Testimony before the U.S.-China Economic and Security Review Commission on "China's Cyber Capabilities: Warfare, Espionage and Implications for the United States"

February 17, 2022

Dakota Cary
Research Analyst, Center for Security and Emerging Technology

I would like to thank Chairman Wong and Vice Chairman Glas for extending an invitation to testify today on China's cyber capabilities. Thank you to the commission members and staff for taking an interest in this important topic and convening three great panels.

China's cyber capabilities are expanding. Talent cultivation and research are critical to that expansion, and China's universities support both. Since 2015, China has standardized its cybersecurity curriculum for university degree programs, launched a program to certify qualifying schools as World-Class Cybersecurity Schools, built a National Cybersecurity Center in Wuhan, and continued work with universities on capabilities research. Over the next decade, China's cyber capabilities are poised to blossom as universities graduate more well-educated cybersecurity degree holders and as research progresses. For the United States to adequately respond to the development of China's cyber talent pipeline and the role its universities play in a capabilities development, it's important to first understand the relationship between the Chinese government and some universities. My written testimony responds to a series of questions posed by the Commission for this hearing, and I am happy to clarify or expand upon my answers during Q&A.

1. **What is known about Chinese universities' cooperation with the Chinese military and intelligence services to carry state-sponsored cyberespionage operations? Why, and in what ways, do Chinese universities facilitate state-sponsored espionage? Please provide specific examples in your answer.**

Chinese universities and their relationship with state hacking teams exist on a spectrum of activities.[1]

At the least-threatening end, from a U.S. security perspective, universities serve in their typical education capacity—giving students the skills they need to be successful cybersecurity professionals, which in turn, develops a national talent base. At the opposite end of the spectrum, schools like Shanghai Jiao Tong University help conduct operations for the Chinese military. In between are a number of universities that help cultivate talent, support research, or enter into joint research partnerships or operate laboratories with, or funded by, the Chinese military and security services.

At the talent-focused end of the spectrum are Zhejiang University and Harbin Institute of Technology. First identified as places of recruitment for Chinese hacking teams by the cybersecurity company FireEye's groundbreaking Advanced Persistent Threat 1 (APT1) report in 2013, these two universities are still graduating students prepared for government service. Talent development at both schools looks different, but they aim for the same output—highly qualified cybersecurity professionals. Zhejiang University students can take classes on writing intelligence reports, alongside classes like how to attack and defend AI systems. Harbin Institute of Technology offers similar courses aimed at getting students recruited by the state. Legacy webpages show many graduates of HIT's cybersecurity school from 2008 to 2014 went to work for the PLA's 54th Research Institute, formerly part of the General Staff

[1] 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). DOI: 10.51593/2020CA010

Department's 4th Department (Electronic Warfare), an organization folded into the PLA Strategic Support Force in 2015. The U.S. Department of Justice indicted four members of the 54th Research Institute in 2020 for the hacking of Equifax in 2017.

One step closer to supporting state hacking operations, schools like Xidian University, Hainan University and Southeast University mix education, hands-on practice, and career placement in interesting and innovative ways that help the security services.

Xidian University works to get its graduate students hands-on experience with a provincial bureau of the Ministry of State Security. The university had a relationship with the Third Department of the PLA General Staff Department before it was reorganized into the Network Systems Department in 2015. Xidian University operates a jointly-administered graduate degree program with the Guangdong Bureau of the China Information Technology Security and Evaluation Center (or Guangdong ITSEC). This bureau of the MSS managed a contracted team that was so prolific in hacking that it earned an APT designation, APT3, from FireEye. Xidian University awards degrees and handles admissions; Guangdong ITSEC facilitates hands-on education and pairs graduate students with MSS employees serving as mentors. Together, Guangdong ITSEC employees and Xidian University graduate students pursue research projects that meet the "actual needs" (实际求) of Guangdong ITSEC—essentially, solving technical problems to enable the MSS's work. The graduate degree program is a clear-cut example of a university and a provincial MSS bureau collaborating to enhance students' education and encourage students to work for state hacking teams.

