February 17, 2022

Winnona DeSombre
Research Fellow - Atlantic Council & Harvard Belfer Center

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”

….

Executive Summary

Commissioner Wong, Commissioner Glas, other distinguished members of the Commission, it is an honor to testify before you today on China's cyber capabilities. I have been asked to brief you on Chinese leaders' efforts to become a "cyber superpower", how China and the U.S. compare in metrics of cyber power, and China's offensive cyber capabilities in contrast to the United States.

I have **5 main points** to make in this testimony:

1. China is a major peer adversary in cyberspace. Its offensive cyber capabilities rival the United States', its operations demonstrate clear development of asymmetric capabilities that enable it to achieve strategic goals, and its cyber defensive capabilities are robust.

2. Xi Jinping has dramatically escalated Chinese rhetoric and capabilities around cyber power. He has modernized his military, shifted propaganda priorities to pursue global information dominance, and is remaking the international supply chain with Chinese companies.

3. China has asymmetric capabilities that the U.S. is currently constrained from developing via international or domestic law, on top of their already impressive arsenal, for both economic espionage and national security use. They use their private sector for cyber operations, and blatantly disregard any efforts to name and shame their behavior.

4. While China and the United States both suffer from a cyber personnel shortage, China's enablement of private sector offensive security contractors and academic institutions, and emphasis on asymmetric capabilities, will allow it to grow capabilities despite these issues.

5. The United States does not currently have adequate cyber defenses, personnel, supply chain security, or international technical and standards leadership to rival China long-term.

To ensure adequate capabilities in response to China's cyber superpower goals, Congress must:

- **Bolster US cyber defenses** by creating federal mandatory breach notification laws, threat information sharing requirements and patching requirements for critical infrastructure;
- **Appropriate funds to secure the global supply chain**, particularly towards semiconductor foundries and open source detection and response efforts in the America COMPETES act;
- **Diversify the US cyber security jobs pipeline** by loosening foreign talent restrictions, increasing cyber visa quotas, doubling education budgets, and expanding the U.S. Digital Service "tour of duty" model to public sector cyber defense jobs; and
- **Work with allies to support U.S. values in the information domain** by encouraging US and allied leadership in the ITU and by asking the Department of Commerce to add Chinese institutions connected to cyber operations to the entities list.

China and the Importance of Cyberspace

How do Chinese leaders view the importance of cyberspace?

The Chinese Communist Party (CCP) wants China to become a "cyber superpower"[1], and is well on its way to achieving that goal. CCP leaders have a clear understanding of the domain and how to use cyber power to achieve existing strategic goals – particularly goals within domestic surveillance, defense, information dominance, economic growth, technical standards, and especially offensive capabilities.[2]

Cyber is a prioritized domain in China's rhetoric, regulation, and action. Becoming a cyber superpower or cyber powerhouse is explicitly stated within their newest Five Year Plan - encompassing plans for economic expansion, national security, talent training, international trade, and more[3]. This comprehensive cyber strategy has already been incorporated into regulatory processes at ministry[4], party[5], and provincial[6] levels of government.

The CCP believes that the U.S. is more vulnerable in cyberspace, and that they can develop asymmetric capabilities that would give them a distinct wartime advantage.[7] We observe this in their mismatch between rhetoric and action – for instance, China espouses ideals of cyber sovereignty[8] while abusing the free and open Internet to sow disinformation in the United States.[9]

Xi Jinping and China's Preparations for Cyberwarfare

Xi Jinping has dramatically escalated Chinese rhetoric around cyber security and warfare, stating openly that "without cyber security, there is no national security".[10] Prior Chinese leaders focused largely on domestic matters: military IT[11], domestic cyber sovereignty[12], and control over domestic virtual society[13]. By contrast, **Xi has pushed China to reach for cyber power** by developing a modernized military, shifting propaganda priorities to global information dominance, and remaking the international supply chain with Chinese companies.

