Atlantic Council

CYBER STATECRAFT INITIATIVE

Crash (exploit) and burn

Securing the offensive cyber supply chain to counter China in cyberspace

Winnona DeSombre Bernsen

CYBER STATECRAFT
INITIATIVE

The Cyber Statecraft Initiative works at the nexus of geopolitics, technology, and security to craft strategies to help shape the conduct of statecraft and to better inform and secure users. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

Author

Winnona DeSombre Bernsen

Cover: Blurred photo of a malware sample in the Ghidra reverse engineering.

Source: Govanify blog post, December 23, 2019, https://govanify.com/post/kh2ai/.

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

2025

Table of contents

Executive summary

If the United States wants to increasingly use offensive cyber operations internationally, *does it have the supply chain and acquisition capabilities to back it up—especially if its adversary is the People's Republic of China?*

Strategic competition between the United States and China has long played out in cyberspace, where offensive cyber capabilities, like zero-day vulnerabilities, are a strategic resource. Since 2016, China has been turning the zero-day marketplace in East Asia into a funnel of offensive cyber capabilities for its military and intelligence services, both to ensure it can break into the most secure Western technologies and to deny the United States from obtaining similar capabilities from the region. **If the United States wishes to compete in cyberspace, it must compete against China to secure its offensive cyber supply chain.**

This report is the first to conduct a comparative study within the international offensive cyber supply chain, comparing the United States' fragmented, risk-averse acquisition model with China's outsourced and funnel-like approach.

Key findings:

1. Zero-day exploitation is becoming more difficult, opaque, and expensive, leading to "feast-or-famine" contract cycles.
2. Middlemen with prior government connections further drive up costs and create inefficiency in the US and Five Eyes (FVEYs) market, while eroding trust between buyers and sellers.
3. China's domestic cyber pipeline dwarfs that of the United States. China is also increasingly moving to recruit from the Middle East and East Asia.
4. The United States relies on international talent for its zero-day capabilities, and its domestic talent investment is sparse – focused on defense rather than offense.
5. The US acquisition processes favor large prime contractors, and prioritize extremely high levels of accuracy, trust, and stealth, which can create market inefficiencies and overly index on high-cost, exquisite zero-day exploit procurements.
6. China's acquisition processes use decentralized contracting methods. The Chinese Communist Party (CCP) outsources operations, shortens contract cycles, and prolongs the life of an exploit through additional resourcing and "n-day" usage.
7. US cybersecurity goals, coupled with "Big Tech" market dominance, are strategic counterweights to the US offensive capability program, demonstrating a strategic trade-off between economic prosperity and national security.
8. China's offensive cyber industry is already heavily integrated with artificial intelligence (AI) institutions, and China's private sector has been proactively using AI for cyber operations.
9. Given the opaque international market for zero-day exploits, preference among government customers for full exploit chains leveraging multiple exploit primitives, and the increase in bug collisions, governments can almost never be sure they truly have a "unique capability."

Recommendations:

1. **Strengthen the supply chain** by creating Department of Defense (DOD) vulnerability research accelerators, funding domestic hacking clubs and competitions, expanding the National Security Agency's (NSA) Centers of Academic Excellence in Cyber Operations (CAE-CO) program, and providing legal protections to security researchers.
2. **Improve acquisition processes** by establishing a government-sponsored vulnerability broker in a federally funded research and development center (FFRDC) to decentralize and simplify exploit purchases while increasing cyber capability budgets and expanding research on automated exploit chain generation.
3. **Adjust policy frameworks** to consider counterintelligence strategies in the zero-day marketplace (burning capabilities of malicious actors while recruiting willing 'responsible' actors into a more formal pipeline), funding n-day research through US Cyber Command (USCYBERCOM) where appropriate and leveraging alliances like the Pall Mall process to counter China's growing cyber dominance.

Without meaningful reforms, the United States risks ceding to China whatever strategic advantage it has left in cyberspace. By fostering a more deliberate offensive cyber supply chain and adjusting acquisition strategies, **the US can retain a steady supply of offensive cyber capabilities to maintain its edge in the digital battlefield.**

Background

Securing the zero-day supply chain (and its private sector market) is crucial to US-China conflict in cyberspace

China and the United States are engaged in strategic competition in cyberspace. While cyber operations are often an overlooked area of geopolitical power, both countries' militaries, intelligence communities, and law enforcement agencies conduct cyber operations. They do so to obtain intelligence crucial to national security, assist conventional military operations, and even create kinetic effects to achieve strategic goals. To make a cyber operation possible, one must have the capacity to break into a particular system: offensive cyber capabilities (and particularly zero-day vulnerabilities) are the necessary strategic resources required to conduct such operations.

> "America has incredible offensive cyber power. We need to stop being afraid to use it."
>
> *– Alexei Bulazel, incumbent special assistant to the president and National Security Council senior director for Cyber.*

> "Geopolitical conflicts are increasingly shifting to cyberspace, including tensions between the U.S. and China. Technology is therefore no longer just an area for opportunity, but also a battleground for control, values and influence."
>
> *– Jeremy Fleming, former GCHQ director.*

The United States clearly wishes to further leverage its cyber prowess in the international arena, particularly against the People's Republic of China (PRC).[1] Doing so would help the United States protect its vital national security and economic interests, international partnerships, and norms. However, to operationalize a "cyber power" strategy, the United States must acquire enough high-end capabilities to ensure it can achieve such strategic goals. Moreover, the timeline for implementing these policies is urgent, given the increasing potential for conflict with China in the coming years. Thus, given the international privatized offensive cyber capability marketplace, how can the United States and its allies continue to ensure the availability of offensive cyber capabilities (focusing on zero-day vulnerabilities), while limiting China's access to those same capabilities?

> "China remains the most active and persistent cyber threat to US Government, private-sector, and critical infrastructure networks."
>
> *– ODNI, 2024 Annual Threat Assessment.*

> "The era of network security has arrived, and vulnerabilities have become a national strategic resource."
>
> *– Qihoo360 CEO Zhou Hongyi, Remarks at the 2017 China National Cyber Security Summit.*

Cyber operations consist of a variety of offensive cyber capabilities — many of the most crucial cyber capabilities involve the exploitation of "zero-day" vulnerabilities (also known as zero-days or 0days). Zero-day vulnerabilities are issues or weaknesses ("bugs") in software or hardware, typically unknown to the vendor and for which no fix is available— in other words, the vendor has had "zero days" to fix the issue. Some of these vulnerabilities are exploitable: an actor with knowledge of the vulnerability could write code that takes advantage of said vulnerability. This results in a "zero-day exploit"—code enabling a range of behaviors that could include establishing access into the computer system the software is installed on, escalating privileges on those systems, or remotely issuing commands.

The work of finding vulnerabilities and writing exploits, thanks to its strategic necessity to governments worldwide, has become a billion-dollar international services industry in the last 20 years. Private firms now often create cutting-edge offensive cyber capabilities for governments. Given the sensitivity around supporting government cyber operations, many of these firms do not openly advertise their services, shrouding the industry in secrecy. Between this secrecy and the variation in products offered (i.e., governments target different technology systems, and no two zero-days are identical), the supply chain for such capabilities is not only opaque to outsiders, but also to governments and even among players in the industry.

Within this highly fragmented and opaque market, large firms, like the United States' L3Harris or ManTech, frequently hold multi-million dollar valuations.[2] Notably, Israel's NSO Group's

1. David DiMolfetta, "Contractors Could Hack Back against Adversaries, Top Cyber Democrat Says,". NextGov, April 2, 2025, https://www.nextgov.com/cybersecurity/2025/04/contractors-could-hack-back-against-adversaries-top-cyber-democrat-says/404233/.
2. "L3harris Trenchant Ltd (Overview)," Pomanda, accessed April 3, 2025, https://pomanda.com/company/09068202/l3harris-trenchant-ltd.

worth reached $1 billion at its peak. [3] Meanwhile, individual US government agencies receive millions of dollars to procure offensive tools.[4] Such companies' tools have clearly been purchased by such government agencies and put to use in modern-day cyber operations. Notably, of all the zero-day vulnerabilities found exploited "in-the-wild" in 2023 and 2024 by Google, around 50 percent of them were attributed to commercial vendors that sell capabilities to government customers.[5] While this statistic only encompasses detected zero-day exploits, this is still a significant set of capabilities being provided by private sector actors.

The offensive cyber capability industry itself is international and ranges in professionalization depending on the region; companies in Russia, Israel, Spain, Singapore, and the United States all have varying relationships with their home governments, other firms (including middlemen and brokers), international government customers, and even cyber-criminal groups. However, the study of offensive cyber capabilities has largely over-indexed on firms based in Israel and Europe rather than the United States' greatest geopolitical rival: China.[6] This is surprising, as the Chinese hacking and cybersecurity ecosystem is robust. Chinese companies have, on multiple occasions, are directly linked to Chinese government-sponsored cyber operations against the United States. Moreover, the development of offensive cyber capabilities in the United States remains largely unstudied or examined in a way that does a disservice to the domestic hacker community.[7]

Why is this question important?

At first glance, it can be difficult to see why the private sector zero-day exploit market—a series of obscure companies selling code that can enable governments to break into widely-used software—would be important in preserving national interests in cyberspace, particularly against China. A simple explanation of this relationship is as follows: the United States and its allies rely on an increasingly digital world, and China is both a savvy adversary and hardened target in cyberspace.[8] When any country's intelligence community wishes to infiltrate high-value, hard-to-access digital targets, it likely must use zero-day exploits or other bespoke (i.e., custom-made or tailored) offensive cyber capabilities. Intelligence organizations from both the United States and China, due to decreasing internal supply and rising demand for such capabilities,[9] have increasingly relied on acquiring such exploits from the private sector zero-day exploit market.[10] However, the private sector zero-day market is murky and more international than policymakers expect; even if the United States and China are truly entering a "New Cold War," both countries still source capabilities from an overwhelmingly opaque international market of offensive cyber capability firms, and do not know if they are being supplied with potentially overlapping capabilities. In short, any cyber operation that relies on an acquired capability, conducted by the United States, China, or anyone else, **carries a counterintelligence and operational security risk, with no guarantee that they can source a similar capability in the future.** Thus, securing the cyber supply chain (understanding the industry, constraining malicious actors, and ensuring availability from trusted parties) is important to address such risks.

While former President Joe Biden's administration sought to constrain private sector actors with additional regulation and

3. Asaf Lubin, "Unpacking WhatsApp's Legal Triumph Over NSO Group," Lawfare, January 7, 2025, https://www.lawfaremedia.org/article/unpacking-whatsapp-s-legal-triumph-over-nso-group.
4. Sam Sabin, "Cyber's Big Budget Week," *Politico*, March 28, 2022, https://www.politico.com/newsletters/weekly-cybersecurity/2022/03/28/cybers-big-budget-week-00020739.
5. Maddie Stone and James Sadowski, "A Review of Zero-Day In-the-Wild Exploits in 2023," Google, March 27, 2024, https://blog.google/technology/safety-security/a-review-of-zero-day-in-the-wild-exploits-in-2023/; Sergiu Gatlan, "Google: Spyware Vendors Behind 50% of Zero-Days Exploited in 2023," BleepingComputer, March 27, 2024, https://www.bleepingcomputer.com/news/security/google-spyware-vendors-behind-50-percent-of-zero-days-exploited-in-2023/; Casey Charrier et al., "Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis," Google Cloud (blog), April 29, 2025, https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends.
6. Dave Aitel, "OffensiveCon23—Information Security Is an Ecology of Horrors and You Are the Solution," YouTube video, accessed March 8, 2025, https://www.youtube.com/watch?v=BarJCn4yChA&ab_channel=OffensiveCon.
7. Halvar.flake, "Book Review: 'This Is How They Tell Me the World Ends,'" ADD / XOR / ROL (blog), February 23, 2021, https://addxorrol.blogspot.com/2021/02/book-review-this-is-how-they-tell-me.html.
8. Jonah Victor, "China's Thickening Information Fog: Overcoming New Challenges in Analysis," Center for the Study of Intelligence 68, no. 23, September 2024, https://www.cia.gov/resources/csi/studies-in-intelligence/studies-in-intelligence-68-no-3-extracts-september-2024/chinas-thickening-information-fog-overcoming-new-challenges-in-analysis/.
9. Evan Rosenfield, "The NSA's Brain Drain Has a Silver Lining," Defense One, April 12, 2023, https://www.defenseone.com/ideas/2023/04/nsas-brain-drain-has-silver-lining/385051/.
10. Winnona DeSombre Bernsen, "Same Same, but Different, Margin Research, February 29, 2024, https://margin.re/2024/02/same-same-but-different/.

placing bad actors on the entities list,[11] these policies were framed around human rights concerns largely out of Europe and Israel. President Donald Trump's administration is moving away from this approach, focusing on China as a geostrategic threat over transnational digital repression framings,[12] as well as signaling willingness to engage with private sector actors in the space. The Trump administration, as of 2025, has accelerated plans for a US Cyber Command (USCYBERCOM) 2.0, focusing on working better with private industry partners.[13] This is a continuation of the first Trump administration's policies: Trump was the first president to delegate the authority for offensive cyber operations down to the secretary of defense (through National Security Presidential Memorandum–13) allowing USCYBERCOM more leeway to conduct operations without presidential approval, albeit still with a robust interagency review process.[14]

If the United States wishes to further leverage its cyber prowess in the international arena by leveraging private sector partners, **does it have the supply chain and acquisition capabilities to back it up—especially if its adversary is the People's Republic of China?** Although the author does not condone general analogies between cyber and other domains, supply chain and acquisition analysis in the cyber domain can be similar to nuclear or other arms proliferation questions. For example, to answer whether a country has the capability to construct a nuclear weapon, one must understand how much enriched uranium the country can easily acquire. Similarly, to answer whether a country can become a cyber power that can access the hardest of digital targets, one must ask how easily it can source and acquire zero-days and other offensive cyber capabilities.

Methodology

This report combines quantitative data analysis and interviews of experts from across the offensive cyber capability ecosystem. The underlying research—conducted over ten months, from June 2024 to March 2025—occurred in three stages.[15] The first was a comprehensive literature review of US-China cyber conflict, how the offensive cyber capabilities industry works, and recent policies on combating the proliferation of spyware from the Biden administration (which has impacted zero-day exploit acquisition and sales). The second then analyzed data scraped from the open internet, largely from the website "CTFTime" (well-known for tracking Capture the Flag (CTF) competitions internationally),[16] as well as secondary sources containing anonymized and aggregated information on the cybersecurity ecosystem. This report includes statistics from this dataset—the full dataset is available upon request. The third stage involved interviewing experts from across the national security and offensive cybersecurity ecosystem. The interviews, which began in December 2024 and concluded in March 2025, comprise the most significant aspects of this research. The approximately thirty experts consulted, both virtually and in person, came from one or more of the following backgrounds:

- Business leaders and senior employees of offensive hacking or vulnerability research companies in the United States, United Kingdom, Australia, New Zealand, and Canada;
- Senior defense acquisition and innovation officials in the US government;
- Security researchers internationally who focus on China or wider Asia-Pacific cyber issues;
- Current and/or former US and Five Eyes (FVEYs) intelligence officials; and
- Current and/or former US national security policy officials.

To narrow the project's scope, and given the foreign intelligence and military concerns China poses, this paper focuses primarily on acquiring zero-days for **foreign intelligence and military customers, rather than for domestic law enforcement.** Although some of the analysis and ultimate policy recommendations may be applicable to law enforcement, the analysis was conducted with intelligence and military end uses in mind. Because of the lack of publicly available reporting on this topic, the interviews are a major part of the paper's findings. A list of interviewees can be found in Appendix B. For security reasons, many interviewees asked to remain unattributed. Anonymous interviewees are not individually cited in

11. Bureau of Industry and Security, "Commerce Removes Sandvine from Entity List Following Significant Corporate Reforms to Protect Human Rights," US Department of Commerce, October 21, 2024 (release), https://www.bis.gov/press-release/commerce-removes-sandvine-entity-list-following-significant-corporate-reforms-protect-human-rights.
12. Thomas Latschan, "Deep Rift between US and Europe Opens up in Munich," *Deutsche Welle*, February 15, 2025, https://www.dw.com/en/deep-rift-between-us-and-eu-opens-up-in-munich/a-71624354.
13. Martin Matishak, Pentagon Fast-Tracks 'Cyber Command 2.0' Review, Requests Authorities Wish List," *The Record*, February 21, 2025, https://therecord.media/hegseth-cyber-command-2-0-review-authorities-wish-list.
14. "NSPM-13 and the Future of Cyber Warfare," Hudson Institute (virtual event), May 5, 2022, https://www.hudson.org/events/2109-virtual-event-nspm-13-and-the-future-of-cyber-warfare52022.
15. This project was originally developed as a Policy Analysis Exercise product for the Atlantic Council during the author's time at Harvard Kennedy School. It has since been revised and updated.
16. "About CTF (Capture the Flag)," CTFTime, accessed March 16, 2025, https://ctftime.org/.

the text to avoid identifying them based on their aggregate comments.

The author's background as a student, cybersecurity practitioner, think tank fellow, and founder of a Washington DC-based hacking conference[17] heavily contributed to sourcing interviews with the hacking and cyber policy community. However, the author recognizes that, given the highly fragmented nature of the offensive cyber capability industry, the findings in this paper are likely only part of the wider truth, and reflect her biases and affiliations. Many sources are former and current industry colleagues. One of the interviewees is her husband, Derek Bernsen, whose DARPA program, Intelligent Generation of Tools for Security (INGOTS), is mentioned in the paper. Any omissions, errors, or factual inaccuracies are the author's alone.

The majority of the paper consists of an analysis of the US supply and acquisition funnel of offensive cyber capabilities, followed by an analysis of China's supply and acquisition funnel, from which the author makes conclusions and recommendations for US policy moving forward. There are plenty of risks to this approach, two of which are mirror imaging bias and "whataboutism" (justifying an approach because another party has conducted similar activity). The author has tried to, wherever possible, seek to remove such fallacies from her analysis. She justifies the overall approach through the following (somewhat obligatory) Sun Tzu quote:

> "知己知彼，百战不殆."
>
> ("Know yourself and your enemy, and you will not know defeat in battle").