Hainan University similarly involved students with the security services, albeit less formally than at Xidian University. A Hainan-based MSS officer and professor at Hainan University were

indicted by the U.S. Department of Justice in 2020 for their cyber espionage operations to support the Chinese intelligence services. Starting as early as 2013, the professor allegedly recruited students from on-campus hacking competitions and offered bounties to students and colleagues to procure software vulnerabilities that facilitated hacking operations. One of the professor's shell companies was even registered to the university library's address.

At Southeast University in 2015, a professor similarly hosted a hacking competition for students.[2] Unlike normal capture-the-flag competitions where participants hack other teams for points, the professor offered students a real-world opportunity to earn points and gain prestige by attempting to access the network of a U.S. Department of Defense contractor. Technical indicators linked the professor, the infrastructure for the attempted hack of the company, and the competition. An alternative, but equally troubling explanation for the collection of evidence is that the professor was assisting an operation from his university equipment, alongside the contracted company, Beijing TopSec.

[2] 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). DOI: 10.51593/2020CA010

Besides this one competition, Southeast University has an enduring relationship with the security services. Southeast University also jointly operates Purple Mountain Lab with the PLA Strategic Support Force, where researchers work together on "important strategic requirements", computer operating systems, and interdisciplinary cybersecurity research.[3] Apart from Purple Mountain Lab, a previous report by the USCC found Southeast University to be a recipient of PLA and MSS funding to support the development of China's cyber capabilities. Although the university's ties to the hacking competition and DOD contractor are intriguing, the most consequential aspect of Southeast University's relationship to the state is its enduring research program.

The deepest entanglement between university faculty and the security services is with schools like Shanghai Jiaotong University (SJTU)—where staff both support operations and conduct research to enhance cyber capabilities. The university's cybersecurity degree program is located on a PLA information engineering base in Shanghai. From 2010 to 2014, evidence emerged,

first from leaks to The New York Times, then through additional reporting by Reuters, that SJTU was engaged in cyber operations against the United States. In that period, some university computers and email addresses were tied to hacking campaigns carried out by the PLA. Although technical indicators tying the university to military hacking campaigns have apparently faded, the university almost certainly still supports operations.[4]

SJTU's Cyberspace Security Science and Technology Research Institute, home to the Network Confrontation and Information System Security Testing program, conducts research that enables cyber operations. Within this program, SJTU claims to work on "network and information system testing and evaluation, security testing for intelligent connected networks, APT attack testing and defense, and key cyber range technology."[5] In their own words, this is a bold admission of their own APT work and their perceived value to the PLA's cyber capabilities. Shanghai Jiao Tong University embodies China's military-civil fusion approach; tuition pays for professors' salaries and the military gets new capabilities as a result of their work.

The complete distribution of universities across the spectrum, from purely educational institutions to active participants in APT activity, is unclear; however, most schools likely fall under typical talent training, with fewer schools maintaining close operational and research ties to the security services.

2. How do Chinese universities' research efforts support the PLA's development of offensive cyber capabilities? Please provide specific examples in your answer.

[3] *Ibid.*

[4] *Ibid*.

[5] *Ibid.*

The PLA and Chinese intelligence services both make use of university research on offensive cyber capabilities. Avenues for collaboration on research include joint research facilities, research grants from the PLA and MSS, research cooperation with provincial governments, and competitions that attract attention from a wide swath of society.

In some instances, as with Southeast University or Shanghai Jiao Tong University, schools openly operate joint research facilities with the PLA. Under these circumstances, the lab-to-field pipeline is clear and direct. Similarly, China's National Cybersecurity Center in Wuhan is home to two universities—Wuhan University and Huazhong University of Science and Technology—and hosts two laboratories that likely facilitate government research.[6] The Offense-Defense Lab and the Combined Cybersecurity Research Institute both stand out as candidates for collaboration with the security services. The 13th bureau of the MSS, which has managed some hacking campaigns in the past, has an office at the Combined Cybersecurity Research Institute. The institute combines university academics with private-sector researchers to work on strategic capabilities.