Xi Jinping has completely reorganized the People's Liberation Army, downsizing the land-based army it has relied on for decades to create a Strategic Support Force that focuses on cyber, space, and electronic warfare.[14] This reorganization has accelerated a shift in military posture from land-based territorial protection to extended power projection[15], with joint forces and technology as key enablers. To compliment the new joint force, Xi has advanced a strategy of military-civil fusion (MCF), restructuring Chinese science and technology enterprise to simultaneously innovate for both economic and military development.[16] These two strategies marry well with Xi's push past "informationization" to "intelligentization"[17] of the PLA, which will integrate artificial intelligence and human computer interaction into military decision making.[18]

Xi Jinping has also stressed the importance of "discourse power"[19] and information dominance[20] in cyberspace. This is a marked shift of priorities from domestic censorship to global information control, and this shift has already been noted by U.S. cybersecurity experts: information operations stemming from China targeting domestic issues have been strategically redirected towards the West over the last two years to sow discord and project power abroad.[21]

Furthermore, Xi Jinping is fundamentally changing the world's cyber infrastructure by pursuing Chinese private sector dominance in international markets, while weaning China off of Western technology. The "Made in China 2025"[22] plan is aimed at making China the key player in the high-tech global supply chain - rapidly shifting Chinese technology off of Taiwanese and U.S. manufactured chips[23], while the Belt and Road Initiative ensures that Chinese private sector technology firms are involved in key infrastructure deals[24] throughout Western Asia, Africa, the Middle East, and Europe.

China, the United States, and Cyberwarfare

US policy papers often refer to China as a near-peer competitor in cyberspace. But make no mistake: **China is a major peer adversary in cyberspace.** As the DOD has openly stated, China is "the only country that can pose a systemic challenge to the United States in the sense of challenging us, economically, technologically, politically and militarily".[25] This is especially clear in the cyber domain: The country's offensive cyber capabilities rival or exceed that of the United States, and its cyber defensive capabilities are able to detect many U.S. operations – in some cases turning our own tools against us. On top of this, China also uses asymmetric capabilities that the United States is constrained against using by either international or domestic law, achieving large tactical advantages.

Chinese Offensive Cyber Capabilities

While China has not yet been attributed to a major disruptive cyber attack, the U.S. intelligence community has openly stated that China "possesses substantial cyber-attack capabilities …[and] can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States".[26] Some capabilities are readily observable in the open source: for example, one critical measure of offensive cyber capabilities is a country's ability to find and exploit software vulnerabilities. A software vulnerability is a security flaw or weakness in software that could be exploited by an attacker. They are crucial tools for cyber operations, especially if the flaw has yet to be fixed in most software products, or if the vendor is unaware of the vulnerability in their product at all.

Hackers in China find vulnerabilities in U.S. software at an alarming rate, and China actively exploits these vulnerabilities in its cyber operations before they can be fixed. Every

year, China holds a hacking competition, the Tianfu Cup, for their top hackers to find vulnerabilities. However, unlike equivalent competitions elsewhere, which commonly disclose the flaws directly to impacted companies, **flaws found at Chinese hacking competitions are given to the Chinese government before companies even hear about them**[27]. A flaw in Apple software reported at Tianfu Cup[28] in 2018 was used in Chinese cyber espionage campaigns for two months before the vulnerability was discovered and fixed. How many vulnerabilities does China find compared to the international community? In 2021, Tianfu Cup reported 30 successful demonstrations exploiting new vulnerabilities in US software products, including Windows 10, Apple iOS, Safari, and Chrome.[29] This was 40% more than the number of successful demonstrations at Pwn2Own (an equivalent international competition with U.S. turnout) that same year.[30]

Outside of competitions, **Chinese companies are punished when they disclose vulnerabilities to vendors without first consulting the Chinese government**: when an engineer at Alibaba found a vulnerability in Log4j, he reported it directly to Apache (the U.S. vendor responsible) instead of to the Chinese government. This was one of the most serious vulnerabilities last year, impacting millions of websites and applications.[31] Instead of rewarding the engineer, the Chinese government suspended its information-sharing partnership with Alibaba Cloud for six months and cited improper disclosure of Log4j as the primary reason.[32]

Control over the information environment is also a critical measure of wartime cyber capability – indeed, the Allied Powers used various forms of propaganda[33] and disinformation[34] during World War II against the Nazi regime. **China has used the modern Internet ecosystem to successfully craft pro-China narratives abroad and prevent anti-Chinese messages from being propagated**. Its propaganda apparatus is attempting to produce targeted content that promotes pro-China narratives in the West, specifically for "international youths"[35], and hired a New Jersey consulting firm to spread pro-Beijing content for the 2022 Olympics via online influencers.[36] Tiktok, a popular Chinese social media app, actively censors content unfavorable to Beijing.[37] China also has a sprawling covert propaganda network conducting disinformation operations on social media, which has begun to develop measurable international reach.[38]

China's Asymmetric Capabilities: Playing a Different Game in Cyberspace

In addition to highly robust offensive cyber capabilities, **China has built asymmetric capabilities that the United States is constrained against developing by international or domestic law.** The United States prioritizes operational tradecraft in cyber operations[39], does not conduct economic espionage, and has clear authorities on who can and cannot conduct military operations in cyberspace.[40] The Chinese government develops cyber programs that do not care whether they are found and attributed, continues to steal American intellectual property in

cyberspace alongside more traditional operations, and directly hires corporations to conduct cyber operations on behalf of the regime.