17. DistrictCon, accessed April 3, 2025, https://www.districtcon.org.

Analysis

This section addresses the relative supply chains for offensive cyberspace operations to the United States and China, building around a tripartite model to encompass a set of industry and government relationships characterized by significant degrees of internal complexity, opacity, and fragmentation. This model addresses (1) what the underlying international market of offensive cyber capabilities looks like, (2) what parts of this international market supply China and/or the United States with offensive cyber capabilities, and (3) how the United States and China acquire such capabilities.

The international offensive cyber supply chain

All software is built by people, and there are three types of bespoke software often used in a cyber operation:[18] (1) exploit code that takes advantage of a software vulnerability, (2) a malware payload, and (3) technical command and control.[19] All three are "offensive cyber capabilities." While individual governments with the right expertise can build their respective capabilities in-house, many rely heavily on commercial vendors.[20] In a 2024 report, the Atlantic Council identified forty-nine commercial vendors along with thirty-six subsidiaries, twenty-four partner firms, twenty suppliers, and a mix of thirty-two holding companies, ninety-five investors, and one hundred and seventy-nine individuals, including many named investors.[21] Despite over-indexing on firms in Italy, Israel, and India, companies and individuals named in this dataset hailed from every major continent except for Antarctica, **suggesting**

Source: Emma Schroeder. Adapted from photograph by Basma Alghali (Unsplash license) and image by Gordon Johnson (Pixabay content license).

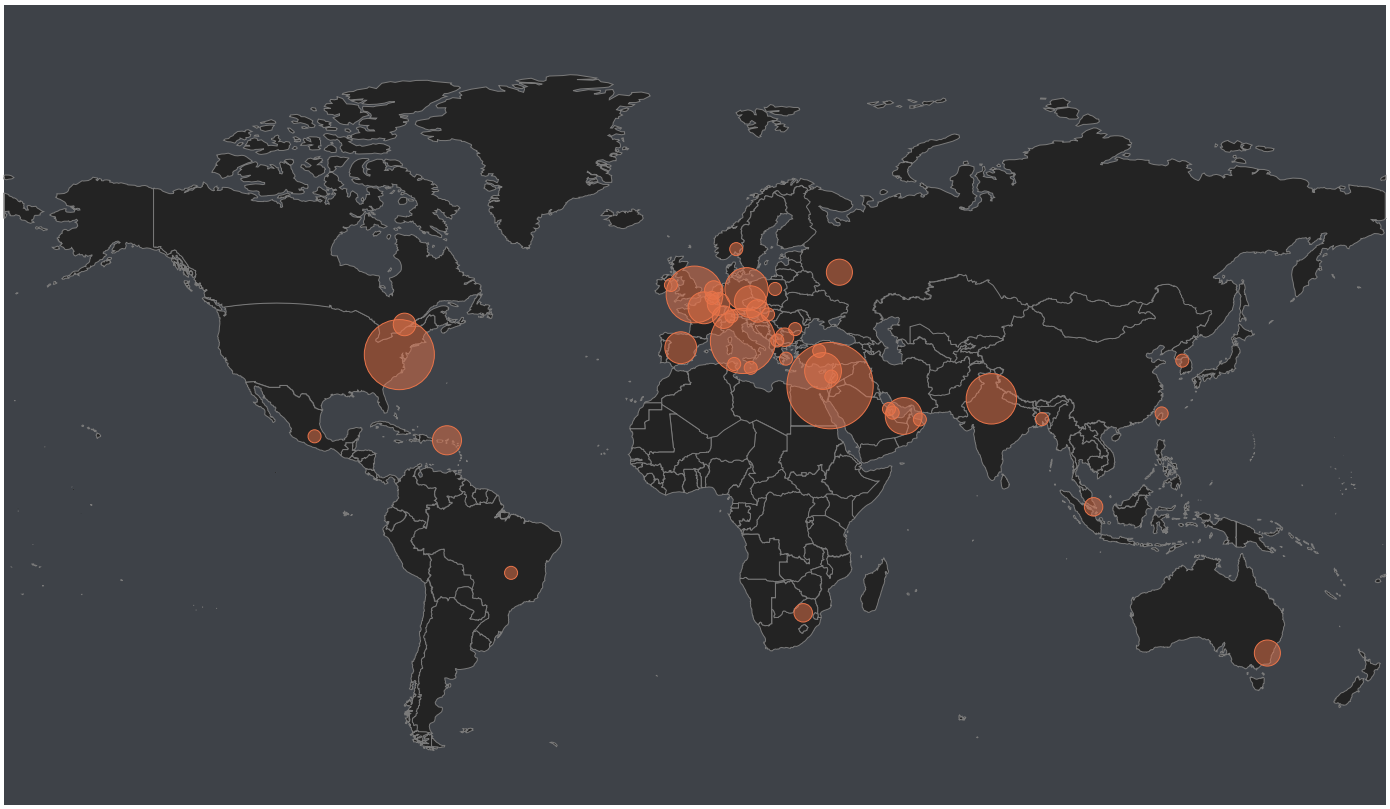
18. This assumes that the target for a cyber operation has been selected and that they do not respond to phishing emails or other forms of access.
19. Winnona DeSombre et al., *A Primer on the Proliferation of Offensive Cyber Capabilities*, *Atlantic Council*, March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/.
20. Gatlan, "Google: Spyware vendors behind 50% of zero-days."
21. Jen Roberts et al., *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*, *Atlantic Council*, September 4, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/.

that each continent likely has hackers that provide offensive cyber capabilities to governments.[22] While only a small subset of these firms can and do sell zero-day exploits, these named vendors are likely just the tip of the iceberg. Top-tier vulnerability research talent exists worldwide, hailing not just from the FVEY countries (the United States, Canada, United Kingdom, New Zealand, and Australia)[23] and China but also from smaller nations like Egypt, Vietnam, and Cyprus (see Figure 1).[24]

Moreover, the above dataset excludes talent not yet plugged into the government cyber marketplace. CTF competitions (hacking contests in a simulated environment), Live hacking competitions (where hackers hack into systems live on stage), and bug bounty programs (usually company-run reward programs that encourage hackers to find and report system vulnerabilities) enable hackers to develop similar skill sets as those required for government-sponsored hacking. These programs and competitions are both common recruiting pipelines for defensive cybersecurity companies and offensive vendors alike.

The number of individuals that participate in such programs globally is staggering. In 2020, HackerOne, a well-respected bug bounty platform, reported around 600,000 users spanning 170 countries.[25] A 2024 survey by Bugcrowd, one of the largest bug bounty and vulnerability disclosure companies on the internet, revealed most of Bugcrowd's over 200,000 hackers hailed from India, Egypt, Nigeria, Pakistan, Nepal, Viet-

Fig. 1: Heatmap of major known commercial vendors for offensive cyber capabilities, suppliers, and investors.



Source: Jen Roberts et al., *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*, Atlantic Council, September 4, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/.

22. Roberts et al., *Mythical Beasts and Where to Find Them*.
23. FVEYs is an intelligence alliance within the five governments rather than set by companies. However, because the five governments often share intelligence, a US company selling offensive cyber capabilities to the US government will often be able to sell to other FVYEs countries without much concern if they wish to expand into international markets.
24. Aitel, "OffensiveCon23—Information Security Is an Ecology of Horrors."
25. Adam Bannister, "Bug Bounty Earnings Soar, but 63% of Ethical Hackers Have Withheld Security Flaws – Study," *The Daily Swig*, February 24, 2020, https://portswigger.net/daily-swig/bug-bounty-earnings-soar-but-63-of-ethical-hackers-have-withheld-security-flaws-study.

nam, Australia, and the United States; [26] 78 percent of them are self-taught, and 58 percent of them were under twenty-five years old.[27] While not all of these individuals possess the skills to find zero-day vulnerabilities and write code to exploit them, multiple security experts interviewed estimated that there are likely thousands of international individuals able to do so, **with numbers in the low hundreds that can be trained to do so well.**[28]

While selling offensive cyber capabilities (and particularly zero-day exploits) to governments is a lucrative profession, it is a risky industry. Creating a zero-day exploit to leverage against a widely used technology product may require between six and eighteen months of full-time engineering and research work.[29] Unless an offensive cyber capability firm has multiple engineers working on different products or uses different payment schemes, this timeline can lead to long downtimes between exploit sales. This "feast-or-famine" payout schedule

What is Required to Create and Sell a Zero-Day Exploit?

Finding a vulnerability in a technology product or system is a highly manual, labor-intensive process that requires in-depth knowledge of how the target product works. Vulnerability researchers usually acquire such knowledge by reading through a target's codebase and dependencies for small idiosyncrasies and mistakes. Depending on the size of the codebase (ranging from hundreds to millions of lines of code), this can be a time-consuming process.

However, finding a vulnerability (or "bug") is only the first step to creating a zero-day exploit. Once a bug is found, there are a series of follow-up questions that need answers. Is the bug exploitable (i.e., can it be used to do anything useful)? If so, can it be exploited reliably, or could it alert the target that something is wrong? Does the exploit work on only one version of the target or across multiple versions? These complex questions usually require additional quality assurance (QA) testing to produce a field-ready exploit, with the QA's rigor depending on the risk aversion of the end customer. Any additional time spent conducting QA tests carries a risk that the technology firm producing the product finds the underlying vulnerability in the meantime and patches it, decreasing the value of the exploit.

Instead of selling a single exploit, it is usually more lucrative and impactful to link the individual exploit (known as an "exploit primitive") with others to create an "exploit chain," using multiple exploit primitives in conjunction with one another to achieve a particular effect, such as gaining full control over a system. As of 2025, exploit chains are no longer just an option for greater impact; now, they are often necessary to achieve any effect on a modern, enterprise-grade system. Many recent offensive security talks at major conferences, alongside security advisories from dominant technology firms, have moved away from analyzing primitives and toward analyzing exploit chains for this reason. However, not every exploit primitive can be used in the same chain. When trying to create a functioning full exploit chains ("full chains"), a company may work with middlemen (or "brokers") to purchase primitives for the exploit chain they want to build. This comes with additional risks. Since middlemen work with other middlemen, the original source of a zero-day exploit is often difficult to ascertain. This also raises the potential that multiple parties have access to the same exploit, which, in turn, leads to a higher likelihood of discovery.

Because only a small number of big technology firms create most of the products used globally today, **bug collisions** (i.e., the parallel independent discovery of a vulnerability by multiple researchers) are also growing increasingly common. This dynamic increases the risk for buyers and sellers, as a bug collision means an exploit is more likely to be used by multiple parties, resulting in a higher risk of discovery or false attribution by the private sector. This also erodes trust between the buyers and sellers of a capability, as the buyer can only take the seller's word that the bug was concurrently discovered rather than resold.

26. Christopher Kissel and Mathew Marden, "The Business Value of Bugcrowd Security Solutions," IDC Business Value, October 2021, https://www.bugcrowd.com/wp-content/uploads/2023/12/business-value-bugcrowd-security-solutions.pdf.
27. "Inside the Mind of a Hacker," Bugcrowd, 2024, https://www.bugcrowd.com/resources/report/inside-the-mind-of-a-hacker/.
28. Background Interview, Founder of Vulnerability Research Company 2, January 8, 2025; corroborated by Background Interview, Independent Security Researcher, January 31, 2025; corroborated by Background Interview, Former US Intelligence Community Official, December 27, 2024.
29. Background Interview, Former ONCD Official, January 8, 2025; corroborated by interview with Derek Bernsen, DARPA Program Manager, January 5, 2025 (Note: Bernsen's comments do not reflect the opinions of DARPA, the DOD, or the US Government); corroborated by Background Interview, Founding Member of a Vulnerability Research Company, January 11, 2025.

carries risks for companies that rely on one or two windfalls a year to pay their overhead and engineering costs.[30]

In addition, finding a customer to sell exploits to is more difficult than it first seems. In general, potential sellers must find an existing government contract through which to sell their exploits or know the right government individual to speak with.[31] Unless an offensive cyber capability firm has hired employees who have recently left a government interested in such capabilities, actual buyers may be extremely hard to find.[32] Thus, international hackers without former government connections normally sell their products to middlemen, many of whom operate internationally.[33] Even then, the exploit may go through multiple levels of middlemen to get to a government customer,[34] frustrating both buyers and sellers. Buyers know that exploits sold to them have extremely high mark-ups, given the number of middlemen involved, and often will not know who the original bug producers are. Meanwhile, sellers are likely aware of the extreme markups, but do not know whether their bugs were sold to multiple governments.[35]

Throughout both the development and sale of an exploit, offensive cyber capability firms are also subject to counterintelligence risks by adversary governments. Since 2022, North Korea has consistently targeted vulnerability researchers globally to steal their tools and exploits.[36] Vulnerability researchers also frequently report being solicited by foreign intelligence at security conferences, falsely claiming to work for FVEYs governments.[37] On the U.S. side, government response to this counterintelligence threat has been half-hearted at best. While the Cybersecurity and Infrastructure Security Agency (CISA) reportedly announced initiatives to protect high-risk communities against cyber threat actors in 2024,[38] security researchers who have tried to contact CISA have not found the program helpful.[39] As a result, the offensive cyber capability industry does not perceive that the US government is interested in protecting this community, even from one of the world's most unpopular and totalitarian nation-states.

As a result, most vulnerability researchers do not spend more than a decade in the profession, instead choosing to pivot into less risky segments of the cybersecurity industry.[40] The individuals who stay in the market tend to do so for some combination of three reasons. First, they firmly believe in the mission—this largely describes either likely former government employees who have moved out to the private sector or individuals who wish to have their work "used for good."[41] Second, they are profit-motivated. The "feast" element of the feast-or-famine model provides an incredible windfall for certain highly skilled individuals. Third, they simply enjoy the challenge. A large portion of the vulnerability research community, and the hacker community writ large, exhibits a large amount of awe for their vocation (i.e., the only person who hacks textile looms, or the first person to "pop," or exploit, the newest iPhone can feel like a superpower).[42] This vocational awe creates camaraderie among the most passionate vulnerability researchers worldwide. For some researchers, exploitation is art, and they will often try to put the art above the artist. In that sense, some individuals in the global market, particularly those who interact

30. Background Interview, Former ONCD Official, January 8, 2025; corroborated by Bernsen interview, January 5, 2025; corroborated by Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025.
31. Background Interview, Founder of Vulnerability Research Company 2, January 8, 2025; corroborated by Background Interview, Founder of Vulnerability Research company 3, January 9, 2025.
32. Bernsen interview, January 5, 2025; corroborated by Background Interview, Former ONCD Official, January 8, 2025.
33. Wallarm, "Zero-Day Marketplace Explained: How Zerodium, BugTraq, and Fear Contributed."
34. Bernsen interview, January 5, 2025; corroborated by On Background Interview, USG Cyber Official, January 26, 2025.
35. This government contracting process may be a uniquely "Western" phenomenon. China analysts posit that the Chinese government has deliberately created avenues for foreigners to offer bugs to the Chinese government in a relatively frictionless way (Interview with Adam Kozy, CEO of SinaCyber, January 17, 2025).
36. Andy Greenberg, "North Korea Hacked Him. So He Took Down Its Internet," *Wired*, February 2, 2022, https://www.wired.com/story/north-korea-hacker-internet-outage/; Clement Lecigne and Maddie Stone, "Active North Korean campaign targeting security researchers," Google: Threat Analysis Group (blog), September 7, 2023, https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/.
37. Background Interview, Former US Intelligence Community Official, December 27, 2025; corroborated by Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025.
38. "High-Risk Communities," Cybersecurity and Infrastructure Security Agency, accessed June 9, 2025, https://www.cisa.gov/audiences/high-risk-communities.
39. Background Interview, Founder, Former Vulnerability Research Vendor, January 8, 2025.
40. Background Interview, Founder, Former Vulnerability Research Vendor, January 8, 2025.
41. Background Interview, Independent Security Researcher, January 31, 2025.
42. Halvar Flake, "OffensiveCon20—Keynote—Why I Love Offensive Work, Why I don't Love Offensive Work," YouTube video, April 17, 2020, https://www.youtube.com/watch?v=8QRnOpjmneo; corroborated by Background Interview, Founder of Vulnerability Research Company 2, January 8, 2025; corroborated by Background Interview, Founder of Vulnerability Research company 3, January 9, 2025; corroborated by Background Interview, Founder of Vulnerability Research Company 1, January 15, 2025.

more with the international community online or participate on international CTF teams, perceive geopolitics as an inconvenient truth.[43] Chinese and Russian researchers can admire the work done by American researchers, and vice versa, while understanding that they will likely never work together.[44]

The DEFCON (DEF CON) hacking conference in Las Vegas, Nevada, in 2014.

Source: Tony Webster, Wikimedia Commons, https://commons.wikimedia.org/wiki/File:DEFCON_22_%2814704446530%29.jpg.

The US acquisition pipeline

> "An individual researcher who isn't informed on what bugs are selling for may sell a good bug for 100k. By the time it makes it to a customer, an individual bug could go for 750k to 1 million dollars."
>
> *– Former ONCD Official.*

> "The system by which zero day vulnerabilities are acquired is horrendously inefficient and broken."
>
> *– Senior DOD official working on offensive cybersecurity research programs.*

Given this international sphere of private sector hackers with the capability to find and exploit capabilities, how does the United States develop and leverage this community to supply its offensive cyber operations? The sections below—and those mirrored in the following section on China—focus on **sources of supply** (companies that provide capabilities and talent pools that support them) and **acquisition methods** (contracts, regulations, and informal roadblocks or enablers).

Supply—International, opaque, and loosely affiliated networks.

Companies—Prime and subcontractor ecosystem.

