U.S. HOUSE JUDICIARY COMMITTEE
Subcommittee on Courts, Intellectual Property, and the Internet

Robert Sheldon
Sr. Director, Public Policy & Strategy
CrowdStrike

Testimony on "IP and Strategic Competition with China: Part III – IP Theft, Cybersecurity, and AI"

September 20, 2023

Chairman Issa, Ranking Member Johnson, members of the Subcommittee, thank you for the opportunity to testify. The People's Republic of China presents significant threats to U.S. national interests today. This Subcommittee, in the previous hearings in this series, has done an admirable job of highlighting the scope and scale of these threats. From military and diplomatic arenas, to all areas of economic and trade relations, the U.S. faces a formidable set of challenges.

Arguably, the cyber domain is the central front of the U.S.-China competition. For two decades, cyber threat actors associated with the Chinese government have been among the most aggressive and persistent adversaries we face. In addition to pursuing national security and defense information, these actors relentlessly target economic data, trade secrets, and intellectual property. They further spy on minorities, religious groups, political dissidents, journalists, activists, and all manner of other participants in civil society.

CrowdStrike, as a leading U.S. cybersecurity company, has a useful vantage point on China's activities in this space. As a cybersecurity technology, threat intelligence, and services provider for the Federal government, as well as a commercial provider serving major technology companies, 15 of the top 20 largest U.S. banks, and thousands of small and medium sized businesses, we confront all manner of cyber threats.

Today, the cyber challenge from China is heightened because it coincides with an ongoing technological revolution related to Artificial Intelligence (AI). Cybersecurity firms increasingly leverage AI to defeat cyber threats rapidly and at scale. But adversaries too are exploring the use of AI to make their own attacks more effective. Both of these trends are likely to accelerate over the coming years.

U.S.-China competition over the foundational technologies that underpin AI complicates matters further. Beijing recognizes AI as a key technology that merits attention and investment in its own right, and has for some time. But export controls and other trade restrictions implemented over the past several years raise the stakes, limiting China's access to supporting technologies like advanced semiconductors. This elevates already significant cyber risks to semiconductor R&D and manufacturing, and the sector more broadly.

Cyber Threats from China

As a brief primer, CrowdStrike tracks threat actors according to three primary motivations: nation state, criminal, or 'hacktivist' interests. When we develop sufficient visibility on these groups to identify or attribute them, we assign them a codename.[1] Under this system, Chinese government-related threat actors are referred to broadly as *PANDAs*. Individual groups receive specific names like *JUDGMENT PANDA* or *VANGUARD PANDA*, which often derive from community-based identifiers.

These groups are numerous and prolific. Out of over 220 named actors CrowdStrike tracks at the time of this writing, over 50 are PANDA groups. For scale, that exceeds the number of groups we track from Russia and North Korea combined. These groups span China's military, intelligence, and security services as well as associated contractor groups. Each one's entire *raison d'etre* is to advance Chinese Communist Party (CCP) interests through hacking campaigns, whether by targeting U.S. or other foreign institutions and entities.

It's clear that certain PANDA actors are quite capable. For example, in July, Chinese threat actors once again exploited authentication flaws in a major software company's office productivity and email platform – this time resulting in threat actors' unauthorized access to the email of two Cabinet Secretaries.[2] Under slightly different geopolitical conditions or adversarial objectives, these incidents could have enabled scaled destructive attacks.

Cybersecurity and AI

The popularization of generative AI tools over the past year, such as DALL-E and ChatGPT, has catalyzed significant experimentation from practitioners across numerous technical disciplines. Like other disciplines, there are many potential applications of generative AI within cybersecurity–for defenders and attackers alike. But the story of AI and cybersecurity long predates the current groundswell of interest precipitated by broad access to these new tools.

