China's Cyber Operations

The Rising Threat to American Security

Dave Aitel, Sophia d'Antoine, Winnona DeSombre,
Isabella Garcia-Camargo, Ian Roos, Nicholas Rostow, Jonathan Smith,
Alison Strongwater, Abraham Wagner, and JD Work

MARGIN RESEARCH

The research described in this report was sponsored by the Defense Advanced Research Projects Agency (DARPA) under Contract No. HR00112190088. The views expressed are those of the authors, and do not reflect any views or opinions of the United States Government.

www.margin.re

Contents

Foreword and Acknowledgements

What began as a research project at the Advanced Research Projects Agency (ARPA) in the 1960s evolved into a communications and information technology revolution never anticipated. These early experiments in new communications technologies gave rise to the most significant paradigm change since the invention moveable type in the 15th century. The vast majority of all communications and information operations now take place on systems connected to the Internet infrastructure. Users adopted them rapidly. All major sectors—national security, finance, utilities—have become highly dependent on this critically important infrastructure.

Dependencies on this infrastructure make users vulnerable to criminals and potential adversaries. The original ARPA effort involved an experiment in networking scientists. It did not take security into account. When this experiment became ARPAnet and then the Internet, the foundation was insecure and prone to hostile attacks of all kinds. Such attacks, together with espionage and cyberwarfare, have become a substantial national security problem. Elements of the Defense Department and military commands and experts in the Intelligence Community consider cyberwarfare as a major threat area. Other federal agencies also respond to the ever-mutating problems posed by hackers.

At present, the most significant foreign cyber threats come from China, Russia, North Korea, and Iran. This research considers the ways these states recruits skilled personnel, organizes potentially malicious activities, and explores specific cyber operations. China stands out as the most significant threat in the cyber arena, with a longstanding interest in information and its power and the usefulness of dominating it. In line with this tradition, the PRC has greatly expanded its cyber capabilities in intelligence collection, espionage, deception, and cyber warfare.

This rapidly growing threat has received increasing notice and discussion in the open literature, although data supporting China's malicious cyber operations are limited. The present analysis is based on an effort to collect a substantial quantity of open-source data generated by Chinese operations using code artifacts inserted into software such as the Linux Kernel. The result is an exploration of China's malicious cyber ecosystem, rather than simply observing the aftermath of hostile cyber activities.

This study effort was made possible with support from the Defense Advanced Research Projects Agency (DARPA). The study team has benefited greatly from discussions with personnel from U.S. Government agencies and offices, as well as former officials and other experts. In particular Daniel Gallington, Anthony Cordesman, J.D. Work, and Justin Sherman have been extraordinarily helpful throughout this process. Also supporting the work have been several research assistants, currently graduate and law students at Harvard University and New York University (NYU) School of Law. The views expressed do not reflect the views of any organization or the U.S. Government.

Dave Aitel
Sophia d'Antoine
Alexei Bulazel
Winnona DeSombre
Isabella Garcia-Camargo
Thomas Garwin
Ian Roos
Nicholas Rostow
Abraham Wagner

August 20, 2022

Executive Summary

This study is based on open source materials. It utilizes a large body of data collected by the research team to examine China's strategy, tactics, and operations in cyberspace as well as Internet communications in Chinese software development and cyber operations. China's interest in cyber grew rapidly in response to what it observed in U.S. military operations starting with Operation Desert Storm in 1991. By 2013, China emphasized cyberspace as a crucially important area in the struggle with principal competitors and adversaries such as the United States and the West more generally.

At present, China's cyber capabilities and operations have increased exponentially to the point where they pose a highly significant national security threat to the United States and all China's perceived adversaries. China continues to invest huge sums in this technology path. It is clear that the threat will continue to become even greater than it now is.

China's starting point with respect to international competition in the cyber arena, as in all other things is control: ***controlling dissent and competition through controlling information*** while supporting its indigenous entrepreneurs and industries. Theft of intellectual property, personal data, state secrets, and espionage form a central part of China's approach to achieving information domination.

In the past 20 years, China revised its cyber objectives to include offensive capabilities and adapted its structures in line with them, undertaking major reorganizations to support these evolving objectives. These dramatic changes and details of the Chinese cyber threat are not well understood or appreciated; they need to become a central part of the U.S. national security discourse with respect to cybersecurity.

- From late 2015 through 2016, the People's Liberation Army (PLA) modernized through reorganization, consolidating previously dispersed units under the Strategic Support Force (SFF).
- China issued new, extensive laws, policies, regulations, and standards to bolster a cyber governance regime designed to enhance control of information.
- China adapted a strategy of Military-Civil Fusion managed by the Chinese Communist Party (CCP) Central Commission for Military-Civil Fusion Development, chaired by President Xi, to enhance cross-sector integration with a view to dominating the multi-billion dollar cyber economy, including with respect to cybersecurity.

China's methods include the promotion of emerging technologies, coordination with higher education, and exploitation of intellectual property and options financing. China prioritizes coordination of space, cyber, and electronic warfare as strategic weapons. It integrates private actors with government and, since 2015, has increasingly replaced criminal hacking groups with

domestic professionals. China also has coopted free-lancers—criminal elements and hackers—on whose patriotism China can rely, while increasingly looking to more conventional, university-developed talent.

The Chinese government entered the competition for talent and has used a number of incentives, including money and positions, to achieve success. China also developed world class cybersecurity schools that emphasize artificial intelligence among other emerging technologies. Seven universities in particular, known as the Seven Sons of National Defense, feed PLA capabilities.

Evolution of China's Cyber Strategy

For more than a century, Chinese leaders have seen the value of greater access to technology and information to support their national objectives and military capabilities. The Chinese Communist Party (CCP) has always understood the importance of controlling information for domestic control and in competition and conflict. Starting in the 1970s, China moved to acquire technologies in order to collect, store, process, and manage information, with the result most visible in areas such as 5G (communications) and AI (artificial intelligence).

China has been operating below the threshold of direct confrontation and at a level of visibility that reflects major advances made in this area. China has used the technology base as an opportunity to radically shape the national ecosystem and exploit it in new and innovative ways. The personal use of connected devices, such as mobile phones, laptops, and others, and social media and other applications provide the means to use the technology base for information and control.

The Chinese government has implemented a number of applications that track individuals and their behavior. Users are able to access Chinese sites, or versions of U.S. sites, but the government monitors and controls interactions with servers and sites outside China.

The technology has also enabled espionage operations on a scale never before imagined. Operations include theft of intellectual property, extraction of personal data, and penetration of strategic systems—activities going well beyond the traditional intelligence mission of stealing secrets for national security purposes. China's targets include vast amounts of data and access to protected networks as well as commercial enterprises to make China more competitive in world markets. As part of their long-term competition with the United States, the Chinese government and CCP view collection and hoarding of information as an investment in the future. It is a strategic aim, not merely a near term tactic.

In the area of cyberwarfare, the western governments see cyberspace as a "fifth domain" of warfare. The Chinese, however, look at cyberspace in the broader context of information space. The ultimate objective is, not "control" of cyberspace, but control of information*,* a vision that dominates China's cyber operations.

Organization of China's Cyber Operations

China's cyber operations have undergone extensive reorganization. As part of its modernization effort, beginning in December 2015 and throughout 2016, the PLA consolidated previously decentralized cyber units into the SSF to improve the PLA's combat capabilities. This effort transformed China's cyber operations from loosely linked operators focused on access to trade secrets into a professional intelligence service engaged in cyber operations to defend critical infrastructure, conduct espionage, and prepare for combat. In addition to the SSF, two civilian ministries, the Ministry of State Security (MSS) and the Ministry of Public Security (MPS), make up the main Chinese state entities engaged in cyber operations.

China also developed an extensive cyber governance regime to maintain control over the domestic flow of information and influence over cyberspace internationally. This regime is comprised of laws, policies, regulations, and standards overseen by several departments under the guidance of the Central Cyberspace Affairs Commission.

The Chinese strategy of "Military-Civil Fusion" (MCF, 军民融合) is designed to facilitate cooperation between China's civilian, commercial, and military and defense sectors and develop the PLA into a "'world class military' by 2049." Expansive in scope, the strategy includes everything from efforts in big data and infrastructure to logistics and national defense mobilization. Domains that have been prioritized for development are cyberspace, security and informatization, biotechnology, and artificial intelligence.

Cybersecurity and Informatization Bodies

- *Central Cyberspace Affairs Commission (CCAC, also known as the Central Commission for Cybersecurity and Informatization CCCI))*: The CCAC was formed in 2014 to integrate the "fragmented bureaucratic structures and policy areas" that had previously composed China's approach to cyber.

- *Cyberspace Administration of China (CAC, 国家互联网信息办公室)*: The CAC is responsible for handling cyberspace and Internet content, enforcing the PRC's various data regulations, and managing information infrastructures, personal data protection, and data security.

- *Strategic Support Force (SSF, 战略支援部队)*: The SSF is a theatre command-level organization that centralizes the military's strategic space, cyber, electronic, and psychological warfare missions.

- *Ministry of State Security (MSS, 国安部*): The MSS is China's main civilian intelligence and anti-espionage authority responsible for domestic and foreign intelligence operations, including human intelligence and cyber operations. It can compel Chinese citizens and organizations to engage in and support intelligence activities.

- *Ministry of Public Security (MPS, 公安部)*: The (MPS) oversees all provincial and local police departments, with responsibility for supervising public information networks, public security work and policing. It shares the counterintelligence mission with, and is directed by, the MSS.

- *Ministry of Industry and Information Technology (MIIT, 工业和信息化部)*: The MIIT is responsible for China's network infrastructure and assigned to tackle issues of data security.

Chinese Cybersecurity Laws

- *Cybersecurity Law (CL)*: The CL was the first of several regulations governing data protection in China and establishes requirements for data storage, as well as guidelines for maintaining network security, and also authorizes government authorities to conduct security checks of networks.
- *Data Security Law (DSL)*: The DSL governs data collected and stored in China and determines the requirements for its storage and transfer depending on its potential impact on national security. It also prohibits Chinese organizations and individuals from transferring data stored in China to the justice or law enforcement institutions of foreign countries without approval.
- *Personal Information Protection Law (PIPL)*: The PIPL is a legal framework designed to regulate how companies collect, process, and transfer personal data and applies to entities that collect, store, use, transmit, provide, or otherwise handle personal information of persons within the PRC, even if that entity is located or conducts business entirely outside of China. It also requires entities that handle critical infrastructure information, and which process a "large amount of personal information" to store personal information within China.

China's Offensive Cyber Security Landscape

As China's quest to become a superpower evolves, Beijing has moved to eliminate barriers between its civilian-commercial industries and the state. Technology firms, particularly domestic cybersecurity enterprises, increasingly stand at the forefront of their fields, offering insight and services that constitute an important intellectual, personnel, and hardware resource for China's government and military even while operating under increasing government restrictions.

Cybersecurity experts have also moved from large firms and established their own companies. A survey of selected Chinese cybersecurity firms indicates specific areas of focus, backgrounds of their founders, and, in some cases, their partners and investors. Most of these firms are dedicated to vulnerability research, threat detection, and security intelligence. Their services offer clients protection from offensive cyber activities. A growing number of these firms also emphasize blockchain security. While their investors are predominantly Chinese venture capital firms, these companies service clients and maintain partnerships around the world. The PLA, China's security services, and policymakers increasingly use this ecosystem to support their cyber operations.

The trajectory of China's cyber industry is closely related to the proliferation of firms engaged in cybersecurity research. As part of its MCF approach, China's leadership has emphasized the need to foster innovation in domestic technologies and has called on private enterprises to contribute to the security of the state and its citizens. People embedded in China's cybersecurity industry stress that start-ups and smaller firms are an important source of this innovation and will continue to play a formative role in China's national cyber strategy.

China's cybersecurity firms operate under rigid constraints. The government touts the strategic benefits of keeping knowledge of vulnerabilities close to home, noting that vulnerabilities are no longer of use once exposed publicly by Chinese hacking teams at competitions. China therefore discourages its security researchers from participating in hacking competitions abroad, particularly those where zero-day vulnerabilities may be publicly disclosed.

Industry leaders in China see their cybersecurity universe as unique. They expect growth to continue to outpace overseas counterparts. Cybersecurity firms, particularly those dealing with personal data security, zero trust, cloud security, and privacy, are more likely to receive funding from the government, state-owned enterprises, and publicly listed companies than other candidates for Chinese government funding.

Cyber Personnel Recruitment and Operations

Competition in cyberspace is, ultimately, a competition for talent. Historically, China has recruited talented cyber personnel by appealing to hackers' patriotism roots and by co-opting existing criminal hacking collectives. China also recruited early generation hackers from universities into the PLA and other government institutions. More recently, China has emphasized professionalism in cybersecurity with education reforms to develop elite institutions, fostering extensive military-civil fusion and militia programs, as well as bolstering relationships with the private sector.

University Recruitment and Involvement in Cyber Operations

Like Western institutions that have trouble fitting gifted, self-educated cyber experts into conventional institutions and institutional categories, China's behavior suggests that Beijing also prefers personnel with a traditional profile. Since 2015, China has sought to replace its criminal hacking groups with domestic professionals. The CCP recognizes that talent is essential to the country's cyber efforts and improving education is central to cultivating this talent, in addition to attracting overseas Chinese talent. Chinese universities develop top talent, conduct sensitive research programs in tandem with or funded by the government, and act as recruitment pipelines for the PLA, MSS, and related contractors.

China's recruitment efforts in cyber are part of a larger effort to recruit expertise in a variety of national security areas. The "Thousand Talents" Plan, for example, attempted to reverse the brain drain of Chinese scientists and academics who studied and remained overseas by incentivizing them to return to China. The Ministry of Education and Central Cyberspace Administration (CAC) also launched an initiative to develop World Class Cybersecurity Schools (一流网络安全学院) to cultivate domestic cybersecurity programs that would allow the country to grow its pool of cyber talent.

China's universities intentionally produce graduates capable of attacking and defending networks, regardless of how they are ranked. Two of the 11 World Class Cybersecurity Schools, Wuhan University and Huazhong University jointly created the National Cybersecurity School at the National Cybersecurity Talent and Innovation Base (国家网络安全人才与创新基地, the National Cybersecurity Center), which also contains two government-focused laboratories.

Academic links to China's military and defense industry run deep. The government has established 29 national defense science and technology laboratories (国防科技重点实验室) in civilian universities, supervised by the PLA. In addition, 36 national defense labs (国防重点学科实验室) and 53 Ministry of Education defense labs (教育部国防重点实验室) operate out of nonmilitary universities. These schools graduate thousands of students who join organizations engaged in defense research every year.

In addition to training next generation offensive cyber talent and conducting cutting edge research on behalf of government ministries, Chinese universities have engaged in cyberattacks and conduct espionage. The APT1 hackers attributed to PLA Unit 61398 had connections to the PLA Information Engineering University (PLAIEU). Members of Unit 61398 were linked to Shanghai Jiao Tong University and likely recruited graduate students for the Unit from Zhejiang University's College of Computer Science and Technology.

The MSS operates the University of International Relations in Beijing and Jiangnan Social University. The MSS uses designated faculty elsewhere for intelligence purposes. The MSS works closely with other universities for training, conducting research, and cyber activities. Faculty at Hunan University and Tianjin University have been designated as MSS experts and awarded prizes by the ministry.

Military Recruitment and Military Civil Fusion

In most offensive cyber campaigns, the PLA relies on contractors; in its earlier efforts in offensive cyber, the PLA recruited hackers. With the reorganization of the military in 2015 and 2016, many of China's cyber operations were transferred from the PLA to the MSS.

The PLA Strategic Support Force (SSF) began civilian recruitment in 2018 but has suffered from issues in hiring and retaining civilian talent. Salary discrepancies and differences in culture between the SSF and the private sector likely make the SSF a less appealing place to work for domestic information security professionals. China has tried to circumvent this problem by eliminating barriers between China's civilian research and commercial sectors, and its military and defense industrial sectors.

The PLA recruits civilians with cyber expertise into a militia reserve force to supplement the regular military. While these reserves would likely be limited to logistics espionage, rather than offensive operations, this force reportedly numbers over 10 million. Military-civil fusion and the militia reserve force help the PLA exploit the civilian sector while retaining control over targeted offensive cyber campaigns.

The Role of Chinese AI in Open Source Code

Open source software (OSS) development solicits input from its community of users through technical standards meetings, code submissions, and online discussions, typically small communities that are targets for adversarial influence campaigns and software supply chain attacks. China exploits this regime and especially the Linux operating system to leapfrog development and to penetrate and manipulate the open code. There is no established trust metric to vet accounts or individuals that submit code. An attacker may contribute to the code libraries and submit deliberately vulnerable code or functional backdoors that will be exploited after the code adopted.

China has developed a robust open source community that chips away at the security of U.S. software. Much of the world's software relies on open source code that is freely available online and that may be redistributed and modified. Multiple open source libraries have been deliberately or accidentally corrupted by maintainers and developers, in China and elsewhere. China has open source code in its sights for malicious operations or operations designed to give advantages to China in its struggle with the United States and others.

By 2020, some 87% of Chinese companies were using open source software. GitHub, a primary platform for open source worldwide, features a large number of Chinese repositories with most major open source projects supported by Chinese companies. Alibaba, PingCAP, Baidu, Tencent, JD, and Huawei are the top six Chinese accounts on GitHub. Worldwide, China is second only to the U.S. in the number of GitHub users and contributors.

The volume of Chinese contributions to Western open source software has skyrocketed. In 2021, Huawei beat out Intel as the top contributor to the Linux Kernel. This software is the baseline of Western technologies like Google's Android, NASA's satellite software, and the Army's Common Operating Environment. Huawei has also contributed code to over 40 mainstream Western technical communities, including Kubernetes, OpenStack, Hadoop, TensorFlow, httpd, and MySQL.