Chinese cyber units continue to conduct economic espionage against companies in the U.S. and globally. Despite the 2015 US-China Cyber agreement in which both countries agreed to refrain from stealing intellectual property[41], China has been flagrantly violating the agreement over the last eight years.[42] While the 2015 agreement initially resulted in intellectual property being stolen at a slower observable rate[43], this is no longer the case.

China no longer cares about being named and shamed in cyberspace. **This apathy enables the regime to conduct far more frequent cyber operations[44] that, while easy to detect, are still wildly successful**. By altering malware readily found online[45] or by using vulnerabilities with known fixes since 2017[46], China demonstrates that it does not care enough about getting caught to spend the time and money required to develop more stealthy capabilities across all their cyber programs.[47] In fact, they make themselves easy to find - some cyber operations attributed to China have been found using tools known by the cyber security industry as belonging to the PLA since 2013.[48] However, these basic operations still successfully penetrate U.S. organizations for both economic espionage and intelligence gathering purposes. **In more recent cases, China has sped up their operational tempo after their cyber operation was discovered.** When the White House publicly announced flaws[49] in Microsoft Exchange used by Chinese hackers, the number of observed attacks from China using the vulnerability skyrocketed – suggesting that China ramped up the campaign to compromise as many computers as possible before U.S. companies could protect themselves.[50]

Finally, **China's civilian commercial entities are heavily involved in Chinese cyber operations**. The CCP's "military-civil fusion" strategy has enabled large numbers of civilian companies like Baidu and Alibaba[51] to participate in classified military research and development.[52] In addition, Chinese contractors have directly engaged in cyber operations for the Chinese government.[53] Chinese telecom and infrastructure companies like Huawei have been implicated in Chinese cyber espionage campaigns in the past.[54] This is particularly alarming given that these same companies are key elements in China's Belt and Road Initiative abroad, and previous infrastructure projects that involved Huawei – like the 2012 African Union building project – were found sending signals back to China.[55]

China's Defensive Capabilities – Large Scale and Able to Detect Western Operations

China also has well established and **large-scale defensive capabilities that are able to detect some Western cyber operations**. It has a cyber security industry of power players providing the full gamut of cyber security products and services[56], and the industry is growing larger. On top of putting in place extensive cyber security regulations for Chinese businesses[57], the Ministry of

Industry and Information Technology (MIIT) also plans on boosting development of and demand for cyber security products, expecting the sector to be worth more than $38.6 billion by 2023.[58]

Two Chinese cyber security firms in particular: Antiy Labs[59] and Qihoo360[60], have openly published analyses of NSA and CIA cyber operations. While these reports are heavily bolstered by the Shadowbrokers and Vault7 leaks respectively and do not provide enough information for independent researchers to validate their claims, Antiy and Qihoo are two of the oldest antivirus companies in China and therefore likely have the data visibility that would make these claims credible. **Chinese MSS contractors have also been able to observe and recreate U.S. made cyberweapons**: one contractor was found using NSA hacking tools a full year before the tools were made public via the Shadowbrokers leak, suggesting that the contractor observed the hacking tools being used against Chinese targets and recreated the tool from those observations.[61]

U.S. Advantages over China in Cyberspace

The U.S. still has power over China in cyberspace. The United States has first mover advantage – U.S. companies own vast swaths of international fiber optic cable, provide some of the world's largest online platforms and produce some of the most widely used technological devices. The United States has a global network of alliances with intelligence partnerships spanning the globe, many of which are in China's sphere of influence. Most importantly, the United States has some of the world's top technical talent and most innovative technology companies.

The CCP knows all of this – and is actively attempting to chip away at those advantages. The Chinese government has pushed policies of technological self-sufficiency to reduce reliance on U.S. technology.[62] This stems from a clear party leadership understanding that their reliance on U.S.-produced operating systems and microprocessors is an urgent security vulnerability. In addition, China actively pushes its own technology companies to expand internationally and leapfrog over their U.S. counterparts. Chinese officials have also squeezed U.S. companies and allies – technology giants like Apple have been pressured use Chinese hardware and invest directly into the country[63], and U.S. intelligence partners have been pressured economically for security and trade concessions.[64]

On top of all this, China is inherently changing the playing field on which we currently operate in cyberspace, through pursuing leadership positions in international technical standards bodies.[65`] Changing the technical standards for how the Internet operates would nullify the United States' first mover advantage over China entirely over time.