While the US government has highly sophisticated cyber capabilities developed in-house, it increasingly purchases offensive cyber capabilities from a wide network of prime and subcontractors. Many of the large firms that sell offensive cyber capabilities to the US government are the same defense contractors that sell it other forms of software or even weapons. Large, traditional prime contractors like Raytheon (rebranded RTX)[45] and L3Harris,[46] as well as more technology-focused firms like Peraton, compete for multi-million dollar government contracts to support cyber operations and provide capabilities to the government.[47] Many individuals who work for these firms are former DOD or Intelligence Community employees.[48]

When large prime contractors cannot fulfill contract requirements, they often portion out the work to subcontractors. Some prime contractors are heavily reliant on small businesses, boutique research firms, and even individual researchers to satisfy contracts. Many of these subcontractors attract high-end vulnerability researchers and exploit developers worldwide, who are looking for flexible hours, high pay, and a company culture that better reflects the hacker community.[49] Some contractors, to boost available capital, are funded or partially owned by venture capital, private equity, or other investment firms, which can shape the company structure and strategy. For example, AE Industrial, a private investment firm, acquired Israeli firm Paragon in 2024, and sought to merge it with US subcontractor

43. Background Interview, Founder, Former Vulnerability Research Vendor, January 8, 2025; corroborated by Background Interview, Founder of Vulnerability Research Company 1, January 15, 2025.
44. Background Interview, Pwnie Award Organizer, January 12, 2025; corroborated by Background Interview, USG China Analyst, January 22, 2025.
45. Aaron Mehta, "Raytheon is Now RTX. Here's What That Means for Its Defense Arm," Breaking Defense, June 23, 2023, https://breakingdefense.com/2023/06/raytheon-is-now-rtx-heres-what-that-means-for-its-defense-arm/.
46. "L3Harris® Fast. Forward., Domain Cyber," accessed March 16, 2025, https://www.l3harris.com/capabilities/cyber.
47. "Peraton Awarded $889M Contract to Support U.S. Army Cyber Command (ARCYBER) and Cyber Mission Partners," Peraton, January 9, 2024, https://www.peraton.com/news/peraton-awarded-889m-contract-to-support-arcyber-and-cyber-mission-partners/.
48. On Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025.
49. Andy Greenberg, "Inside Endgame: A Second Act for the Blackwater of Hacking," Forbes, February 14, 2014 [update], https://www.forbes.com/sites/andygreenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/; On Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025.

RedLattice, which it also owns.[50] The United States also likely sources its tooling through its intelligence-sharing relationship with the FVEYs.[51] Given its existing close cooperation between the five countries' signals intelligence (SIGINT) agencies and emphasis on "cooperative security", this cooperation likely translates to capability sharing as well.[52]

The services and products such firms provide (whether as the subcontractor or the prime contractor) differ based on their government contract vehicle. Internal research and development services contracts enable government research teams to break into harder targets by providing supplement staff.[53] Procurement contracts for zero-day exploits exist in various forms, and subscription models for a company's full catalog (i.e., a flat fee for year-long access to everything the company finds) are not uncommon.[54] For less sophisticated government clients, private sector firms may provide Access-as-a-Service models (i.e., black-box and end-to-end solutions) where the contractor guarantees product maintenance for a specified timeframe.[55] These Access-as-a-Service models combine zero-day exploits with other tooling into an all-in-one spyware solution, such as NSO Group's Pegasus spyware.[56] Many prime contractors and subcontractors in the United States and FVEYs experience similar issues and risks listed in the previous section (i.e., feast-or-famine timeframes, middlemen, counterintelligence risks, and general difficulty of the field), which impacts recruitment.

Some companies that provide capabilities directly to the US government have been innovating in the nexus between artificial intelligence (AI) and cyber operations. However, while individual researchers use AI to assist with code auditing and fuzzing, many focused on this field affiliate with academic institutions or large US technology ("Big Tech") firms rather than government contractors.[57] Open, unclassified offensive initiatives do exist. For example, the Intelligent Generation of Tools for Security (INGOTS) program, within the Defense Advanced Research Projects Agency (DARPA), seeks to automate the creation, modification, modeling, and analysis of exploit chains.[58] However, INGOTS is an exception to the norm. Most of the US intelligence community experiments with AI in-house,[59] and US policymakers currently spend far more money to encourage companies to use AI for defensive applications (e.g., DARPA's AIxCC partnership with Anthropic, Google, Microsoft, OpenAI, the Linux Foundation, and the Open Source Security Foundation to design, test, and improve novel AI systems to automatically find and fix vulnerabilities in code).[60]

The DOD's AI strategy (originating in 2018 with updates in 2020 and 2023) has revolved around "Responsible AI"—developing and using AI capabilities in accordance with the DoD AI Ethical Principles while delivering better, faster insights and improved mission outcomes.[61] While the Trump administration has been moving away from "Responsible AI" strategies, its new Project Stargate, an injection of $500 billion over the next

50. A.J. Vicens, "Israeli Spyware Firm Paragon Acquired by US Investment Group, Report Says," Reuters, December 16, 2024, https://www.reuters.com/markets/deals/israeli-spyware-firm-paragon-acquired-by-us-investment-group-report-says-2024-12-16/.
51. Josh Gold, "The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative,'" NATO Cooperative Cyber Defence Centre of Excellence," October 30, 2020, https://ccdcoe.org/library/publications/the-five-eyes-and-offensive-cyber-capabilities-building-a-cyber-deterrence-initiative/.
52. Gold, "The Five Eyes and Offensive Cyber Capabilities."
53. On Background interview, Former US Intelligence Community Official, December 27, 2024; corroborated by Background Interview, Independent Security Researcher, January 31, 2025.
54. Aitel, "OffensiveCon23—Information Security Is an Ecology of Horrors."
55. Background Interview, Independent Security Researcher, January 31, 2025.
56. Winnona Desombre et al., *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service*, *Atlantic Council*: *Scowcroft Center*, March 2021, https://www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf.
57. Yizheng Chen et al., "DiverseVul: A New Vulnerable Source Code Dataset for Deep Learning Based Vulnerability Detection," Association for Computing Machinery: Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses (October 2023), 654–68, https://doi.org/10.1145/3607199.3607242; Ziyang Li, Saikat Dutta, and Mayor Naik, "LLM-Assisted Static Analysis for Detecting Security Vulnerabilities" (Version 2), Cornell University: arXiv, November 24, 2024, https://doi.org/10.48550/ARXIV.2405.17238.
58. System for Award Management, (2024, September 1). "Intelligent Generation of Tools for Security (INGOTS) Contract Opportunity," US General Services Administration, accessed March 16, 2025, https://sam.gov/opp/98406eb5b34641468e25287249077c48/view.
59. "Research Overview," National Security Agency: Central Security Service, accessed June 9, 2025, https://www.nsa.gov/Research/Overview/#:~:text=We%20bring%20increased%20depth%2C%20resilience,teaming%20with%20artificial%20intelligence%20agents.
60. "Overview – Interview with Dr. Kathleen Fisher," AixCC: AI Cyber Challenge, accessed April 5, 2025, https://aicyberchallenge.com/overview/.
61. DOD Data, Analytics, and Artificial Intelligence Adoption Strategy, US Department of Defense, June 27, 2023 [publication clearance date], https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.

four years building new AI infrastructure in the United States, is giving significant funding to OpenAI, whose investments in cybersecurity have been largely defensive in nature.[62]

Domestic talent—Decentralized, defense-forward.

Feeder systems into US and US-affiliated offensive security firms come from a loose conglomerate of internship programs, cybersecurity conferences, and hacking competitions. Technology companies sponsor many of these conferences and competitions to encourage talent to go into defensive cybersecurity careers (a worthwhile but orthogonal field for the purposes of this paper's analysis). The bug bounty industry, as well as the defensive cybersecurity industry in the United States, hires plenty of hackers and former government cyber engineers (who might otherwise apply to work in offensive capability development) into defensive or more IT-focused roles.[63] Some programs have formal relationships with the government, like the CyberCorps Scholarship for Service program, Hack the Pentagon, or University-based NSA Centers of Excellence.[64] However, many of these programs funnel students into defensive jobs. Notably, of the 461 NSA cyber centers of excellence, only twenty-one are certified to train students in cyber operations.[65]

Few universities have applied (i.e., non-theoretical) offensive cyber programs that feed directly into the private vulnerability research industry.[66] Many students who learn how to hack in college do so through extra-curricular security clubs or CTF teams. In 2024, among all registrants, the United States had the most registered academic teams competing in CTFs on popular platforms.[67] Many CTFs that US teams compete in are at cybersecurity conferences,[68] hosted by academic institutions,[69] or sponsored by technology companies.[70] However, without consistent funding, alumni engagement, and professor buy-in, these clubs and teams often risk disappearing entirely due to lack of overt support from their home universities.[71]

Moreover, few university programs produce engineers ready to write fully functioning exploits. Multiple vulnerability research firms interviewed referenced a "**training valley of death**," where entry-level engineers out of university still require a year or more of talent development before they can produce a marketable product.[72] While some intermediate-level trainings exist in companies or at conferences, they are currently insufficient—in either technical depth or timeframe.[73]

The US government has created more support for hacking contests, but at a much smaller scale than in other countries. The US National Institute of Standards and Technology (NIST) published a report on cyber competitions in 2016, suggesting that parts of the US government have historically understood the importance of such contests in developing offensive talent.[74] NIST currently supports the US Cyber Games to recruit, train, and develop the team representing the United States in international cybersecurity competitions, this program engages with 2,000 individuals in a single contest, the US Cyber Open, and annually trains approximately 150

62. Executive Order No. 14179, "Removing Barriers to American Leadership in Artificial Intelligence," 90 FR 8741 (January 23, 2025), https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence; "Security on the Path to AGI," OpenAI, March 26, 2025, https://openai.com/index/security-on-the-path-to-agi/; Emil Sayegh, "Stargate AI Project: The $500 Billion Gamble to Dominate the Future," Forbes, January 22, 2025,. https://www.forbes.com/sites/emilsayegh/2025/01/22/stargate-ai-project-the-500-billion-gamble-to-dominate-the-future/.
63. "SkillBridge and CSP Coordinators," Microsoft: Military Affairs, accessed March 16, 2025, https://military.microsoft.com/mssa/faqs/skillbridge-and-csp-coordinators/.
64. "CAE Institution Map," CAE in Cybersecurity Community, June 9, 2025 [map update], https://www.caecommunity.org/cae-map; "CyberCorps: Scholarship for Service," US Office of Personnel Management, accessed March 16, 2025, https://sfs.opm.gov/.
65. CAE in Cybersecurity Community, "CAE Institution Map."
66. Background Interview, Former US Intelligence Community Official, December 27, 2024; corroborated by Background Interview, Independent Security Researcher, January 31, 2025.
67. Data gathering by Winnona DeSombre—full data available upon request.
68. "DEF CON 24 Hacking Conference, Capture the Flag," DEF CON Communications, Inc. accessed March 16, 2025, from https://defcon.org/html/defcon-24/dc-24-ctf.html.
69. "CSAW'25 Capture the Flag, US-Canada, Mena, Europe, India, Mexico," New York University OSIRIS Lab, accessed March 16, 2025, from https://www.csaw.io/ctf.
70. Capture the Flag with Google," Google CTF, accessed March 16, 2025, https://capturetheflag.withgoogle.com/.
71. Background Interview, Former US Intelligence Community Official, December 27, 2024; corroborated by Background Interview, Independent Security Researcher, January 31, 2025.
72. Background Interview, Founder of Vulnerability Research Company 1, January 8, 2025, corroborated by Background Interview, Founder, Vulnerability Research Company 3, January 9, 2025; corroborated by Background Interview, Independent Security Researcher, January 31, 2025.
73. Advanced Cyber Training Program, accessed May 14, 2025, from https://www.mantech.com/focus-areas/cyber-training/.
74. Katzcy Consulting, "Cybersecurity Games: Building Tomorrow's Workforce," National Institute for Standards and Technology (NIST), 2016, https://www.nist.gov/system/files/documents/2017/04/24/cyber_games-_building_future_workforce_final_1031a_lr.pdf.

students.[75] Unfortunately, it is far from the lofty, nationwide efforts pitched in NIST's initial paper and is dwarfed by the sheer size of Chinese sponsored competitions (as shown in later sections).

Undermining all these efforts is the anti-government sentiment that remains strong within the US cybersecurity and hacking community, which likely contributes to difficulty in maintaining an offensive talent pipeline. Much of the original US hacking community emerged from countercultural activities like phone phreaking (i.e., bypassing Pacific Bell telephone lines to make long-distance phone calls without paying). Law enforcement responses from the 1960s to the early 2000s treated many hackers as criminals rather than innovators. In 1990, the Secret Service's Operation Sundevil seized more than forty computers and 23,000 data disks from teenagers in fourteen American cities and charged individuals who managed hacker magazine "Phrack" with interstate transport of stolen property. The charge was based on information published by Phrack that later proved to have been already publicly available.[76] The arrests and subsequent court cases resulted in the creation of the Electronic Frontier Foundation.[77] While the US government has made significant strides toward repairing the relationship with domestic hackers in recent years, anti-government sentiment still persists.[78]

Reliance On and Integration with the Wider International Hacking Community

The US hacking community relies on and interacts heavily with the international hacking community. Multiple FVEYs vulnerability research company employees and founders interviewed **claimed to hire individuals from other FVEYs countries, Europe, and South America to provide services.**[79] This international nature of US talent is most publicly apparent at the upper echelons of vulnerability research and exploitation competitions. Pwn2Own, sponsored by the American-Japanese cybersecurity software company Trend Micro, is the epitome of Western live-hacking competitions for vulnerability research companies. While initially starting at a security conference in Canada, the competition has expanded to events in the United States, Canada, Japan, Ireland, and Germany.[80] While the United States had the most participating teams by country at Pwn2Own Ireland in 2024, they numbered only four teams out of seventeen, which included countries like the Netherlands, France, Vietnam, Taiwan, and South Korea (see Figure 2).

Fig. 2: Number of teams participating in Pwn2Own Ireland 2024, by country.

Pwn2Own Ireland 2024 Participants

Country	# Teams	Country	# Teams
US	4	TW	1
NL	2	GE	1
FR	2	KR	1
UK	2	CH	1
VN	2	AU	1

Source: Dustin Childs, "Pwn2Own Ireland 2024: Day Four and Master of Pwn," Trend Micro, Zero Day Initiative, October 25, 2025, https://www.thezdi.com/blog/2024/10/25/pwn2own-ireland-2024-day-four-and-master-of-pwn.

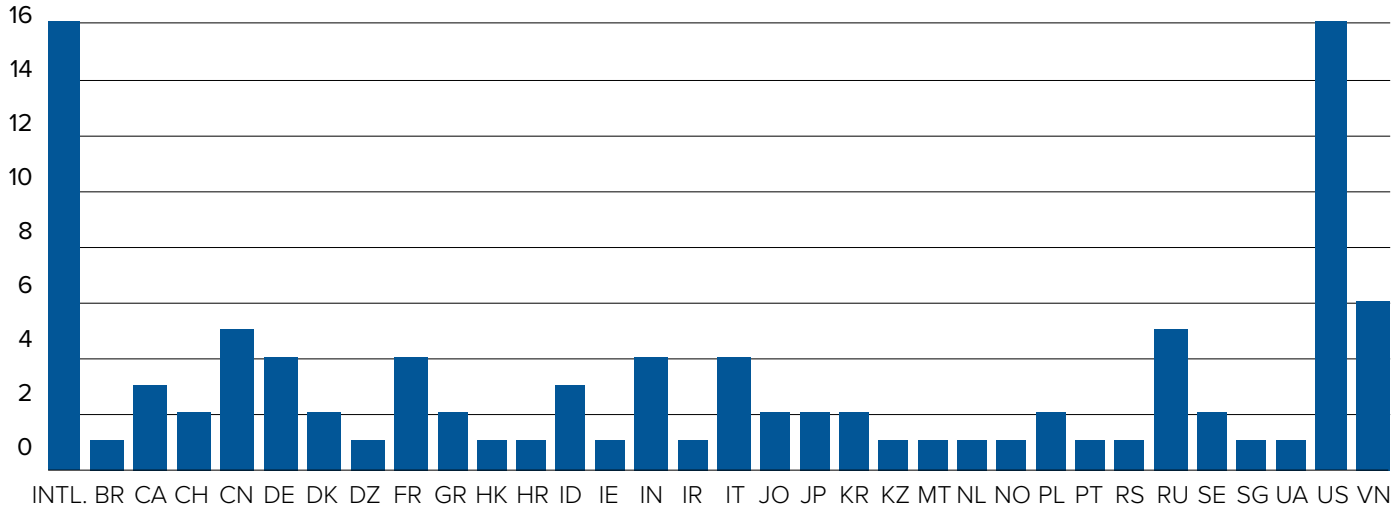
The talent pipeline for offensive security in the United States also corroborates this claim, particularly when looking at CTF competitions. CTFs serve as talent development and recruitment for both vulnerability research firms and the wider cybersecurity industry. Data from the CTFTime website (used widely in the West for tracking CTF competitions) shows the United States, as a country, has the most registered teams (16,774 as of August 19, 2024).[81] However, there are just as many teams that are "international" in nature—over 16,000 either do not align with a single country, or have members competing and collaborating on the same team from multiple countries (see Figure 3).

The most famous CTF competition in the world also corroborates this trend. DEF CON CTF, held annually in Las Vegas during DEF CON - the world's largest hacker conference, attracts both university students and seasoned industry professionals

75. National Cyber Workforce Strategy, June 25, 2024. https://web.archive.org/web/20240816044309/https://www.whitehouse.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf.
76. John Perry Barlow, "A Not Terribly Brief History of the Electronic Frontier Foundation," November 8, 1990, Electronic Frontier Foundation. https://www.eff.org/pages/not-terribly-brief-history-electronic-frontier-foundation.
77. "A History of Protecting Freedom Where Law and Technology Collide," Electronic Frontier Foundation, October 7, 2011, https://www.eff.org/about/history.
78. Aitel, "OffensiveCon23—Information Security Is an Ecology of Horrors."
79. Background Interview, Founder of Vulnerability Research Company 1, January 8, 2025, corroborated by Background Interview, Founder, Vulnerability Research Company 3, January 9, 2025; corroborated by Background Interview, Founder, Former Vulnerability Research Vendor, January 8, 2025.
80. Zero Day Initiative Blog, Trend Micro, accessed March 16, 2025, https://www.thezdi.com/blog.
81. Data gathering by Winnona DeSombre—full data available upon request.

Fig. 3: Teams on CTFtime by country, as of August 2024 (Thousands).

(far left column represents "unaligned" or "international" teams).



Source: Winnona DeSombre Bernsen, data from CFTtime.com.

alike. Of the top twelve scoring teams in 2024, none of them came solely from the United States. All the top teams with US players were either international teams who practiced remotely with each other to qualify as a team, or multiple single-country teams that merged with each other to compete (see Figure 4).[82] For example, the 2024 winner was Maple Mallard Magistrates, a joint Canadian and US team formed by participants at Carnegie Mellon University, Korean-American Vulnerability Research Company Theori, Inc.,[83] and the University of British Columbia. Notably, joint Chinese and Russian teams, as well as single-country teams out of China placed within DEF CON CTF 2024's top twelve.