Chinese military leaders want to use AI for offensive cyber operations. An analysis of 343 AI-related contracts executed by the PLA in 2020 shows a focus on procuring AI for intelligence, information warfare, and navigation and target recognition in autonomous vehicles. Military academics in China also look to use AI for stealth, scale, and adaptability in information operations, as well as for hyper-targeted phishing attacks.

President Xi Jinping's stated goal in AI—to pursue both world leadership and self-reliance in AI technology—is in line with China's use of open source technologies. Open source is also featured in China's AI innovation plans. The MIIT New Generation AI Innovation Key Task List contained a task on "open source, open platforms," to use open source and expand the number of data sets, models, and users for machine learning technologies.

China circumvents an overreliance on proprietary Western software by utilizing open source alternatives. After the United States sanctioned Huawei in 2019, the firm was barred from importing most U.S.-made chips and was no longer able to use the Android operating system in their phones. Subsequently, the United States has sought to prevent investment in Huawei and other Chinese companies with connections to the defense sector.

Preempting Chinese Cyber Operations

The present effort to discover suspicious cyber activity uses new AI techniques to create an analysis pipeline that surfaces highly significant insights about Chinese contributions to the Linux kernel, including the HULK robot. The analysis pipeline consists of a technology stack that ingests the Linux Kernel Mailing List (LKML) and the Linux Git repository, annotates the data, and then creates graphs of the annotated data searchable by analysts. Thus far, it has been possible to analyze the 36,000 contributors to the Linux kernel, highlighting 30 individuals exhibiting suspicious behavior, of which several are known to have submitted "hypocrite commits" that introduced exploitable vulnerabilities to the kernel. The individuals highlighted by the algorithm exhibit the same type of behavior, allowing analysts to explore this behavior in far greater detail than previously possible.

The HULK Robot is not the only automated bug-finding tool belonging to Chinese institutions. The Chinese government funds university labs conducting automated bug hunting in the Linux Kernel, which likely has a defensive purpose, but can easily be transferred to, or shared with, the larger Chinese national security community conducting research on offensive cyber activities.

Defending Against Chinese Deception and Misinformation

Apart from defending against China's espionage and other data collection efforts, the United States and its allies must anticipate and deflect the strategic use of deception and misinformation. Such tactics have often been employed throughout China's political and military history. The historical failure to take these tactics seriously has inflated China's ability to succeed where they decide to compete. This this aspect of the Chinese culture goes back for generations, and it is not well-known or understood in the West. Indeed, it is one of the main reasons Beijing has been so successful.

China's use of deception and misinformation in the cyber area multiplies the country's political and economic advantages. The Chinese government's control over domestic cyber operations includes sophisticated deception operations with regard to the outer world. The United States is not likely to be able to determine how much China has shaped the content of data. Knowing that China has "official" uses of cyber technologies does not itself enable the United States to drill into China's cyber landscape and understand it fully. A new approach is needed.

Hacker conferences, where "hacker" is not synonymous with "criminal," constitute an important source of knowledge about vulnerabilities and threats as well as innovations. Such conferences, especially those focused on security, offer ideal venues for recruiting and a space for government organizations, private companies, established hacking groups, and up-and-coming individuals to network. Sponsored by both the government and large tech companies such as Baidu, Alibaba, and Venustech, conferences like XPwn2017 and Tianfu Cup are often used by the PLA and MSS to recruit university students and other individual hackers.

Cutting off the exchange of knowledge between U.S. and Chinese cyber industries would undermine the ability of service providers to protect their products and network infrastructures and would also undercut visibility into changing developments in potential offensive cyber activities. But domestic cyber enterprises, as in most countries, also play a vital role in providing infrastructure, talent, and resources to State operations, sometimes by choice, sometimes under legal and political pressure.

1. Introduction

For the past century, Chinese leaders have seen the value of greater access to technology and information to support their national objectives and military capabilities.[1] The Chinese Communist Party (CCP) has always understood the importance of controlling information for purposes of domestic control and achievement of global ambitions. The essential role of information in China's policy with respect to competition and conflict is well-documented as a matter of China's national policy.[2]

Starting in the 1970s, China moved to acquire microelectronics, computer, and communications technology in order to collect, store, process, and manage information. The result is visible in areas such as 5G (communications) and AI (artificial intelligence) technology. During the 1990s, China developed a greater interest in the area of cyber warfare, which it then termed "information warfare;" China closely observed how these new technologies supported U.S. military operations in the Gulf War, Kosovo Afghanistan, and Iraq.[3]

These observations led China to adjust their military strategy with the goal of "winning local wars under conditions of informationization." By 2004, this concept had become central to China's warfighting doctrine and developing capabilities. China's 2013 *Science of Military Strategy* study emphasized that cyberspace had become a new and essential domain of the military

[1] See Dean Cheng, *Cyber Dragon: Inside China's Information and Warfare Operations* (Santa Barbara: Praeger, 2017), Michael Pillsbury, *The Hundred Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt & Co., 2015), Nick Beecroft, *The West Should Not Be Complacent About China's Cyber Capabilities* (Washington: Carnegie Endowment for International Peace, July 6, 2021), Gordon G. Chang, *The Great U.S.-China Tech War* (New York: Encounter Books, 2020) and Anthony H. Cordesman, *China: The Civil-Military Challenge,* (Washington: Center for Strategic and International Studies, January 4, 2022).

[2] See State Council Information Office, *Tenth Five Year Plan for National Economic and Social Development, Informationization Key Point Special Plans* (October 18, 2022), http://www.cia.org.cn/information/_01xxhgh_3.htm. See also Zheng Weiping and Liu Minfu, *Discussion on the Military's New Historic Missions* (Beijing: People's Armed Police Publishing House, 2005). This evolved as part of Plan 863. See Evan Feigenbaum, *China's Techno-Warriors* (Stanford: Stanford University Press, 2003).

[3] See Lyu Jinghua, *What Are China's Cyber Capabilities and Intentions?* (Washington: Carnegie Endowment for International Peace, April 1, 2019) and China State Council, *New Generation Artificial Intelligence Development Plan* (Beijing, July 2017). See also Katharin Tai and Yuan Yi Zhu, "A historical explanation of Chinese cybersovereignty," *International Relations of the Asia-Pacific* (2022) and Nicholas Lyall, "China's Cyber Militias," *The Diplomat* (March 1, 2018).

struggle. The point also was made in the 2015 *China's Military Strategy* issued by the Ministry of National Defense.[4]

For some time, China has been open about its path, developed in response to what China has seen taking place in both the United States and Russia.[5] The Chinese military cyber strategy is consistent with domestic policies supporting economic competition and controlling dissent. China's peacetime strategy for cyber operations can be characterized as controlling information at home and stealing secrets abroad.

China has exploited technology in new and innovative ways. Paradoxically, technologies that in the West were hailed as democratizing access to information have in China become instruments of government control. The explosive growth in personal use of connected devices, such as mobile phones, and laptops, and social media and other applications provided the means of information control.

Within China, users are able to access Chinese sites, or versions of U.S. sites, while the government monitors and controls interactions with servers and sites outside China. Most recently the Chinese government has implemented a number of applications that track individuals and their behavior.

Internationally, China has been operating below the threshold of direct confrontation yet at a level of visibility that reveals major advances in cyber capabilities. Technology has enabled theft of commercial, military, and personnel secrets on a scale previously unimagined. Encompassing both telecommunications and Internet operations, China's worldwide efforts include the theft of intellectual property, extraction of personal data, and penetration of strategic systems.[6]

These activities go well beyond the intelligence mission of stealing secrets for national security or military purposes. They target vast amounts of wide-ranging data and access to large numbers of protected networks. These activities support China's surveillance of its own people and commercial enterprises that may or may not be owned by the state or government officials and military officers.

China takes a holistic approach to information collection. Unlike U.S. intelligence agencies that collect data for national security purposes, China uses the data collected to support national security missions and commercial enterprises in an effort to enhance their competitiveness. Exactly how successful this effort will be is an open question. As with other espionage operations,

[4] This official military document also defined for the first time cyberspace as a new domain of national security and international competition and looked at security threats to their own cyber infrastructure.

[5] Chinese military analysts frequently quote a RAND Corporation study stating that cyber warfare is strategic warfare in the information age, as was nuclear warfare in the 20th century. See Timothy R. Heath, *U.S. Strategic Competition with China: A RAND Research Primer* (Santa Monica: The RAND Corporation, November 16, 2021), and Joe McReynolds, (ed.), *China's Evolving Military Strategy* (Washington: The Brookings Institution, 2016).

[6] See Beecroft, *op. cit.* Examples cited here are the mass exploitation of vulnerabilities in the Microsoft Exchange Server (2021), theft of data on millions of U.S. citizens connected to the government, and theft of secret data on the F-35 fighter jet.

the answer lies not in the volume of information collected, but rather in what operational value can be obtained from what is collected.

The Chinese themselves have repeatedly said that they are engaged in a long-term competition with the United States. They view the large-scale collection and hoarding of information as an investment in the future. It is a strategic aim, not merely a tactic for the near term.

China has a different perspective on cyberspace from western nations. Whereas the United States and its friends and allies have come to see cyberspace as a "fifth domain" of warfare, along with land, sea, air and more recently space, the Chinese look at cyberspace in the broader context of information space, where the ultimate objective is not "control" of cyberspace, but rather ***control of information***. This vision dominates their operations both domestically and internationally.

In addition to defending against China's espionage and other data collection efforts, the United States, its friends, and allies must anticipate and deflect the PRC's strategic use of deception and misinformation.[7] Although these tactics have often been employed throughout China's political and military history, other governments do not seriously address them.[8] This failure inflates China's ability to succeed in those areas in which it decides to compete. This aspect of the Chinese strategic culture goes back for generations, is not generally well-known or understood in the West, and has contributed to Beijing's international success.

China's use of deception and misinformation in the cyber area multiplies the country's political and economic advantages. The Chinese government's control over domestic cyber operations includes sophisticated deception operations with regard to the outer world. The United States is not likely to be able to determine how much China has shaped the content of data. Knowing that China has "official" uses of cyber technologies does not itself enable the United States to drill into China's cyber landscape and understand it fully. A new approach is needed.

The DARPA Social Cyber Initiative

A central objective of the DARPA Social Cyber program has been to understand the culture and the anthropology of the software development process, specifically focusing on protecting open-source software (OSS) from insertions of malicious code. As part of this effort, researchers have analyzed various ways in which personnel who engage in the development of malicious code

[7] See Lucian W. Pye and Nathan Leites, *Nuances in Chinese Political Culture* (Santa Monica: The RAND Corporation, November 1970), Susan D. Blum, *Lies That Bind: Chinese Truth, Other Truths* (Lanham: Rowan & Littlefield, 2007), and Miles Maochun Yu, *Understanding China's Strategic Culture Through Its South China Sea Gambit* (Stanford: Hoover Institution, May 2011).

[8] The Cox Committee—the House Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, 105th Congress, 2d Session, Report 105-851, March. 25, 1999 devoted three volumes to Chinese theft of nuclear weapons design information and high technology from companies, often with the connivance of corporate management, in pursuit of long-term Chinese strategic objectives. A substantial number of other works written before and since the Cox Committee Report have stressed the same themes. See, e.g., Wang Jisi, "The Plot Against China? How Beijing See the New Washington Consensus," *Foreign Affairs* (July/Aug. 2021), 48-57.

and OSS projects are recruited and trained in China, especially, but also Russia, North Korea, and Iran.

China is unique in that it has a large and growing high-tech sector that produces products that are embedded in networks and systems throughout the world. These companies have apparently legitimate needs for intimate involvement with global open-source software development but also close ties to the government and military establishment. The potential for malicious activity through embedded hardware and software is obvious.

China's cyber operations and capabilities have progressed at a pace previously unseen and on a scale well beyond what has been reported within the U.S. national security community.[9] China's effort goes beyond malicious and offensive cyber operations undertaken by the military (PLA). China has outsourced some offensive cyber operations to commercial entities, offering a far larger talent pool. The expanded scope of cyber operations includes theft, exploitation of data for national security and commercial activities, and exploits and other malicious cyber tools supporting an expanded cyberwarfare capability.

This activity represents a serious national security concern worthy of far greater attention in both the policy and technical domains. Current research has found that Chinese cyber capabilities are greater than previously supposed. The nature of the threat and operational components have resisted identification by traditional intelligence methods, as the source data do not form part of the usual collection regime. AI analytical tools, such as those used in this study, rely on a major software development effort that has been an integral part of the DARPA program.

The present analysis considers the operational mechanisms by which such malicious code is and can be distributed by these actors or their surrogates.[10] In each case, the effort involved the search of open-source source materials, with native-language speakers as part of the effort. The study used software tools to extract and analyze the available data. The research team has worked to identify and characterize code inserted into the Linux kernel and other software utilities by developers in China and the other threat countries and to develop methods that recognize signatures of malicious code insertion.

The effort aims to tie specific individual actors, identified by email addresses or other identifiers, to the code inserted. The result provides real-time indications and warning and crucially important information that should inform the development of targeted responses.

[9] See, for example, Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the Peoples Republic of China 2021* (October 2021). This recent report on China barely mentions the growing cyberwar threat. It does note, however, that "the PRC is advancing its cyberattack capabilities and has the ability to launch cyberattacks—such as disruption of a natural gas pipeline for days to weeks—in the United States." See also, Lauren Kahn, What the Defense Department's 2021 China Military Power Report Tells Us About Defense Innovation," *Lawfare* (February 15, 2022).

[10] An important objective of the DARPA SocialCyber program is to understand the culture and the anthropology of the software development process with regard to malicious code and OSS projects, considering the "models" or ways in which personnel who engage in the development of malicious code and OSS projects are recruited and trained.

Hacking and Hacking Competitions

Cybersecurity or "hacking" competitions are contests in which participants are tasked with finding and exploiting vulnerabilities in software, hardware, or networks in exchange for monetary prizes. In contrast to "black hat" hackers, who break into networking systems for nefarious reasons, typical participants in these competitions are white hat hackers, who look for vulnerabilities in computer systems in order to help businesses identify, and ultimately repair, security failings.[11]

Well-known examples of these competitions include Pwn2Own[12], a biannual contest in Vancouver where previous winners have hacked into Windows, Mac OS X, iOS, Android, and other software and hardware, at the Defcon convention consisting of several different competitions, as well as presentations where hackers and experts share discoveries.[13] Several universities[14] and private businesses[15] conduct competitions of their own, and U.S. government and military departments host a variety as well.[16]

These competitions are an integral part of a healthy and flourishing cyber industry in any country. Teams that participate in network security competitions typically share exploits with software and hardware providers so that the companies can then fix any vulnerabilities[17] Moreover, competitions create an opportunity for hackers to come together and exchange knowledge and discoveries, providing a shared space for innovation in cybersecurity.

Teams from China have historically dominated at these competitions,[18] but several factors have limited their access to contests overseas, including logistical restraints, the Chinese

[11] Dan Rafter, "What is the difference between black, white and gray hat hackers?" *Norton* (February 25, 2022), https://us.norton.com/internetsecurity-emerging-threats-black-white-and-gray-hat-hackers.html.

[12] Brian Gorenc, "Pwn2Own Vancouver returns for the 15th Anniversary of the Contest," *Zero Day Initiative* (January 12, 2022), https://www.zerodayinitiative.com/blog/2022/1/12/pwn2own-vancouver-2022-luanch.

[13] "DEF CON Hacking Conference Home," accessed August 18, 2022, https://defcon.org/.

[14] CARE Lab, "2022 SE Event Theme: The CARE Lab is Hit with Ransomware," Temple University, accessed August 18, 2022, https://sites.temple.edu/socialengineering/2022-se/ransomware/; "Collegiate Penetration Testing Competition," Rochester Institute of Technology, accessed August 18, 2022, https://cp.tc; "CSAW," NYU Tandon School of Engineering, accessed August 18, 2022, https://www.csaw.io.

[15] "Facebook CTF," accessed August 18, 2022, https://www.facebook.com/officialctf.

[16] "US Cyber Challenge: Cyber Quests Spring 2022," accessed August 18, 2022, https://uscc.cyberquests.org/; "CyberForce Program," Department of Energy, accessed August 18, 2022, https://cyberforce.energy.gov; "Hack the Pentagon," *HackerOne*, accessed August 18, 2022, https://www.hackerone.com/hack-the-pentagon.

[17] Publicly disclosing these bugs incentivizes tech companies to actually repair them, rather than sweep them under the rug J.D. Work, "China Flaunts its Offensive Cyber Power," *War on the Rocks* (October 22, 2021).

[18] Michael Mimoso, "Keen Team of China Takes Down Safari and Flash at Pwn2Own," *Threatpost* (March 13, 2014), https://threatpost.com/keen-team-of-china-takes-down-safari-and-flash-at-pwn2own/104790/;

government's desire to develop the domestic cybersecurity industry, and concerns that vulnerabilities would no longer be of use once publicly exposed in foreign competitions, ceding a potentially useful strategic resource.[19]

In addition to Beijing now largely prohibiting Chinese citizens from participating in overseas hacking competitions[20] and requiring those that do participate to disclose any discovered vulnerabilities to the government ahead of time,[21] private sector enterprises have developed several hacking competitions within China.[22] The military and government historically have conducted several of these contests and continue to do so.[23]

The most well-known of these competitions, the Tianfu Cup, was established directly in response to the desire to keep "hackers and their knowledge" within China, offering large monetary prizes in exchange for exploits.[24] The contest is backed by the country's major tech enterprises .[25] Participants in past competitions have been able to infiltrate prominent Western networks, such as Google Chrome, iOS, Safari, and Microsoft Exchange.[26]

The vulnerabilities demonstrated in the Tianfu Cup may be exploited before they are publicly exposed in competition, as it is "almost certain" that the Chinese government receives access to exploits before they are made public through the contest.[27] As these vulnerabilities lose

Swati Khandelwal, "Chinese Hackers won $215,000 for Hacking iPhone and Google Nexus at Mobile Pwn2Own," The Hacker News (October 27, 2016), https://thehackernews.com/2016/10/hacking-team-pwn2own.html.