Funding from the PLA or the MSS also secures access to offensive cyber capabilities from universities. In a previous USCC-commissioned report from 2012, Northrop Grumman researchers demonstrated that a number of schools received money from specific programs designed to enhance China's offensive cyber capabilities. Today, such programs likely continue.

Some schools are working with provincial governments to conduct research into cyber capabilities. Zhejiang University, a school I've mentioned for its high-quality education and is a known favorite for recruiting hacking talent, is working with the Zhejiang Provincial government to operate Zhejiang Labs.[7] Zhejiang Labs is conducting research on AI's application to cybersecurity and key cyber range technologies. Huazhong University of Science and Technology, which I've mentioned in context of the National Cybersecurity Center, is also a partner of Zhejiang Labs. The National University of Defense Technology (NUDT), a PLA university, is represented on an oversight board for the laboratory. This relationship typifies more general access to technology development conducted outside the military and in coordination with other government bodies and universities.

Finally, China has copied parts of the United States' innovation strategy to incentivize research at universities that can produce sought-after capabilities. DARPA hosted a Cyber Grand Challenge in 2016 to spur innovation in automated software vulnerability discovery, patching, and exploitation technology.[8] These tools offer both offensive and defensive capabilities that promise to increase the scale and pace of software vulnerability discovery—a key component of

[6] Dakota Cary, "China's National Cybersecurity Center" (Center for Security and Emerging Technology, July 2021). https://doi.org/10.51593/2020CA016

[7] Dakota Cary, "Down Range" (Center for Security and Emerging Technology, forthcoming).

[8] Dakota Cary, "Robot Hacking Games" (Center for Security and Emerging Technology, September 2021). https://doi.org/10.51593/2021CA005

cyber operations, and cybersecurity generally. China has emulated that competition system and since 2017 has hosted at least a dozen rounds of competitions to develop the technology.

Just two years after the People's Liberation Army's National University of Defense Technology won the first competition in 2017, the military started managing competitions of its own to concentrate resources on the development of tools to automate the vulnerabilities lifecycle. By last year, a laboratory run by the PLA Equipment Development Department hosted its first such competition. These management and oversight roles situate the PLA in an ideal position to evaluate and attract the best tools and talent. The 13th Bureau of the MSS has also hosted some of these competitions, which, when supported by enough funding, can spur technological innovation and investment. This competition structure is the most open form of research for cyber capabilities, as it allows the military (or any government agency) to draw on research from universities and the private sector.

3. How do Chinese universities help the Chinese military and intelligence services identify and recruit talented cybersecurity professionals? Please provide specific examples in your answer.

China's mechanisms for identifying and recruiting talent are typical for governments. There is some evidence that typical job promotion events, like career fairs or alumni engagement events, serve to promote jobs in the military or intelligence services at most universities.

Some schools shoulder additional responsibility for talent cultivation and recruitment, however. Xinhua News, China's state-run news agency, reported in 2017 that the PLA Strategic Support Force, which includes the department responsible for hacking operations—along with those responsible for space missions and operations support, signed an agreement with nine entities "to train high-end talents for new combat forces." According to Xinhua, "The universities will coordinate in recommending high-level talents in emerging S&T disciplines for priority consideration for recruitment by the [Strategic Support Force]; the SSF will designate key personnel for cultivation to go to research institutes and key laboratories for academic exchanges and further training; jointly, they will organize international and domestic competitions to find and select talents with special expertise, the best of whom will be recruited by the SSF."[9]

The full agreement between the PLA and these nine institutions is not public, so the program's particulars are unclear. Six of the entities participating are universities and three are defense industry enterprises.