For most of the history of cybersecurity, defenses were primarily reactive. Researchers or incident responders would investigate a breach, identify a related indicator (e.g., Web domain) or file, and add details about it (e.g., a file hash) to a register of suspicious or malicious content. Periodically (e.g, once a day), a security vendor would push updates from this register out to security tools like

---

[1] For further detail on the rationale for this system, see *George Kurtz, Testimony on Cybersecurity and Supply Chain Threats,* Senate Select Committee on Intelligence (February 23, 2021) https://www.crowdstrike.com/wp-content/uploads/2021/03/george-kurtz-senate-testimony-on-cybersecurity-and-supply-chain-threats-022321.pdf, footnote 2.

[2] See Nakashima, Ellen. Menn, Joseph. Harris, Shane. *Chinese hackers breach email of Commerce Secretary Raimondo and State Department officials.* The Washington Post, July 14, 2023. https://www.washingtonpost.com/national-security/2023/07/12/microsoft-hack-china/; and *Results of Major Technical Investigations for Storm-0558 Key Acquisition*, Microsoft, September 6, 2023. https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/.

legacy antivirus solutions. Among the many problems with this approach, five were particularly untenable:

1. The model essentially assumed one or more sacrificial victims in order to identify the malicious activity in the first instance.
2. The need for a human "in the loop," deciding that something is malicious, meant that the process would scale very poorly.
3. The latency caused by once daily updates meant attackers could breach multiple victims in a single campaign without initially risking detection from security tools.
4. A single change to a malicious file's binary, or signature, such as by modifying the header of the file, would allow previously-known malware to run undetected.
5. Logs were preserved on-premise and could be tampered with, meaning no immutable record of their activity would be preserved.

This broken model was disrupted a decade ago when CrowdStrike (and later other vendors) introduced technology focused on detecting and preventing indicators of attack. Rather than using a file scan on a computer as a proxy for whether an organization was compromised, the innovation focused on detecting anomalous behavior in the chain of system events. The new approach would deploy a tiny software agent to every endpoint on a network. The agent would stream hashes of system events back to a secure cloud environment. AI and Machine Learning applied against this data in the cloud, as well as AI deployed in the software agent itself, would work in concert to detect and prevent threats in real-time.

Crucially, this approach would work at scale even for completely novel threats. Exhibiting a few shared attributes or characteristics of known malicious activity would be sufficient to trigger a detection and prevention. Helpfully, as the corpus of training data (both legitimate and malicious) grew over time, the AI underpinning this capability became more precise. This drove down the risk of false positives and false negatives.[3]

While the example above describes next-generation antivirus capabilities, there are numerous other cybersecurity applications and tools that similarly benefit from AI. Identity Threat Detection and Response tools can apply AI against data gathered from previous authentication history and elsewhere to dynamically issue multi-factor authentication (MFA) challenges during suspicious login attempts.[4] Vulnerability management tools can leverage AI to dynamically score vulnerabilities in order to help defenders prioritize patching and mitigation.[5]

Large Language Models (LLMs) also have applications for cyber defense. There's a notable deficit of skilled cybersecurity professionals, with one industry study estimating the unmet demand for cybersecurity workers in 2022 to be 411,000; and another study estimating that employer demand

---

[3] *See Charlotte AI: AI Powered Protection,* CrowdStrike, https://www.crowdstrike.com/falcon-platform/artificial-intelligence-and-machine-learning/.

[4] *See CrowdStrike White Paper on Defending the Enterprise with Conditional Access Anywhere,* CrowdStrike, https://www.crowdstrike.com/resources/white-papers/defending-the-enterprise-with-conditional-access/.

[5] *See How Falcon Spotlight's ExPRT.AI Works*, CrowdStrike, https://www.crowdstrike.com/wp-content/uploads/2021/10/crowdstrike-ml-rating-infographic.pdf.

for cyber workers exceeded supply by 32% .[6] But the use of LLMs can make core cybersecurity workflows more accessible, because users can now interface with tools via natural language.[7] This will enable practitioners to more easily make more meaningful contributions more quickly.