[19] 韩大鹏, 周鸿祎:马云提新零售 我想了几个月想到了"大安全", 新浪科技 (September 12, 2017), https://perma.cc/EFD6-SRSS; Cyberspace Administration of China, 360：自觉担当责任维护网络安全 (November 11, 2018), https://perma.cc/ENA2-WZ3F..

[20] Yingzhi Yang, "China discourages its hackers from foreign competitions so they don't help others," *South China Morning Post* (March 21, 2018).

[21] See, for example, Patrick Howell O'Neill, "How China built a one-of-a-kind cyber-espionage behemoth to last," *MIT Technology Review* (February 28, 2022).

[22] "国家网络安全宣传周", accessed August 18, 2022, http://www.zzctf.com/#schedule; "Real World CTF," accessed August 18, 2022, https://realworldctf.com.

[23] Dakota Cary, "Robot Hacking Games," *CSET* (September 2021).

[24] O'Neill, "How China built a one-of-a-kind cyber-espionage behemoth to last."

[25] Included here are Qi An Xin, Cyber Kunlun, Huawei, Baidu, Alibaba, Qihoo 360, Tsinghua University, the Chinese Academy of Sciences, NSFocus, TopSec, Venustech, Asiainfo Security, and Clover Sec. "天府杯," accessed August 18, 2022, http://www.tianfucup.com.

[26] Jamie Tarabay, "China Shows Its Hacking Prowess at $2 Million Contest," *Bloomberg* (October 29, 2021).

[27] Work, "China Flaunts its Offensive Cyber Power."

their potency once publicly disclosed, as there is usually only a short window before they are repaired.[28]

Hacking competitions such as the Tianfu Cup serve an important signaling role for China, demonstrating "the continued ability to hold key Western systems and networks at risk, highlight[ing] the substantial depth of China's offensive cyber inventories, and show[ing] off a talent base of aggressive hackers undeterred by blowback from international exposure of its activities."[29] Participants in the competition also appear to be "mindful of the potential military and intelligence utility of their work," with one even comparing their research to the PLA's hypersonic weapons development.[30]

While contests like the Tianfu Cup do provide an opportunity for China to demonstrate its strength in cybersecurity, it is more beneficial to the U.S. to maintain the international and collaborative nature of its own competitions. These competitions not only provide insight into existing vulnerabilities in network systems, but also novel methods and techniques developed by hackers which are essential to the U.S. and its allies, as they continue to provide opportunities for hackers from China to participate in hacking competitions held within those countries. To do otherwise would inhibit the United States' ability to learn about the innovations developed by Chinese hackers.

These competitions also provide an opportunity to recruit cyber talent from China. Some reports indicate that competitors in the Tianfu Cup have not been able to obtain meaningful employment in China and have instead sought to find work in western States.[31] While it is important to remain alert for exploitation or espionage, there is an opportunity for the United States to attract cyber talent from China.

Here the U.S. must balance preventing security threats with retaining foreign talent. Current efforts "to protect research security" and anti-Asian sentiment "are jeopardizing the appeal of the United States as a magnet for international talent," with more than half of faculty of Chinese origin considering leaving the U.S., a potentially tremendous loss of skill and talent.[32]

[28] Notoriously, Google researchers determined that a vulnerability in the iPhone operating system disclosed in the 2018 Tianfu Cup was used in a hacking campaign targeting Uyghurs in the two months between the competition and Apple's repairs. O'Neill, "How China built a one-of-a-kind cyber-espionage behemoth to last."

[29] Work, "China Flaunts its Offensive Cyber Power."

[30] *Ibid.*

[31] *Ibid.*

[32] Jessica Chen Weiss, "The China Trap: U.S. Foreign Policy and the Perilous Logic of Zero-Sum Competition," *Foreign Affairs* (September 2022), https://www.foreignaffairs.com/china/china-trap-us-foreign-policy-zero-sum-competition.

2. China's Motivations and Strategy

Authoritarian countries such as China, Russia, Iran, and North Korea threaten U.S. infrastructure, elections, supply chains, and network security. Without a serious, substantial commitment to make "revolutionary leaps ahead in cyberspace," the United States can never hope to deter "bad actors."[33] While cybersecurity experts disagree on how best to understand and counter the threats, many have sounded the alarm, pointing to a "growing threat of cyber-attacks" from foreign governments.[34] The biggest threat, according to FBI Director Christopher Wray, comes from the People's Republic of China (PRC).[35] The Office of the Director of National Intelligence echoed this concern in its 2022 Annual Report, calling China "the broadest, most active, and persistent cyber-espionage threat to U.S. Government and private sector networks."[36]

Because cybersecurity is often a game of catch-up, where one appears to always be a step behind those engaging in offensive cyber activities, understanding the motivations behind a hostile offensive actor can help develop more effective methods of response, including deterrence, than presently exists. Such methods can be based, not only on technical responses, but on social, economic, and other alternative approaches derived from granular knowledge of the problem and its sources. China does not offer an exception to this logic.

Offensive cyber activities are always grounded in the real world; as a result, they are tied to the geopolitical realities that prompt states to act. Understanding China's national cyber strategy and its role in China's broader national security and political strategies and goals therefore is indispensable to an effective U.S. cybersecurity response.

Looking at China's historical trajectory and development in the area, as well as public statements by officials and other actors, provides insight into the PRC's approach to information communication technologies and how it has changed over time. This knowledge can help build a better understanding of how and why Beijing makes the decisions it does when it comes to cyberspace.

[33] See John Ratcliffe and Abraham Wagner, "U.S. Needs New 'Manhattan Project' to Avoid Cyber Catastrophe," *Newsweek* (May 18, 2022), https://www.newsweek.com/us-needs-new-manhattan-project-avoid-cyber-catastrophe-opinion-1706557.

[34] Jalen Small, "U.S. Intel, Google Warn of Cyberattacks from China, Russia, North Korea," *Newsweek* (April 28, 2022), https://www.newsweek.com/us-intel-google-warn-cyberattacks-china-russia-north-korea-1701553.

[35] *Ibid.*

[36] *ODNI Report on Best Practices to Protect Privacy, Civil Liberties, and Civil Rights of Americans of Chinese Descent in the Conduct of U.S. Intelligence Activities* (May 31, 2022). https://www.dni.gov/index.php/newsroom/reports-publications.

Elements of China's Cyberstrategy

There are two general elements to China's cyber strategy. Within the country, there has been a shift towards the development and professionalization of the domestic cyber industry and, more recently, a push to integrate this industry into the national security apparatus. Internationally, the PRC has focused on investing in physical and legal/political infrastructures, including international institutions, as a means to "legalize," or at a minimum formalize, the PRC's preferred conditions for cyberspace.

A national narrative that sees China's cyber decisions as responsive to and compelled by hostile actions by the United States and its allies towards an entirely innocent China drives these shifts. China's reliance on domestic censorship and surveillance, which means that China is unable to relinquish control over the internet within its borders, undergirds its cyberspace decisions.

Understanding how these two elements shape China's cyber strategy is critically important, not only to see where China's policies in cyberspace come from, but also to anticipate the direction the country may take, particularly in light of its expansion of population controls during the COVID-19 pandemic and its ostensible support of Russia's invasion of Ukraine. It is also essential for the United States to develop its own effective cyber strategy.

The current U.S. approach of naming, shaming, and indicting members of advanced persistent threats (APTs) has done little to deter offensive cyber campaigns. Actors based in China continue to use or reuse already identified infrastructure to engage in additional, antagonistic cyber campaigns. The United States might be better served by supplementing its existing actions with a concentrated effort to facilitate the development of information communication technology (ICT) infrastructures and engaging more proactively in international institutions beyond the United Nations to affect the standard and norm-setting processes of international cyber rule-making.[37]

China's Changing Cyberstrategy

In 2013, as a result of observed U.S. and Russian practices, China made cyber warfare an essential part of its military strategy. This decision went beyond its previous understanding of "informatization" as important to defense and stability in the 1990s. From 2013 to 2019, China incorporated cyber operations into its stated strategy of "Active Defense" to supplement its defensive capabilities in the event of an offensive cyber strike against the country. Starting in 2013, China has invested heavily in this capability. At the same time, Beijing has also invested in offensive cyber capabilities and related cyber espionage activities supporting national security, domestic surveillance, and businesses competing internationally.

In more recent years, China has shifted from an orientation denominated "peaceful rise" to direct strategic competition with the United States. A 2019 CSIS White Paper still touted promoting peaceful cooperation with regional countries but highlighted that China's evolving

[37] There is substantial debate whether norm-setting or international rule making is of any use, as much of what takes place in the cyber arena is espionage and criminal activity where such norms are not possible. See generally, Abraham Wagner and Nicholas Rostow, *Cybersecurity and Cyberlaw* (Durham: Carolina Academic Press, 2020).

military capabilities served as "a clear warning of growing strategic rivalry between an existing and emerging superpower."[38]

China continues to pursue a more assertive stance against what it sees as the efforts of the United States to stifle and contain its growth."[39] Under Xi Jinping, the Chinese Communist Party (CCP) has sought to expand its own national power by molding China into a "Cyber Great Power." Although the meaning of this moniker has evolved over time, Stone and Wood have identified three consistent components of this strategy: cyberspace governance, cybersecurity, and informatization.[40] China also understands that advancing these components both domestically and abroad is necessary to becoming a Cyber Great Power.[41]

As part of its efforts to develop its technological security objectives, the CCP has adopted a strategy of "Military-Civil Fusion" (MCF, 军民融合). MCF seeks to facilitate cooperation between China's civilian, commercial, and military and defense sectors to streamline technological innovation and develop the PLA into a "'world class military' by 2049."[42] The strategy aims to unify the military, research institutions, commercial enterprises, and government and defense agencies to allow the government to pursue a variety of strategic priorities.[43]

It is "startlingly expansive in scope, including everything from efforts in big data and infrastructure to logistics and national defense mobilization."[44] Included among the domains that have been prioritized by the CCP for development are Cyberspace and Security and

[38] Anthony Cordesman, *China's New 2019 Defense White Paper* (Washington: Center for Strategic and International Studies, July 24, 2019).

[39] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*, *Annual Report to Congress* (2021).

[40] Alex Stone and Peter Wood, *China's Military-Civil Fusion Strategy* (China Aerospace Studies Institute and BluePath Labs, 2020), https://static1.squarespace.com/static/5e356cfae72e4563b10cd310/t/5ee37fc2fcb96f58706a52e1/1591967685829/CASI+Chin%20a%27s+Military+Civil+Fusion+Strategy-+Full+final.pdf, and Lyall, *op. cit.*

[41] For example, China launched a "Global Data Security Initiative in 2020 that it hoped would "provide a blueprint for the formulation of international principles on data security." Graham Webster and Paul Triolo, "Translation: China Proposes 'Global Data Security Initiative'," *New America* (September 7, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-proposes-global-data-security-initiative/.

[42] U.S. Department of State, *Military-Civil Fusion and the People's Republic of China* (January 5, 2022).

[43] Emily S. Weinstein*, Testimony before the U.S.-China Economic and Security Review Commission on "U.S. Investment in China's Capital Markets and Military- Industrial Complex,"* (Washington: Center for Security and Emerging Technology, March 19, 2021), https://www.uscc.gov/sites/default/files/2021-03/Emily_Weinstein_Testimony.pdf.

[44] Elsa B. Kania and Lorand Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*, (Washington: Center for New American Security, January 28, 2021), https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy.

Informatization, Biotechnology, and Artificial Intelligence.[45] MCF is managed by the CCP Central Commission for Military-Civil Fusion Development (中央军民融合发展委员会), which is personally chaired by Xi. The Commission reports to the CCP Politburo and the Standing Committee of the Politburo. Many provincial and municipal governments have also formed local MDF development committees.[46]

This strategy of cross-sector integration was apparent in the most recent three-year draft plan released by the Ministry of Industry and Information Technology (MIIT).[47] Highlighting the country's progress in 5G, big data, artificial intelligence, Internet of vehicles (IoV), industrial internet, and the internet of things (IoT), the plan proposed a series of principles and objectives to facilitate China's cybersecurity development and turn the country into a "manufacturing powerhouse and a cyber powerhouse." The plan emphasizes the need for coordination between the market and the government.[48] Under this plan, the MIIT expects the value of the cybersecurity industry to exceed 250 billion RMB (approximately $39 billion) by 2023.

The plan proposes a number of initiatives for promoting security applications of emergent technologies and deepening government integration into the industry. The measures include increasing investment, adopting intellectual property and options-based financing models, promoting cybersecurity companies by means of consultation and financing, monitoring corporate finances and operations, coordinating with higher education enterprises to strengthen cybersecurity curricula, and carrying out industrial vocational skill improvement campaigns.

China considers cyberspace to be the connective tissue of its growing military capabilities and cyberspace superiority to be *essential* to compete with the United States. The PLA prioritizes "the coordinated employment of space, cyber, and EW as strategic weapons" as both an offensive means—to disrupt an adversary's operational system—and as a critical component of strategic deterrence, either by means of targeted strikes or collecting data for intelligence purposes.[49] The Chinese military is actively integrating information technologies, such as AI, cloud computing, and big data analytics, in anticipation of the requirements of future warfare.

[45] Alex Stone and Peter Wood, *China's Military-Civil Fusion Strategy* (China Aerospace Studies Institute and BluePath Labs, 2020). https://static1.squarespace.com/static/5e356cfae72e4563b10cd310/t/5ee37fc2fcb96f58706a52e1/1591967685829/CASI+Chin%20a%27s+Military+Civil+Fusion+Strategy-+Full+final.pdf.

[46] Interview with Greg Levesque, *China's Military-Civil Fusion Strategy*, The National Bureau of Asian Research (June 30, 2021), https://www.nbr.org/publication/commercialized-militarization-chinas-military-civil-fusion-strategy/.

[47] Cybersecurity Administration of the PRC and Ministry of Industry and Information Technology, *Open Solicitation of Opinions on the Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021-2023)* (Ben Murphy ed., Etcetera Language Group, Inc. trans., CSET 2021), https://cset.georgetown.edu/wp-content/uploads/t0381_cyber_3_year_plan_draft_EN.pdf.

[48] *Ibid.,* 3.

[49] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*, *Annual Report to Congress* (2021).

This commitment to the adoption of advanced technologies, along with the centralization of cyber units within the PLA, the increasing frequency of Chinese threat activity groups, and the shift in public rhetoric towards more open confrontation with the United States suggests that Beijing feels increasingly confident with the ability of its cyber entities to withstand confrontation.

Towards International Cyber Rulemaking

China has long bristled at the need to comply with established international conventions, viewing itself at a structural disadvantage to the western states that built these institutions even though China participated in the creation of every international institution. This story-line holds that the United States and its allies have used their dominance in the global arena (and in particular in market institutions) to exploit and treat China unfairly. Commentators and public figures in China have bemoaned the country's relative lack of *huayuquan* (话语权, discourse power)—the "influence generated by the concepts, logic, values, and ideology contained in the country's arguments and discourse."[50] The CCP, and in particular Xi Jinping, has repeatedly expressed its dissatisfaction with the international governance regime and voiced its desire to reshape the global system to one that better reflects the "PRC's state-centric, authoritarian model."[51]

The PLA has emphasized the use of global influence as a critical element of warfare, suggesting that, because "social opinion has already become an important factor in determining the war situation contested by both sides," the military should target cognitive dominance as a means to influence the perceptions of an opposing state's leadership in the case of war.[52] Contradictions do not bother the Chinese government. At the same time that it complains about the existing international legal order, China benefits from it, and has benefited greatly from the existing "liberal international order," selectively engaging with international institutions, principles, and markets, largely to its advantage.[53]

As a result of these attitudes, China has adopted several different tactics aimed at increasing its influence in international norm-setting institutions and "reforming" the global governance system in a way that better reflects China's worldview.[54] Chinese tactics reflect a persistent tension in China's international engagement, in which the country seeks to remain integrated with

[50] Kamo Tomoki, *Institutional Discourse Power and the New Five-Year Plan*, The Kazankai Foundation (Aug. 6, 2020), https://www.kazankai.org/politics_list.php?no=0, quoted in Yatsuzuka Masaaki, "China's Efforts to Seize Control of Discourse Power in Cyberspace," *Asia-Pacific Review* (March 18, 2022).

[51] Daniel W. McLaughlin, "Rewriting the Rules: Analyzing the People's Republic of China's Efforts to Establish New International Norms," *Journal of Indo-Pacific Affairs* (March 8, 2021).

[52] Xiao Tianliang, *Zhanluexue* [Science of Military Strategy] (National Defense University Press 2015), *quoted in* Yatsuzuka Masaaki, "China's Efforts to Seize Control of Discourse Power in Cyberspace," *Asia-Pacific Review* (March 18, 2022).

[53] Jessica Chen Weiss and Jeremy L. Wallace, "Domestic Politics, China's Rise, and the Future of the Liberal International Order," *International Organization* (February 2021).

[54] Elizabeth Economy, "Xi Jinping's New World Order," *Foreign Affairs* (January 2022), https://www.foreignaffairs.com/articles/china/2021-12-09/xi-jinpings-new-world-order.

the global world order while "protecting Chinese independence and national security" and using its power on the international stage in ways all students of international relations find familiar.[55]

Given the relative novelty of cyber technologies and the lack of established regulations and norms governing their use, cyberspace provides a unique opportunity for the PRC to improve its international *huayuquan*, influence international affairs, and create a rule regime that is favorable to its own interests. China's proposed rules for cyberspace, in addition to parroting the need for cooperation and a shared commitment to international peace and security, call for a commitment to state sovereignty, that is, recognition that boundaries are not to be permeable unless a state wishes its boundaries to be permeable, as the core international rule in cyberspace.[56]

Sovereignty, while obviously essential for all states, provides a bulwark for authoritarian states against other states asserting rights or the defense of rights that threaten to undermine state control. In contrast to the perspective that requires some individual human rights to be upheld above all others, most authoritarian and some democratic states emphasize that human rights can only be asserted within the boundaries of state power—thus state requirements for national security, stability, and the like can supersede individual rights.