Fig. 4: Top scoring teams at the 2024 DEF CON CTF, and their countries of origin.

Place	Team
1	Maple Mallard Magistrates 🇺🇸🇨🇦🇰🇷
2	💦 🇺🇸🇨🇦🇪🇪🇰🇷🇦🇺🇳🇴/international
3	Super Dice Code 🇺🇸🇰🇷🇯🇵/international
4	RePokemonedCollections 🇨🇳🇷🇺
5	Straw Hat 🇨🇳
6	mhackeroni 🇮🇹
7	if this works we'll get fewer for next year 🇹🇼
8	HypeBoy 🇰🇷
9	cold fusion 🇰🇷
10	Next Year's Organizers 🇺🇳/international
11	Friendly Maltese Citizens 🇺🇳/international
12	Never Stop Exploiting 🇨🇳

Source: Winnona DeSombre Bernsen from an initial CFTtime scoreboard for DEF CON CTF 2024, accessed April 5, 2025, https://ctftime.org/event/2462/.

82. cts🌸(@gf_256), "The real CTF skill is Mergers & Acquisitions," X (then as Twitter: https://t.co/jpQClGf1KU), May 28, 2023, 6:03 p.m., https://x.com/gf_256/status/1662942688155451395.
83. Theori (Company Profile and Financial), Crunchbase, accessed March 16, 2025, https://www.crunchbase.com/organization/theori.

US offensive cyber capability acquisition methods

Organizations that contract capabilities for cyber include federal intelligence agencies, military, and law enforcement—such as the NSA, USCYBERCOM,[84] and the Federal Bureau of Investigation (FBI). Contract requirements differ by agency. Some organizations can ingest single exploits, while others do not have the in-house talent to independently weaponize capabilities. Normally, the latter organizations require end-to-end, black-box solutions that necessitate additional engineering work and safeguards.[85]

Government contracts for offensive cyber are compliance-heavy and favor large primes

The contracting ecosystem, with its many compliance requirements, inherently favors large prime contractors despite the earlier noted heavy reliance on small businesses, boutique research firms, and even individual researchers to fulfill contracts.[86]

Put simply, small cyber businesses find it incredibly difficult to navigate DOD acquisition processes.[87] Little reporting on the specifics of US offensive cyber capability acquisitions is openly available. Yet, the general US software contracting requirements offer valuable insight. The feast-or-famine timelines of zero-day exploit contracts require a company to have existing capital to withstand long downtimes between sales (like a large prime contractor), in which smaller companies may be one faulty bug away from going bankrupt.[88] Any prime contractor on a government contract (i.e., a contractor bidding directly on a government contract) must also meet the incredibly stringent standards within the Federal Acquisition Regulations, including having cleared individuals for classified government contracts, meeting cybersecurity and other regulatory requirements,[89] and getting financial systems audited.[90]

Clearance requirements are also a large pain point for small exploit businesses, as many exploit contracts are classified. Businesses must go through the complex and costly Facility Clearance process to bid or even perform on such contracts,[91] which is difficult for smaller vendors.[92] Moreover, certain contracts have active clearance prerequisites, which requires a vulnerability research company to have the resources to obtain employee clearances (or find another vendor to sponsor the needed clearances). This can also exclude foreign companies from the bidding process (as foreigners, in general, cannot hold US security clearances).[93]

Despite the hacker community's international nature, some customers also informally restrict the nationalities of employees who may work on contracts, limiting the ability of companies who wish to hire hackers abroad.[94] Despite all these regulations, interviewees confirmed that many of these smaller firms and foreigners may, in effect, actually be working on such contracts anyway, via the sales of their services and products to added layers of contractors (or middlemen) at, of course, an additional expense to the government.[95]

On the government side, additional focused regulations and policies trigger based on the product or agency's risk aversion

84. Justin Doubleday, "CYBERCOM Embraces the Non-Traditional as Acquisition Program Grows," *Federal News Network*, April 15, 2024, https://federalnewsnetwork.com/defense-news/2024/04/cybercom-embraces-the-non-traditional-as-acquisition-program-grows/.
85. Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025; corroborated by Background Interview, Independent Security Researcher, January 31, 2025; corroborated by Background Interview, Former ONCD Official, January 8, 2025; corroborated by Background Interview, Senior DOD Cyber Official 1, January 23, 2025.
86. Background Interview, Founding Member of vulnerability research company, January 11, 2025.
87. Interview with Ian Roos, VP of Intelligence, Margin Research, March 9, 2025.
88. On Background Interview, Former ONCD Official, January 8, 2025; corroborated by Bernsen Interview, January 5, 2025; corroborated by Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025; corroborated by Background Interview, Founder, Former Vulnerability Research Vendor, January 8, 2025; corroborated by Background Interview, Independent Security researcher, January 31, 2025.
89. "Government Contractor Requirements," National Institute of Standards and Technology (NIST), August 2, 2024 [update], https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/government-contractor-requirements.
90. Chelsea Meggitt, "Prime Contractors – Move from Sub to Prime Contracting," Collaborative Compositions, September 13, 2022, https://collaborativecompositions.com/prime-contractors-move-from-sub-to-prime-contracting/
91. "Facility Clearances," Defense Counterintelligence and Security Agency, accessed March 16, 2025, https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Facility-Clearances/.
92. Roos interview, March 9, 2025.
93. Background Interview, Former ONCD Official, January 8, 2025; corroborated by Bernsen interview, January 5, 2025; corroborated by Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025.
94. On Background Interview, Founder, Vulnerability Research Company 3, January 9, 2025; corroborated by Background Interview, Founder of Vulnerability Research Company 1, January 8, 2025; corroborated by Background interview, Founder, Former Vulnerability Research Vendor, January 8, 2025.
95. Background Interview, Former ONCD Official, January 8, 2025.

Aside from the procurement process, additional regulations trigger (and place added burdens on the government buyer) depending on the type of offensive cyber capability acquired. If an exploit is sold to the government individually, the government organization must send the exploit through the Vulnerabilities Equities Process (VEP). All vulnerabilities sold to the United States government go through the VEP. Effectively, it is an interagency process that balances whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched or to use the vulnerability for national security and law enforcement purposes.[96] It is possible to get a waiver to circumvent the VEP, but only if the government agency can assert a deeply pressing national security need for immediate use.[97]

If the exploit is sold as part of an end-to-end spyware solution (or via an Access-as-a-Service model), other regulations also trigger. The US government, under Executive Order 14093, must ensure that a solution does not pose "significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person."[98] Biden signed the order in 2023 to prevent the US government from supporting businesses that also enable human rights abuses abroad while mitigating the risk of such businesses to US government interests. Because end-to-end spyware solutions enable less sophisticated clients to conduct cyber operations, vendors providing such solutions have been caught selling to authoritarian countries, many of whom had not yet built high-end cyber operations organizations in-house and did not have regulations to deter government spying on civil society organizations, political opposition groups, or journalists. The most famous example of a vendor engaging in such activity was the Israeli company NSO Group, whose sale of its Pegasus spyware to the Saudi government resulted in the spying on and subsequent assassination of Washington Post journalist Jamal Khashoggi.[99]

The US military and intelligence communities also have additional internal requirements for procured zero-day vulnerabilities, particularly in the name of stealth and risk-aversion. Zero-day exploits provide the lowest risk of detection in a cyberspace operation (as they do not rely on previously known "n-day" vulnerabilities) and can offer initial access to a system by exploiting pre-existing weaknesses rather than having to somehow manufacture weaknesses in an adversary system. However, to further minimize the discovery risk of an operation, a government buyer may further require a seller to submit its product to QA testing for reliability to see whether and how often an exploit fails.[100] Failure means that the exploit does not succeed in triggering the desired activity and potentially leaves suspicious artifacts on the target device.[101] The reliability requirement adds cost and time, and it can also create risk of intellectual property and trade secret theft if the third party conducting QA is a competitor of the original seller.[102]

0-days v. n-days: what's the difference?

The focus on zero-day exploits as capabilities in this paper may suggest that zero-day exploits are the dominant methods of exploiting systems. The opposite is true: zero-day exploits are not the dominant way to exploit systems and get information in the offensive ecosystem. Oftentimes, the simplest methods of obtaining access are the most effective, even if they may get attributed, or "burned." While simple methods can include phishing emails or social engineering, they can also include "n-day exploits"—exploit code that uses known vulnerabilities to achieve a certain goal, effectively relying on a target not regularly updating their systems.

A zero-day exploit, when compared to an n-day, or other more common capability, is similar to comparing an F-35 fighter jet to a commercially-made drone: one is an exquisite, highly tailored capability, while the other can be made cheaply and at scale—however, while there are incredibly important things an F-35 can do that drones cannot, both can fly from point A to point B and deliver a payload.

96. "Vulnerabilities Equities Policy and Process for the United States Government," Trump White House Archives, November 15, 2017, https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.
97. Background Interview, CTO of Defense Contractor in the DOD / IC Space, January 22, 2025; corroborated by interview with JD Work, Professor at National Defense University, January 31, 2025.
98. Executive Order 14093, "Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security," *88 FR 18957* (2023, March 30), https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to.
99. Stephanie Kirchgaessner, (2021, July 18). Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests," *The Guardian, July 18, 2021*, https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus.
100. Background Interview, Independent Security Researcher, January 31, 2025; corroborated by Background Interview, Founder of Vulnerability Research Company 1, January 8, 2025; Background Interview, DOD Cyber Official, January 23, 2025; corroborated by Bernsen interview, January 5, 2025.
101. On Background Interview, CTO of Defense Contractor in the DOD / IC space, January 22, 2025.
102. On background interview, Independent Security Researcher, January 31, 2025; corroborated by Background Interview, Founder of Vulnerability Research Company 1, January 8, 2025.

A government buyer's interest in stealth can, at times, create market inefficiencies. Various vendors interviewed claimed that certain government customers may not tell a seller what type of target or exploit they want, leading to an inefficient process, where vendors might work on an exploit that a government customer has no intent to purchase.[103] Alternatively, vendors said that other government customers purchase a company's entire catalog of exploits to hide the specific exploit they are after. However, this is likely a decreasing practice given the increasing cost of zero-day exploits.[104] Both of these practices likely seek to increase operational security and avoid the risk that anyone outside the government buyer learns of any intended targets in cyberspace, especially when dealing with a market of increasingly international firms.

Given the increasing costs of exploits and stagnating budgets, US government customers can also become territorial against others within the interagency. Some vendors interviewed noted that government customers can become possessive and completely unwilling for their vendors to share exploits with other customers.[105] This can cause vendors to avoid selling even completely distinct products to other government agencies, for fear of damaging the relationship with a current buyer.[106] While buying bugs jointly is a potential interagency option, it is rare. Coordinating the movement of funding between agencies is time-consuming, requiring forethought that is not consistent with the normal marketplace tempo.[107] Throughout this relationship, trust between the supplier and end client is key. There is a risk that the government client will cut into the supplier's bottom line by being too risk-averse and territorial.[108] There is also the risk that the supplier has worked with untrustworthy parts of the international supply chain, resulting in an untrustworthy product for the government client. In this field, trust is currency.

International and regional policies around exploit sales affecting government purchasers are also on the horizon. In 2024, the United Kingdom and France initiated the Pall Mall Process as an international dialogue meant to establish guiding principles for the "development, facilitation, purchase, and use of commercially available cyber intrusion capabilities."[109] The process emerged from international outrage over NSO Group's sales to numerous authoritarian countries worldwide, alongside additional revelations that the offensive cyber capabilities market was growing rapidly. This mission, in theory, is much broader than "end-to-end" spyware: it encompasses development, sales (from brokers or companies), and use of spyware– which includes the acquisition, development, and maintenance of zero-day exploits.[110] The consultation summary report initially included laudable proposals around zero-day exploitation, such as encouraging VEP programs internationally and creating clear guidelines for vendors in the space.[111] However, several follow-on reports on Pall Mall have focused mainly on applying international law frameworks toward government use of such capabilities or state-by-state policies guides. This suggests not only a divergence in stakeholder interest for what topic Pall Mall should tackle first but also a divergence in understanding of how to translate international norms to an operational level across countries.[112]

US Big Tech companies as a strategic counterweight

Because the use of zero-day exploits in cyber operations inherently takes advantage of weaknesses in private sector software products, US domestic technology companies' cybersecurity measures are a strategic obstacle to US offensive cyber

103. Background Interview, Independent Security Researcher, January 31, 2025; corroborated by Background Interview, Founder of Vulnerability Research Company 2, January 8, 2025.
104. Background Interview, Independent Security Researcher, January 31, 2025; corroborated by Background Interview, Founder, Former Vulnerability Research Vendor, January 8, 2025.
105. Background Interview, Independent Security Researcher, January 31, 2025; corroborated by Background Interview, Founder of Vulnerability Research Company 1, January 8, 2025; corroborated by Background Interview, Founder, Former Vulnerability Research Vendor, January 8, 2025.
106. Background Interview, Independent Security Researcher, January 31, 2025; corroborated by Background Interview, Founder of Vulnerability Research Company 1, January 8, 2025; corroborated by Background Interview, Founder, Former Vulnerability Research Vendor, January 8, 2025.
107. Background Interview, Member of Defense Science Board, Study on Cyber as a Strategic Capability, January 15, 2025.
108. Background Interview, Founder, Former Vulnerability Research Vendor, January 8, 2025; corroborated by Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025; corroborated by Background Interview, Independent Security researcher, January 31, 2025; corroborated by Background Interview, Former U.S. Intelligence Community Official, December 27, 2025.
109. "Pall Mall Process: Consultation on Good Practices Summary Report,". UK Foreign, Commonwealth and Development Office, January 8, 2025, https://www.gov.uk/government/publications/the-pall-mall-process-consultation-on-good-practices-summary-report.
110. UK Foreign, Commonwealth and Development Office, "Pall Mall Process: Consultation On Good Practices Summary Report."
111. UK Foreign, Commonwealth and Development Office, "Pall Mall Process: Consultation On Good Practices Summary Report."
112. Louise Marie Hurel et al., "The Pall Mall Process on Cyber Intrusion Tools: Putting Words into Practice," March 14, 2025, https://rusi.org/explore-our-research/publications/commentary/pall-mall-process-cyber-intrusion-tools-putting-words-practice.

goals. In many ways, this is a strategic obstacle by design. The public outcry over US intelligence community's efforts to influence the distribution of deliberately insecure products,[113] or mandating backdoors into existing technology products[114] has shifted US policy away from built-in eavesdropping tools and towards ensuring that US products are secure by design.[115] However, companies like Google, Apple, Meta, Microsoft, or Cisco are frequent targets for vulnerability research and exploitation because their products are so prevalent. Any private sector vendor, with or without insider knowledge, can easily assume that a zero-day exploit against a widely used application will likely be more attractive to a potential government customer, and thus are incentivized to exploit those applications. This is particularly obvious in the mobile market, where Android (developed by Google) is on 71 percent of all mobile phones globally, and iOS (developed by Apple) is on 28 percent—in other words, 99 percent of global mobile phones run US Big Tech software.[116] As a result, plenty of offensive cyber capability firms worldwide have been found selling products with iOS and Android exploits.[117]

US Big Tech companies, to protect against exploitation and government operations against their users, have invested heavily into cybersecurity defenses, taken steps to make their products secure, and thwarted government attempts to make their products less secure through regulation.[118] The complexity and robustness of cybersecurity mitigations (such as sandboxing, logging crashes, and other exploit mitigations) have prolonged development cycles for exploits (from days or weeks in the early 2000s to 6 to 18 months or more)[119] and have also driven up prices.[120]

The actions by US Big Tech companies have made zero-day exploitation incredibly difficult over the last decade for five reasons. First, security measures have resulted in hyper-specialization within the offensive cyber capabilities industry. As product codebases become ever more complex, learning how a product works to find vulnerabilities becomes more time consuming, and vulnerability researchers have fewer incentives to look at more than one product.[121] Second, thanks to layered security measures, most vulnerability research shops now must not only find single exploits (i.e., exploit primitives), but also be able to chain them into exploit chains to successfully gain access to the newest iOS or Android phone.[122] Third, the act of chaining exploits together and maintaining the chain for a government customer has also become increasingly complicated,[123] with large technology firms employing quick turnarounds to fix vulnerabilities (i.e., "quick-patch cycles").[124] Fourth, some US Big Tech companies have created threat-hunting teams, like Google's Project Zero, dedicated to

113. "The Clipper Chip," Electronic Privacy Center, accessed April 5, 2025,. https://archive.epic.org/crypto/clipper/.
114. "Amicus Briefs Apple v. FBI," Electronic Privacy Information Center, accessed April 5, 2025, https://epic.org/documents/apple-v-fbi-2/.
115. "Secure by Design: It's Time to Build Cybersecurity into the Design and Manufacture of Technology Products," Cybersecurity and Infrastructure Security Agency (CISA), accessed April 5, 2025, https://web.archive.org/web/20250102030020/https://www.cisa.gov/securebydesign.
116. "Mobile Operating System Market Share Worldwide May 2024 – May 2025," chart, StatCounter GlobalStats, accessed April 4, 2025, https://gs.statcounter.com/os-market-share/mobile/worldwide.
117. Maddie Stone, "0-days exploited by commercial surveillance vendor in Egypt," Google Threat Analysis Group, September 22, 2023,. https://blog.google/threat-analysis-group/0-days-exploited-by-commercial-surveillance-vendor-in-egypt/; Bill Marczak et al., "Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains," Munk School Citizen Lab, University of Toronto. April 18, 2023, https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/.
118. "Apple Can No Longer Offer Advanced Data Protection in the United Kingdom to New Users," Apple Support (UK), February 24, 2025,. https://support.apple.com/en-gb/122234.
119. Background interview, Founder of Vulnerability Research Company 1, January 15, 2025; corroborated by Background Interview, Founder of Vulnerability Research Company 2, January 8, 2025; corroborated by Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025; corroborated by Background Interview, Founder of Vulnerability Research company 3, January 9, 2025.
120. Background interview, Founder of Vulnerability Research Company 1, January 15, 2025; corroborated by Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025; corroborated by Background Interview, Founder of Vulnerability Research company 3, January 9, 2025.
121. Work interview, January 8, 2025; corroborated by Background Interview, Founder, Former Vulnerability Research Vendor, January 8, 2025.
122. Background Interview, Founder of Vulnerability Research Company 2, January 8, 2025; corroborated by Background Interview, Founder of Vulnerability Research company 3, January 9, 2025; corroborated by Background Interview, Founder of Vulnerability Research Company 1, January 15, 2025; corroborated by Background Interview, Founding Member of Vulnerability Research Company, January 11, 2025.
123. Flake, "OffensiveCon20—Keynote—Why I Love Offensive Work, Why I don't Love Offensive Work."
124. About Project Zero, Project Zero, accessed June 9, 2025, https://googleprojectzero.blogspot.com/p/about-project-zero.html.

researching zero-days found "in-the-wild" (i.e., being actively exploited by an attacker)[125] and conducting novel research[126] to directly thwart efforts made by offensive firms to exploit any devices.[127]

Finally, Western Big Tech firms have begun suing offensive cyber capability firms in US federal courts. While the lawsuits do not yet involve US firms, the precedent set in these cases may open US contractors to risks of future lawsuits. In 2019, WhatsApp sued NSO Group for violating the Computer Fraud and Abuse Act (CFAA), the primary US anti-hacking law, and the WhatsApp platform's terms of service.[128] This case was widely regarded as a win for human rights. Namely, a large company with a wide history of providing products to human-rights-abusing governments, who primarily used the platform to spy on domestic civil society groups and even against US government personnel, was forced to cease their activities exploiting WhatsApp software and to pay significant fines.[129] However, because the argument laid out in the case relied on an explanation of how NSO's exploits worked, both vendors and government officials alike have concerns about the ripple effects it may cause in the zero-day research community.[130] In particular, NSO Group was found in violation of the CFAA because their Pegasus spyware used a WhatsApp exploit to deliver Pegasus to WhatsApp users across all major operating systems, even despite the fact that they were likely doing so on behalf of a government customer.[131] While, unlike with the Israel-based NSO Group, the national security carve-out in the CFAA could protect most US firms, this particular part of the anti-hacking law has not yet been tested in US courts.[132]

China's acquisition pipeline

Chinese offensive cyber capability firm No Sugar Tech's website.