China and the U.S. vis-a-vis Cyber Personnel

One global issue impacting both China and the United States is the global shortage of talented cybersecurity personnel. While China and the United States both suffer from a personnel shortage, **China's multi-stakeholder approach to personnel development, its relationship with corporate and academic institutions, and its emphasis on developing asymmetric capabilities will enable it to overcome these issues** in the short term, while developing a formidable force long term.

The CCP is well aware of its shortage of cyber security professionals - estimating the deficit at 1.4 million jobs.[66] This is three times as much as the current deficit estimate in North America.[67] **Considering how effective current Chinese cyber capabilities are despite this deficit, China will likely overcome potential issues stemming from this shortage**.

China's cyber talent is currently bolstered by linking research universities to military and intelligence organizations via military-civil fusion: at least 15 Chinese civilian universities have been implicated in cyberattacks, illegal exports or espionage thus far, and over 150 are able to contribute to classified weapons and defense projects/[68] In addition, China has purchased surveillance tools[69] (and potentially vulnerabilities[70]) from foreign contractors to bolster its capabilities domestically. China's MIIT has also artificially boosted demand of cyber security products by mandating that key industries devote 10% of their IT budget to cyber security within the next two years.[71]

The United States, by contrast, is not nearly as well equipped. The United States is also looking to fill its shortage of approximately 300-400 thousand cyber security jobs, but it is held back by policies that discourage engineers from coming into government service. These include: lack of upward mobility, noncompetitive pay, and long security clearance processing backlogs.

To make matters worse, visa processing issues discourage engineering talent from coming to the US entirely, preventing U.S. institutions from taking advantage of such talent. As a result, the United States has a smaller personnel gap, but far more difficulty in filling it - and it may only get worse: if left unaddressed, the labor shortage is expected to grow by at least 20% every year.[72]

Comparative Indexes of CCP Cyberpower - a Red Herring

Do not be fooled by indexes that say otherwise - **in cyberspace, China is a major peer player.** Indexes that attempt to measure Chinese and U.S. cyber power suffer from **three pitfalls**: choosing irrelevant or incorrect proxies, believing the fallacy of sophistication, and using overly Western measurements of power.

Finding proxies for cyber power is incredibly difficult – this is especially the case for offensive cyber capabilities, which are often deliberately hidden away from the prying eyes of researchers. Thus, finding relevant proxies requires deep knowledge of a country's cyber governance and its cybersecurity industry. Due to lack of industry experience, researchers creating cyber power indexes may use misleading proxy data for China's robust cyber capabilities. For example, the IISS cyber power index used semiconductor sale[73] as a proxy for cyber empowerment and dependence - when semiconductor *manufacturing*[74] is far more important for supply chain security.[75]

Researchers also fall into the fallacy of sophistication when measuring cyber attacks – comparing the Stuxnet worm: an incredibly complex piece of software designed to target Iranian nuclear centrifuges allegedly created by the U.S. and Israel[76], to lower-level attacks perpetrated by the Chinese government. Given how vulnerable the U.S. already is in cyber defense, as well as the well-worn arsenal of online attacks available to our adversaries that barely require technical skills – such as disinformation, phishing scams, or dropping USBs in a parking lot[77], this is a false dichotomy. Whether a cyber operation is sophisticated or artful is far less important than whether a cyber operation achieves the intended goal.

Fundamentally, using Western metrics of cyber power to measure China's cyber power misses the point that China's goals in cyberspace are inherently different from Western goals. As Western powers talk about their cyber capabilities with increasing openness, some indexes[78] may decide that China's lack of open offensive cyber doctrine is the same as not having an offensive cyber doctrine. This is an extreme assumption considering the People's Liberation Army (PLA) reorganization, well-honed Ministry of State Security (MSS) cyber operations structures, and its well-developed offensive security industry exports. Indexes that look for openly available strategy documents and international partnership agreements may be missing Chinese goals entirely.