University Partners of the PLA Strategic Support Force

- University of Science and Technology of China
- Shanghai Jiao Tong University

[9] "Strategic Support Force to Cooperate with Nine Local Organizations to Cultivate High-End Talents for New Combat Forces," 李国利 and 宗兆盾, Xinhua News Agency (New China News Agency; 新华社), July 12, 2017. https://perma.cc/PM8L-3WU4

- Xi'an Jiaotong University
- Beijing Institute of Technology
- Nanjing University
- Harbin Institute of Technology

Partnering Defense State-Owned Enterprises

- China Aerospace Science and Technology Corporation [CASC]
- China Aerospace Science and Industry Corporation [CASIC]
- China Electronics Technology Group Corporation [CETC]

4. **Is there significant cooperation occurring between U.S. universities and Chinese universities linked to state-sponsored cyberespionage? If so, does this cooperation create risks for the United States in general and for these U.S. universities in particular? Please address whether current export controls and sanctions lists are adequate to mitigate these risks in your answer.**

Each university mentioned here, and their relationship with U.S. institutions, is different. Some institutions, like Zhejiang University, are world-renowned for their cybersecurity education program. The university attracts the best minds of cryptography studies from around the world and its graduates are highly-prized, fiercely intelligent individuals that the United States should welcome. Conversely, institutions like Shanghai Jiaotong University have relatively little international collaboration and more important operational roles. Sanctioning schools that have helped on past cyber operations might feel like a worthwhile policy initiative, but I contend it is not.

The tools needed to conduct hacking campaigns are ubiquitous. All that most operators need is a computer, an internet connection, and training. Even if these institutions were subject to export controls, it's unlikely such policies would matter much to China's cyber capabilities. Beyond the cyber domain, such policies have merit. Advanced research often requires advanced tools, so a listing on the Department of Commerce's Entity List is still appropriate. But policymakers should not expect it to slow the development of China's cyber capabilities.

U.S. institutions that collaborate with these Chinese institutions are not at any greater risk of intelligence collection than other institutions because of their relationship. This is to say that, as in the United States, PRC policymaker intelligence requirements drive the collection and analysis cycle of operations. If a university is researching a technology that the CCP has determined to be of value, Chinese hacking teams will try to collect it, regardless of whether the school collaborates with Chinese institutions.

But what about scientific collaboration on cybersecurity research with these institutions? Again, the United States may benefit more from this collaboration than China does. Cyber defense is a team sport. Researchers who find and disclose software vulnerabilities responsibly can help secure all users of that system. A new technique for identifying malware will help everyone else defend from attack. In short, the more sharing of defensive research the better. As for the development of offensive techniques, Chinese institutions likely lead U.S. universities because the U.S. government does not work with

universities to conduct offensive research for cyber operations. Although the U.S. government does designate some schools as Centers of Academic Excellence in cyber research, there is by no means a pipeline of offensive research from U.S. universities to the U.S. government. Instead, the relationship between China's security services and some of its universities offers a window into its research and operational priorities.

5. **What is known about how Chinese technology companies' cooperation with the Chinese military and intelligence services to carry out state-sponsored cyberespionage operations? Do Chinese technology companies located within China assist in tasks such as identifying adversary vulnerabilities, developing exploits, or acquiring and processing data collected through cyberespionage?**

The Chinese Party-state's relationship with big tech companies is currently being re-written. As Adam Kozy noted in his testimony, there is an existing mandate for firms to support Chinese intelligence collection. The Chinese government has made clear in recent months that the CCP rules, and companies obey. The CCP has gone so far as to cause the delisting of Didi Chuxing, a ride hailing company, from the New York Stock Exchange.[10] CEOs have been cowed and even disappeared for months. How this new era of control over tech companies impacts their relationship with the security services is unclear, but we do know about their past relationship.

Some cybersecurity companies work hand-in-hand with the PLA and security services, supporting hacking campaigns, training operators, or educating the next generation of hackers. Companies like Beijing TopSec work on all three facets. Chinese media outlets indicate that Beijing TopSec trains PLA hackers. As discussed earlier, Beijing TopSec was also tied to the Southeast University hacking competition and hack of Anthem Insurance. The company has also set up shop at China's National Cybersecurity Center in Wuhan, where it works with the universities on campus to educate the next generation of cybersecurity professionals. Beijing TopSec is also a partner of the combined cybersecurity research institute on the National Cybersecurity Center's campus. Other cybersecurity companies, such as Qi'anxin, Qihoo360, and NSFocus, also fit the bill.