Cybersovereignty would recognize that a state has the right to control information communication technologies and data within the state's territories free from the interference of other states.[57] While nearly all states recognize an interest "in being able to lay claim to sovereignty over certain parts of the Internet"—such as accessing data for law enforcement or restricting offensive content—China's understanding of cybersovereignty tends toward the "extreme end of a continuum."[58]

Thus, in China there is no individual right, such as the right to free speech or free access to information, that can justify the intrusion of another state into China's internal affairs. While many democratic countries assert that the internet should be free and open to global traffic, advocates of a more absolute conception of cybersovereignty, such as China and other authoritarian states, emphasize a territorially bound approach.[59]

From this perspective, international principles, norms, and laws should reinforce the state's right to control cyberspace within its territory and occasionally outside its borders as well when its

[55] Katharin Tai and Yuan Yi Zhu, "A Historical Explanation of Chinese Cybersovereignty," *International Relations of the Asia Pacific* (2022).

[56] Ministry of Foreign Affairs, *China's Positions on International Rules-making in Cyberspace* (October 10, 2021), https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html.

[57] *Ibid.*

[58] Tai and Yi Zhu, *A Historical Explanation of Chinese Cybersovereignty*, *op. cit.*

[59] Justin Sherman, *How Much Cyber Sovereignty is Too Much Cyber Sovereignty?*, (New York: Council on Foreign Relations, October 30, 2019), https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty. For competing views of the sovereignty issue see Jack Goldsmith, "The Internet and the Abiding Significance of Territorial Sovereignty," *Indiana Journal of Global Legal Studies* (1998).

sovereignty is threatened. China calls for information and communications technology (ICT) product and service providers to prevent the installation of malware on their systems or other means that can be used to obtain personal information or "manipulate users' systems and devices" and presses these providers to commit to notifying partners and users about ICT system vulnerabilities.[60]

In many ways, China's promotion of cybersovereignty is merely an extension of its commitment to the supremacy of state power and the CCP over all else. China's sense of urgency is much stronger when it comes to cyber than with respect to other areas unless it is Taiwan or the South China Sea: the CCP always has seen regulating information as indispensable to its power to control.[61] China's desire to maintain its existing censorship structures and retain its ability to assert control over information sits at the center of its ideas about cybersovereignty.

It is not merely that China relies on the idea of sovereignty to justify the Great Firewall, but rather that, as an authoritarian state, the idea of sovereignty itself cannot be readily unbound from the state's need to control. The state must be able to intervene when activists post critiques,[62] when CEOs become too outspoken,[63] and when repressed populations refuse to conform[64]—to allow otherwise, as political officials fear it, threatens the very idea of the state itself. Because of this fear for the supremacy of the government an CCP, China places sovereignty at the center of proposed principles for international cyber law, fearing that if "conventional international laws" were applied, it would make censorship more difficult.[65]

Cybersovereignty undergirds several of China's domestic cyber policies, particularly those targeting the dispersion of information and data. The 2017 Cybersecurity Law requires certain types of data to be stored within the country and authorizes government authorities to conduct security checks of network systems.[66] The 2021 Data Security Law makes it illegal for Chinese organizations and individuals to transfer data stored in China "to the justice or law enforcement institutions of foreign countries" without prior approval from Chinese government officials.[67] The

[60] Ministry of Foreign Affairs, *China's Positions on International Rules-making in Cyberspace.*

[61] Tai and Yi Zhu, *A Historical Explanation of Chinese Cybersovereignty*, *op. cit.*

[62] Amy Qin, A "Prominent Chinese-American Artist Is the Latest to Fall Afoul of China's Censors," *New York Times* (November 20, 2019), https://www.nytimes.com/2019/11/20/arts/design/china-censorship-arts-hung-liu.html.

[63] Sam Peach, "Why did Alibaba's Jack Ma disappear for three months?," *BBC* (March 20, 2021).

[64] John Sudworth, "Xinjiang Police Files: Inside a Chinese Internment Camp," *BBC* (May 24, 2022), https://www.bbc.co.uk/news/resources/idt-8df450b3-5d6d-4ed8-bdcc-bd99137eadc3.

[65] Yatsuzuka Masaaki, "China's Efforts to Seize Control of Discourse Power in Cyberspace," *Asia-Pacific Review* (March 18, 2022).

[66] Lauren Maranto, *Who Benefits from China's Cybersecurity Laws*, (Washington: Center for Strategic and International Studies, June 25, 2020).

[67] Bezanson, et al, "China's New Data Privacy Law is Sweeping and Serious: Avoid the High Cost of Noncompliance," *The National Law Review* (August 24, 2021),

2021 Personal Information Protection Law, similar to law in other countries, enforces data localization requirements for the personal information of persons within the borders of the PRC.[68]

The National Intelligence Law requires any organization or citizen within China or Chinese organizations outside of the country to support Chinese intelligence services by providing access to data, infrastructure, or any other resources the government deems necessary to protect national security.[69] In addition, the 2021 Regulations on the Management of Network Product Security Vulnerabilities require domestic and foreign individuals and organizations to report zero-day vulnerabilities to the MIIT within 48 hours of discovery.

The regulations forbid actors from sharing vulnerabilities with organizations and individuals abroad. Alibaba Cloud was in fact recently disciplined by Chinese authorities when one of its engineers reported a "world-threatening software vulnerability related to Log4j" to the nonprofit maintaining the software without notifying the MIIT, which became aware of the problem a couple of weeks later through another report.[70]

Although many of these requirements are not unusual for states seeking to implement data protection regimes for individuals within the country, in China, they are part of a larger system of censorship and information control aimed at suppressing dissent. To preserve the Party's dominion over information, China seeks to retain absolute control over its data infrastructures and has advocated global cybersecurity principles that would bolster its efforts at control.

In order to promote the adoption of its proposed cyber rules and to increase its international influence, China has made concerted efforts in regional and international institutions to advance principles supporting this position, particularly in standard setting bodies. In the United Nations, for example, the Shanghai Cooperative Organization (SCO), led by the PRC, has proposed an international code of conduct emphasizing national sovereignty while cautioning against outside intervention.[71]

China has taken other measures in global institutions to further its goals. It joined with Russia to establish an "Open-Ended Workgroup Group for the cyber normative processes in the

https://www.natlawreview.com/article/china-s-new-data-privacy-law-sweeping-and-serious-avoid-high-cost-noncompliance.

[68] Roger Creemers and Graham Webster, "Translation: Personal Information Protection Law of the People's Republic of China," *DigiChina* (August 20, 2021), https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

[69] *Military and Security Developments Involving the People's Republic of China*, Office of the Secretary of Defense (2021), https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF; 中国人民代表大会， 中华人民共和国国家情报法 (2018), http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml.

[70] Zeyi Yang, "Beijing punishes Alibaba for not reporting Log4j loophole fast enough," *Protocol* (December 22, 2021), https://www.protocol.com/bulletins/alibaba-cloud-log4j.

[71] Masaaki, "China's Efforts to Seize Control of Discourse Power in Cyberspace," 19.

UN," which aims to develop international norms for governing cyberspace.[72] Beijing has placed Chinese nationals in "high-level posts in international organizations," including the International Telecommunication Union (ITU), which is led by Zhou Houlin.[73] China has simultaneously pushed to give more authority to ITU.

China published a policy notice indicating its plan to become more involved in standards organizations, including the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).[74] Beijing is attempting to shape the global internet governance regime to favor its preferred principles and uses increased contributions to international organizations' budgets as an argument for increased political influence.

In addition to advocating cybersovereignty, China views protecting and ensuring access to critical ICT infrastructure as a central tenet of its proposed rules for cyberspace.[75] Cyber is often spoken about in the abstract, but it is always anchored in the real world. Cyberspace cannot exist without its underlying physical infrastructure—cables, servers, computers, electricity, etc. Control of the physical infrastructure therefore conveys ultimate power over cyberspace itself—the power to dictate its shape, form, execution, and, above all, the power to turn everything off.

The way these physical infrastructures are conceived and constructed carries forward into the future, establishing the parameters for how cyberspace can be shaped and used. Almost all global data, for instance, flows through undersea cables, which typically utilize the routes of telegraphic cables, which in turn were laid by past imperial powers to facilitate communication between home countries and their colonial outposts or, in the case of transatlantic cables to facilitate communication and commerce among friendly states with similar economic systems and political values.[76] States have good reason to worry that foreign suppliers of communications equipment with embedded software could be used for espionage at any time and to deny service to some or all users during a crisis or wartime.[77]

This reality has not been lost on the United States and China. Both have balked at the threat of foreign influence on critical domestic information technology infrastructures while simultaneously recognizing the opportunity to project influence by facilitating the expansion of these infrastructures in developing states. China has pointed to the "unbalanced development and widening digital divide among countries" as a central concern when considering international rules-making in cyberspace and has accused other countries, predominately the United States and

[72] *Ibid.*

[73] *Id.* at 20.

[74] *Id.* at 21.

[75] Ministry of Foreign Affairs, *China's Positions on International Rules-making in Cyberspace.*

[76] Roxana Vatanparast, "The Infrastructures of the Global Data Economy: Undersea Cables and International Law," HARVARD INTERNATIONAL LAW JOURNAL (2020); and Nicole Starosielski, *The Undersea Network* (Durham: Duke University Press, 2015).

[77] William Yuen Yee, *With U.S. Restrictions on Huawei and ZTE, Where Will Rural America Turn?* (Washington: Center for Strategic and International Studies, December 10, 2020).

its allies of "willfully suppress[ing] other States' ICT enterprises and impos[ing] unfair and unjust barriers on global ICT supply chain and trade."[78]

For example, after Canada followed the United States and banned Huawei and ZTE equipment from its 5G network based on national security concerns, Chinese officials vowed retaliation and accused the Canadian government of "acting in collusion with the United States to suppress Chinese enterprises."[79] As the Chinese government sees it, limiting the ability of Chinese tech companies to participate in foreign markets is a tactic borne out of U.S. fears of China's growth. Given this view of western policy as constraining China and maintaining domination of technological infrastructures, the PRC:

(1) feels justified in retaliating to these measures, and

(2) recognizes that control of the physical infrastructures for data is a prerequisite to uncontested participation in, and control over, global technology markets.

Consequently, in addition to its drive to improve its authority in international political and legal institutions, China has pursued a variation of its "dual circulation" approach to information communication technologies fostering domestic capabilities to reduce its reliance on others while simultaneously promoting the export of its tech products and services to other states.[80] With regard to the latter, China seeks to increase its influence over global ICT infrastructures by building information communication technology projects in other countries through its Belt and Road Initiative (BRI)—the "biggest infrastructure undertaking in the world."[81] Xi Jinping views the BRI as "as a conduit through which China can transmit its political and cultural values."[82] This effort has led China and some 146 other states to sign memoranda of understanding.[83]

As part of the BRI, the Digital Silk Road (DSR) provides assistance in "telecommunications networks, artificial intelligence capabilities, cloud computing, e-commerce and mobile payment systems, surveillance technology, smart cities, and other high-tech areas" to

[78] Ministry of Foreign Affairs, *China's Positions on International Rules-making in Cyberspace.*

[79] Chinese Embassy Ottawa (@ChinaEmbOttawa), *Twitter* (May 20, 2022), https://twitter.com/ChinaEmbOttawa/status/1527731501240025089; *CBC News*: The National, China Reacts to Canada Banning Huawei from 5G network, *YouTube* (May 20, 2022), https://www.youtube.com/watch?v=fhMVo778aFs.

[80] David Sacks, "What is China Learning From Russia's War in Ukraine," *Foreign Affairs* (May 16, 2022), https://www.foreignaffairs.com/articles/china/2022-05-16/what-china-learning-russias-war-ukraine.

[81] *Assessing China's Digital Silk Road Initiative* (New York: Council on Foreign Relations, December 18, 2020), https://www.cfr.org/china-digital-silk-road/; OECD, *China's Belt and Road Initiative in the Global Trade, Investment and Finance Landscape*, OECD Business and Finance Outlook (2018), https://www.oecd.org/finance/Chinas-Belt-and-Road-Initiative-in-the-global-trade-investment-and-finance-landscape.pdf.

[82] Economy, "Xi Jinping's New World Order."

[83] Green Finance & Development Center, *Countries of the Belt and Road Initiative*, https://greenfdc.org/countries-of-the-belt-and-road-initiative-bri/#.

participating countries through Chinese technology companies, such as Huawei and ZTE.[84] Within the DSR framework, Chinese companies and financiers have played a critical role in funding and building telecommunication infrastructures in several countries in Africa, Asia, South America and other regions, and Chinese technology firms have captured an increasingly larger portion of several technology markets.[85] For example, in 2021, two Chinese companies, Hikvision and Dahua, supplied nearly 40 percent of surveillance cameras worldwide, reaching more than 80 countries.[86]

Although not without difficulties, the BRI has been successful in, not only providing China with a foothold in investment-hungry countries, but also garnering support for other pursuits on the international stage. When the U.N. Human Rights Council debated the merits of the Hong Kong National Security Law, the 53 countries in support of China were mostly developing countries in which China had invested or that wanted Chinese investment, while the 27 that criticized its position were predominantly "industrialized Western countries."[87] Chinese investment through BRI has also led many in Southeast Asia and Africa to perceive Chinese economic influence as greater than that of the United States, even though overall U.S. investment in each region outpaces that of China.[88]

China's presence and investment in these countries have contributed greatly to its soft power, although missteps, onerous repayment terms, and corruption can engender resentment from local populations. The BRI and DSR in particular have given China direct access to physical infrastructure, especially maritime ports and information communication technology networks, in partnering states, bolstering the PRC's global logistics and operations network and allowing China to have a foothold in critical infrastructure within the country. This access not only can improve China's political capital in international norm-setting institutions by generating support, but also ensures that China has technological access worldwide.

[84] *Assessing China's Digital Silk Road Initiative* (New York: Council on Foreign Relations, December 18, 2020), https://www.cfr.org/china-digital-silk-road/.

[85] Motolani Agbebi, *China's Digital Silk Road and Africa's Technological Future*, (New York: Council on Foreign Relations, February 1, 2022), https://www.cfr.org/blog/chinas-digital-silk-road-and-africas-technological-future.

[86] Reconnecting Asia, *Mapping China's Digital Silk Road* (October 19, 2021), https://reconasia.csis.org/mapping-chinas-digital-silk-road/; Richard Ghiasy and Rajeshwari Krishnamurthy, "China's Digital Silk Road and the Global Digital Order," *The Diplomat* (April 13, 2021), https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/. Many of which were laid by Huawei in coordination with a U.K. company. Hengtong Group, was the fourth largest provider of undersea cables. The Beidou satellite navigation system has been adopted by several countries in Asia, Africa, and the Middle East.

[87] Masaaki, "China's Efforts to Seize Control of Discourse Power in Cyberspace,“ 26.

[88] Jennifer Hillman and David Sacks, *China's Belt and Road: Implications for the United States* (New York: Council on Foreign Relations, March 2021), https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/findings.

China's Cyber Strategy After COVID and Ukraine

Prior to the coronavirus pandemic, China's trajectory in cyber was centered on the areas articulated above: improving domestic technology industries and local ICT infrastructures to limit the country's dependence on other states and promoting international principles and standards that prioritized principles of state sovereignty and non-interference. While China remains committed to these positions, the pandemic, subsequent economic woes, and Russia's invasion of Ukraine have shifted calculations. Alarm at Sinophobic attitudes in the West, particularly in response to the coronavirus and now sabre rattling over Taiwan, and the "hawkish stance" of Washington, has driven a rise in patriotic and nationalist attitudes in young Chinese citizens.[89]

Simultaneously, however, the CCP has leaned heavily on xenophobic conspiracy theories to explain the spread of the coronavirus within the state, blaming the virus on everything from lobsters imported from Maine[90] to mail sent from South Korea.[91] Jockeying among government departments and a commitment to pursuing "common prosperity" drove a crackdown on local tech firms, with the state fining several companies, including Alibaba, Tencent, Baidu, and ByteDance, for antitrust violations and disciplining others under data privacy regulations. Didi's car service app was suspended in China a mere two days after its initial public offering in the United States for failing to complete a cybersecurity review with the CAC. The company's investors recently voted to delist in the United States in an effort to revive business in China.[92]

China has extended technology-enabled social control measures during the COVID-19 pandemic with smartphone apps determining where people can go based on their COVID status. The government can manipulate the COVID status to restrict travel for reasons unrelated to COVID. According to a recent report, local authorities prevented fraud victims from travelling to recover funds from a bank in the hinterland by altering COVID status in this way.

Russia's 2022 invasion of Ukraine "confirm[ed] Chinese leaders' belief that they are entering a more dangerous era and that they must prepare for a greater likelihood of war."[93] Cognizant of the havoc that Western sanctions have played on Russia's economy, China has moved to decrease its own vulnerability to possible sanctions, including forbidding senior Party

[89] Cheng Li, How *Washington's Hawkish China Policy Alienates Young Chinese*, (Washington: The Brookings Institution, November 4, 2021), https://www.brookings.edu/opinions/how-washingtons-hawkish-china-policy-alienates-young-chinese/.

[90] Olivia Solon, Keir Simmons and Amy Perrette, "China-linked Disinformation Campaign Blames Covid on Maine Lobsters," *NBCNews* (October 21, 2021), https://www.nbcnews.com/news/china-linked-disinformation-campaign-blames-covid-maine-lobsters-rcna3236.

[91] "China Says Imports Are Causing Outbreaks of Covid-19," *Economist* (April 21, 2022), https://www.economist.com/china/2022/04/21/china-says-imports-are-causing-outbreaks-of-covid-19.