Source: No Sugar Tech, accessed April 5, 2025, https://www.nosugartech.com.

> "This market [for offensive cyber] is basically land reclamation. Look at the legion model of Huawei and Qi Anxin - they've got 10,000 people, and we have a team of 100."
>
> *– Leaked discussion between co-founders of Chinese cyber mercenary company iSoon, January 14, 2022.*

> "Why would the PLA want to work with us? We are a non-Chinese party … they cannot control what we tell people. [But] the PLA could always go through a third party, or go through someone else … I [would] not have a problem selling something to the Chinese government."
>
> *– Thomas Lim, former founder of Singaporean Exploit Firm COSEINC (Risky Business podcast, 2014).*

125. Ben Hawkes, "0day 'In the Wild,'" Project Zero, May 15, 2019, https://googleprojectzero.blogspot.com/p/0day.html.
126. Ravie Lakshmanan, "Google Project Zero Researcher Uncovers Zero-Click Exploit Targeting Samsung Devices," The Hacker News, January 10, 2025,. https://thehackernews.com/2025/01/google-project-zero-researcher-uncovers.html
127. All bugs found by Project Zero are disclosed to the affected company directly, and the company is given 90 days to fix the underlying issue before Google publishes technical details about the bug openly—encouraging rapid remediation of the vulnerability. However, Big Tech's actions have not been without scrutiny. In 2020–21, Google's Project Zero unilaterally and publicly shut down multiple Western-led counter-terrorism operations in cyberspace because they found the operations used vulnerabilities in Android and Chrome products. See: Patrick Howell O'Neill, "Google's Top Security Teams Unilaterally Shut Down a Counterterrorism Operation," MIT Technology Review, March 26, 2021, https://www.technologyreview.com/2021/03/26/1021318/google-security-shut-down-counter-terrorist-us-ally/; Michael Coppola, "Google: Stop Burning Counterterrorism Operations," author blog, June 24, 2024, https://poppopret.org/2024/06/24/google-stop-burning-counterterrorism-operations/.
128. Suzanne Smalley, "NSO Ruling Is a Victory for WhatsApp, but Could Have a Small Impact on Spyware Industry,". The Record, January 10, 2025, https://therecord.media/nso-whatsapp-ruling-may-have-limited-impact-on-spyware-ecosystem.
129. Asaf Lubin, "Unpacking WhatsApp's Legal Triumph Over NSO Group," Lawfare, January 7, 2025, https://www.lawfaremedia.org/article/unpacking-whatsapp-s-legal-triumph-over-nso-group.
130. Background Interview, Member of Defense Science Board, Study on Cyber as a Strategic Capability, January 15, 2025.
131. Lubin, Unpacking WhatsApp's Legal Triumph Over NSO Group."
132. 18 U.S.C. § 1030(f).

Supply—Well established, comprehensive feeder systems

Companies—Prime and subcontractor ecosystem, with outsourcing of both capability and operations to the private sector.

China's offensive cyber capabilities firms are also a mix of both large prime contractors and smaller bespoke companies. However, unlike US defense primes, prime contractors for China's offensive cyber projects are often the same Chinese big tech firms that sell products in the global market. China's major cybersecurity firms, such as QiAnXin, Huawei, Qihoo360, and NSFocus provide services directly to the Chinese military—Qihoo360, China's leading antivirus company, assisted with China's hack of the US health insurance company Anthem.[133] Many of the large technology firms also have internal bespoke teams that focus on offensive security work. However, unlike the Google Project Zero model, such internal teams directly provide research on exploitation to the government rather than making government-funded zero-day research hard. Chinese large technology firms also directly fund or subcontract work to small- and medium-sized offensive security start-ups.[134] Cofounders of such offensive security start-ups are usually serial entrepreneurs, who also encourage families to enter the industry.[135] For large tech firms that do not have embedded offensive security teams or bid for government contracts directly, China's 2021 Vulnerability Disclosure Law forces engagement with the overall offensive pipeline regardless (as explained in the sections below).

Chinese offensive cyber capabilities firms (both prime and subcontractors), such as No Sugar Tech shown in the image above, provide multiple offensive-cyber services at once. These can include various offerings, such as selling targeting platforms, various hacking services, or even access to victims' devices and data directly to the Chinese government—**an outsourcing of both capability and operations to the private sector.** This is a much broader remit than US firms, which often only provide the capabilities. When Chengdu-based offensive security company iSoon's marketing materials and internal chat logs were leaked online in 2023, researchers discovered that iSoon sold all three services (hack-for-hire, selling victim data gained by directly hacking targets, and targeting platforms for such hacking) to a variety of Chinese government clients.[136] iSoon also subcontracted for the major Chinese cybersecurity company Qi An Xin, while sourcing vulnerabilities and other capabilities from other firms when they could not source services in-house.[137] For example, iSoon cooperated with Chengdu 404 on research regarding "software vulnerability of information systems"—Chengdu 404 was previously indicted by the US Department of Justice (DOJ) for conducting computer intrusion campaigns against more than 100 global victims.[138]

Chinese researchers also experiment heavily with changing the underlying cyber landscape by using AI, with government support. As early as 2017, the Chinese government began to integrate "intelligentization" into its armed forces and contractors: the concept of incorporating numerous emerging technologies—including decentralized computing, data analytics, quantum computing, AI, and unmanned or robotic systems—into the PLA's conceptual framework.[139] Chinese cyber actors have been using large language models since 2024 to create deepfakes for disinformation campaigns,[140] but this likely only scratches the surface. Researchers believe China already utilizes even more cutting-edge AI research in cyber operations. Since 2021, at least six Chinese universities with links to known Chinese state-sponsored cyber operations have been conducting cutting-edge AI research.[141] Moreover, China's AI industry has deep connections with its offensive cyber industry. Since 2021, an AI tool created by Huawei, a sanctioned Chinese company, has been a dominant contributor to the Li-

133. "The Chinese Private Sector Cyber Landscape," Margin Research, , April 25, 2022, https://margin.re/2022/04/the-chinese-private-sector-cyber-landscape/.
134. Margin Research, "The Chinese Private Sector Cyber Landscape."
135. Background Interview, U.S. Government China Cyber Analyst, January 9, 2025.
136. Cyber Treat Research Team, "A comprehensive Analysis of I-Soon's Commercial Offering," HarfangLab, March 1, 2024, https://harfanglab.io/insidethelab/isoon-leak-analysis/.
137. DeSombre Bernsen, "Same Same, but Different."
138. DOJ Office of Public Affairs, "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged in Connection with Computer Intrusion Campaigns Against More Than 100 Victims Globally," release [archives], US Department of Justice, September 16, 2020, https://www.justice.gov/archives/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer; Natto Team, "i-SOON: Kicking off the Year of the Dragon with Good Luck … or Not," *Natto Thoughts* [Substack newsletter], February 28, 2024, https://nattothoughts.substack.com/p/i-soon-kicking-off-the-year-of-the.
139. Elsa Kania, "AlphaGo and Beyond: The Chinese Military Looks to Future 'Intelligentized' Warfare," Lawfare, June 5, 2017, https://www.lawfaremedia.org/article/alphago-and-beyond-chinese-military-looks-future-intelligentized-warfare.
140. Derek B. Johnson, "Chinese Hackers Turn to AI to Meddle in Elections, *CyberScoop*, April 5, 2024, https://cyberscoop.com/microsoft-ai-election-taiwan/.
141. Dakota Cary, "Academics, AI, and APTs. How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research," Center for Security and Emerging Technology, March 2021, https://cset.georgetown.edu/publication/academics-ai-and-apts/.

nux kernel. A majority of contributions from Huawei's AI tool, known as "HULK bot," are fixing previously unknown vulnerabilities (the tool is a machine-learning enabled fuzzer).[142] Despite Western-led efforts to prevent Chinese firms from obtaining semiconductors able to support the training of high-end large language models, this has not impacted Chinese AI firms as deeply as initially expected and suggests that Chinese cyber operators will increasingly be able to utilize AI research in the future.[143]

Domestic talent—Large, centralized, state-sponsored

While the United States relies on an international talent pool to secure these capabilities, China largely relies on its domestic talent but is moving to capture more of the market in East Asia. China has an incredibly robust domestic talent pool of offensive hacking talent: the Chinese hacking ecosystem, as judged by their CTF competitions alone, is immense. Government sponsorship ensures large-scale funding, extensive participation, and stable career pipelines for top competitors—China's top ten CTF national competitions attract over 11,000 participants on average.[144] This is in stark contrast to the 2,000 individuals participating in the US Cyber Open, the top contest within the US's relative handful of government-sponsored contests. By sheer numbers alone, it is unsurprising that **China each year has more graduates in the science, technology, engineering, and mathematics (or "STEM") fields than the United States produces in total college graduates.**[145]

Of course, the Chinese CTF ecosystem is only part of a comprehensive and deliberate feeder system from universities, cybersecurity conferences, and hacking competitions into the Chinese offensive cyber apparatus. Chinese military universities and high-end science and engineering schools produce high-caliber graduates in deeply applied offensive cybersecurity research, some of whom are encouraged to develop final projects that involve hacking into US companies.[146] Many of them, upon graduating, either work on offensive teams of existing offensive security firms, found an offensive cyber start-up, or work directly for high-end teams in China's Ministry of State Security (MSS) or People's Liberation Army (PLA).[147] Talent pools from China's higher education are also supplemented by a wide array of government-sponsored hacking competitions and conferences. The Chinese government has hosted hundreds of official CTF and other industry standard hacking competitions, often in partnership with many of its ecosystem's offensive security companies and with universities that provide financial incentives for students to participate.[148] Many other CTF competitions were directly founded by top Chinese teams that used to compete internationally,[149] while other competitions have involved breaking into real foreign technology products or even enterprise systems.[150] The Chinese government and its major offensive firms seek to recruit directly from these competitions.[151]

Unlike the United States, the People's Republic of China (PRC) has the unique advantage of having a hacking community that originated in explicit, patriotic alignment with state interests, making such hackers easier to recruit. One of China's first hacker groups was the Hongke Union who, in 2001, famously took down the White House website and defaced websites of US businesses in retaliation for the collision between a US

142. Dave Aitel et al., *China's Cyber Operations: The Rising Threat to American Security*, Margin Research, August 20, 2022, https://margin.re/content/files/2024/02/China-s-Cyber-Operations-Full-Report-Updated.pdf.

143. Kelly Ng et al., "DeepSeek: The Chinese AI App that Has the World Talking," *BBC News*, February 4, 2025, https://www.bbc.com/news/articles/c5yv5976z9po.

144. Dakota Cary and Eugenio Benincasa, *Capture the (Red) Flag: An Inside Look into China's Hacking Contest Ecosystem*, *Atlantic Council*, October 18, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/capture-the-red-flag-an-inside-look-into-chinas-hacking-contest-ecosystem/.

145. Remco Zwetsloot et al., "China is Fast Outpacing U.S. STEM PhD Growth," Center for Security and Emerging Technology, August 2021, https://cset.georgetown.edu/publication/china-is-fast-outpacing-u-s-stem-phd-growth/; Brendan Oliss, Cole McFaul, and Jaret C. Riddick, "The Global Distribution of STEM Graduates: Which Countries Lead the Way?" Center for Security and Emerging Technology, November 27, 2023, https://cset.georgetown.edu/article/the-global-distribution-of-stem-graduates-which-countries-lead-the-way/; Melanie Hanson, "*College Graduation Statistics*," Education Data Initiative, March 15, 2024 [update], https://educationdata.org/number-of-college-graduates.

146. On background Interview, U.S. Government China Cyber Analyst, January 9, 2025. See also information on Real World CTF: Cary and Benincasa, *Capture the (Red) Flag*.

147. Background Interview, U.S. Government China Cyber Analyst, January 9, 2025. See also information on Real World CTF: Cary and Benincasa, *Capture the (Red) Flag*.

148. Cary and Benincasa, *Capture the (Red) Flag*.

149. Eugenio Benincasa, "From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem," ETH Zurich Center for security Studies, June 10, 2024, https://css.ethz.ch/en/center/CSS-news/2024/06/from-vegas-to-chengdu-hacking-contests-bug-bounties-and-chinas-offensive-cyber-ecosystem.html, https://doi.org/10.3929/ethz-b-000675181.

150. Cary and Benincasa, *Capture the (Red) Flag*.

151. Interview with Dakota Cary, Fellow, Atlantic Council Global China Hub, January 8, 2025.

spy plane and a Chinese fighter jet off of Hainan Island.[152] In the early to mid-2000s, as China was experiencing unprecedented economic growth, China's hackers either professionalized and created technology companies, were co-opted directly into China's growing cyber forces, or both. For example, the head of the Green Army, Jiye Shen (a.k.a. "Goodwill" on hacker forums), created the internet security company NSFocus in 2000.[153]

Meanwhile, the PLA, in 2005, directly recruited Tan Dailin (谭戴林, a.k.a. Wicked Rose), a student from the Sichuan University of Science and Engineering, to design hacking tools for the Chinese military.[154] Wicked Rose then formed a patriotic hacking group to break into DOD computer systems in 2006.[155] MSS, China's foreign intelligence organization, also began recruiting talent both directly and indirectly during the early 2000s.[156] This organization has suited the many hackers less able to conform to physical fitness tests or other rigid requirements the PLA typically requires of its military recruits, with just as many benefits.[157]

The Chinese government has spent the last decade effectively closing off its domestic talent pool from outside influence. From 2016 to 2021, China effectively began to prevent hackers from sharing research with the global hacking community. In July 2016, Wooyun, a vulnerability disclosure platform created by the Chinese "ethical hacking" community, which had engaged frequently with Taiwanese and other international hackers, was suddenly taken down, and its founding members were arrested by Chinese authorities without charges.[158] Some China researchers speculate that the takedown was an action taken at the behest of the MSS, China's primary intelligence service, who wished to control the vulnerability marketplace.[159] In 2018, China announced a regulation ("Regulating the Promotion of Cybersecurity Competitions") effectively banning hackers from travelling abroad to participate in hacking competitions, as well as requiring any vulnerabilities found through domestic competitions to be directly reported to the Ministry of Public Security (MPS), China's law enforcement organization, and other relevant departments.[160] Chinese hacker participation at contests like Pwn2Own dropped to zero, and the number of presentations given by Chinese researchers at Taiwanese conferences fell precipitously.[161]

More recently, China has expanded its reach into East and Southeast Asia through hacking competitions and partnerships with regional researchers, seeking to secure additional talent on its own terms. Academics from the Harbin Institute of Technology and Beijing University of Posts and Telecommunications have advocated for actively engaging with hacking communities in East Asia seeking to influence future international standards for how vulnerabilities are discovered and managed.[162] While Chinese hackers cannot participate in most Western hacking competitions, Chinese CTF events often attract or even outright invite talent in the wider East and South Asian regions to participate. The QiangWang Cup and RealWorldCTF (respectively, linked to the PLA and MSS) are two Chinese hacking contests that historically have had participants from Vietnam, Japan, Russia, Ukraine, and even the United States.[163] Moreover, China prolifically sponsors and hosts international hacking conferences to draw in international talent. Chinese researchers, while unable to participate in most outside hacking

152. Wun Nan, "From Hackers to Entrepreneurs: The Sino-U.S. Cyberwar Veterans Going Straight," *South China Morning Post*, August 21, 2013, https://www.scmp.com/news/china/article/1298200/hackers-entrepreneurs-sino-us-cyberwar-veterans-going-straight.

153. Scott J. Henderson, *The Dark Visitor: Inside the World of Chinese Hackers*, Lulu.com (2007),' https://books.google.com/books?id=NYIiAQAAMAAJ.

154. Adam Kozy, "Testimony before the U.S.-China Economic and Security Review Commission Hearing on 'China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States,'" February 17, 2022, https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf.

155. Ken Dunham and Jim Melnick, *"'Wicked Rose' and the NCPH Hacking Group*," Krebs on Security, November 2012, https://krebsonsecurity.com/wp-content/uploads/2012/11/WickedRose_andNCPH.pdf.

156. Kozy interview, January 17, 2025.

157. Kozy interview, January 17, 2025.

158. Gene Lin, "Founder of China's Largest 'Ethical Hacking' Community Arrested," *Hong Long Free Press*, March 31, 2020, https://hongkongfp.com/2016/07/30/founder-chinas-largest-ethical-hacking-community-arrested/.

159. Kozy interview, January 17, 2025.

160. Translation: "Notice on Regulating the Promotion of Cybersecurity Competitions," Center for Security and Emerging Technology, May 13, 2021, https://cset.georgetown.edu/publication/notice-on-regulating-the-promotion-of-cybersecurity-competitions/; Cary and Benincasa, *Capture the (Red) Flag*.