Recommendations for Congressional Action

Based on current open source observations, the United States does not currently have adequate cyber defenses, personnel, supply chain security, or international technical and standards leadership to rival China long-term in cyberspace. **In addition, given how secretive cyber is as a domain, China's capabilities likely exceed the findings compiled here**. To ensure adequate U.S. capabilities in response to China's cyber superpower goals, Congress must:

1) Bolster US Cyber Defenses

If breaking into United States systems were more difficult, China would have to expend many more resources ensuring its cyber capabilities were up to the task. Creating federal mandatory breach notification laws pertaining to U.S. critical infrastructure, mandating threat information

sharing for critical infrastructure sectors to the government, and expanding patching requirements[79] to federal contractors will be excellent steps in the right direction.

2) Appropriate Funds to Secure the Supply Chain

In order to ensure security and integrity of the global supply chain, Congress must appropriate additional funds to semiconductor foundries in the CHIPS act[80], as well as allocate funding for research into federal software bill of materials and other key areas where Chinese cyberwarfare may impact the U.S. economy. Directing research into detection and interception of malicious software in open source before it becomes a problem is key – language in the America COMPETES Act can be altered to accomplish this goal[81].

3) Diversify the US Cyber Security Jobs Pipeline

To keep up with China's rapidly growing cyber personnel, Congress should loosen restrictions on contractors to hire foreign talent in the EU or elsewhere, expand the H1-B visa quota for cyber security and engineering talent, double Cybercorps Scholarship for Service funding from 20 million to 40 million dollars[82], fund cyber security education at levels similar to the National Defense Education Act during the space race, and expand the U.S. Digital Service "tour of duty" model[83] to public cyber defense jobs.

4) Work with Allies to Support U.S. Values in the Information Domain

Encouraging US and allied leadership in international standards bodies like the ITU will continue to show support for a free and open Internet. In addition, Congress can move beyond naming and shaming to impose costs on Chinese cyber threat groups by asking the Department of Commerce or Treasury to add Chinese institutions connected to cyber operations to the entities list and sanctions list. This would effectively ban them from using U.S.-produced operating systems and microprocessors, which Chinese firms currently rely heavily on. Note that this must be paired with clear guidelines on how Chinese institutions could get themselves removed from the list to encourage more responsible behavior.

Works Cited

---

[1] DigiChina. "Lexicon: 网络强国 Wǎngluò Qiángguó." Accessed February 8, 2022. https://digichina.stanford.edu/work/lexicon-网络强国-wangluo-qiangguo/.

[2] Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, and Anina Schwarzenbach. "Harvard Belfer National Cyber Power Index 2020." Harvard Belfer Center, September 2020. https://www.belfercenter.org/publication/national-cyber-power-index-2020.

[3] Center for Security and Emerging Technology. "CSET Original Translation: China's 14th Five-Year Plan." Accessed February 8, 2022. https://cset.georgetown.edu/publication/china-14th-five-year-plan/.

[4] DataGuidance. "China: MIIT Issues Notice on the 14th Five-Year Plan for Information and Communication Industry," November 16, 2021. https://www.dataguidance.com/news/china-miit-issues-notice-14th-five-year-plan.

[5] DigiChina. "Translation: 14th Five-Year Plan for National Informatization – Dec. 2021." Accessed February 8, 2022. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.

[6] "Outline of the 14th Five-Year Plan (2021-2025) for National Economic and Social Development and Vision 2035 of the People's Republic of China_ News_ 福建省人民政府门户网站." Accessed February 8, 2022. https://webcache.googleusercontent.com/search?q=cache:86P649lhIskJ:https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm&hl=en&gl=us&strip=1&vwsrc=0.

[7] Federation Of American Scientists. "China's Science of Military Strategy (2013)." Accessed February 8, 2022. https://fas.org/blogs/secrecy/2015/08/china-sms/.

[8] Peterson, Dahlia. "How China Harnesses Data Fusion to Make Sense of Surveillance Data." *Brookings* (blog), September 23, 2021. https://www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/.

[9] "ATA-2021-Unclassified-Report.Pdf." Accessed February 8, 2022. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

[10] New America. "Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference." Accessed February 8, 2022. http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/.

[11] Council on Foreign Relations. "The 18th Party Congress and Chinese Cyberpower." Accessed February 8, 2022. https://www.cfr.org/blog/18th-party-congress-and-chinese-cyberpower.

[12] "China's Internet Governance_ A New Conceptualization.Pdf." Accessed February 8, 2022. https://dukespace.lib.duke.edu/dspace/bitstream/handle/10161/18308/

[13] Tanner, Murray Scot, Peter W Mackenzie, CNA Corporation, Marine Corps University (U.S.), and Press. *China's Emerging National Security Interests and Their Impact on the People's Liberation Army*, 2015. https://search.ebscohost.com/direct.asp?db=mth&jid=JOEQ&scope=site.

