models (LLMs) in vulnerability research and exploit development, as well as to enable vulnerability-patching systems for domestic networks.
- **Rest of the World**. While state-nexus threat activity is on the rise globally, CrowdStrike observed a concentration of activity in South Asia and the Middle East. Often, this threat activity is responsive to domestic politics and intra-regional conflict. However, many nation states increasingly leverage cyber capabilities more broadly, including by targeting U.S. entities, for intelligence collection and intellectual property theft.

Criminal and Hacktivist Threats

By volume, a meaningful share of threat activity targeting our customers comes from eCrime actors that seek to monetize malicious cyber activity. I'll share a few observations about that activity, as well as politically-motivated "hacktivist" actors, which continue to proliferate.

- **eCrime** actors continued to represent a meaningful majority of cyber threat activity by volume in 2024. The number of publicly named victims and CrowdStrike Intelligence's

direct observations of adversarial activity demonstrate that "Big Game Hunting" ransomware actors (i.e., those that target enterprises) remain the most significant eCrime threat to organizations across all geographical regions and industries. Over the past year, these actors continued a previously-observed trend of increasingly leveraging dedicated leak sites to publicly expose data in order to extort victims. However, if there's a positive news story anywhere in the cyber domain in 2024, it's that coordinated law enforcement operations like that which targeted BITWISE SPIDER (LockBit) in mid-February and Operation Endgame[7] in May sharply decreased the volume of key indicators we monitor like spam and bot activity, and ultimately forced adversaries to search for other initial-access methods. (I'll return to this theme in the *Recommendations* section, below.)

- **Terrorist organizations** are increasingly developing and maturing their offensive cyber operational capabilities. In 2024, CrowdStrike Intelligence attributed (that is, graduated from a cluster of linked activity to a formally named adversary) three terrorist-related adversaries: one affiliated with Hamas, one with the Houthi movement in Yemen, and one with Lebanese Hezbollah. More broadly within the hacktivist space, we observed a potential emerging trend where a number of hacktivists were observed engaging in financially-motivated eCrime in addition to threat activity furthering traditional social, political, or nationalist ideologies.

Recommendations

I'd like to conclude with a few recommendations for various government entities as well as enterprises and their defenders. Our respective responsibilities differ, but across the board, our shared goal must be to raise the cost for the adversary to infiltrate our networks and reduce the impact if they do. This means we need to harden our defenses and degrade the ability of the adversary to wage successful, undetected attacks.

To this point, I've mainly focused on the threat environment and the policy landscape for confronting those threats. But I'd be remiss if I didn't at least briefly highlight some of the operational capabilities that all enterprises–whether private or public sector–can leverage to actually defend themselves. From my experience, the highest-leverage approaches are:

- Taking increasing care to defend **identity** across the enterprise. Compromised identities are at the core of most of the threat activity CrowdStrike has observed and responded to over the past several years. Better identity security enables a radical reduction in threats. Identity Threat Detection and Response (IDTR) tools are an important, intelligence-informed layer of the broader identity picture.
- Maintaining **visibility** across increasingly complex, distributed, and federated networks. Today, that requires instrumenting and monitoring traditional endpoints like laptops and desktops, network infrastructure, cloud environments, mobile and IOT devices, and

[7] "Operation Endgame: Coordinated Worldwide Law Enforcement Action Against Network of Cybercriminals," Federal Bureau of Investigation, May 30, 2024. https://www.fbi.gov/news/press-releases/operation-endgame-coordinated-worldwide-law-enforcement-action-against-network-of-cybercriminals.

increasingly, Software-as-a-Service (SaaS) applications. Such monitoring generates valuable security telemetry, designed to alert defenders to threats across each of these vectors. Endpoint Detection and Response (EDR) tools are essential to this end.

- Developing an **integrated** picture of IT extended environments, particularly in the face of increasing cross-domain threats (i.e., those targeting different platforms and systems). Use of technologies like Next-Generation Security Information and Event Management (NextGen SIEM) tools can help make this duty more straightforward for organizations of all sizes.

Executive Branch. The federal government can enhance national security by doing cybersecurity well, adopting best-in-class technologies, and disrupting adversary infrastructure. As the federal government takes on initiatives to modernize and create efficiencies during this period of transition–as well as review and deprecate legacy programs and systems–there's a significant opportunity to move the needle in each of these areas.

While key U.S. federal departments and agencies have come a long way over the past number of years on defense, there's still progress to be made. The U.S. government itself faces among the most severe threat environments of any organization globally. Federal organizations must lead by example by ensuring federal departments and agencies have the best tools, best training, and most informed concepts of operations for defense available. This will require appropriately resourcing and empowering Federal CIOs and CISOs. Helpfully, findings from successfully defending federal agencies can support the development of best practices of value to other sectors, like academia, commercial enterprises, and nonprofits.[8]

Several key departments can also do more to proactively meet and defeat cyber threats. Government missions and responsibilities change over time, catalyzed by evolving opportunities, constraints, and conditions. Based on current competencies and authorities, and my observations from facilitating collaboration widely over a long period, I'll outline a few suggested focus areas. For its part, DHS, including CISA, can double down on promoting federal cybersecurity so agencies are coordinated and operationally aligned to defeat threats. Threat actors are adept at exploiting gaps and seams, so a unified approach is essential. In recent years, the federal government has deployed 920,000 endpoint detection and response (EDR) sensors, which has helped.[9] The task now is to layer additional mission capabilities into this infrastructure to improve vulnerability management, IT hygiene, and to enable better and more responsive managed threat hunting. CISA can also refocus on critical infrastructure cybersecurity, particularly in light of continued, consequential attacks from actors like VANGUARD PANDA and OPERATOR PANDA.

---

[8] For specific recommendations on improving federal cybersecurity, *see Rob Sheldon, Testimony on "Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs"* U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection (September 19, 2023). https://www.crowdstrike.com/wp-content/uploads/2023/11/9.19-CHS-Federal-Cyber-Testimony.pdf.

[9] "Securing Federal Networks: Evolving to an Enterprise Approach," Cybersecurity and Infrastructure Security Agency, January 13, 2025. https://www.cisa.gov/news-events/news/securing-federal-networks-evolving-enterprise-approach.

The FBI tends to lead on performing threat actor infrastructure takedowns and coordinated law enforcement actions. Efforts along these lines do take place and can be successful, such as with Operation Endgame (cited above). Still, from my vantage, over the past decade the threat environment has worsened more rapidly than our capacity to execute such operations has increased. It's now worth asking: in collaboration with international partners, what might we do to increase the tempo of disruptions by 5x? Or by 10x? It may take that scale to durably impact threat actors' operations sufficiently to raise their cost of doing business and offer meaningful relief to victims. CISA can do more to promote this mission area by providing textured, real-time insights from stakeholders, including major IT and cybersecurity providers and critical infrastructure entities, about the most pressing threats. This can inform prioritization.

The National Security Agency, Cybercommand, and other elements of the U.S. defense and intelligence enterprise have complementary roles in disrupting threat actors and their infrastructure. A full discussion is beyond the scope of this testimony but I will highlight the importance of ongoing efforts to secure the Defense Industrial Base.

Legislative Branch. For Congress' part, it's appropriate to perform oversight to ensure federal agencies are actively pursuing the objectives outlined above as well as ensuring resource alignment and accountability. Further, to the extent that some of the defense I outlined above appear out of reach for the average small business in your state, it's appropriate to engage in a more meaningful conversation than we as a community have had to date on the use of tax credits, rebates, or other incentives to make best-in-class cybersecurity tools and training more accessible.

Thank you again for the opportunity to testify today, and I look forward to your questions.

###