161. Interview with Security Researcher Chi-en (Ashley) Shen, January 9, 2025.

162. 对漏洞治理体系革新发展的思考与建议, 哈尔滨工业大学 (张兆心, 孔珂) / 北京邮电大学 (刘欣然) [Thoughts and suggestions on the innovation and development of vulnerability management system, Harbin Institute of Technology (Zhang Zhaoxin, Kong Ke) / Beijing University of Posts and Telecommunications (Liu Xinran)], China Information Security Magazine, May 1, 2024.https://www.scribd.com/document/816402725/%E7%94%B5%E5%AD%90%E5%88%8A202405. Corroborated by Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025.

163. Cary and Benincasa, *Capture the (Red) Flag*.

competitions, still have a large presence at "Hack in the Box" Dubai and other conferences, which reflects the coordination and sharing that China and the United Arab Emirates have in cyberspace. Chinese conference "GeekCon" (active in China from 2014 to 2021) re-established itself in Singapore from 2021 onwards, soliciting international talks and insinuating that they still abided by China's vulnerability disclosure laws.[164] Elite Chinese and South Korean offensive security research companies (Pangu Team and POCSecurity, respectively) consistently collaborate to recruit international talent to MOSEC, a conference on mobile security hosted in Shanghai every year.[165]

It is clear that China, while limiting the activities of its domestic hackers, already sources some vulnerabilities from foreign hackers living abroad. COSEINC, a Singaporean vulnerability research company run by Thomas Lim (a Singaporean national with ties to China),[166] was put on the US entities list in 2021, likely for selling exploits to the Chinese government.[167] Lim, a known entity in East Asia's vulnerability research circles, publicly stated that he was not against selling his products to the Chinese government.[168] China may also be tricking researchers into handing over bugs to the Chinese state. In 2021, Taiwanese vulnerability researcher Orange Tsai reported a vulnerability to Microsoft that impacted its exchange servers two days after a Chinese Advanced Persistent Threat (APT) group began exploiting the same vulnerability in its operations. This suggests that either two separate individuals (one Chinese and one Taiwanese) independently discovered the vulnerability, or information about the vulnerability was somehow obtained from the researcher by a Chinese entity.[169]

China's offensive cyber capability acquisition methods.

Government contracts for offensive cyber care less about stealth than access and provide additional resources to firms.

The Chinese system accepts higher operational risk for the sake of speed and flexibility. China's acquisition system has decentralized mechanisms, such that even provincial and municipal government entities contract directly with local cyber firms. iSoon's former website listed over fifty-six different clients, ranging from the MPS to a wide variety of various provincial, city, and municipal public security bureaus—effectively the equivalent of FBI field offices.[170] Based on the leaks, iSoon held individual contracts for goods and services with several municipal and provincial level bureaus (similar in size to the Cincinnati or Pittsburgh police departments) purchasing hack-for-hire capabilities. Chinese legal scholars have also bemoaned China's national intelligence apparatus's lack of clear pre-, mid-, and post-supervision structures for intelligence operations more broadly.[171] This suggests that decentralization is a feature of the overall system rather than an exception.[172]

Unlike in the United States, where government acquisition is slow and risk-averse, Chinese firms can operate opportunistically, sometimes combining cybercrime with state-sponsored activity, with minimal fear of reprisal as long as they align with state interests. Internal discourse from within the Chinese hacker community suggests that, despite China's cybersecurity laws and ancillary legislation on regulating vulnerabilities, there is a grey zone for what activity is permitted, versus what may get a patriotic Chinese hacker "invited to tea" at MPS or MSS offices.[173] One famous example is Wicked Rose, who, af-

164. Cary and Benincasa, *Capture the (Red) Flag*; corroborated by Interview with Security Researcher Chi-en (Ashley) Shen, January 9, 2025.

165. MOSEC 2023, accessed March 16, 2025, https://www.mosec.org/en/2023/.

166. "China, Singapore, United States: Blacklisted by the US, Zero Day Distributor COSEINC Works on for China's Pwnzen," Intelligence Online, August 11, 2021,. https://www.intelligenceonline.com/surveillance--interception/2021/11/08/blacklisted-by-the-us-zero-day-distributor-coseinc-works-on-for-china-s-pwnzen,109703349-art.

167. David Sun, "Singapore Cyber-Security Firm Blacklisted by the U.S. Along with Those Linked to Pegasus Spyware," *The Straits Times*, November 4, 2021, https://www.straitstimes.com/singapore/singapore-cyber-security-firm-blacklisted-by-the-us-along-with-those-linked-to-pegasu.

168. Patrick Gray and Adam Boileau, "Risky Business #310—Export Exploits? Wassenaar Says No," Risky Business Podcast, February 14, 2014, https://risky.biz/RB310/.

169. Matthieu Faou, Thomas Dupuy, and Mathieu Tartare, "Exchange Servers under Siege from at least 10 APT Groups," ESET Research, March 10, 2021, https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/.

170. 安洵信息-专业领先 信誉卓著. [Anxun Information – Professional leadership and outstanding reputation.], accessed March 16, 2025, https://web.archive.org/web/20240219105947/http:/www.i-soon.net/pc_partner.html.

171. 我国国家情报监督体系构建研究.[Research on the construction of my country's national intelligence supervision system.] (2025). 情报杂志 [Intelligence Magazine], *44*(2), 38–43.

172. Schwarck, E. (2024, November 15). *The Power Vertical: Centralization in the PRC's State Security System*. Retrieved March 16, 2025, from https://jamestown.org/program/the-power-vertical-centralization-in-the-prcs-state-security-system/. Note: Operational decentralization should not be conflated with lack of oversight. Vertical leadership of local MSS units, where personnel authority rests with the internal party organs of a higher level unit within the central Ministry of State Security, has been in place since 2016–2017.

173. On Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025.

ter creating the NCPH hacker group and defacing multiple US websites, was arrested by the MPS in 2009 for engaging in domestic cybercrime.[174] He likely received a commuted sentence in exchange for an agreement to contract for the MSS just two years later (which resulted in Wicked Rose founding Chengdu 404, a company indicted by the DOJ in 2020), and was likely permitted to continue his criminal activities as long as they targeted victims outside China.[175] China researchers interviewed have also suggested that the Chinese government gives hackers significant leeway, while underpaying them for services and handling its most sensitive matters in-house.[176] While the Chinese government deliberately depresses prices and exercises monopsony power, its decentralized model and allowance of a "grey zone" enables a more flexible contracting environment that enables smaller players. Small and medium-sized companies like iSoon, Chengdu 404, and others have been shown to obtain contracts through a mix of "guanxi" (networking and relationship building) and formal contracting processes.[177]

Most importantly, the PRC's overall contracting process, including the loose leash on its corporate hackers-for–hire, largely does not penalize organizations when they are caught or attributed. In 2013, the security firm Mandiant published a report on APT1, the first publicly-outed Chinese threat group, and attributed it to the Chinese PLA Unit 61398.[178] While the report initially sent shockwaves through the Chinese state security apparatus, many quickly realized that naming and shaming did not result in strategic level or department level pain.[179] Rather, most US policies that resulted from "naming and shaming" threat groups fell into two groups: DOJ indictments of individual Chinese hackers (who likely were not planning on leaving China for a US-extradition friendly state anyway) or economic sanctions on Chinese offensive security companies that did not plan on doing much business with Western firms.[180] Thus, while middle managers of China's security services likely must prioritize both operational tradecraft and obtaining intelligence of strategic value to the Chinese Communist Party, the goal of obtaining such intelligence significantly outweighs the requirement to adhere to tradecraft and professionalism, as there are few real costs of attribution on the managers of such operations.[181] Of course, like the grey zone, there are likely exceptions to this rule, such as if a single Chinese company causes the wider CCP intelligence apparatus to "lose face."[182]

China's apparent preference for results over attribution also enables Chinese organizations to utilize riskier capabilities (such as noisier, easier-to-detect n-day vulnerabilities) and to reuse infrastructure, even when it allows Western organizations to better detect them. In that sense, truly "burning" (or disposing of) a capability is much rarer in China.[183] Moreover, this preference provides room for private-sector hackers to experiment. Some Chinese offensive cyber capability shops can also observe what other countries' offensive teams are doing "in-the-wild" and attempt to echo the techniques of other countries' APT groups.[184] For example, Chinese APTs were able to exploit a vulnerability linked to NSA hacking tools leaked online in 2017, prior to the leak itself, suggesting that either an elite Chinese team found the same bug as the NSA during a similar timeframe, or they were able to detect the NSA exploit, reverse engineer it, and then use it themselves.[185]

174. Kozy, "Testimony before the U.S.-China Economic and Security Review Commission Hearing," February 17, 2022; DOJ Office of Public Affairs, "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged."
175. Kozy, "Testimony before the U.S.-China Economic and Security Review Commission Hearing," February 17, 2022; DOJ Office of Public Affairs, "Seven International Cyber Defendants, Including "Apt41" Actors, Charged."
176. Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025.
177. Dina Temple-Raston, "192. Return to the Leak that Unmasked China's Hackers-for-Hire," podcast transcript, Recorded Future News, December 17, 2024, https://pod.wave.co/podcast/click-here/192-return-to-the-leak-that-unmasked-chinas-hackers-for-hire-a648d800.
178. Dan McWhorter, "Mandiant Exposes APT1 – One of China's Cyber Espionage Units – and Releases 3,000 Indicators," Google Cloud Blog, February 19, 2013, https://cloud.google.com/blog/topics/threat-intelligence/mandiant-exposes-apt1-chinas-cyber-espionage-units.
179. Kozy, "Testimony before the U.S.-China Economic and Security Review Commission Hearing," February 17, 2022.
180. "Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise," release, US Department of the Treasury, February 8, 2025, https://home.treasury.gov/news/press-releases/jy2792; DOJ Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," release [archives], US Department of Justice, May 19, 2014, https://www.justice.gov/archives/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
181. Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025.
182. Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025.
183. Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025; corroborated by Kozy interview, January 17, 2025; corroborated by Interview with Mei Danowski, Natto Thoughts, January 8, 2025.
184. Kozy interview, January 17, 2025.
185. Threat Hunter Team, "Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak," Symantec and Carbon Black, May 6, 2019, https://www.security.com/threat-intelligence/buckeye-windows-zero-day-exploit.

Finally, CCP intelligence and law enforcement mechanisms clearly provide consistent resourcing to their offensive firms, likely to help shorten the feast-or-famine cycles. Experts following the Chinese cyber capabilities market largely agree that the Chinese government likely has a method of vulnerability sharing among both their private sector and government operators, with tiers of access and privileges.[186] The sources of vulnerabilities likely range from hacking competitions like the Tianfu Cup,[187] acquisitions from existing contractors (both foreign and domestic), and vulnerability reports into the MSS-operated China National Vulnerability Database (CNNVD), and other government vulnerability databases.

China's combination of revealed results-forward preference over stealth, and commitment to resource sharing with its private sector, results in a unique vulnerability resourcing process, where small subsets of more elite hacking "A-teams" get early access to the zero-day vulnerabilities. However, once the vulnerability is discovered, the Chinese government opens the capability to other groups.[188] This was famously evidenced in the 2021 Microsoft Exchange attacks, where a Chinese APT group exploited a vulnerability targeting Microsoft Exchange two days before the vulnerability was reported to Microsoft on January 5th.[189] Before Microsoft could issue a patch for the vulnerability, multiple other Chinese APT groups began using the same exploit in their campaigns.[190] Microsoft released a patch for the vulnerability on March 2nd – one day later, Chinese threat groups began exploiting the vulnerability en-masse.[191] However, while the Microsoft Exchange vulnerability is the most notorious example, Chinese threat analysts have seen this pattern play out for even non-critical vulnerabilities in other public-facing services, such as web servers, virtual private networks (VPNs), and other edge devices.[192] This rapid weaponization of both 0day and n-day vulnerabilities also explains why certain campaigns use relatively new vulnerabilities or access points to gain entry into targets that are relatively low-hanging fruit—at this point, the "D-teams" have obtained access to the capabilities previously used by "A-teams."[193] In some senses, this results in an enormous ability to efficiently weaponize offensive cyber capabilities—this system enables organs of the PRC government to efficiently build, acquire, and weaponize capabilities ranging from the mediocre to the exquisite.[194] It also stands in stark contrast to the US model, effectively extending the shelf-life of a purchased capability.

Currently, China has yet to engage with the Pall Mall process or other international codes of practice to regulate the acquisition and use of offensive cyber capabilities.

China uses its CTF and regulatory ecosystem to solicit bugs informally from hackers for national security use; its major technology companies are strategic allies in sourcing exploits.

As stated previously, China effectively prevented its domestic vulnerability research talent pool from sharing research with the wider community between 2016 and 2021. During this time, China began ramping up hacking opportunities and vulnerability disclosure programs domestically: the CNNVD (the previously mentioned MSS-run vulnerability database) grew its partnerships from fifteen technical support units and partner companies in 2016 to 151 companies in 2023.[195] This expansion drew in Chinese Big Tech firms like Tencent, Huawei, and Hikvision, which would report vulnerabilities in their own products. Other partners also included specialized offensive capability firms. Moreover, hackers who could no longer compete internationally were encouraged to compete in Chinese live-hacking competitions, like the famous Tianfu Cup, founded in 2018 as a "Chinese Pwn2Own."[196] However, both the

186. Cary interview, January 8, 2025; corroborated by Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025; corroborated by Background Interview, USG China Analyst, January 22, 2025.
187. Patrick Howell O'Neill, "How China Turned a Prize-Winning iPhone Hack against the Uyghurs," MIT Technology Review, May 6, 2021, https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/.
188. Cary interview, January 8, 2025; corroborated by Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025; corroborated by Background Interview, USG China Analyst, January 22, 2025.
189. Faou, Dupuy, and Tartare, "Exchange Servers under Siege."
190. Faou, Dupuy, and Tartare, "Exchange Servers under Siege."
191. Faou, Dupuy, and Tartare, "Exchange servers under Siege."
192. Cary interview, January 8, 2025; corroborated by Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025; corroborated by Background Interview, USG China Analyst, January 22, 2025.
193. Cary interview, January 8, 2025; corroborated by Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025; corroborated by Background Interview, USG China Analyst, January 22, 2025.
194. On Background Interview, USG China Analyst, January 22, 2025.
195. Dakota Cary and Kristin Del Rosso, *Sleight of Hand: How China Weaponizes Software Vulnerabilities*, *Atlantic Council*, September 6, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/.
196. Karen Chiu, "Chinese Hackers Break into Chrome, Microsoft Edge and Safari in Competition," *South China Morning Post*, November 19, 2019, https://www.scmp.com/abacus/tech/article/3038326/chinese-hackers-break-chrome-microsoft-edge-and-safari-competition.

Tianfu Cup and the CNNVD have ties to the Chinese intelligence and law enforcement apparatus. In 2017, researchers found that if a vulnerability was reported to the CNNVD that had value to MSS cyber operations, the CNNVD would delay publishing the vulnerability, write an exploit for the vulnerability, and use it in operations.[197] Meanwhile, the Tianfu Cup was (and remains) a vulnerability feeder system for the MPS, China's national police. Vulnerabilities submitted as part of the Tianfu Cup competition are sent straight to the MPS, which would be used in law enforcement operations against Uighurs and other minority groups.[198] If the vulnerabilities were not already full exploit chains (i.e., ready-to-use), the MPS would disseminate the proof-of-concept code to private firms to further exploit.[199]

In addition to its domestic researchers, China has even integrated its respective heavyweight tech firms into its offensive cyber programs. Unlike US Big Tech companies, which act as a strategic blocker against the US vulnerability ecosystem, Chinese technology companies (and even foreign tech companies operating in China) are far more beholden to the Chinese government and have largely been co-opted into the CCP's vulnerability acquisition funnel. This is unsurprising. While Chinese technology firms have similar market caps to their Western counterparts, their primary consumers are still domestic Chinese users. For example, Huawei, the leading smartphone company in China, only makes up 4 percent of the global smartphone market.[200]

China began integrating "civil-military fusion" concepts into its cybersecurity industry starting in 2017, embedding military units into its domestic cybersecurity companies.[201] Setting up a PLA military-civil fusion center in a company enables the Chinese military to connect with industry peers and resources almost seamlessly by embedding military members into companies to work side-by-side with internal staff.[202] Various entities, including universities and private companies, use this model to collaborate with the Chinese government to submit zero-days, co-partner on defense research labs, and set up private IT infrastructure for state-sponsored hacking operations.[203]

PRC's integration of technology companies into its offensive pipeline does not end with staffing choices. State policies demand forced disclosures of vulnerabilities. Since 2021, the PRC has required all software companies operating in China to (reluctantly or otherwise) report vulnerabilities that impact any systems, regardless of source, directly to the PRC government. In 2021, China released new regulations on vulnerability management, the Regulations on the Management of Network Product Security Vulnerabilities (RMSV),[204] which mandates reporting all industry-wide discoveries of vulnerabilities to the Chinese government within 48 hours.[205] This affects all technology companies operating in China, including foreign software firms. In the disclosure, companies are encouraged to upload proof-of-concept code and instructions on how to replicate the vulnerability, which would undoubtedly be helpful to Chinese offensive missions.[206] It also has impacted US critical infrastructure firms: one of the companies found to comply with the Chinese law is Schneider Electric, a US industrial control systems and energy company, whose products (and subsequent vulnerabilities) are likely offered with minimal alteration in both the US and Chinese markets.[207]

Companies that do not comply with the law are penalized. In 2021, an engineer in Chinese company Alibaba found and disclosed a critical zero-day vulnerability impacting Apache Log4j (a widely used software application) to the US Apache Foundation (maintainers of Log4j) instead of notifying Chinese regulators.[208] As a result, Chinese regulators suspended a

197. Priscilla Moriuchi and Bill Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications," Recorded Future, November 16, 2017, https://www.recordedfuture.com/blog/chinese-mss-vulnerability-influence.
198. Howell O'Neill, "How China Turned a Prize-Winning iPhone Hack against the Uyghurs."
199. DeSombre Bernsen, "Same Same, but Different."
200. Monsoor Iqbal, "TikTok Revenue and Usage Statistics (2025)," Business of Apps, February 25, 2025 [update], https://www.businessofapps.com/data/tik-tok-statistics/; "WeChat Users by Country 2025," World Population Review, accessed May 14, 2025, https://worldpopulationreview.com/country-rankings/wechat-users-by-country; Emmanuel Oyedeji, "Huawei Overtakes Apple to Become the Leading smartphone Brand in China," Techloy, January 23, 2025, https://www.techloy.com/huawei-overtakes-apple-to-become-the-leading-smartphone-brand-in-china/.
201. Danowski interview, January 8, 2025.
202. Danowski interview, January 8, 2025.
203. Benincasa, "From Vegas to Chengdu.'"
204. Stewart Scott et al., *Dragon Tails: Preserving International Cybersecurity Research*, *Atlantic Council*, September 14, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/.
205. Andy Greenberg, "How China Demands Tech Firms Reveal Hackable Flaws in Their Products," *Wired*, September 6, 2023, https://www.wired.com/story/china-vulnerability-disclosure-law/.
206. Vulnerability laws create 'bug bounties with Chinese characteristics.' (2024, January 10). Retrieved March 16, 2025, from https://therecord.media/china-vulnerability-disclosure-military-government-dakota-cary.
207. Greenberg, "How China Demands Tech Firms Reveal Hackable Flaws."
208. Scott et al., *Dragon Tails*.

cooperative partnership with Alibaba regarding cybersecurity threats and information-sharing platforms for six months.[209] It is important to note that this RMSV process is separate from and, in many ways, completely counterproductive to the internationally accepted bug bounty and coordinated vulnerability disclosure process.[210] Instead of interfacing directly with the manufacturer of a technology product and encouraging them to be more secure, China's RMSV regulation circumvents this process by (1) mandating that the Chinese government be notified first instead of the company and (2) persuading the sharing of exploit code, but only with the government.