[92] Brian Liu and Raquel Leslie, "China's Tech Crackdown: A Year-in-Review," *Lawfare* (January 7, 2022), https://www.lawfareblog.com/chinas-tech-crackdown-year-review; Chang Che and Jeremy Goldkorn, "China's 'Big Tech Crackdown': A Guide," *SupChina* (August 2, 2021), https://supchina.com/2021/08/02/chinas-big-tech-crackdown-a-guide/.

[93] Sacks, "What is China Learning From Russia's War in Ukraine."

officials, as well as their spouses and children from holding overseas assets,[94] and has noted which countries have not joined sanctions.[95]

Xi Jinping and other public officials in China have taken increasingly frequent steps to push for unification with Taiwan including hardline public statements,[96] purportedly asserting that the Taiwan Strait is not international waters,[97] limiting mainland tourism to the island, conducting military exercises along the coast in 2022, and allegedly sponsoring hackers to interfere with Taiwan's elections in 2020.[98] These actions and perceptions likely will only further accelerate China's defense spending and commitment to improving its military capabilities.[99]

China's domestic and international attitudes and behavior suggest that Beijing feels an increased sense of urgency about global instability and competition. Xi Jinping appears to be consolidating more central control over state apparatuses—although there have been some grumblings—and is willing to use them to advance his vision.[100] One result has been a rise in the number of targeted offensive cyber campaigns against U.S. network systems from actors based in

[94] Chun Han Wong, "China Insists Party Elites Shed Overseas Assets, Eyeing Western Sanctions on Russia," WALL STREET JOURNAL (May 19, 2022), https://www.wsj.com/articles/china-insists-party-elites-shed-overseas-assets-eyeing-western-sanctions-on-russia-11652956787.

[95] Sacks, "What is China Learning From Russia's War in Ukraine. Many Taiwanese worry that they might be the next to suffer an invasion by a more powerful neighbor. Those fears are not unreasonable. While Ukraine and Taiwan differ in many ways, as relatively young democracies living alongside larger authoritarian neighbors with long-standing designs on their territory, the two face strikingly similar strategic predicaments.

[96] *Ibid.*

[97] *Ibid.*

[98] *Ibid.*

[99] See Hua Chunying (@SpokespersonCHN), TWITTER (May 23, 2022) (stating that "the core and essence of the one-China principle or one-China policy is "one China" in reference to Taiwan), https://mobile.twitter.com/SpokespersonCHN/status/1528737191056543745.

[100] See Colum Murphy and Philip Glamann, "Mixed Messages From China Leaders Feed Speculation of Split," BLOOMBERG (May 10, 2022). The authors suggest that public statements by Xi Jinping and Li Keqiang indicated "divergent views within the system on Covid and its impact," but noting that Xi still "remains in firm control of the levers of power." See also, Paul Mozur, Joy Dong and Isabelle Qian, "Students Protest Covid Lockdowns at Elite Beijing University," *The New York Times* (May 16, 2022) (pointing to a number of sporadic protests in response to lockdowns in Shanghai and other cities as part of China's zero-Covid strategy).

.

China. The Department of Justice has been able to connect a number of such actors to hacking groups with links to PRC government departments.[101]

Mandiant reported that 2021 saw more zero-day vulnerabilities exploited than ever before, primarily by state-sponsored groups from China.[102] They also determined that APT41, a hacking group associated with the MSS, had exploited several zero-day vulnerabilities, including Log4J mere hours after its disclosure, "to compromise the networks of at least six U.S. state governments."[103] Several members of APT41, two of whom were arrested, were previously indicted in 2019 for compromising the network systems of over 100 companies in the United States and abroad.[104]

For the United States, these realities should be alarming. China's domestic rhetoric and increased military build-up indicate that there is no end in sight to "strategic competition." The increase in hacking attacks also suggests that U.S. efforts to deter and deflect foreign sponsored offensive cyber campaigns are having little to no effect. Defend Forward, the current U.S. strategy for cyber, emphasizes "operating[ing] in cyberspace outside the United States" against adversaries "before they could do harm."[105] It also stresses public attribution of cyberattacks in conjunction with more "tangible actions, such as sanctions and indictments," in order to impose operating costs on the malicious actors in question.[106]

Whether or not any costs arise is doubtful, particularly in the case of China, as threat groups such as APT41, even after being indicted, continue to operate with little compunction or constraint. Beijing has long protested the U.S. attribution methodology, seeing it as a kind of coercive diplomacy aimed at tarnishing the country's reputation for little reason other than that China

[101] See, for example, *United States v. Ding Xiaoyang, et al.,* No. 21-cr-1622 (S.D. CA, May 28, 2021). See also Garrett Hinck and Tim Maurer, "What's the Point of Charging Foreign State-Linked Hackers?" *Lawfare* (May 24, 2019).

[102] James Sadowski, *Zero Tolerance: More Zero-Days Exploited in 2021 Than Ever Before*, (Mandiant, April 21, 2022), https://www.mandiant.com/resources/zero-days-exploited-2021.

[103] Derek B. Johnson, "Chinese APT Leveraged Zero Days — including Log4j — to Compromise US State Governments," *SC Media* (March 8, 2022), https://www.scmagazine.com/analysis/apt/chinese-apt-leveraged-zero-days-including-log4j-to-compromise-u-s-state-governments.

[104] *United States v. Lizhi, et al,* No. 20-cr-158 (D.C. DC, 2020). See also, Department of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally*, (September 16, 2020), https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

[105] David Vergun, "Leaders Discuss DOD's Cyber Strategy to Protect America, Partners," *DOD News* (December 6, 2021), https://www.defense.gov/News/News-Stories/Article/Article/2862784/leaders-discuss-dods-cyber-strategy-to-protect-america-partners/. See also, Emma Schroeder, Stewart Scott, and Trey Herr, *Victory reimagined: Toward a more cohesive US cyber strategy,* (Washington: Atlantic Council, June 14, 2022).

[106] Jon Bateman, *The Purposes of U.S. Government Public Cyber Attribution*, (Carnegie Endowment, March 28, 2022), https://carnegieendowment.org/2022/03/28/purposes-of-u.s.-government-public-cyber-attribution-pub-86696.

engages in active hackism as a state policy.[107] After all, alternative and more direct communication channels between the two countries exist, and, from China's perspective, they are being shamed for activities for which there are no established international norms of conduct and in which the United States itself engages.[108]

In this context, Beijing puts to one side the principle of non-interference in the internal affairs of another State, which China extols when it suits it. It is not pedantry in this connection to recall Thucydides' mantra for all aggressors: "the strong do what they have the power to do and the weak accept what they have to accept."[109]

Non-state Chinese actors appear to be following in the footsteps of their foreign counterparts, publishing a report calling out U.S. NSA malware on the Linux platform.[110] Some maintain that this step will "improve geopolitical stability" by decreasing China's "sense of vulnerability due to lack of capability."[111] The argument holds that a lack of "visibility into adversary activity" breeds paranoia and may incentivize first strike attacks. The hope is that improving visibility on both sides of the equation can mitigate paranoia.[112]

The argument is less persuasive when speaking of public attribution accusations made by the U.S. government, as officials often withhold evidence for attribution as classified information, which, from the perspective of China, may make the accusation appear frivolous or unfounded. "Ill-substantiated" public attribution can in fact exacerbate miscommunications or degrade consensus-building among states, as it relies on "the vacuum of applicable rules" dictating standards for evidence when accusing another state of a cyberattack.[113]

[107] Those indicted are outside U.S. jurisdiction and are highly unlikely to ever stand trial. See Hinck and Maurer, *What's the Point of Charging Foreign State-Linked Hackers?, op. cit.* Since 2013 the Department of Justice has brought 24 cases and 195 counts against 93 foreign nationals for state-linked hacking activity, mostly Chinese. Defendants in none of these cases have appeared, as they are outside U.S. jurisdiction and cannot be extradited, and there have been no convictions.

[108] Lu Chuanying, *A Chinese Perspective on Public Cyber Attribution*, (Washington: Carnegie Endowment, March 28, 2022), https://carnegieendowment.org/2022/03/28/chinese-perspective-on-public-cyber-attribution-pub-86699.

[109] Thucydides, *History of the Peloponnesian War* (Rex Warner Trans., London, 1954, 1972), 402.

[110] *Top-tier Backdoor of US NSA Equation Group*, Pangu Lab (February 2022), https://www.pangulab.cn/files/The_Bvp47_a_top-tier_backdoor_of_us_nsa_equation_group.en.pdf.

[111] Richard Bejtlich (@taosecurity), *Twitter* (February 23, 2022), https://twitter.com/taosecurity/status/1496486704395567115.

[112] Lorenzo Franceschi-Bicchierai, "Chinese Cybersecurity Company Doxes Apparent NSA Hacking Operation," *VICE* (February 23, 2022), https://www.vice.com/en/article/v7dxg3/chinese-cybersecurity-company-doxes-apparent-nsa-hacking-operation.

[113] Fan Yang, *The Problem With Ill-Substantiated Public Cyber Attribution: A Legal Perspective*, Carnegie Endowment (March 28, 2022), https://carnegieendowment.org/2022/03/28/problem-with-ill-substantiated-public-cyber-attribution-legal-perspective-pub-86695.

Thus, China's approach involves staunch defense against foreign penetration while engaging in foreign penetration for its own account. The United States has to shape its response to meet this reality, which a one-dimensional Defend Forward strategy simply does not do. China's two-dimensional approach to cybersecurity suggests that the United States should center its cybersecurity response in the same areas.

While this response would not require the United States to abandon its Defend Forward strategy entirely, the decision to focus on competing with China has led it to prioritize developing domestic cyber capabilities while downgrading the importance of effective engagement in international institutions. A result is that China appears to have a free hand in this field of endeavor. The consequences predictably will be grave for the United States and allies.[114]

U.S. strategy is not comprehensive. Combined with the decentralization of cyber operations across the U.S. government, it has led to a U.S. cyber approach that is of questionable effectiveness, relying for effectiveness to too great an extent on domestic law enforcement. Of course, law enforcement is an important part of any strategy. But, as in the areas of counter-terrorism, espionage, covert operations, and military operations, it should not be the only instrument. A heavy legal focus has been largely criticized already, as almost all criminal cases brought against Chinese and other foreign actors have never gone to trial as the named defendants are outside U.S. jurisdiction.

At the same time the United States may be better served by concentrating more effort in affecting the international "rule of law" by engaging more directly with international and regional institutions, not merely with money, but with personnel, and by investing more directly in developing allied ICT infrastructure—again, not merely with money, but with personnel, equipment, and direct support. If Defend Forward seeks to match China in cybersecurity, it must do so on all fronts, not just in response to cyberattacks.

The Role of Deception and Misinformation in Chinese Cyber Strategy

The use of false, misleading, and deceptive information has played a critically important role in China's military strategy for generations, going back to ancient times. Chinese literature from Sun Tzu through Mao Zedong has emphasized deception more than most other military doctrines.[115] In contrast to many other militaries, however, which typically view the use of deception as an ancillary tactic in support of the larger goal of defeating an opponent in direct

[114] Abraham Wagner, Thomas Garwin, Nicholas Rostow, Sophia d'Antoine and David Aitel, *Cybersecurity Policy and Planning: Technologies for Keeping the Nation Safe,* (Los Angeles: Center for Advanced Studies on Terrorism, May 2018).

[115] *Sun Tzu on the Art of War,* translated by Lionel Giles (London: Luzai & Company, 1910), and Lucian W. Pye, *Spirit of Chinese Politics* (Cambridge: MIT Press, 1968). See also Barton Whaley, *Stratagem: Deception and Surprise in War* (Boston: Artech House, 2007). Sun Tzu wrote "All warfare is based on deception. Hence when able to attack, we must seem inactive: when we are near, we must make the enemy believe we are far away; when far away we must make him believe we are near. Hold out baits to entice the enemy. Feign disorder and crush him." Quoted in Pye and Leites, *Nuances in Chinese Political Culture, op. cit.*

combat, Chinese military strategy focuses heavily on perceiving and manipulating information available to opponents as a central element of combat.[116]

This appreciation of the value of deception emerges from a realistic perspective of war[117] —warfare is, by definition, deadly and unconventional.[118] Because predetermined strategies cannot be relied upon in the chaos of war, deception as a means to influence an adversary's perception of the capabilities and intentions in play can sharply influence the conditions on the ground.[119] By relying on this tactic to create or improve an advantage, deception can also minimize risk in direct confrontations.[120]

Deceptive tactics are as old as warfare itself. China may be a more successful practitioner of the art of deception than its western counterparts.[121] Yet western military strategists also recognize the utility of deception in military operations[122] and regularly deploy deceptive tactics in supporting operations.[123] Contemporary international law distinguishes between lawful and unlawful deception and prohibits perfidy.[124]

Actions that may seem to indicate inconsistency in Chinese political and military actions in fact reflect a persistent understanding that this variability is merely a byproduct of a military philosophy that encourages pursuing advantageous conditions when the opportunity arises. Thus, for example, although Beijing promised Hong Kong significant autonomy for 50 years after its handover from Britain, China's recent crackdown and the implementation of the National Security Law are a reflection of the CCP's current interest in promoting domestic legitimacy and seizing the opportunity to increase its power in the region.[125]

The digital revolution has greatly expanded the methods and opportunities for perception-based tactics, with cyberspace in particular providing a new and expanding arena for deceptive or

[116] *Chinese Tactics*, Army Techniques Publication (ATP) 7-100.3 (August 9, 2021), https://irp.fas.org/doddir/army/atp7-100-3.pdf.

[117] *The Longer Telegram: Toward a new American China strategy*, (Washington: Atlantic Council, January 28, 2021), https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/the-longer-telegram/.

[118] Mark Metcalf, *Deception is the Chinese Way of War*, (U.S. Naval Institute, February 2017), https://www.usni.org/magazines/proceedings/2017/february/deception-chinese-way-war#footnotes.

[119] *Ibid.*

[120] *The Longer Telegram: Toward a new American China strategy*, *op. cit.*

[121] See Blum, *Lies That Bind: Chinese Truth, Other Truths, op. cit.*

[122] Military Deception, Joint Publication 3-13.4 (January 26, 2012).

[123] John Mark Mattox, "The Moral Limits of Military Deception," *Journal of Military Ethics* (2002).

[124] Gary D. Solis, *The Law of Armed Conflict (3rd ed.)* (Cambridge: Cambridge University Press, 2022), 358-63.

[125] Lindsay Maizland, *Hong Kong's Freedoms: What China Promised and How It's Cracking Down*, (New York: Council on Foreign Relations, May 19, 2022); and Yuri Momoi, "China's rewrite of Hong Kong's history 50 years in the making," *Nikkei Asia* (July 2, 2022).

propaganda-based operations. Using new technologies, China has been able to proliferate information and disinformation on a scale never before imagined.[126] These technologies have afforded states unprecedented access to other states' infrastructure, whether through cyber or physical information communication infrastructures, such as 5G.[127]

These activities are referred to as the "intelligentization of warfare" so that military and political innovation "produce products that enable commanders to see and assess the battlefield condition in front of him before an opponent can do so and then act first."[128] Battlefield commanders have been trying to see through the fog of war since the invention of gunpowder if not the first appearance of fog itself.

The dissemination of misinformation or other propaganda is a means of leveraging China's access to these existing infrastructures in other states. Social media has provided a particularly useful route for influence operations. Rand Waltzman has noted "because audiences worldwide rely on the Internet and social media as primary sources of news and information, they have emerged as an ideal vector of information attack."[129] A Tweet can be efficiently leveraged to snowball content. Malicious actors can readily exploit a person's cognitive vulnerabilities and dependencies, gaming inclinations to react to eye-catching pictures or sensationalist headlines and leverage the social media algorithms that favor viral stories regardless of veracity.[130]

The CCP relies on a combination of government personnel and services, military operations, domestic and international news outlets and publications, and a variety of commercial services, as well as organic grassroots support, to create, publicize, and disseminate targeted information or misinformation campaigns. Diplomats, as the face of the country, play an especially important role in shaping domestic narratives for overseas consumption and are viewed in China as having their roots in the country's historical military struggle as an extension of a "civilian army."[131] Despite the fact that many social media platforms are not accessible within

[126] See Scott W. Harold, Nathan Beauchamp-Mustafaga, and Jeffrey W., Hornung, *Chinese Disinformation Efforts on Social Media* (Santa Monica: The RAND Corporation, 2021).

[127] Timothy L. Thomas, *The Chinese Way of War: How Has it Changed*. (McLean: The MITRE Corp, 2020).

[128] *Ibid.*

[129] Rand Waltzman, The *Weaponization of Information: The Need for Cognitive Security* (Santa Monica: The RAND Corporation, April 2017).

[130] Arthur de Liedekerke and Michael Zinkanell: *Deceive and Disrupt: Disinformation as an Emerging Cybersecurity Challenge* (Vienna: Austrian Institute for European and Security Studies, June 2020). See also, Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument." *American Political Science Review* (2017), https://gking.harvard.edu/50c.

[131] Graham Allison, Alyssa Resar, and Karina Barbesino, *The Great Diplomatic Rivalry: China vs the U.S.,* (Cambridge: Harvard Belfer Center, August 2022).