[14] "Costello and McReynolds - CHINA STRATEGIC PERSPECTIVES 13.Pdf." Accessed February 8, 2022. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

[15]"Saunders - Chairman Xi Remakes the PLA Assessing Chinese Mil.Pdf." Accessed February 8, 2022. https://ndupress.ndu.edu/Portals/68/Documents/Books/Chairman-Xi/Chairman-Xi.pdf.
[16] "What Is Military Fusion - Department of State." Accessed February 8, 2022. https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.
[17] "How Does China Aim to Use AI in Warfare?" Accessed February 8, 2022. https://thediplomat.com/2021/12/how-does-china-aim-to-use-ai-in-warfare/.
[18] Defense One. "How Chinese Strategists Think AI Will Power a Military Leap Ahead." Accessed February 8, 2022. https://www.defenseone.com/ideas/2021/09/how-chinese-strategists-think-ai-will-power-military-leap-ahead/185409/.
[19] "Doshi et. al - China as a Cyber Great Power Beijing's Two Voices in Telecommunications." Accessed February 8, 2022. https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf.
[20] Burke, Edmund, Kristen Gunness, Cortez Cooper, and Mark Cozad. *People's Liberation Army Operational Concepts*. RAND Corporation, 2020. https://doi.org/10.7249/RRA394-1.
[21] Nimmo, Ben, Camille François, C Shawn Eib, and Léa Ronzaud. "Spamouflage Goes to America,"https://graphika.com/reports/spamouflage-dragon-goes-to-america/.
[22]Council on Foreign Relations. "Is 'Made in China 2025' a Threat to Global Trade?" Accessed February 8, 2022. https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.
[23] Reuters. "Taiwan Chip Industry Emerges as Battlefront in U.S.-China Showdown." Accessed February 8, 2022. https://www.reuters.com/investigates/special-report/taiwan-china-chips/.
[24] Council on Foreign Relations. "China's Digital Aid: The Risks and Rewards." Accessed February 8, 2022. https://www.cfr.org/china-digital-silk-road.
[25] U.S. Department of Defense. "Official Talks DOD Policy Role in Chinese Pacing Threat, Integrated Deterrence." Accessed February 8, 2022. https://www.defense.gov/News/News-Stories/Article/Article/2641068/official-talks-dod-policy-role-in-chinese-pacing-threat-integrated-deterrence/.
[26] U.S. Office of the Director of National Intelligence. "Annual Threat Assessment of the US Intelligence Community". Accessed February 8, 2022. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.
[27] War on the Rocks. "China Flaunts Its Offensive Cyber Power," October 22, 2021. https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/.
[28] Patrick Howell O'Neill. "How China Turned a Prize-Winning IPhone Hack against the Uyghurs." Accessed February 8, 2022. https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/.
[29] The Record by Recorded Future. "Windows 10, IOS 15, Ubuntu, Chrome Fall at China's Tianfu Hacking Contest," October 17, 2021. https://therecord.media/windows-10-ios-15-ubuntu-chrome-fall-at-chinas-tianfu-hacking-contest/.
[30] The Record by Recorded Future. "Pwn2Own 2021 Hacking Contest Ends with a Three-Way Tie," April 9, 2021. https://therecord.media/pwn2own-2021-hacking-contest-ends-with-a-three-way-tie/.
[31] "Why Is the Log4j Cybersecurity Flaw the 'Most Serious' in Decades?" *New York Post* (blog), December 20, 2021. https://nypost.com/2021/12/20/why-is-the-log4j-cybersecurity-flaw-the-most-serious-in-decades/.