Thanks to reporting by Zach Dorfman, we know that some big tech companies are sometimes tasked with helping the security services process large swaths of data, and that such companies often do so begrudgingly.[11] Such labor is considered a cost of doing business, not another profitable venture for the firm. This relationship is interesting because it suggests a few things about the Chinese security services: 1) they are either not capable, or inadequately staffed, to deal with the tasks policymakers are asking of them, 2) they are not able to attract, retrain, or train the talent necessary to perform these tasks, and 3) they see existing talent in private-sector firms as both acceptable and accessible when help is required.

[10] Stevenson, Alexandra, and Paul Mozur. 2021. "With Its Exit, Didi Sends a Signal: China No Longer Needs Wall Street." *The New York Times*, December 3, 2021. https://www.nytimes.com/2021/12/02/business/china-didi-delisting.html.

[11] Dorfman, Zach. 2020. "Tech Giants Are Giving China a Vital Edge in Espionage." Foreign Policy. December 23, 2020. https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/.

China has taken steps in recent years to increase its technical talent pipeline, so as these degree holders become more common, the pressure for collaboration on data processing may ebb.

China recently expanded its collection of private cybersecurity research to improve state capabilities. In late 2021, the Ministry of Industry and Information Technology began requiring any individual or company doing business in China to disclose software vulnerabilities to the ministry within 48 hours of becoming aware of the vulnerability. The rule effectively co-opts the entire software security ecosystem of China into its hacking operations, allowing operators to collect software vulnerabilities before the companies themselves become aware of them. According to the cybersecurity company Recorded Future, the MSS has run a capabilities pipeline like this in the past. The MSS delayed publication of submitted vulnerabilities to China's public software vulnerability database, and subsequently used vulnerabilities that were particularly severe to facilitate hacking operations.

A notable exception to this rule—one that apparently caused the company to lose a government contract—occurred in 2021 when an Alibaba employee first reported a now-famous Log4j vulnerability to Apache. China's government appears to have been skipped in the reporting process. Why the Alibaba researcher did not report the vulnerability to the government first is unclear. After his company was reprimanded, researchers might be hesitant to skip over the government again in the future.

The policy dramatically changes the relationship between private-sector cybersecurity researchers and state hacking teams, effectively conscripting researchers that might otherwise not have chosen to report a software vulnerability to the state.

6. Is there any evidence that Chinese telecommunications companies based outside of China have built "backdoors" in their systems embedded in foreign countries' infrastructure that the PLA or MSS can take advantage of during a crisis or conflict?

Purpose-built backdoors are difficult to identify. Faulty lines of code appear all the time by accident, so building some on purpose may not be necessary or worthwhile. Moreover, purpose-built backdoors are indistinguishable from accidental ones.

But backdoors are also unnecessary if the firm cooperates with the government. Documents obtained by The Washington Post indicate Huawei works with the Chinese government to facilitate domestic surveillance, using techniques like relationship mapping, voice ID, and other tools.[12] China's National Security Law allows the government to compel companies to work with the government to facilitate espionage. Huawei's prevalence in foreign telecommunications networks would be a great asset to Chinese intelligence services. After the

[12] *The Washington Post*. 2021. "Documents Link Huawei to China's Surveillance Programs," December 14, 2021. https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.

African Union realized the data on its servers, which were running on Huawei tech, was downloaded to servers in Shanghai daily, scrutiny of the firm and its relationship with the Chinese government rightly increased.[13] Until leaked documents confirm China's use of Huawei's networks, we can only speculate about Huawei's involvement in the operation and its relationship with the intelligence services.

7. The Commission is mandated to make policy recommendations to Congress based on its hearings and other research. What are your recommendations for Congressional action related to the topic of your testimony?

In late 2021, a video of a Chinese woman in Australia on the phone with police in China went viral. The woman received a call from her father's cell phone. When she answered, she found herself face-to-face with a Chinese police officer. The officer pressured her about the content of a twitter account she was allegedly running. Her father sat in the police officer's office and looked on. The woman's distress throughout the phone call is, at times, haunting. She is pushed to return to China, asked when her visa will expire, and told to stop her online activity.