China, several public officials maintain Twitter and other similar accounts, adopting an assertive style of communicating known as "wolf-warrior diplomacy."[132]

Liu Xiaoming, who recently stepped down as China's ambassador to the United Kingdom, is one of the party's most successful foot soldiers on this evolving online battlefield. He has constantly posted items deriding Western anti-Chinese bias to his followers on Twitter and attacked his detractors. His posts were retweeted more than 43,000 times from June through February 2022 alone. More than half the retweets Liu received from June through January, however, came from accounts that Twitter had suspended for violating the platform's rules against manipulation. Overall, more than one in ten of the retweets 189 Chinese diplomats received in that time frame came from suspended Twitter accounts.[133]

Researchers with the Australian Strategic Policy Institute and DoubleThink Lab have discovered evidence of commercial services that disseminate CCP propaganda through Chinese-language content farms and news outlets.[134] Through websites such as Au123.com and Qiqis.org, state actors are able to "disseminate propaganda or manipulate how the reporting of events is framed," often targeting people within Taiwan or overseas diaspora communities.[135] During prominent or noteworthy events, such the 2019 Hong Kong protests or the investigation of the January 6th Capitol Hill riots in the United States, these large content farms promote CCP narratives and frameworks surrounding the event. [136]

In another example, China commissioned thousands of inauthentic accounts to engage in information operations "in response to potential or planned rare earths production activities." The rare earths industry is of "strategic significance to the PRC," which dominates the global rare earths market.[137] Identified by Mandiant by the moniker "DRAGONBRIDGE," the influence campaign stretched across several social media platforms, sharing content in both English and Chinese that promoted CCP interests in the industry.

When the U.S. Department of Defense awarded a $120-$240 million to the Australian company Lynas to build a rare Earth minerals facility in Texas, thousands of these inauthentic accounts claimed to be Texans protesting the environmental impact of the facility. DRAGONBRIDGE accounts engaged in similar activities in response to the discovery of a new

[132] "Welcome to Wolf-Warrior Diplomacy," *Bloomberg News* (December 3, 2020), https://www.bloomberg.com/news/newsletters/2020-12-04/welcome-to-wolf-warrior-diplomacy. *See also* Wolf Warrior (Wu Jing dir., 2015).

[133] Erica Kinetz, "Army of fake fans boosts China's messaging on Twitter," *Associated Press* (May 11, 2021), https://apnews.com/article/asia-pacific-china-europe-middle-east-government-and-politics-62b13895aa6665ae4d887dcc8d196dfc.

[134] Dr. Jacob Wallis et al, *Influence for Hire: The Asia-Pacific's Online Shadow Economy*, ASPI (2021).

[135] *Ibid.*, 17.

[136] https://www.taiwannews.com.tw/en/news/4267630

[137] Mandiant Threat Intelligence, *Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance* (June 28, 2022).

rare earths bearing zone by the Canadian miner Appia and the announcement of plans for another processing facility in Oklahoma by the American company USA Rare Earth.[138]

According to two experts, "the militarization of China's internet trolls" has resulted in an over 20 million strong so-called volunteer Internet army under the Communist Youth League (CYL). This collective could easily flood international social media platforms if it jumped the Great Firewall, as some have done in the past."[139]

Chinese Twitter accounts posting propaganda have also been shared by Huawei executives, ambassadors, and other influential figures to "amplify" the accounts and gain traction. A number of fake personalities (false digital personas) were also created to share and comment on disinformation, which were not traced back to Bangladesh, the origin of much of the propaganda found by the report. On YouTube, a network of "Spamouflage" outlets that were creating or sharing pro-Chinese media surrounding Hong Kong were traced back to Bengali owners.[140]

During the COVID-19 pandemic, the scope and visibility of China's disinformation efforts expanded significantly. Following the initial discovery of the novel coronavirus in Wuhan, the Chinese government pursued a disinformation campaign designed to divert blame for the pandemic and deflect attention away from the country's early handling of the crisis. Chinese diplomats and official accounts openly spread false and misleading information.[141]

China's disinformation efforts around COVID-19 later moved away from overt tactics and embraced covert methods apparently following the Russian example. The CCP began to deploy more subtle and unofficial information manipulation strategies, including through the use of Internet sites and fake social media accounts to push out misleading information.[142]

[138] *Ibid*.

[139] Jianli Yang and Nick Monaco, "Why the US Must Take China's Disinformation Operations Seriously," *The Diplomat* (January 28, 2022), https://thediplomat.com/2022/01/why-the-us-must-take-chinas-disinformation-operations-seriously/

[140] Ben Nimmo, Ira Hubert, I., and Yang Cheng, "Spamouflage Breakout Chinese Spam Network Finally Starts to Gain Some Traction," *Graphika* (February 2021). https://public-assets.graphika.com/reports/graphika_report_spamouflage_breakout.pdf.

[141] In March 2020, for example, a spokesperson for the Chinese Ministry of Foreign Affairs tweeted an article which falsely suggested that the virus had originated in the United States and been brought to Wuhan by the U.S. Army. See Edward Wong, Matthew Rosenberg, and Julian Barnes, "Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say," *New York Times*, (April 22, 2020. See also, Linda Sanchez, Bolstering *the Democratic Resilience of the Alliance Against Disinformation and Propaganda* (NATO Parliamentary Assembly, October 10, 2021), https://www.nato-pa.int/document/2021-bolstering-democratic-resilienceof-alliance-against-disinformation-and-propaganda

[142] Jessica Brandt, and Torrey Taussig, *The Kremlin's disinformation playbook goes to Beijing: China has abandoned its low profile for a high-stakes strategy*, (Washington: The Brookings Institution, May 19, 2020). Chinese operatives are considered responsible for the online dissemination of a false news story in March 2020 claiming that the U.S. administration was set to announce a national lockdown. This shift towards a reliance on covert methods is likely to shape future Chinese disinformation efforts beyond the pandemic.

Several reports point to a number of Advanced Persistent Threat (APT) groups using COVID-19 themed lures to deploy their malware. As a blog post from the Director of Threat Research at Bitdefender explains, a "lure based around fake news has significant chance of undermining targets' mental defenses and cyber-hygiene training." Victims interact with news lures for several reasons including a wish to be 'up-to-date' or current, a sense of urgency, socio-political polarization, curiosity, and fear.

China has invested heavily in information campaigns domestically and around the world aimed at influencing public opinion on the genocide in Xinjiang.[143] In addition to urging Party Members to mobilize on this front, the CCP has leveraged foreign news outlets, journalists, and influencers on Twitter, YouTube, and other social media platforms to spread Party narratives, disseminate Uyghur testimonial materials, and discredit foreign media outlets reporting negatively about the province.[144] Chinese government officials also have exploited the work of several U.S. and other Western reporters to discredit information about human rights abuses in Xinjiang and bolster the legitimacy of CCP alternative claims.[145]

China regularly deploys misinformation campaigns in Taiwan in addition to other cyber-based tactics. In one incident, several posts on a local online bulletin board claimed that the Chinese consulate rescued stranded Taiwanese tourists in Japan during Typhoon Jebi in September 2018 but only if they identified as "Chinese." The disinformation was intended to spark public anger against the Taiwanese consulate and to portray the Taiwanese government as incapable of rescuing its citizens.[146]

During Taiwan's 2020 elections, China rehashed contentious domestic issues from Taiwan's 2018 referenda, such as queer sex education and pensions reform. These issues in 2018 were able to divide voters based on age, education, income, and geography. This method is particularly useful because polarization creates the impression of weakness in democracies. Furthermore, even when reporters want to verify these stories, they often face pressure not to investigate. During the election season, when Taiwan's top military official died in a helicopter crash, Apple Daily reporters were dissuaded from fact-checking a fake news story indicating that

[143] "ANI, CCP buys media influence by paying millions to US dailies, magazines," *The Times of India* (July 4, 2021), https://timesofindia.indiatimes.com/world/china/ccp-buys-media-influence-by-paying-millions-to-us-dailies-magazines-report/articleshow/84109897.cms.

[144] Ryan Fergus et al, *#StopXinjiangRumors: The CCP's decentralised disinformation campaign*, ASPI (2021), https://www.aspi.org.au/report/stop-xinjiang-rumors.

[145] Bethany Allen-Ebrahimian, "The American blog pushing Xinjiang denialism," *Axios* (August 11, 2020).

[146] Linda Zhang, "How to Counter China's Disinformation Campaign in Taiwan." *Military Review* (September-October 2020). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2020/Zhang-Disinformation-Campaign/.

the general was rescued; their managers instead directed them to publish the incorrect news, as other outlets had already published it.[147]

China has used similar tactics in partnership with its allies. Following the Russian invasion of Ukraine and the European Commission's subsequent decision to block Russian state channels, as well as Twitter's, YouTube's, and Facebook's efforts to restrict their reach, Russia has raced to create workarounds. Researchers have uncovered a coordinated campaign to pay TikTok (owned by ByteDance) influencers to push pro-Kremlin views, while the data science company Trementum Analytics has documented pro-Russia trolls spamming YouTube videos about Ukraine with pro-Russian comments.[148]

TikTok has also admitted to censoring content critical of China overseas, especially content involving human rights abuses.[149] Working with the Russians because of China's alignment with Moscow with respect to the invasion of Ukraine, Chinese social media platforms Weibo, WeChat, and Douyin restricted anti-war content, suggesting that Chinese authorities pressured ByteDance to restrict content in Russia.[150]

In addition, several Chinese companies, as well as the government, have accumulated vast amounts of data generated by individuals in the United States and other countries. As is typical, most smartphone apps collect significant amounts of data, such as location data, which is then sold as datasets through data brokers or other services.[151] China is merely one of myriad consumers of such data. China has allegedly collected large healthcare datasets "through both legal and illegal means, for purposes only it can control."[152]

[147] They were told it was not up to them when other outlets had already published it. See Aaron, Huang, *Combatting and Defeating Chinese Propaganda and Disinformation* (Cambridge: Harvard Belfer Center, 2021).

[148] U.S. Department of State, *People's Republic of China Efforts to Amplify the Kremlin's Voice on Ukraine* (May 3, 2022), https://www.state.gov/disarming-disinformation/prc-efforts-to-amplify-the-kremlins-voice-on-ukraine/, and Elizabeth Dwoskin, "China is Russia's most powerful weapon for information warfare," *Washington Post* (April 8, 2022), https://www.washingtonpost.com/technology/2022/04/08/russia-china-disinformation/.

[149] National Security Institute, *Don't Trust TikTok's Plan to Secure Americans' Data,* (The SCIF, June 30, 2022), https://thescif.org/dont-trust-tiktok-s-plan-to-secure-americans-data-700a6ab7bfb4.

[150] Salvatore Romano, Marc Faddoul, Claudio Agosti, Giulia Giorgi, and Louise Doherty. "Tracking Exposed Special Report: TikTok content restriction in Russia." *Tracking Exposed* (March 15, 2022). https://tracking.exposed/pdf/tiktok-russia-15march2022.pdf.

[151] Kevin Collier, *TikTok a privacy threat? Sure, but so are most of your smartphone apps*, NBCNews (July 13, 2020).

[152] Michael Kans, "Data Brokers and National Security," *Lawfare* (April 29, 2021), https://www.lawfareblog.com/data-brokers-and-national-security.

Notably, the popular app TikTok has repeatedly claimed that U.S. users' data was inaccessible to TikTok employees based in China.[153] This claim was proved false when leaked audio from several internal TikTok meetings revealed that China-based employees of ByteDance had repeatedly accessed nonpublic data of U.S. users.[154] While it is unclear what data these employees accessed, TikTok collects information, including biometric identifiers such as faceprints and voiceprints.[155]

The company's stated efforts to remedy the problem by localizing the data on servers in the United States leaves much to be desired, as diverting the data flow would not prevent backdoor technical access by engineers in China.[156] TikTok has also dubiously maintained that it "has never and would never share U.S. user data with the Chinese government," but local laws requiring information sharing for national security purposes undercut this claim.

While it is clear that China has expended considerable resources to shape and influence public opinion, the efficacy of these efforts is less apparent.[157] Many nations have in fact responded poorly to China's overseas propaganda and diplomatic efforts and have attempted to develop counteractive measures in response.[158] In addition, a clear casual mechanism connecting information operations to potential benefits—such as amplifying disorder to impede the decision-making of governmental bodies—has yet to be validated.[159]

It is also important to be prudent in assessing disinformation campaigns; misattributing influence operations to state actors, for example, runs the risk of assigning malice to motives that may be benign.[160] Overstating the significance of misinformation campaigns can lead to the

[153] Christiana Silva and Elizabeth de Luna, "It Looks like China Does Have Access to U.S. TikTok User Data," *Mashable* (July 2, 2022), https://mashable.com/article/tiktok-china-access-data-in-us.

[154] Emily Baker-White, "Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China," *Buzzfeed* (July 17, 2022), https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.

[155] Miriam Kohn, "Clearview AI, TikTok, and the Collection of Facial Images in International Law." CHICAGO JOURNAL OF INTERNATIONAL LAW, (June 1, 2022).

[156] National Security Institute, "Don't Trust TikTok's Plan to Secure Americans' Data," *The SCIF* (June 30, 2022), https://thescif.org/dont-trust-tiktok-s-plan-to-secure-americans-data-700a6ab7bfb4.

[157] Lotus Ruan and Gabrielle Lim, "Balancing Reality and Fear: Why an Alarmist Take on Chinese Influence Operations Is Counterproductive," *Just Security* (July 21, 2021).

[158] Fergus Hanson, Emilia Currey, and Tracy Beattie. "The Chinese Communist Party's Coercive Diplomacy." (Aspi.org.au, 2020), https://www.aspi.org.au/report/chinese-communist-partys-coercive-diplomacy.

[159] Paul Stockton, *Defeating Coercive Information Operations in Future Crises,* (Baltimore: Johns Hopkins University Applied Physics Laboratory, 2021. https://www.jhuapl.edu/Content/documents/DefeatingCoerciveIOs.pdf.

[160] Lotus Ruan and Gabrielle Lim, "Balancing Reality and Fear: Why an Alarmist Take on Chinese Influence Operations Is Counterproductive," *Just Security* (July 21, 2021) (describing how a content farm in Taiwan spread pro-China articles and false information "primarily for monetary gains").

adoption of measures that harm more than help. The firm HaiEnergy used 72+ "news" sites and fake social media accounts to spread Hong Kong/Xinjiang propaganda alongside other conspiracy theories about the United States and its allies. The post indicates that there may have been some connection with the Shanghai Haixun Technology Company, which is host of these sites.[161]

Most states engage in cyber operations because the barriers to entry are low—costs are lower relative to other tactics, the risk to personnel or resources is minimal, infrastructure costs are low, and the injury done to the other party is not physical.[162] As a result of their internal systems of censorship, China and Russia have the experience and preliminary infrastructure in place to adopt misinformation tactics.[163] Misinformation campaigns may therefore be adopted primarily for their ease of use.

In this sense, responding to disinformation or influence campaigns with overly stringent policies or measures that target a wide swathe of individuals and companies based on their national origin can exacerbate practices that continue to Balkanize cyberspace, inhibit the development of and exchange of digital technologies, and limit access to and insight into overseas cyber practices. Several authoritarian states such as Russia and China already have capitalized on fears of "fake news" and the threat it poses to national security to engage in censorship and other suppressive practices.[164]

[161] Ryan Serabian and Daniel Kappellman Zafra, *"HaiEnergy" Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites* (Mandiant, August 4, 2022).

[162] Dorothy Denning, "Barriers to entry: are they lower for cyber warfare?," *IO Journal* (2009).

[163] Gillian Bolsover, *Computational Propaganda in China: An Alternative Model of a Widespread Practice*, Samuel Woolley and Philip N. Howard, Eds. Working Paper (Oxford: Project on Computational Propaganda, November 2017) (discussing the use of bots and organized groups of fake accounts on social media to promote positive propaganda about the Chinese State on issues such as Tibet).

[164] *Ibid*.

3. Organization of China's Cyber Activities

Following China's changing priorities in cyberspace, the country's government and military reorganized and professionalized cyber operations. Beginning in December 2015 and throughout 2016, the PLA undertook a mass organizational restructuring as part of efforts to modernize. Previously decentralized cyber units were consolidated into a singular supervising body, the Strategic Support Force (SSF), in order to improve the PLA's combat capabilities.

This process transformed China's cyber operations from loosely linked operators predominantly concerned with gaining access to trade secrets to a professional intelligence service that engages in cyber as a means of defending critical infrastructure, conducting espionage, and preparing for combat. In addition to the SSF, two civilian ministries, the Ministry of State Security (MSS) and the Ministry of Public Security (MPS), make up the known Chinese government entities engaged in cyber operations.

The PRC also has developed an extensive cyber governance regime aimed at maintaining control over the flow of information within its borders, improving resilience to adverse cyber operations and reducing security vulnerabilities, achieving technological autonomy, and expanding influence over cyberspace internationally.[165] This regime is comprised of laws such as the Data Security Law, Cybersecurity Law, and Personal Information Protection law, policies, regulations, and standards. Several different departments under the central guidance of the Central Cyberspace Affairs Commission oversee the regime.

The following descriptions provide a brief introduction to China's major regulatory bodies engaged in cybersecurity, as well as three of the relevant laws. While there are a number of subordinate bodies and regulations not included, and the government and military rely on several other departments' expertise when engaging in cyberspace, the organizations listed below play the principal roles in effectuating the PRC's cyber policies.

Cybersecurity and Informatization Bodies

Central Cyberspace Affairs Commission (CCAC, also known as the Central Commission for Cybersecurity and Informatization (CCCI)): Established in 2014, the CCAC was formed to integrate the "fragmented bureaucratic structures and policy areas"[166] that had previously composed China's approach to cyber.[167] The Commission is comprised of senior Party leaders, as

[165] Adam Segal, *China's Alternative Cyber Governance Regime*, (New York: Council on Foreign Relations, March 13, 2020), https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.

[166] Rogier Creemers, "China's Cyber Governance Institutions."

[167] In 2014, the CCP incorporated its propaganda office, the State Internet Information Office, into its "newly formed, multi-agency CCP Central Leading Small Group for Cybersecurity and Informatization."

well as the directors of several ministries and committees, and is led by Xi Jinping and Li Keqiang.[168] While its operations are largely opaque, the Commission's role includes overseeing and facilitating the implementation of cybersecurity and informatization policies across departments and agencies.[169]

Cyberspace Administration of China (CAC, 国家互联网信息办公室): The CAC is responsible for handling cyberspace and internet content and enforcing the PRC's various data regulations.[170] The CAC manages critically important information infrastructures, personal data protection, and data security (along with the Ministry of Public Security). Its activities include rulemaking, administrative licensing, enforcement, and representing the country in "international cyber-related activities."[171] The expanding nature of the CAC's regulatory mission has given the agency significantly more clout when compared with similar counterparts.