[32]Greig, Jonathan. "Chinese Regulators Suspend Alibaba Cloud over Failure to Report Log4j Vulnerability." ZDNet. Accessed February 8, 2022. https://www.zdnet.com/article/log4j-chinese-regulators-suspend-alibaba-partnership-over-failure-to-report-vulnerability/.
[33] History. "Inside America's Shocking WWII Propaganda Machine," December 19, 2016. https://www.nationalgeographic.com/history/article/world-war-2-propaganda-history-books.
[34] Matthew Shaer. "Fighting the Nazis With Fake News." Smithsonian Magazine. Accessed February 8, 2022. https://www.smithsonianmag.com/history/fighting-nazis-fake-news-180962481/.
[35] Recorded Future. "Elephants Must Learn to Street Dance: The Chinese Communist Party's Appeal to Youth in Overseas Propaganda," February 3, 2022. https://www.recfut.com/elephants-street-dance-chinese-communist-party-appeal-youth-overseas-propaganda/.
[36] "Chinese Government Deploying Online Influencers amid Beijing Olympics Boycotts." OpenSecrets News, December 13, 2021. https://www.opensecrets.org/news/2021/12/chinese-government-deploying-online-influencers-amid-beijing-olympics-boycotts/.
[37] Alex Hern. "Revealed: How TikTok Censors Videos That Do Not Please Beijing." *The Guardian*, September 25, 2019, sec. Technology. https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing.
[38] Nimmo, Ben, Ira Hubert, and Yang Cheng. "Spamouflage Breakout," Accessed February 8, 2022. https://public-assets.graphika.com/reports/graphika_report_spamouflage_breakout.pdf.
[39] Adams et al. "Responsible Cyber Offense." Lawfare, August 2, 2021. https://www.lawfareblog.com/responsible-cyber-offense.
[40] LII / Legal Information Institute. "10 U.S. Code § 394 - Authorities Concerning Military Cyber Operations." Accessed February 8, 2022. https://www.law.cornell.edu/uscode/text/10/394.
[41] U.S.–China Cyber Agreement. Accessed February 8, 2022. https://sgp.fas.org/crs/row/IN10376.pdf
[42] Marketplace. "China's State-Backed Cyberattacks Are Part of a Larger Plan," December 9, 2021. https://www.marketplace.org/2021/12/09/chinas-state-sponsored-industrial-espionage-is-part-of-a-larger-system/.
[43] NBC News. "Are Chinese Hackers Slowing Down Their Cyber Attacks on the U.S.?" Accessed February 8, 2022. https://www.nbcnews.com/tech/tech-news/are-chinese-hackers-slowing-down-their-cyber-attacks-u-s-n601961.
[44] "A Peek into BRONZE UNION's Toolbox." Accessed February 8, 2022. https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox.
[45] Ibid
[46] ComputerWeekly.com. "Nation State APT Groups Prefer Old, Unpatched Vulnerabilities." Accessed February 8, 2022. https://www.computerweekly.com/news/252483043/Nation-state-APT-groups-prefer-old-unpatched-vulnerabilities.
[47] DeSombre et al. "Countering Cyber Proliferation: Zeroing in on Access-as-a-Service - Atlantic Council," March 1, 2021. https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.
[48] Security Affairs. "Attackers behind Operation Oceansalt Reuse Code from Chinese Comment Crew," October 19, 2018. https://securityaffairs.co/wordpress/77228/apt/operation-oceansalt.html.

[49] Temple-Raston, Dina. "China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying." *NPR*, August 26, 2021, sec. Investigations. https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.
[50] Greenberg, Andy. "Chinese Hacking Spree Hit an 'Astronomical' Number of Victims." *Wired*. Accessed February 8, 2022. https://www.wired.com/story/china-microsoft-exchange-server-hack-victims/.
[51] "Myths and Realities of China's Military-Civil Fusion Strategy." Accessed February 8, 2022. https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy.
[52] "What Is Military Fusion - Department of State." Accessed February 8, 2022. https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.
[53] CyberScoop. "DOJ Reveals Indictment against Chinese Cyber Spies That Stole U.S. Business Secrets," November 27, 2017. https://www.cyberscoop.com/boyusec-china-doj-indictment/.
[54] Bloomberg. "Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack," December 16, 2021. https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack.
[55]Solomon, Salem. "After Allegations of Spying, African Union Renews Huawei Alliance." VOA. Accessed February 8, 2022. https://www.voanews.com/a/after-allegations-of-spying-african-union-renews-huawei-alliance/4947968.html.
[56] Cybercrime Magazine. "China Cybersecurity Companies," September 18, 2018. https://cybersecurityventures.com/china-cybersecurity-companies/.
[57] Bird, Bird LLP-Amanda Ge, James Gong, Tiantian Ke, and Clarice Yue. "China Data Protection and Cybersecurity: Annual Review of 2021 and Outlook for 2022 (II)." Lexology, January 26, 2022. https://www.lexology.com/library/detail.aspx?g=0a24afb9-7f27-4b18-9486-3ba3ddc688e6.
[58] South China Morning Post. "China Drafts Plan to Grow Its Cybersecurity Industry as Threats Grow," July 13, 2021. https://www.scmp.com/tech/policy/article/3140963/china-drafts-three-year-plan-boost-its-cybersecurity-industry-amid.
[59] "FROM EQUATION TO EQUATIONS - Antiy Labs | The Next Generation Anti-Virus Engine Innovator." Accessed February 8, 2022. https://www.antiy.net/p/from-equation-to-equations/.
[60] Qihoo360. "The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China's Critical Industries for 11 Years." Accessed February 8, 2022. https://blogs.360.cn/post/APT-C-39_CIA_EN.html.
[61] Symantec Threat Hunter Team. "Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak." Accessed February 8, 2022. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit.
[62] "Doshi et. al - China as a Cyber Great Power Beijing's Two Voices in Telecommunications." Accessed February 8, 2022. https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf.
[63] AppleInsider. "Apple Made Secret 5-Year $275B Deal with Chinese Government." Accessed February 8, 2022. https://appleinsider.com/articles/21/12/07/apple-made-secret-5-year-275b-deal-with-chinese-government.