The episode highlights a dark reality about China's authoritarian system and its sweeping claim over Chinese people abroad. Individuals and their families can be subjected to cruel pressure and manipulated to perform tasks against their will. This extends to Chinese companies, too. In cases of scientific cooperation, research and development, and security research, that same pressure can open doors for the Chinese intelligence services and the PLA. In these instances, Chinese citizens are the victims of a deeply repressive system. I want to emphasize my personal feelings of grief and distress for people who live under authoritarian rule without recourse for change.

At the same time, the United States benefits from foreign talent, and China's graduates are among the best in the world. There are no policy mechanisms that will divorce the relationship between universities and the Chinese state—they are bound together under the CCP's authoritarianism. But this relationship does not mean the United States must cut itself off from interacting with these universities or hiring their graduates. Instead, policymakers should consider offering visas to family members of individuals immigrating from China. Such a policy could attract high-end, PhD talent that drives research and innovation. Without family members in China that can be subjected to pressure from the CCP, the United States can more assuredly welcome these talented individuals.

The United States should consider listing some universities, such as Shanghai Jiao Tong University or Southeast University, on the Department of Commerce's Entity List. Listing these schools will not prevent their work on cyber capabilities for the Chinese government, nor will it change their relationship

[13]Sherman, Justin. n.d. "What's the Deal with Huawei and This African Union Headquarters Hack?" New America. Accessed February 9, 2022. https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/whats-the-deal-with-huawei-and-this-african-union-headquarters-hack/.
John Aglionby, Emily Feng And Yuan Yang. 2020. "African Union Accuses China of Hacking Headquarters." Financial Times. April 24, 2020. https://archive.vn/WRobn.

with the government. Their capabilities development will not slow either. But, by listing these universities, policymakers can prevent other departments at these universities from accessing United States talent via collaboration, or some high-end technologies necessary to conduct research. I will emphasize that these actions will not change China's hacking capabilities, slow their development, or fundamentally change the relationship with the Chinese government. But such actions could have knock-on effects in other areas of research.

In the course of my study of China's hacking teams, its universities, and its education system, it is clear to me that China has learned many lessons from the United States. China's university cybersecurity degree programs are based on the standards created by the NIST's National Initiative for Cybersecurity Education. Its awards for excellence in cybersecurity education are based on the joint National Security Agency/Department of Homeland Security program to certify some universities as centers of academic excellence in cyber defense, cyber operations, and cybersecurity research. China's Robot Hacking Games, referenced earlier in my testimony, are based on DARPA's 2016 Cyber Grand Challenge. China has hosted more than a dozen rounds of competitions for Robot Hacking Games. In contrast, the United States has not hosted any since 2016. Time and again, China has studied the U.S. system, copied its best attributes, and in many cases expanded the scope and reach.

Policymakers should be flattered. We are moving in the right direction. But the market for cybersecurity jobs in the United States indicates that we are not graduating enough students with relevant degrees. The resulting increase in wages for cybersecurity professionals as demand goes unmet will help draw students' attention to the field, but policymakers can do more to encourage interest in the field at the high school level. Supporting existing programs and expanding the opportunity for more rising students is the quickest path to success. Policymakers should look to work with high schools and universities to ensure access to quality computer science education and host public competitions and events that draw attention and interest to the field. Ongoing research by my colleagues at CSET preliminarily indicates that just over 1 percent of high school students in the United States are enrolled in AP Computer Science, with even fewer participating in cybersecurity competitions. Progress at the high school level is starting to take root, however. From 2018 to 2021, the proportion of high schools offering computer science courses lept from 35 percent to over 50 percent.[14] Twenty-three states even require high schools to offer computer science classes.[15] In the coming months, CSET will provide policymakers analysis and recommendations to support such programs.

In the face of an inadequate solution to separating China's universities and the government, policymakers should instead focus on infusing the United States' cybersecurity talent pipeline with vigor, attracting qualified professionals from abroad, and supporting ongoing cybersecurity education initiatives domestically. Xi Jinping is often quoted saying that "Cybersecurity is, ultimately, a competition for talent." He's not wrong.