The CAC is a joint party-state entity referred to as "two nameplates for a single office" (一个机构两块牌子).[172] Under this structure, the CAC is technically a party office (Office of the CCAC) and a state office (State Internet Information Office, SIIO) operating together. The two offices likely share the same leadership team and internal institutions, but the name under which the organization operates at a given time is contingent upon the work it is conducting at the moment.[173] It is unclear to what extent, if any, the CAC operates independently from the CCAC. Open government information that is typically produced by administrative agencies, such as implementation rules and annual budgets, is not provided by the CAC.[174]

In 2018, this leading small group was elevated to a CCP central commission and became the CCAC. Jamie P. Horsley, "Behind the I of China's Cyber Super-Regulator," *DigiChina* (August 8, 2022), https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/.

[168] Including "the CAC, the Ministry of Public Security, the Ministry of Industry and Information Technology, the Ministry of Foreign Affairs, the National Development and Reform Commission, the Ministry of Education, the Ministry of Science and Technology, the Ministry of Finance, the Ministry of Culture, the State Administration for Press, Publications, Radio, Film and Television, the PLA General Staff and the People's Bank of China." Creemers, "China's Cyber Governance Institutions," p. 5; Xiaosong Zhang and Jichai Zhu, "Xi Jinping Stresses at the Cybersecurity and Informatization Work Conference to Keenly Grasp the Historical Opportunity in Informatization Development, and Move Forward the Construction of a Cyber Power through Indigenous Innovation," trans. *China Copyright and Media* (April 22, 2018), https://chinacopyrightandmedia.wordpress.com/2018/04/22/xi-jinpings-speech-at-the-national-cybersecurity-and-informatization-work-conference/.

[169] Creemers, "China's Cyber Governance Institutions," p. 6.

[170] 国务院关于机构设置的通知, 国务院 (March, 24, 2018), http://www.gov.cn/zhengce/content/2018-03/24/content_5277121.htm.

[171] Horsley, "Behind the Facade of China's Cyber Super-Regulator."

[172] *Ibid.*

[173] "部分机构编制用语释义" (August 8, 2017), http://lc.ynbb.gov.cn/zwgk/zcfg/content_21189.

[174] Horsley, *Id*, "the Facade of China's Cyber Super-Regulator."

There are several subordinate entities under the CAC, including the National Committee for the Standardization of Information Security (Technical Committee 260, responsible for centralizing technical information security standards), the Chinese Academy of Cyberspace Studies, CNCERT/CC (responsible for monitoring and responding to cyber-attacks), the China Internet Network Information Center (responsible for overseeing the domain name system for .cn and Mandarin-language domain names), and the Cybersecurity Association of China (responsible for assisting government departments with implementing various data and cyber regulations).[175]

Strategic Support Force (SSF, 战略支援部队): The Strategic Support Force was established on December 31, 2015, in the first wave of the PLA's modernization process. Drawing from the previous General Staff Department (GSD), General Armament Department (GAD), and General Political Department,[176] the SSF is a theatre command-level organization that centralizes the military's strategic space, cyber, electronic, and psychological warfare missions into a joint force.[177] The organization provides "command, control, communications, computers, intelligence, surveillance, and reconnaissance support" [178] to other services in the military and has established five regional support bases to coordinate with the five theater commands.[179] Unlike other service branches, the SSF reports directly to the top administrative body of the military, the Central Military Commission, led by President Xi Jinping.

Within the SSF, cyber operations are centralized under the Networks Systems Department (网络系统部), which consolidated, among other entities, the previous Third Department of the GSD (3PLA), where the bulk of cyber operations and research occurred, the Fourth Department (4PLA), which traditionally handled computer network attacks, and the Informatization Department, which was responsible for counter-network defense. There have been a number of subunits of the SSF and its predecessors that have been identified as being involved in foreign-directed cyber-warfare. Some key examples include the following.

PLA Unit 61486, previously part of the 12th Bureau within 3PLA, was tied by CrowdStrike to a group of Shanghai-based hackers that targeted European, American, and Japanese government officials, military contractors, and space and satellite research companies.

PLA Unit 61419, based in Qingdao, Shandong, was linked to several cyberattacks on Japan and South Korea in 20210 conducted by the group Tick. These cyber-attacks targeted approximately 200 companies and research institutes in Japan, including the Japan Aerospace

[175] Creemers, "China's Cyber Governance Institutions."

[176] Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review* (2018).

[177] Pollpeter, Kevin L., Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica: The RAND Corporation, 2017).

[178] Joel Wuthnow and Philip C. Saunders, *Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications* (Washington: National Defense University Press, March 2017).

[179] Philip C. Saunders, "Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Nuclear Forces," *USCC* (June 10, 2021).

Exploration Agency. *Unit 61419* consists of several subordinate units, possibly including *Unit 61680*, located in Wenquan, Jimo, and *Unit 61650*, which lists the same address as *Unit 61419*.

More recently, Insikt Intelligence linked the threat activity group RedfoxTrot to *Unit 69010*, located in Ürümqi, Xinjiang. The group primarily targets government, defense, and telecommunications centers in Central Asia, India, and Pakistan. In 2020, RedfoxTrot gained access to the ShadowPad malware, which provides a Windows backdoor that allows attackers to either steal data or download further malware to the system.

Ministry of State Security (MSS, 国安部): The MSS is China's main civilian intelligence and anti-espionage authority. It reports directly to the State Council, the chief administrative body of the Chinese government responsible for executing the law and supervising the government bureaucracy, and the CCP Politburo Standing Committee. The ministry engages in both domestic and foreign intelligence operations, including human intelligence and cyber operations. It was given broad powers under the 2017 National Intelligence Act to compel Chinese citizens and organizations to engage in and support intelligence activities, as well as monitor domestic and foreign individuals and entities.[180]

The organization structure of the MSS consists of a central ministry; provincial state security departments; and state security bureaus, several of which have been linked to malicious cyber activities. The *Shanghai Security Bureau*, which itself is composed of 18 subordinate branch offices, has primarily been traced to human intelligence operations, including a recent case in 2018 where a former U.S. intelligence officer sold classified information to a Chinese intelligence officer operating as a member of the Shanghai Academy of Social Science (SASS).

Under the direction of the *Tianjin State Security Bureau*, Members of APT 10 (aka Red Apollo, CVNX, Stone Panda, MenuPass, and POTASSIUM) who worked for Huaying Haikai Science and Technology Development Company targeted intellectual property, business, and technological information at companies in industries ranging from aviation to pharmaceuticals to banking. The U.S. Justice Department indicted three members of this group in 2018.[181]

A group of self-described analysts known as Intrusion Truth has worked to expose several Chinese threat groups, including linking APT17 to the *Jinan State Security Bureau*, and identifying the following companies as associated with an MSS officer: Jinan Quanxin Fangyuan Technology Co. Ltd., Jinan Anchuang Information Technology Co. Ltd., Jinan Fanglang Information Technology Co. Ltd., and RealSOI Computer Network Technology Co. Ltd.

Ministry of Public Security (MPS, 公安部): The Ministry of Public Security is the national security organization that oversees all provincial and local police departments. It is a component organ of the State Council. Among its stated responsibilities include supervising public

[180] For example, The European External Action Service (EEAS) estimates there are approximately 250 Chinese intelligence agents operating in Brussels alone.

[181] *United States v. Zhang Zhang-Gui, et al.,* No. 18-cr-3132 (S.D. CA, October 25, 2018). An additional indictment was made in New York. See *United States v. Zhu Hua, et al.,* No. 18-cr-891 (S.D. NY, December 17, 2018).

information networks. While the ministry is primarily concerned with public security work and policing, due to its "growing internal database, technical sophistication and cyber capabilities,"[182] it is seen as sharing a counterintelligence mission with (and directed by) the MSS.

This shared mission typically involves monitoring dissidents and foreigners located within China. The 11th Bureau of the MPS, the Cybersecurity Protection Bureau, is responsible for fighting cybercrime and overseeing the multi-level protection system for information security, which often overlaps with the administrative authority of the CAC, particularly with regard to data protection.[183]

Ministry of Industry and Information Technology (MIIT, 工业和信息化部): Although the CAC has absorbed much of the MIIT's cyber responsibilities, the agency has remained responsible for the nation's network infrastructure. Its Cybersecurity Management Bureau often coordinates with the CAC to tackle issues of data security. More recently, the MIIT has coordinated with Huawei, Tencent, and other technology companies and elite universities to develop an independent open source hosting platform in China, relying on Gitee, the Chinese alternative to GitHub.[184] The MIIT, along with the Ministry of Civil Affairs, manages the Open Atom Open Source Foundation, China's first open source consortium.[185]

Laws

Cybersecurity Law

The Cybersecurity Law, effective June 1, 2017, was the first of several new regulations governing data protection in China.[186] This law establishes localization requirements for storing select data in China, provides guidelines for maintaining network security, and also authorizes government authorities to conduct network security checks.[187] Application of the law is generally limited to network owners, managers, providers, and businesses in sensitive cyber and technology sectors. The definition of a network—"any system comprising computers and related equipment

[182] According to testimony given by Congressional Innovation Fellow John Costello in 2016 for the U.S.-China Economic Security Review Commission.

[183] Creemers, "China's Cyber Governance Institutions."

[184] *工信部携 Gitee 入场，国内开源生态建设进入快车道*, Gitee Blog (July 14, 2020), https://blog.gitee.com/2020/08/17/gitee-gxb/.

[185] Open Atom Foundation (March 5, 2022), https://www.openatom.org.

[186] Rogier Creemers, Paul Triolo and Graham Webster, *Translation: Cybersecurity Law of the People's Republic of China* (New America, June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[187] Lauren Maranto, *Who Benefits from China's Cybersecurity Laws* (Washington: Center for Strategic and International Studies, June 25, 2020).

that gathers, stores, transmits, exchanges, or processes information"—means that effectively any business that manages an email or other data network can fall under the law.[188]

Data Security Law (DSL)

The Data Security Law (DSL), effective September 1, 2021, governs data collected and stored in China and determines requirements for storage and transfer depending on potential impact on national security.[189] The law defines data security as "ensuring data is in a state of effective protection and lawful use through adopting necessary measures, and to possessing the capacity to ensure a persistent state of security" (Art. 3). The DSL prohibits Chinese organizations and individuals from transferring data stored in China "to the justice or law enforcement institutions of foreign countries without the approval of Chinese authorities.[190]

Personal Information Protection Law (PIPL)

The Personal Information Protection Law (PIPL), effective November 1, 2021, is a comprehensive legal framework designed to regulate how companies collect, process, and transfer personal data.[191] Article 3 dictates that the PIPL applies to entities that collect, store, use, transmit, provide, or otherwise handle personal information of "natural persons within the borders of the People's Republic of China," even if that entity is located or conducts business entirely outside of China. The PIPL requires operations or entities that handle critical infrastructure information, and which process a "large amount of personal information" to store personal information on the territory of Mainland China (Art. 40).

[188] Jack Wagner, "China's Cybersecurity Law: What You Need to Know," *The Diplomat* (June 1, 2017), https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

[189] DigiChina, *Translation: Data Security Law of the People's Republic of China* (June 29, 2021), https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/#_ftnref11; Junck et al, China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies, *Lexology*.

[190] Bezanson et al, "China's New Data Privacy Law is Sweeping and Serious: Avoid the High Cost of Noncompliance," *The National Law Review* (August 24, 2021), https://www.natlawreview.com/article/china-s-new-data-privacy-law-sweeping-and-serious-avoid-high-cost-noncompliance.

[191] Roger Creemers and Graham Webster, "Translation: Personal Information Protection Law of the People's Republic of China," *DigiChina* (August 20, 2021), https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

4. The Private Sector and Cybersecurity Firms

China's Technology Sector

As China's "decade-long quest to become a superpower" begins to come to fruition, the nation has increasingly moved to eliminate barriers between its civilian-commercial industries and the State.[192] Many technology companies, particularly domestic cybersecurity enterprises, stand at the forefront of their fields. They offer insight and services that, not only are unparalleled in quantity, but also a tremendous resource for China's government and military. Understanding China's domestic cybersecurity ecosystem therefore provides insight into the development of China's political and military strategy.

In recent years, China's cybersecurity industry has expanded rapidly, with experts moving from positions in larger technology firms to establish companies of their own, often maintaining their earlier connections. These firms operate under ever more restrictive government policies, which, in conjunction with a hostile U.S. environment for Chinese technology, has driven many to focus their efforts on overseas markets.[193]

The technology giant Tencent, for example, has "pour[ed] capital into gaming studios in the U.K., Germany, Netherlands, Finland, Sweden, Romania, Russia, Czechia, Japan, Canada and of course, the United States."[194] TikTok, owned by the company ByteDance, was downloaded more in 2020 than any other mobile application.[195] Recent reports allege that ByteDance employees based in China have "repeatedly accessed" the data of users in the United States, despite company testimony to the contrary.[196] Xiaomi, a Chinese smartphone business, was reportedly the "world's best-selling smartphone brand" in June 2021.[197] Countless other communications,

[192] Patrick Howell O'Neill, "How China built a one-of-a-kind cyber-espionage behemoth to last," *MIT Technology Review* (February 28, 2022), https://www.technologyreview.com/2022/02/28/1046575/how-china-built-a-one-of-a-kind-cyber-espionage-behemoth-to-last/; U.S. Dep't of State, *Military-Civil Fusion and the People's Republic* of China (2020), https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

[193] Zeyi Yang, "How Chinese tech companies took over the world in 2021," *Protocol* (December. 29, 2021), https://www.protocol.com/china/china-world-2021-review/.

[194] *Ibid.*

[195] Rei Nakafuji, "TikTok overtakes Facebook as world's most downloaded app," *Nikkei Asia* (August 9, 2021), https://asia.nikkei.com/Business/Technology/TikTok-overtakes-Facebook-as-world-s-most-downloaded-app.

[196] Emily Baker-White, "Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China," *BuzzFeed News* (June 17, 2022).

[197] Zeyi Yang, "How Chinese tech companies took over the world in 2021," *Protocol* (December 29, 2021).

gaming, app, and cryptocurrency companies have established a presence in countries around the world.

Aware of dependence on the United States and other countries for technology supplies, particularly semiconductors, China has moved to separate its technology systems, relying on tactics such as defense procurement by the military to keep uncompetitive but important technology companies, such as "fledging semiconductor companies," afloat.[198] These practices, in addition to U.S. sanctions and fears of being cut off from overseas semiconductor supplies, have fueled a booming industry in China, with over 22,000 new semiconductor companies registered in 2020.

Technology giants Baidu, Alibaba, Huawei, and Xiaomi have invested in semiconductor chip production.[199] For the past two years, China has provided the biggest market for chip-manufacturing supplies and has stockpiled tools and equipment for making semiconductors.[200] Many Americans have advocated measures that would limit exports of this equipment, although these calls have so far gone unheeded.[201]

Despite their essential role in economic development and national security, Chinese technology companies, particularly those in social media, gaming, and information, are sometimes viewed as a risk to the CCP. The CCP fears the concentration of wealth and power in dominant companies and their leaders, the technology sector's ability to facilitate the uncontrolled flow of information and provide a kind of virtual gathering space for domestic activism, and, therefore, the potential for erosion of social stability.

These and other specific industry concerns spurred a regulatory crackdown on technology companies since the end of 2020. The State Administration for Market Regulation (SAMR, 国家市场监督管理总局) fined Tencent, Baidu, and ByteDance, among others, for antitrust practices.[202] The CAC sanctioned others, such as Didi and Kanzhun, for data security violations. Still more companies were subject to regulatory actions for "disorderly expansion of capital" (or effectively for "grow[ing] at the expense of the public interest"). Alibaba's Ant Group had its public listing suspended by regulators in November 2020.[203]

[198] Bradford Waldie, "How Military-Civil Fusion Steps Up China's Semiconductor Industry," *DigiChina* (April 1, 2022), https://digichina.stanford.edu/work/how-military-civil-fusion-helps-chinas-semiconductor-industry-step-up/.

[199] Zeyi Yang, "Chinese companies are making their own semiconductors," *Protocol* (March 13, 2021), https://www.protocol.com/china/chinese-companies-make-own-semiconductors.

[200] Jenny Leonard, Ian King, and Debby Wu, "China's Chipmaking Power Grows Despite US Effort to Counter It," *Bloomberg* (June 13, 2022), https://www.bloomberg.com/news/articles/2022-06-13/china-s-growing-clout-in-global-chip-market-rings-alarm-bells-in-washington#xj4y7vzkg.

[201] *Ibid.*

[202] Chang Che and Jeremy Goldkorn, "China's 'Big Tech crackdown': A guide," *SupChina* (August 2, 2021), https://supchina.com/2021/08/02/chinas-big-tech-crackdown-a-guide/.

[203] *Ibid.*

Although this crackdown appears to be slowing down, it reflects a number of tensions in the private technology sector and between the Chinese government and this industry. While the capacity and opportunity for growth in technology benefits the economy and provides support for national security, Beijing recognizes that the tendency for wealth concentration in the industry creates "unfair market competition."[204] More importantly, the Party is highly motivated "to increase state control of the digital economy and all the data in the trade."[205]

Though China's regulatory actions seem to have created a progressively restrictive environment, the increased regulatory focus on technology companies may benefit China's cybersecurity interests, even as investors may have "run for the hills."[206] Regulatory actions may redirect capital to more important technologies, increase the presence of Chinese companies abroad by limiting their ability to expand in domestic markets, and reduce competition from foreign firms by creating conditions that compel them to exit the market.[207]

While China's cybersecurity industry currently represents only a small portion of the global market, and Covid, regulatory demands, and economic concerns appear to be slowing the sector's rate of growth, it would be wrong to assume that this situation will constrain overall development.[208] China's private cybersecurity companies have raised their worldwide profile and will only continue to do so as the country's talents, skill, and infrastructure continue to improve.