[64] BBC News. "Five Eyes: Is the Alliance in Trouble over China?," May 4, 2021, sec. Asia. https://www.bbc.com/news/world-56970640.
[65] "The International Telecommunication Union: The Most Important UN Agency You Have Never Heard Of." Accessed February 8, 2022. https://www.csis.org/analysis/international-telecommunication-union-most-important-un-agency-you-have-never-heard.
[66] Center for Security and Emerging Technology. "China's National Cybersecurity Center." Accessed February 8, 2022. https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/.
[67] ISC2. "ISC2 Cybersecurity Workforce Study 2021" Accessed February 8, 2022. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.
[68] Joske, Alex. "The China Defence Universities Tracker." Accessed February 8, 2022. https://www.aspi.org.au/report/china-defence-universities-tracker.
[69] DeSombre et. al. "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets," Atlantic Council, November 8, 2021. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/.
[70] Uren, Tom. "Srsly Risky Biz: Thursday, November 11." Substack newsletter. *Seriously Risky Business* (blog), November 10, 2021. https://srslyriskybiz.substack.com/p/srsly-risky-biz-thursday-november-3a2.
[71] South China Morning Post. "China Drafts Plan to Grow Its Cybersecurity Industry as Threats Grow," July 13, 2021. https://www.scmp.com/tech/policy/article/3140963/china-drafts-three-year-plan-boost-its-cybersecurity-industry-amid.
[72] KOAA. "Deep Dive: Cybersecurity Professional Shortage a Serious Concern for National Security," June 8, 2021. https://www.koaa.com/news/deep-dive/cybersecurity-professional-shortage-a-serious-concern-for-national-security.
[73]IISS. "Cyber Capabilities and National Power: A Net Assessment." Accessed February 8, 2022. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.
[74] "Government Incentives and US Competitiveness in Semiconductor Manufacturing 2020." Accessed February 8, 2022. https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-in-Semiconductor-Manufacturing-Sep-2020.pdf.
[75] Reuters. "Taiwan Chip Industry Emerges as Battlefront in U.S.-China Showdown." Accessed February 8, 2022. https://www.reuters.com/investigates/special-report/taiwan-china-chips/.
[76] Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*. Accessed February 8, 2022. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
[77] Shevchenko, Sergei. "Agent.Btz - A Threat That Hit Pentagon." Accessed February 8, 2022. http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html.
[78] IISS. "Cyber Capabilities and National Power: A Net Assessment." Accessed February 8, 2022. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.
[79] TechCrunch. "US Federal Agencies Told to Patch Hundreds of Security Bugs." Accessed February 8, 2022. https://social.techcrunch.com/2021/11/03/cisa-directive-hundreds-security-patches/.
[80] Congress.gov. "H.R.7178 - 116th Congress (2019-2020): CHIPS for America Act." June 11, 2020. https://www.congress.gov/bill/116th-congress/house-bill/7178.

[81]Congress.gov. "Text - H.R.4521 - 117th Congress (2021-2022): Bioeconomy Research and Development Act of 2021 [America COMPETES Act of 2022]." February 4, 2022. https://www.congress.gov/bill/117th-congress/house-bill/4521/text.
[82] "CyberCorps(R) Scholarship for Service (SFS) (Nsf21580) | NSF - National Science Foundation." Accessed February 8, 2022. https://www.nsf.gov/pubs/2021/nsf21580/nsf21580.htm.
[83] United States Digital Service. "Apply to USDS." Accessed February 8, 2022. https://usds.gov/apply.