Despite this, Chinese technology firms still contribute to finding bugs in Western technology firms. Chinese researchers accounted for 27 percent of all vulnerabilities reported to the bug bounty programs of Apple, Google Android, and Microsoft from 2017 to 2023.[211] Many of these contributions are also from security companies that have links to the Chinese intelligence apparatus.[212] These contributions are frequently linked to a small handful of individuals within these companies, and a company's contributions to such bug bounty programs fall when one or more Chinese hackers transitions between security companies.[213] Given the strict chokehold the CCP holds on these firms and their vulnerability reporting pipelines, researchers in the US speculate that the CCP's security services recognize that some slackening of restrictions is necessary to retain a truly robust talent pool, especially for hackers that are motivated by international recognition rather than mission or money.[214] It is also likely beneficial to the PRC that its hackers and companies are seen as responsible stakeholders in the global cybersecurity market.

209. "China Regulator Suspends Cyber Security Deal with Alibaba Cloud," Reuters, December 22, 2021, https://www.reuters.com/world/china/china-regulator-suspends-cyber-security-deal-with-alibaba-cloud-2021-12-22/.
210. Scott et al., *Dragon Tails*.
211. Benincasa, "From Vegas to Chengdu."
212. Benincasa, "From Vegas to Chengdu."
213. Benincasa, "From Vegas to Chengdu."
214. Background Interview, China Area Specialist in the Vulnerability Research Space, January 16, 2025.

Key findings

During the literature review, data analysis, and expert interviews (as laid out in the above sections), nine key findings emerged:

1. **Zero-day exploitation is becoming more difficult, opaque, and expensive.** The global hacking ecosystem is highly international and fragmented. The amount of time and capital required to develop an impactful capability has escalated dramatically in the last decade, leading to riskier feast-or-famine contract cycles. The growing number of publicly discovered zero-day threats does not detract from this market trend, in fact, the increase suggests a concurrent rising number of players in the international market. Multiple sources interviewed estimate the number of individuals consistently producing zero-day exploits is in the low hundreds globally.
2. **Middlemen create market inefficiency and erode trust in the market.** Given the lack of transparency in the zero-day market, middlemen with prior government connections further drive up costs and create inefficiency in the US and FVEYs market, while eroding trust between buyers and sellers.
3. **The United States relies on international talent, while China relies on domestic might.** The US offensive cyber workforce relies heavily on international talent pools in South America, Europe, and other FVEYs countries. China's domestic cyber pipeline dwarfs that of the United States, but China is also increasingly moving its supply network out to the Middle East and East Asia.
4. **Talent investment in US offense is lacking.** US government investment into the offensive talent pipeline, however sparse, has focused on defensive jobs, whereas China has well established and comprehensive feeder systems within its offensive apparatus. US talent in exploit development also experiences a "Training Valley of Death" between junior and intermediate levels.
5. **US acquisition favors large prime contractors, slows acquisition in pursuit of stealth, and adds additional risk through opacity.** US cyber capability acquisition favors large defense contractors, who take on heavy compliance burdens while shifting project requirements to smaller firms. The US government internally prioritizes extremely high levels of accuracy, trust, and stealth, which can create market inefficiencies and a reliance on high-cost, exquisite zero-day exploit procurements. Certain US government customers deliberately lengthen the contract cycle by refusing to share information about desired capabilities with firms, leading to an inefficient process where firms may work on an exploit that a customer has no intent to purchase.
6. **China's acquisition uses decentralized contracting methods, outsources operations, shortens contract cycles through additional resourcing, and prolongs the life of an exploit through "n-day usage."** While China also relies on large prime contractors, government ministries have decentralized government procurement processes, such that even provincial government offices issue contracts to firms. China's regulatory environment actively encourages vulnerability reporting to the state, often integrates corporate research with government offensive strategies, and widely enables private sector hack-for-hire operations. China has also shortened the feast-or-famine contract cycle for exploits by providing additional resources to its private sector firms, and it continues to use exploits after their discovery.
7. **US cybersecurity goals, coupled with Big Tech's dominance, are strategic counterweights to the US offensive capability program.** Because zero-day exploits in cyber operations take advantage of weaknesses in private sector software products, the global market dominance of the US Big Tech companies ensures that, as such, they act as a strategic obstacle to US offensive cyber goals. This demonstrates a strategic trade-off between economic prosperity (and global trust in US products), and national security. In contrast, China's tech firms have a far less global market share, and they are a strategic enabler of China's offensive cyber program.
8. **International partnerships for unique offensive cyber capabilities attempt to leverage different circles, but the opaque market offers no guarantees.** The United States leverages international alliances, particularly within the FVEYs intelligence-sharing network, to bolster its cyber capabilities. In contrast, China focuses on cultivating regional influence and integrating offensive cyber capabilities from East Asia and the Middle East. However, given the opaque international market, preference for full chains leveraging multiple exploit primitives, and the increase in bug collisions, there is no 100 percent guarantee of unique capability.
9. **China leans forward on AI in cyber operations.** China's offensive cyber industry is already heavily integrated with AI institutions, and China's private sector has been proactively using AI for cyber operations. The US government's primary efforts with both AI and cyber have largely been defensive in nature, or within the intelligence community internally, although some DARPA programs have encouraged open offensive innovation.

Recommendations

> "We are not going to deter the adversary with defenses only... I will work to strengthen our offensive cyber capabilities to ensure the President has the options. He needs to respond to this growing threat."
>
> *– Katie Sutton, Nominee for Assistant Secretary of Defense for Cyber Policy (2025).*

It is impossible for the United States to match China's supply of zero-day exploits by sheer numbers alone, and adopting the Chinese policies for acquisition and supply is the equivalent of stooping to the level of an authoritarian state. However, there are myriad ways to materially and quickly bridge this gap. Informed by analysis from over 30 expert interviews and open-source data gathering, this report concludes by offering **ten** recommendations across **supply**, **acquisition**, and **operations** to close this capability gap. Each of these recommendations must be filtered through a consideration of **timeline** (swift action is needed given the increasing potential for conflict with China in the coming years), **feasibility** (cyber is one of the last bipartisan domains but with implications for contentious national issues and cross-cutting networks of civil society, government, and industry stakeholders), **buy-in** from the hacker community (alienation or acceptance from this community will determi**ne failure or success), and maintaining Western values** (to learn from CCP cyber models without adopting them wholesale).

Supply:

1. The United States government should create vulnerability research accelerators through existing investment vehicles.

The United States struggles to obtain capabilities from skilled smaller firms, relying on prime contractors with burdensome overhead costs. Creating Vulnerability Research Accelerators (VRAs) through the DOD's Strategic Capabilities Office (SCO), In-Q-Tel, or the Defense Innovation Unit (DIU) could significantly bolster the supply of zero-day exploits by fostering the growth of small, specialized research teams. This would circumvent the de facto requirement for a small business to go through a prime contractor to sell offensive capabilities to the government. These accelerators would focus on supporting small businesses (those with at least five dedicated vulnerability researchers), ensuring that funding and resources are directed toward those generating the original research rather than prime contractors with existing relationships with the government. The VRAs would help these companies navigate the complex federal contracting process, get Small Business Administration certifications, hold and pay for security clearances, and connect companies directly to government contracts. By doing so, the accelerator would significantly lower the barrier to entry and reduce administrative burdens that often deter small but highly skilled teams from engaging with government contracts directly.

2. The NSA should expand its CAE-CO program, provide grants to private organizations that support existing CTFs and offensive security conferences, and directly fund CTF teams at top universities.

Domestic CTF teams at universities die without adequate funding and support. The NSA should bolster the pipeline of skilled vulnerability researchers while demonstrating that the US government values and invests in offensive security talent. It could do so by providing grants to private organizations or academic institutions that support CTF competitions, offensive security conferences, and university-based CTF teams. Directly sponsoring CTFs and hacker clubs at leading universities would nurture talent at the source, as CTFs have long been a testing ground for some of the world's best exploit developers and security researchers. Government funding, paired with resources and mentorship, would encourage students to view vulnerability research as a viable career path, ultimately fostering a new generation of skilled researchers. The NSA, through these grants, could also encourage additional academic institutions to create programs that comply with CAE-CO accreditations or postgraduate programs that solve the "Training Valley of Death," taking apprentice vulnerability researchers to cyber "journeymen" status.

This program should also pair with grants among FVEYs and other allies to fund companies that conduct "cyber journeyman"-like training, host international CTFs and security conferences, or hire international researchers at higher rates than Chinese or other firms, expanding the pool of talent while strengthening partnerships abroad. This approach would help cultivate both domestic and international pipelines of vulnerability researchers, ensuring that the United States and its partners remain competitive in offensive security innovation. This is most important to do within international fora outside the US sphere of influence. For example, offensive conferences in South Korea, Thailand, and Singapore could provide ample networking opportunities with hackers who risk of getting pulled into China's vulnerability acquisition orbit. The international hacker community tends to view the US government with skepticism, but it is notably more receptive to private companies that are perceived as supporting the community—even if those companies work closely with the government. By positioning itself as an enabler rather than a direct participant, the US government can build trust while supporting the development of offensive security skills.

3. DOD and Congress must expand programs on AI-enabled vulnerability research and consider n-day exploitation where possible.

Investing in technologies that reduce dependency on zero-days—such as automation, AI-driven vulnerability discovery, and novel exploitation techniques—would future-proof US cyber capabilities, effectively "intelligentizing" DOD's cyber organizations. As software security continues to advance, traditional exploit chains are becoming harder to develop and maintain. While defense is important, the DOD must also prioritize research into next-generation exploitation methods that can help sustain offensive capabilities in the long term—particularly for other, harder targets in East Asia. Expanding government programs, like AIxCC and INGOTS,[215] while encouraging offensive firms to create additional tools, like Google's OSSFuzz,[216] would enable firms already conducting vulnerability research to do so in a more scalable manner while also assisting defensive efforts. Alternatively, creating a section under the National Defense Authorization Act (NDAA) for "automated code auditing" or "exploit chain generation for both n-day and 0day" for the armed services could send a demand signal to the wider defense innovation ecosystem, encouraging venture capital and other investment firms to find ways to scale the labor-intensive process of vulnerability research.

To combat excess slowdowns due to risk aversion, as well as to extend the life of an acquired capability, USCYBERCOM should also consider additional policies around n-day exploitation and use. This could lengthen the lifecycle of an acquired capability, prevent excess waste and time in contract cycles, and also provide additional resourcing to junior-level talent in offensive cyber firms (who can likely exploit n-days but are not yet able to reliably conduct zero-day exploitation). USCYBERCOM is an ideal organization to try new policies around n-day acquisition as, while stealth is important in military operations, it is not required for all of them.

4. DOJ should provide legal guidance and counter-intelligence protection to vulnerability researchers.

Vulnerability researchers in the private sector, particularly those who participate in bug bounties, often rely on their companies or entities like the Security Research Legal Defense Fund[217] to defend themselves from lawsuits that seek to chill their research. The legal challenges are only more numerous for individuals selling these capabilities for national security purposes, especially if the individual is selling capabilities for classified purposes, which cannot be disclosed in court without greymail concerns. While the US government has clear interests in protecting security research (e.g., through DOJ policies not criminally prosecute good faith security research and the CFAA's subsection for a national security carve out to hacking),[218] as well as protecting individuals from counterintelligence threats, there is no centralized task force actively looking to protect hackers (especially ones without clearances), and no policy priority to ensure that civil lawsuits are settled with an eye on how they impact private sector hacking supply chains.[219]

One potential solution is to empower the DOJ's Civil Division to intervene in civil lawsuits through existing procedural mechanisms if an offensive capability firms' researcher faces a lawsuit by a technology company (particularly if the researcher works for government interests).[220] This would likely need pairing with a publication on transparent criteria for how to define "government interest" for CFAA purposes, and how firms can seek protection under those terms (similar to how the DOJ's "good-faith security research" policy published in 2022 clarified what cases DOJ would or would not prosecute against hackers).[221] Another approach would be to establish a federally funded legal defense fund modeled after the Security Research Legal Defense Fund, providing independent legal support to security researchers working on US government contracts. Additionally, a task force could be created within the FBI or the Office of the Director of National Intelligence's (ODNI) National Counterintelligence and Security Center (paired with the first "demand" option below) to address coun-

215. "AixCC AI Cyber Challenge," accessed March 16, 2025, https://aicyberchallenge.com/.

216. Abhishek Arya et al., "OSS-Fuzz: Continuous Fuzzing for Open Source Software," Google / OSS-Fuzz, 2025 (beginning with original post 2016), https://github.com/google/oss-fuzz.

217. "Security Research Legal Defense Fund," accessed March 16, 2025, https://www.securityresearchlegaldefensefund.org/.

218. 18 U.S.C. 1030(f); Justice Manual, "9-48.000—Computer Fraud and Abuse Act," US Department of Justice, February 19, 2015, https://www.justice.gov/jm/jm-9-48000-computer-fraud.

219. "Counterintelligence," Federal Bureau of Investigation, accessed March 16, 2025, https://www.fbi.gov/investigate/counterintelligence.

220. "South Dakota High School Activities Ass'n—United States' Motion To Intervene As Plaintiff-Intervenor," US Department of Justice, Civil Rights Division, August 6, 2015, https://www.justice.gov/crt/south-dakota-high-school-activities-assn-united-states-motion-intervene-plaintiff-intervenor.

221. DOJ Office of Public Affairs, "Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act," release [archives], US Department of Justice, May 19, 2022, https://www.justice.gov/archives/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act.

terintelligence concerns raised by hackers and provide a clear point of contact for researchers facing foreign threats or legal retaliation. These measures would help foster a safer and more reliable environment for the private sector supply chain supporting US cyber operations.

Demand:

1. Create a government-sponsored vulnerability broker for the US intelligence community within a federally funded research and development center.

On the demand side, establishing a government-sponsored broker for vulnerability acquisition could streamline the fragmented and opaque market, particularly for companies without existing connections into the US federal contracting system and individual researchers who may reach out to private sector middlemen. The current landscape relies heavily on private brokers, who often inflate prices and obscure the true value of individual exploits. A government-backed intermediary could improve efficiency, offer more predictable payment structures, and reduce the risks associated with relying on third-party brokers. While this effort could be coordinated at a National Security Council (NSC) level, a Federally Funded Research and Development Center (FFRDC) would likely be the best place to implement such a program. This is because, thanks to interagency equities and Title 10 / Title 50 concerns, there is likely no single agency within the Intelligence Community or DOD that a government-sponsored middleman could work without spawning duplicate structures across the ecosystem, causing a drain of government resources.[222]

Such a program would likely need an individual at the helm with experience in exploit acquisition, one who would understand the needs of the various agencies and also be able to interface directly with the hacker community. Any bug would still need to go through the VEP,[223] and then funnel vulnerabilities to existing contracts based on need. This middleman program should also be able to solicit bugs regardless of origin, directly contracting with friendly international suppliers beyond even the FVEYs. This program could also offer additional insights into the zero-day supply chain for future coordination amongst the FVEYs and additional regional allies.

2. Decentralize, Internationalize, and Simplify the Process for Purchasing Bugs.

Government acquisition moves at a glacial pace, even for cyber capabilities. The US government must find ways to decentralize purchasing authority away from prime-heavy government contracts. Secretary of Defense Pete Hegseth, in March 2025, began moving towards more efficient software acquisition mechanisms. However, this effort is largely tailored to commercial software solutions (which zero-day exploits are not).[224] The DOD could create an acquisition vehicle specifically for cyber capabilities used in support of SIGINT or defensive efforts, particularly for cheaper capabilities purchased directly from researchers or small firms. This could be in the form of creating a Software Acquisition and Practices (SWAP) for offensive cyber specifically, or by expanding programs for offensive cyber acquisitions under Other Transaction Authorities.[225] Any acquisition mechanism, to succeed, cannot contain US person or clearance requirements, allowing companies the flexibility to hire international talent.

Congress could also alter the US government's Simplified Acquisitions Program to enable the US government to purchase offensive cyber capabilities. All products that support overseas contingency operations[226] or that facilitate defense against or recovery from a cyber-attack can already be purchased via the micro-purchase program (if the cost is less than $20,000) and can be acquired through the Simplified Acquisitions Program (if the cost is less than $800,000 domestically or $1.5 million abroad).[227] It is far more likely that lower-tier vulnerabilities will fall under the Simplified Acquisitions program than the micro-purchase program, but the micro-purchase program could provide for one-off technical projects or additional resources given to offensive cyber capabilities firms, which could supple-

222. Also, the White House Office of Budget Management (OMB) is in charge of designating all IT-related government-wide acquisition contracts. See: Clinger Cohen Act of 1996 (40 U.S.C. 1401 et seq, 1996) in *Department of Defense Chief Information Officer Desk Reference, Volume I Foundation Documents*, August 2006, https://dodcio.defense.gov/portals/0/documents/ciodesrefvolone.pdf.