Threat actors will also leverage AI, and we've observed "chatter" from threat actors discussing the possibilities.[8] While this description is not exhaustive, a few near-term threats that merit monitoring include:

- *Lure crafting*. Adversaries could leverage LLMs to write more persuasive lures for phishing attacks that, for example, trick victims into clicking a malicious link. This is particularly salient for threat actors working in a non-native language.
- *Vulnerability discovery*. Adversaries could employ AI techniques to assist in *fuzzing* or assessing crash dumps or related data to identify vulnerabilities.
- *Exploit and malware development*. LLMs have already proven a fairly effective aid in software development, and adversaries could use them to assist in the production of malicious code. Although still subject to hallucinations (e.g., calling non-existent functions or code libraries), outputs are likely to improve as LLMs themselves continue to improve over time.
- *Bulk data processing*. Adversaries could use AI to facilitate the processing of large collections of open source data, or data exfiltrated from breaches, for a variety of malicious purposes. These include identification of sensitive information that could later be used for targeting or extortion.
- "*Deepfakes*." Generative AI can produce deceptive audio or video, which might later be amplified on traditional or social media, to facilitate extortion or influence operations.[9]

In addition to leveraging AI for the purposes described above, a few other issues at the nexus of cybersecurity and AI merit continued attention:

- Adversaries will seek to compromise accounts for paywalled generative AI tools. They could seek access for any number of purposes.
- Adversaries will attempt to defeat AI leveraged in legitimate cybersecurity tools through adversarial examples. To the extent this is successful, the tools' capabilities will degrade or fail.
- Adversaries may target legitimate AI tools themselves with data poisoning and prompt injection attacks. This would affect outputs for other users.
- There's longstanding interest from adversaries in intellectual property related to the systems (e.g., semiconductors, semiconductor fabrication, and cloud providers) that serve as

---

[6] *See The National Cyber Workforce and Education Strategy,* Office of the National Cyber Director, The White House, July 31, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

[7] See, for example, *Charlotte AI: Accelerate Cybersecurity with Generative AI Workflows* CrowdStrike, https://www.crowdstrike.com/products/charlotte-ai/.

[8] This section draws heavily from analysis on a forthcoming episode ("AI through the lens of Adversaries and Defenders") of CrowdStrike's Adversary Universe Podcast, which will be released later this month. https://www.crowdstrike.com/resources/adversary-universe-podcast/. This section also references techniques associated with Machine Learning.

[9] *See Contextualizing Deepfake Threats to Organizations,* Cybersecurity Information Sheet by NSA, FBI, CISA, September 2023. https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF

the substrate for AI development. This will likely increase as AI develops and export controls impact commercial markets for these technologies.

Recommendations

Continued AI innovation. Although threat actors will leverage AI, it's important to recognize the significant, current benefits AI is driving in cybersecurity tools today. These tools overperform by a wide margin legacy tools that do not leverage AI. Continued innovation in this space is essential. Adversaries will continue to leverage AI to innovate, regardless of the rules of the road for defenders.

Threat intelligence. The security community should continue to monitor threat actors interested in intellectual property theft and the use of AI for malicious purposes. The more we understand about these groups, their targeting practices, their resources, and their constraints, the more accurate a threat model we can develop to help defend targeted industries, organizations, and individuals.

U.S. Federal cybersecurity. The U.S. government faces among the most severe threat environments of any organization globally. To the extent that threat actors are able to leverage AI to enhance their capabilities, the U.S. government will be an early target. Moreover, findings from successfully defending Federal agencies can support the development of best practices of value to other sectors, like academia, commercial enterprises, and nonprofits.[10]

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

###

[10] 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://homeland.house.gov/hearing/subcommittee-on-cybersecurity-and-infrastructure-protection-hearing-entitled-evaluating-cisas-federal-civilian-executive-branch-cybersecurity-programs/