[14] "2021 State of CS Report." Code.org. Accessed January 28, 2022. https://advocacy.code.org/stateofcs

[15] "State of Computer Science Education - CS Advocacy." Accessed January 28, 2022. https://advocacy.code.org/2018_state_of_cs.pdf.

Appendix for Testimony before the U.S.-China Economic and Security Review Commission on "China's Cyber Capabilities: Warfare, Espionage and Implications for the United States"

February 17, 2022

Dakota Cary
Research Analyst, Center for Security and Emerging Technology

Appendix

U.S. companies that produce software often have bug reporting programs. These programs allow hackers to submit software vulnerabilities they find in a company's product to the firm in return for compensation. The more severe the bug, the higher the payout. Some security researchers earn enough money to make a career out of this process.

Some companies in the United States host a marketplace for firms and researchers. These marketplaces facilitate the submission of software vulnerabilities to firms and payment to researchers. In short, they are the middleman.

The software vulnerabilities submitted by researchers are the same kinds of vulnerabilities that facilitate hacking campaigns. In 2021, China's Ministry of Industry and Information Technology implemented a policy requiring researchers in China to submit any software vulnerability they find to the government for evaluation. This policy effectively weaponizes the cybersecurity researcher ecosystem in China—allowing state hacking teams to pull software vulnerabilities for campaigns from any researcher in China who discovers them.

The United States is home to many of the world's leading software companies. These companies pay researchers from around the world to help secure their products. This relationship is critical for firms to secure their products from exploitation by criminals and foreign governments. The table below shows the total dollar amount, as well as the percentage of overall payments, paid to researchers in a given country. One of the largest software bug platforms in the United States US provided this data, and wishes to remain unnamed. Behind researchers in the United States, those in China rank second in providing software vulnerabilities to U.S. firms in exchange for cash. In 2021, these Chinese researchers received 10 percent of the $44 million spent by U.S. companies on this particular platform.

The data provides the following insights:

- China's talent pool for software security rivals the United States, India, Russia, and the United Kingdom. Although this data is from one year and from one marketplace, a holistic analysis would likely position these countries in a similar order.

- China's policy that researchers must submit vulnerabilities to the Ministry of Industry and Information Technology creates an incredibly valuable pipeline of software capabilities for the state. The policy effectively bought at least $4m worth of research for free. Some vulnerabilities may fetch much more on the black market so these values are probably discounted. Moreover, there may be a significant gap between what a company pays for a vulnerability and the cost of the ensuring damage the same bug could have caused if left unpatched.
- U.S. companies benefit from the participation of Chinese cybersecurity researchers. Evaluating the counterfactual—if Chinese researchers did not, or were not allowed to submit vulnerabilities—is difficult. Some bugs might have just been found first by someone from China,

but also found later by other researchers. It's hard to know. But what is clear is that U.S. companies derive significant value from Chinese hackers who submit software vulnerabilities to firms.

- International researchers accounted for 85 percent of the payouts of software bugs submitted to U.S. companies on this particular platform in 2021. No other figure can capture the extent to which U.S. firms benefit from international cooperation. The data emphasizes that cybersecurity is a team sport.

Payments made by U.S. companies to researchers in 2021.

Country of Researcher/Recipient	Total Amount Paid	Percentage of Total Amount Paid by US
United States of America	$6,718,923	15%
China	$4,220,302	10%
India	$4,055,807	9%
Russian Federation	$2,047,212	5%
United Kingdom of Great Britain and Northern Ireland	$2,029,512	5%
Germany	$1,698,018	4%
Canada	$1,674,918	4%
Netherlands	$1,190,940	3%
Argentina	$1,103,724	3%
Australia	$1,072,930	2%
France	$1,029,796	2%

Spain	$982,472	2%
Belgium	$892,722	2%
Morocco	$820,959	2%
Sweden	$807,166	2%
Vietnam	$735,786	2%
Brazil	$730,918	2%
Ukraine	$712,147	2%
Nepal	$667,125	2%
Turkey	$661,353	1%

Source: Information provided to CSET on a private basis by a large U.S.-based software bug reporting platform.