223. Trump White House Archives, "Vulnerabilities Equities Policy and Process for the United States."

224. Pete Hegseth, "Memorandum for Senior Pentagon Leadership, Commanders of Combatant Commands, Defense Agency, and DOD Field Activity Directors, Subject: Directing Modern Software Acquisition to Maximize Lethality, US Department of Defense," March 6, 2025, https://media.defense.gov/2025/Mar/07/2003662943/-1/-1/1/DIRECTING-MODERN-SOFTWARE-ACQUISITION-TO-MAXIMIZE-LETHALITY.PDF.

225. *Other Transaction Authority (OTA)*, Defense Acquisition Encyclopedia / AcqNotes, accessed April 7, 2025, https://acqnotes.com/acqnote/careerfields/other-transaction-authority-ota.

226. 10 U.S.C. § 101(a)(13)(A) (2025): "[a 'contingency operation' is a military operation that] is designated by the Secretary of Defense as an operation in which members of the armed forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States…" This term has been used to describe Operation Enduring Freedom and other Global War on Terror operations, as well as US operations with North Atlantic Treaty Organization (NATO) countries after Russia's invasion of Ukraine (Operation Atlantic Resolve).

227. 48 CFR § 2.101 – Definitions (2025).

ment government operations and lessen the burden of feast-or-famine cycles.[228]

3. Resource such processes accordingly.

Raising the budget for zero-day acquisition across the government is also essential to ensure companies do not go out of business when making exclusive sales to the government. Increased funding would allow the US government to secure higher-quality vulnerabilities and reduce concerns that a single purchase of a critical exploit does not ruin the acquisition budget for the rest of the fiscal year. Additionally, while big-ticket iOS and Chrome vulnerabilities garner widespread attention, real cyber operations often rely on lower-profile but highly specialized exploits tailored to niche devices and environments. These require not only technical sophistication but also partnerships, trust, and deep operational knowledge—especially when targeting software specific to a particular region or industry. Policymakers must recognize this complexity and resource the ecosystem accordingly, ensuring both intelligence-gathering and operational effectiveness while holding stakeholders accountable for outcomes. Expanding cyber-specific pathways of the Simplified Acquisitions Program (which already exist for "facilitating defense against or recovery from cyber [attacks]") and raising the cap for cyber capabilities up to $3 million that fall under a simplified acquisitions program would further assist this effort to buy higher quality, harder target exploits.

Policy:

1. Identify highly skilled foreign researchers and hire them wherever possible.

When zero-day exploits and bespoke cyber capabilities are created by a finite pool of international talent (and especially if the number of highly skilled vulnerability researchers globally is indeed in the low hundreds), talent recruitment becomes a zero-sum game. To maintain a competitive edge, the United States and its allies must focus not only on acquiring superior capabilities but also on attracting and retaining top talent—both foreign and domestic—while actively countering adversary advancements through a combination of acquisition, disruption, and strategic talent recruitment. Many top-tier vulnerability researchers might qualify for the "Gold Card" visa program by lowering the tier requirement (e.g., $500,000 instead of $5 million).[229] Moreover, many private sector technology firms would also likely be interested in recruiting this talent for defensive purposes. US firms can hire vulnerability researchers to make the ecosystem safer.

US alliances also become particularly useful in this regard. As China attempts to expand its offensive hacking talent pool to researchers in East Asia, South Asia, and the Middle East, encouraging companies that provide cyber capabilities to the FVEYs to hire foreign talent, work with foreign firms, and invite foreign researchers to cybersecurity conferences will likely be a necessary counter strategy to prevent this from occurring. While recruiting hundreds of hackers through the FVEYs seems like a daunting task, this is far less than the over 1600 German nuclear and rocketry scientists brought over to the United States alone from the Cold War-era program, Operation Paperclip.[230]

2. Catch and burn capabilities.

Not every researcher will want to work for the US government or its allies. While some researchers prefer to focus on the work, many Chinese researchers enjoy the mission of working for their home governments. This likely comprises a significant pool of potential vulnerabilities in China every year. The MSS currently has 324 partner companies, who have disclosed almost 4,000 vulnerabilities to the CNNVD.[231] Thus, the US intelligence community should actively identify offensive capabilities not just leveraged by adversary states, but also offensive capabilities likely being sold to adversary states, to either disclose them to vendors who can fix them or use them in false flag operations. This will assist US companies in making their products more secure, while also imposing costs on an adversary.

3. Deepen offensive cyber collaboration among allies.

Replicating these policies among US partners and allies is crucial to shaping and maintaining the base of offensive talent and capability. Shielding up-and-coming talents from the Chinese sphere of influence will be vital to maintaining a long-term competitive advantage. If the FVEYs cannot convince individuals to come directly to FVEYs countries, getting them out of China's sphere of influence would suffice. Creating diplomatic programs through the US State Department focusing on tech-

228. Alternatively, if the secretary of defense simply designates USCYBERCOM's hunt forward and other offensive cyber operations against adversaries as non-kinetic "contingency operations," the entire US government could take advantage of its Simplified Acquisitions Program to purchase bugs in the name of contingency operations and cyber defense. However, this would likely be seen as deeply escalatory.

229. Agustina Vergara Cid, "Trump's Immigration 'Gold card' Could Be a Win for America—With These Changes, *The Hill*, March 7. 2025 https://thehill.com/opinion/immigration/5181185-trumps-immigration-gold-card-could-be-a-win-for-america-with-these-changes/.

230. "A10. Operation Paperclip: How German Scientists Were Brought to the US after World War II," Worcester Institute for Senior Education, accessed May 14, 2025, https://assumptionwise.org/event-5375339.

231. Dakota (@dakotaindc.bsky.social), "New MSS ecosystem numbers from those 324 companies," Bluesky, March 18, 2025, 9:05 p.m., https://bsky.app/profile/dakotaindc.bsky.social/post/3lkoyj7hstk2i.

nical talent exchange and industry-wide collaboration (which would benefit both defensive and offensive vulnerability research talent) would be ideal to do so. While key countries in Europe and South America would likely be an important start beyond the FVEYs, deepening cyber relationships with South Korea and Thailand (two treaty allies) would likely be key countries to engage.

However, the more countries that the US partners with, the higher the risk that the United States funds a capability that may be used to commit human rights abuses or to spy on US persons. The Pall Mall initiative, which attempts to establish global norms around ethical hacking and responsible offensive cybersecurity practices, represents a step toward addressing this complexity, if the coalition focuses on actual acquisition of capabilities rather than use. Encouraging the Pall Mall process to create better guidance on hiring foreign and uncleared talent to address counterintelligence risks and creating a coalition of countries willing to sell exploits to one another with proper human rights safeguards (particularly with the goal of stepping away from China's sphere of influence) would be crucial steps towards developing a coalition with proper guardrails in place.

Conclusion

Given the finite international zero-day marketplace, it is imperative that the United States and its allies continue to ensure the availability of such capabilities (understanding the industry, rooting out malicious actors, and developing trusted sources) while limiting China's access to those same capabilities. If the United States fails to do so, it risks losing its competitive edge to adversaries—most notably China—who are investing heavily in cultivating their domestic cyber talent pipeline and enabling a more flexible, market-driven approach to acquisition. China's permissive regulatory environment and government-backed support for private-sector hacking companies have allowed it to scale its capabilities rapidly. Without a corresponding investment in the US ecosystem—both in terms of talent development and acquisition reform—the United States could face long-term strategic disadvantages.

The current landscape is bleak. China has a larger supply of hackers than the United States, and its offensive pipeline has grown incredibly robust in the last decade. If, from an operational perspective, China is already a peer adversary in cyberspace,[232] China's hacking capabilities will likely exceed those of the United States very soon, if it has not already.

However, this moment also presents an opportunity. The United States can strengthen its position by embracing policies that nurture a robust domestic talent pipeline, reduce barriers to entry for small vulnerability research businesses, and streamline the government's acquisition process to work more effectively with the private sector. Investing in legal protections, expanding support for hacker communities, and fostering international partnerships can secure the supply chain while building trust between the government and researchers.

Ultimately, the United States must not only maintain parity with China but also ensure that it remains at the forefront of offensive cybersecurity capabilities. Choices made today will determine whether the United States can sustain its cyber advantage or whether, when called upon to do more, the US offensive cyber supply chain crashes and burns itself.

232. Adam Segal, "China Has Raised the Cyber Stakes: The 'Salt Typhoon' Hack Revealed America's Profound Vulnerability," *Foreign Affairs*, January 21, 2025, https://www.foreignaffairs.com/united-states/china-has-raised-cyber-stakes.

Acknowledgements

This paper could not have been written without the assistance of my many mentors and colleagues in hacking and cyber policy. Thank you for fielding my tireless questions, vouching for me to potential interviewees, and reviewing my copious notes. A special thank you to the Atlantic Council, Trey Herr, and Nikita Shah for giving me the opportunity to pursue this project, to Margin Research for their partnership and assistance with data gathering, and to Mark Griffin and the local Washington DC hacker community for their interview corroboration assistance.

This paper is dedicated to my husband Derek (who has tirelessly supported my four-year odyssey through graduate and law school), Sophia d'Antoine, and all the members of our shared Book Club. While this thesis was produced over the last year, our discussions over the last half-decade have deeply influenced the final product.

About the author

Winnona DeSombre Bernsen is a Master of Public Policy/Juris Doctor candidate at Harvard Kennedy School and Georgetown Law and a non-resident fellow at the Atlantic Council. She was formerly a security engineer at Google's Threat Analysis Group, tracking targeted threats against Google users, and she is the founder of the offensive security conference DistrictCon, held in Washington DC. In recent years, Winnona has organized policy content at DEF CON and authored multiple pieces on offensive cyber capability proliferation.

Appendices

Appendix A: Abbreviations and key terms

Access-as-a-Service: a form of offensive cyber capabilities service that provides black-box technological solutions to customers looking to break into devices.

artificial intelligence (AI): the ability of computers or machines to perform tasks that traditionally require human intelligence, such as learning, reasoning, problem-solving, and perception

Advanced Persistent Threat (APT): a sophisticated, sustained cyber campaign in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged period of time.

bespoke: This term refers to tailored or customized entities, services, or products within the information security environment.

bug bounty programs: Programs run by companies to encourage hackers to find and report security vulnerabilities in their software. Hackers receive monetary rewards ("bounties") for valid reports, enabling companies to identify and fix issues before malicious actors exploit them.

bug collision: The parallel, independent discovery of a vulnerability by multiple researchers.

Capture the Flag (CTF): Hacking competition in a simulated environment where participants solve security challenges, like exploiting vulnerabilities, reverse engineering, or cryptography, to "capture flags" (hidden tokens representing successful completion).

China National Vulnerability Database (CNNVD): A national vulnerability database of the PRC, operated by the MSS, China's foreign intelligence service.

Chinese Communist Party (CCP): China's, or PRC's, ruling political party. It holds ultimate authority over the state, military, and society.

Computer Fraud and Abuse Act (CFAA): United States federal law that criminalizes and provides for civil penalties for various forms of computer-related fraud and abuse.

Cybersecurity and Infrastructure Security Agency (CISA): component of the United States Department of Homeland Security responsible for cybersecurity and infrastructure protection

Defense Advanced Research Projects Agency (DARPA): research and development agency of the United States Department of Defense responsible for the development of emerging technologies for use by the military.

Exploit Broker: An intermediary company or middleman that purchases vulnerabilities and exploits from researchers and sells them to government agencies or other clients.

exploit chain: A sequence of multiple exploit primitives used in conjunction with one another to achieve a particular effect, such as gaining full control over a system.

exploit primitive: a basic exploit that, on its own, may not be enough to compromise a system but can be leveraged in combination with other primitives to achieve a more significant effect.

Federal Bureau of Investigation (FBI): the domestic intelligence and security service of the United States and its principal federal law enforcement agency.

Federally Funded Research and Development Center (FFRDC): public-private partnerships that conduct research and development for the United States Government—famous examples include Lawrence Livermore National Laboratory, MIT Lincoln Laboratory, and MITRE.

Five Eyes (FVEYs): An intelligence-sharing alliance comprising five countries: the United States, United Kingdom, Canada, Australia, and New Zealand.

live hacking: Live onstage demonstrations of hackers exposing system bugs or hacking into systems.

Ministry of Public Security (MPS): China's national police agency, responsible for law enforcement, domestic security, and maintaining public order.

Ministry of State Security (MSS): China's primary civilian intelligence and security agency, responsible for foreign intelligence, counterintelligence, and internal security.

National Security Agency (NSA): The US intelligence agency under the DOD tasked with SIGINT collection and cybersecurity.

n-day exploit: A tool or piece of code that exploits an n-day vulnerability (a known security flaw), typically targeting systems that have not yet applied the vendor's patch.

n-day vulnerability (n-day): A publicly disclosed software vulnerability that is known to the vendor, and a patch is likely available. Yet, it is still exploitable if systems remain unpatched.

National Defense Authorization Act (NDAA): U.S. federal law that sets the annual budget and authorizes appropriations for the U.S. Department of Defense, nuclear weapons programs of the Department of Energy, and other defense-related activities.

National Institute of Standards and Technology (NIST): agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.

People's Liberation Army (PLA): The armed forces of the PRC, controlled by China's ruling party, the CCP.

People's Republic of China (PRC): The official name of mainland China, governed by the CCP.

Proof of Concept (PoC): Sample code showing that a particular vulnerability is exploitable. It proves an attack is feasible but may not be a fully reliable exploit.

quality assurance (QA): systematic efforts taken to assure that the product delivered to customer meet with the contractual and other agreed upon performance, design, reliability, and maintainability expectations of that customer.

Regulations on the Management of Network Product Security Vulnerabilities (RMSV): a set of regulations in China that mandate network product providers to promptly report any security vulnerabilities in their products to the CCP.

signals intelligence (SIGINT): intelligence derived from electronic signals and computer systems used by foreign targets.

Strategic Capabilities Office (SCO): rapid prototyping organization within the DOD to address high priority operational and strategic challenges.

US Cyber Command (USCYBERCOM): The unified combatant command of the DOD responsible for conducting cyberspace operations.

US Department of Defense (DOD): United States Department in charge with coordinating and supervising the U.S. armed services.

US Department of Justice (DOJ): United States Department that oversees the domestic enforcement of federal laws and the administration of justice.

Vulnerabilities Equities Process (VEP): process used by the U.S. federal government to determine on a case-by-case basis how it should treat zero-day vulnerabilities.

zero-day vulnerability (0day / zero-day): A software vulnerability that is unknown to the software vendor and has not yet been patched.

zero-day exploit: A tool or piece of code that takes advantage of a zero-day vulnerability to compromise a system.

Appendix B: List of Cited Interviewees

1. JD Work, Professor at National Defense University.
2. Ian Roos, VP of Intelligence, Margin Research.
3. Mei Danowski, Natto Thoughts.
4. Dakota Cary, Fellow, Atlantic Council Global China Hub.
5. Adam Kozy, CEO of SinaCyber.
6. Derek Bernsen, DARPA Program Manager. Note, Mr. Bernsen's comments do not reflect the opinions of DARPA, the DOD, or the US Government.
7. Chi-en (Ashley) Shen, Security Researcher.
8. Former US Intelligence Community Official (Background Interview)
9. Founder of Vulnerability Research Company 1 (Background Interview).
10. Founder of Vulnerability Research Company 2 (Background Interview).
11. Founder, Vulnerability Research Company 3 (Background Interview).
12. Founder, Former Vulnerability Research Vendor (Background Interview).
13. Former ONCD Official (Background Interview).
14. U.S. Government China Cyber Analyst (Background Interview).
15. Founding Member of Vulnerability Research Company (Background Interview).
16. Pwnie Award Organizer (Background Interview).
17. Member of Defense Science Board, Study on Cyber as a Strategic Capability (Background Interview).
18. China Area Specialist in the Vulnerability Research Space (Background Interview).
19. Security Researcher with Experience in Collection and Cyber Operations (Background Interview).
20. CTO of Defense Contractor in the DOD / IC space (Background Interview).
21. USG China Analyst (Background Interview).
22. DOD Cyber Official (Background Interview).
23. Senior DOD Cyber Official 1 (Background Interview).
24. Senior DOD Cyber Official 2 (Background Interview).
25. USG Cyber Official (Background Interview).
26. Independent Security Researcher (Background Interview).
27. Former Senior Intelligence Official (Background Interview).

Appendix C: Image Credits

1. Cover Image: Blurred photo of a malware sample in the Ghidra reverse engineering. Source: Govanify blog post, December 23, 2019, https://govanify.com/post/kh2ai/.
2. The International Offensive Cyber Supply Chain (Depictive Image): Global Network connected with datapoints. Source: Emma Schroeder. Adapted from photograph by Basma Alghali (Unsplash license) and image by Gordon Johnson (Pixabay content license).
3. US Acquisition Pipeline (Depictive Image): The DEF-CON (DEF CON) hacking conference in Las Vegas, Nevada, in 2014. Source: Tony Webster, Wikimedia Commons, https://commons.wikimedia.org/wiki/File:DEFCON_22_%2814704446530%29.jpg.
4. Figure 1: Heatmap of major known commercial vendors for offensive cyber capabilities, suppliers, and investors 2024. Source: Jen Roberts et al., Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights, Atlantic Council, September 4, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/.
5. Figure 2: Number of teams participating in Pwn2Own Ireland 2024, by country. Source: Dustin Childs, "Pwn2Own Ireland 2024: Day Four and Master of Pwn," Trend Micro, Zero Day Initiative, October 25, 2025, https://www.thezdi.com/blog/2024/10/25/pwn2own-ireland-2024-day-four-and-master-of-pwn.
6. Figure 3: Teams on CTFTime by country, as of August 2024 (far left column represents "unaligned" or "international" teams. Source: Report author.
7. Figure 4: Top scoring teams at the 2024 DEF CON CTF, and their countries of origin. Source: Report author from an initial CFTtime scoreboard for DEF CON CTF 2024, accessed April 5, 2025, https://ctftime.org/event/2462/.
8. China's Acquisition Pipeline (Depictive Image): Screenshot of Chinese offensive cyber capability firm No Sugar Tech's website. Source: No Sugar Tech, accessed April 5, 2025, https://www.nosugartech.com.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org