China's Cybersecurity Landscape

Cybersecurity professionals interested in the development of China's cyber industry have long focused on developments in law, government ministries, and leading industry corporations. But as the country's technology enterprises have matured, researchers and engineers employed in China's cybersecurity industry have used their expertise and experience from working in technology conglomerates to form their own firms, creating a growing and thriving cyber ecosystem. The PLA, security services, and policymakers use this ecosystem to support their cyber operations.

The evolution of Chinese cyber policy and the trajectory of the nation's cyber industry are closely related to the proliferation of firms engaged in cybersecurity research. As part of its MCF approach, China's leadership has emphasized the need to foster innovation in domestic technologies and has called on private enterprises to contribute to the security of the state and its

[204] Arjun Kharpal, "China has signaled easing of its tech crackdown — but don't expect a policy U-turn," *CNBC* (May 17, 2022), https://www.cnbc.com/2022/05/18/china-signals-easing-of-its-tech-crackdown-but-dont-expect-a-u-turn.html.

[205] Charles Mok, *quoted in* Arjun Kharpal, "China has signaled easing of its tech crackdown — but don't expect a policy U-turn."

[206] Kevin Klyman, "China's Tech Crackdown Could Give It an Edge," *The Diplomat* (April 30, 2022), https://thediplomat.com/2022/04/chinas-tech-crackdown-could-give-it-an-edge/.

[207] *Ibid.*

[208] James Tarabay and Sarah Zheng, "Chinese Firm That Accused NSA of Hacking Has Global Ambitions," *Bloomberg* (May 31, 2022), https://www.bloomberg.com/news/articles/2022-05-31/chinese-firm-that-accused-nsa-of-hacking-has-global-ambitions?sref=OuEBXo2C.

citizens.[209] Institutions and individuals embedded in China's cybersecurity industry have stressed that start-ups and smaller firms are an important source of this innovation in network security. These companies, along with and under the guidance of China's technology giants, have played and will continue to play a formative role in the development of China's national cyber strategy.

Rapid Growth of Chinese Cyber Technology

While their direct engagement with government authorities varies, China's cybersecurity firms operate under increasingly rigid constraints. Zhou Hongyi, one of Qihoo 360's founders, has been vocal[210] in touting the strategic benefits[211] of keeping knowledge of vulnerabilities, such as weaknesses in software code, close to home, noting that vulnerabilities are no longer of use once exposed publicly by Chinese hacking teams at competitions.[212] Cognizant of this fact, China has discouraged its security researchers from participating in hacking competitions abroad, particularly those where zero-day vulnerabilities may be publicly disclosed.[213]

Those researchers that are approved to attend must disclose any discovered vulnerabilities to the government ahead of time.[214] Recent regulations also mandate that individuals and companies within China share zero-day vulnerabilities with the government within two days of discovery.[215] Vulnerabilities shared in hacking competitions within the PRC can and have been exploited by government hacking campaigns to infiltrate software and hardware providers, such as Google and Apple, before they can be patched.[216] They have also been used to target individuals belonging to vulnerable populations, such as Uyghur Muslims.

As the country's cyber capabilities improve at an unparalleled pace, maintaining ties with China's tech industry is of critical importance, not only for technological and economic advancement, but also for cybersecurity purposes. Experts in China stand at the forefront of

[209] Mohammed Shihab, *Expanding Cyber Demands Embolden China's Homegrown Cybersecurity Darlings: China is building a welcoming ecosystem for its homegrown tech darlings*, *The Diplomat* (September 23, 2019).

[210] 韩大鹏, 周鸿祎:马云提新零售 我想了几个月想到了“大安全”, 新浪科技 (September 12, 2017), https://perma.cc/EFD6-SRSS.

[211] Cyberspace Administration of China, 360：自觉担当责任维护网络安全 (November 11, 2018), https://perma.cc/ENA2-WZ3F.

[212] See, for example' Patrick Howell O'Neill, *How China built a one-of-a-kind cyber-espionage behemoth to last, MIT Technology Review* (February 28, 2022).

[213] Yingzhi Yang, "China discourages its hackers from foreign competitions so they don't help others," *South China Morning Post* (March 21, 2018).

[214] 'Patrick Howell O'Neill, "How China built a one-of-a-kind cyber-espionage behemoth to last."

[215] Cyberspace Administration of China, 工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知 (July 13, 2021), https://archive.ph/9cL8j#selection-627.1-627.18.

[216] Patrick H. O'Neill, "How China built a one-of-a-kind cyber-espionage behemoth to last."

vulnerability research and have developed expertise and insight in regard to offensive and defensive techniques necessary to combat infiltration and exploitation.

Cutting off the exchange of knowledge between U.S. and Chinese cyber industries would undermine the ability of service providers to protect their products and network infrastructures and would also undercut visibility into changing developments in potential offensive cyber activities. But domestic cyber enterprises, as in most countries, also play a vital role in providing infrastructure, talent, and resources to State operations, sometimes by choice, sometimes under legal and political pressure.

Industry leaders in China, such as Tophant's CEO Chen Xie, see China's cybersecurity "universe" as unique and expect growth to continue to outpace overseas counterparts.[217] According to Xie, cybersecurity firms, particularly those dealing with personal data security, zero trust, cloud security, and privacy, are more likely to receive funding from the government, state-owned enterprises, and publicly listed companies when compared with other industries.

Analysts interested in the development of China's cybersecurity industry and national cyber strategy would be remiss to neglect investigating the make-up and distribution of local firms. Understanding this rapidly evolving technology base is critical to U.S. cybersecurity efforts.

The discussion below provides a survey of selected Chinese firms that sheds insight into China's private cybersecurity sector. Industry leaders and tech giants, themselves relatively new companies, dominate the space, setting the direction of the industry while investing in and supporting the explosive growth of small firms.[218] Many smaller firms were founded by previous employees of these industry giants, and some still maintain partnerships with the larger companies.

While cybersecurity makes up a small portion of the work of some of the tech giants, many of these firms focus on vulnerability research, threat detection, and security intelligence, and their services and products offer their clients protection from offensive cyber activities. A growing number of these firms also focus on blockchain security. While their investors are predominantly Chinese venture capital firms, these companies service clients and maintain partnerships worldwide.

Industry Leaders and Internet Giants

The China Cybersecurity Industry Alliance (CCIA, 中国网络安全产业联盟) is a non-profit group comprised of enterprises, institutions, and individuals who work in network security and is supervised by the Cybersecurity Coordination Bureau of the Cyberspace Administration of China.[219] This Alliance conducts a yearly public survey on network security companies in China, which it then uses to produce a list of the top 50 most competitive network security companies in

[217] 斗象科技 CEO 谢忱：中美–安市场分化明显，"平行宇宙"初现 - FreeBuf网络安全行业门户

[218] China Cybersecurity Industry Alliance, 2022 年 CCIA50 强、成长之星&潜力之星榜单 (June 23, 2022), https://perma.cc/NFY5-PBWK.

[219] China Cybersecurity Industry Alliance, http://www.china-cia.org.cn.

China.[220] The CCIA considers the majority of the companies in the table below to be "leaders" in cybersecurity.

These lead companies help determine the direction of trends in the field and provide funding for other cybersecurity firms and projects.[221] These companies constitute the dominant players in China's cybersecurity industry. A few of them are "strategic planners," giants in the IT and internet industries. They have dedicated a portion of their substantial resources to network security, predominately for strategic support to the business and represent a small portion of the company's total operations.

Company Name	2022 CCIA Ranking	Founded	Area of Focus
Qi An Xin Technology (奇安信)	1	2014	Network Security, Antivirus
Sangfor Technologies (深信服）	2	2000	Cloud Computing, Network Security
Beijing Venustech Inc. (启明星辰)	3	1996	Network Security
Topsec Technologies Group (天融信)	4	1995	Network Security
Huawei (华为)	5	1987	Information and Communications Technology
NSFocus Technologies Group Co Ltd (绿盟科技)	6	2000	Network and Web Security, Threat Intelligence
Tencent (腾讯)	7	1998	Online Gaming, Social Networking, E-Commerce, Multimedia, Communications
Alibaba Cloud (阿里云）	8	2009	Cloud Computing, Data Management
New H3C Technologies (新华三）	9	2003	Digital infrastructure
DBAPP Security (安恒信息)	10	2007	Network Security
Qihoo 360 (三六零)	11	2005	Antivirus, Internet and Mobile Security
Asiainfo Security （亚信安全）	12	1995	Software Development, IT Services

[220] China Cybersecurity Industry Alliance, 2022年CCIA50强、成长之星&潜力之星榜单 (June 23, 2022), https://perma.cc/NFY5-PBWK. For the 2021 results, *see* China Cybersecurity Industry Alliance, 2021年CCIA50强、成长之星&潜力之星榜单, (last visited June 26, 2022).

[221] China Cybersecurity Industry Alliance, 2022年CCIA50强、成长之星&潜力之星榜单.

By virtue of their size and status within the industry, China's largest technology firms often work with the government to advance the PRC's cyber objectives. Qi An Xin, for example, has particularly close ties to government and regulatory organizations. Its products and services "have been adopted by over 90% of China's central government departments, central government-led enterprises, and large banks." [222]

In 2019, China Electronics Corporation, a state-owned enterprise, invested in the company, making Qi An Xin the national network security team.[223] Qi An Xin served as the "Official Cyber Security Services and Anti-Virus Software Sponsor of the Olympic and Paralympic Winter Games Beijing 2022."[224] In 2020, the firm was designated an "invisible champion" by the Beijing City Government, a moniker awarded "to companies that develop technology critical to China's national strategy."[225]

Other established cybersecurity companies have partnered with local authorities and universities to service China's National Cybersecurity Center (NCC) and establish research facilities at the site. These companies include Qi An Xin, TopSec, Tencent, Huawei, Integrity Tech (北京永信至诚科技), Qihoo 360, NSFocus, and DeepBlue AI (深兰科技).[226] These firms often receive government financing and subsidies, partner with government enterprises, and provide products, services, resources, and talent—not unlike their counterparts in other countries.

U.S. officials have accused TopSec and Qihoo 360 of providing talent and services to the PLA, and, in 2013, linked the firm to the hack of the health insurance company Anthem.[227] Venustech, Huawei, Alibaba, Baidu, Qihoo360, NSFocus, TopSec, Qi An Xin, Integrity Tech, and Tencent have sponsored the Tianfu Cup hacking competition, along with other organizations.[228] Qihoo 360's coordination with government authorities is particularly notable. The company delisted from the New York Stock Exchange in 2016 and re-listed in China to improve its access to PRC

[222] Qi An Xin Technology Group, LinkedIn, https://www.linkedin.com/company/qi-an-xin-group/about/.

[223] *Ibid*

奇安信，关于奇安信, https://perma.cc/E5DN-JER7.

[224] Qi An Xin, About Us, https://perma.cc/V6XD-UEMX.

[225] James Tarabay and Sarah Zheng*,* "Chinese Firm That Accused NSA of Hacking Has Global Ambitions," *Bloomberg* (May 31, 2022).

[226] Dakota Cary, *China's National Cybersecurity Center A Base for Military-Civil Fusion in the Cyber Domain,* (Washington: Center for Emerging and Security Technology, July 2021).

[227] "US embassy cables: China uses access to Microsoft source code to help plot cyber warfare, US fears," *The Guardian* (December 4, 2010); Ellen Nakashima, "Security firm finds link between China and Anthem hack," *Washington Post* (February 27, 2021).

[228] Tianfu Cup, http://www.tianfucup.com (June 26, 2022).

government and military contracts.[229] It has since cultivated close ties with the government.[230] The U.S. Department of Commerce placed Qihoo 360 on its Bureau of Industry and Security (BIS) Entity List in 2020.

The State Department has linked Qihoo 360 to COSEINC, a Singapore-based exploit broker that was placed on the BIS Entity list in 2021 for "malicious cyber activities."[231] Thomas Lim, COSEINC's founder, established the SyScan hacking conference in 2004. Qihoo 360 began sponsoring the conference in 2012[232] and purchased the brand from Lim in 2015, changing the name to SyScan 360.[233]

Lim cooperated with Pangu Lab, a cybersecurity research group that dominates technology competitions and has accused the U.S. National Security Agency (NSA) of placing an exploit on the Linux platform.[234] He was often invited to speak at MOSEC, a mobile security conference organized by Pangu and sponsored by several organizations, including Venustech (2015-2019), Huawei (2019-2021), Ant Group (2016-2021), Cyber Kunlun (2021), Qi An Xin (2010-2021), Baidu (2017-2021), Qihoo 360 (2015-2019), and Microsoft (2016).[235] The conference has also partnered with KnownSec and Tencent.

CloverSec (四叶草安全), designated by the CCIA as a "growth star" of the internet security industry, is another well-known company that helps to organize a number of security conferences and hacking competitions, including the Tianfu Cup.[236] These competitions are an integral part of a healthy and flourishing cyber industry in any country. Teams that participate in network security competitions typically share exploits with the software and hardware providers so that the companies can then fix any vulnerabilities.

The firm specializes in vulnerability detection and protection and has close ties to government authorities. Its founder, Ma Kun (马坤), was a well-known member of Honker Union

[229] Mohammed Shihab, "Expanding Cyber Demands Embolden China's Homegrown Cybersecurity Darlings: China is building a welcoming ecosystem for its homegrown tech darlings," *The Diplomat* (September 23, 2019).

[230] Elsa B. Kania and Lora Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy* (Washington: Center for New American Security, January 28, 2021).

[231] U.S. Dep't of State, *The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities* (November 3, 2021), https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/.

[232] Aqniu, 即将在太平洋彼岸召开的 SySan36 (May 25, 2017), https://web.archive.org/web/20220425030511/https:/www.aqniu.com/industry/25427.html.

[233] Christopher Bing, "UPDATE 5-U.S. blacklists Israeli hacking tool vendor NSO Group," *Reuters* (November 3, 2021), https://www.reuters.com/article/usa-cyber-nso-group-idCNL1N2RU19S.

[234] See discussion of Pwnzen Infotech Ltd, *infra.*

[235] MOSEC, 2021 Mobile Security Conference (July 30, 2021), https://www.mosec.org/en/2021/.

[235] Clover Sec, https://wwwseclover.com/stat1/.

[236] *Ibid*.

(HUC, 中国红客联盟), an early hacking collective emerged in response to the U.S. bombing of the Chinese embassy in Belgrade and became famous for infiltrating the video game company Blizzard Entertainment.[237]

Ma Kun started the company after working to detect vulnerabilities for CNCERT, a "non-government non-profit cybersecurity technical center" responsible for China's cybersecurity emergency response community.[238] The firm's investors include Ant Group, an affiliate company of Alibaba that deals with fintech.[239]

Many cybersecurity professionals in China start by working for established firms such as the ones above and then leave to form their own companies, taking with them years of experience and expertise in vulnerability and other security research. Others gain experience and develop personal networks from participating in security research competitions before venturing into the professional industry. Regardless of their origin, one or more of the larger tech conglomerates often back and support many of these firms. Qihoo 360 is particularly committed to fostering growth in the security market to promote a safe security ecosystem.[240] The companies below represent a small sampling of the breadth of cybersecurity research and development enterprises in China's technology market.

Examples of Chinese Cyber Firms

Company Name	Area(s)	Industry Leader/Giant Connection(s)
Tophant (斗象科技)	Vulnerability research, offensive & defensive research	Alibaba, Baidu
Cyber Kunlun (赛博昆仑)	Vulnerability research, advanced threat detection	Alibaba, Baidu, Huawei, NSFocus, Qi An Xin, Qihoo 360, TopSec, VenusTech
Chaitin Tech (长亭科技)	Vulnerability research, infiltration testing	Alibaba, Huawei, Tencent

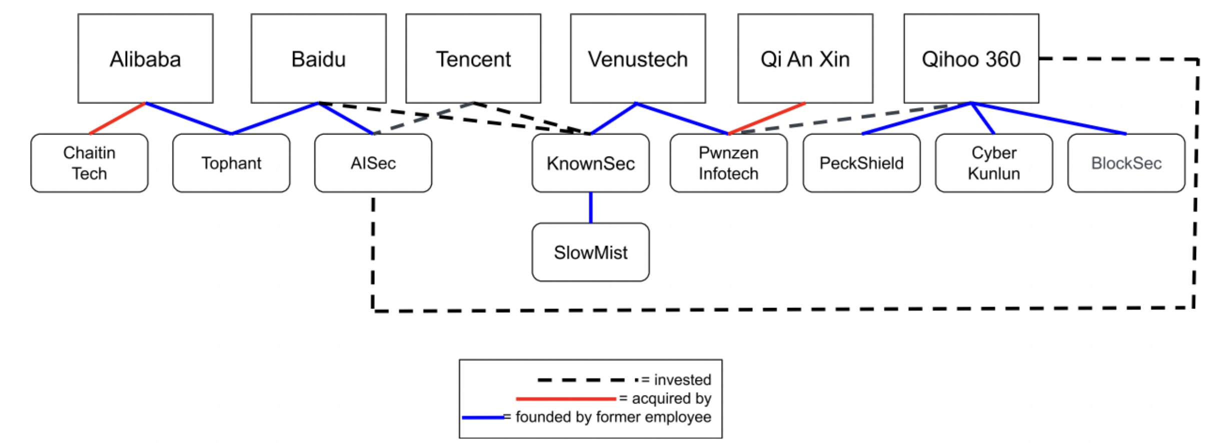
[237] 李泽辰, 四叶草安全马坤：从黑客到安全公司，从付不起工资到超三千万融资, 猎云网 (December 16, 2015), https://web.archive.org/web/20220419054719/https:/www.lieyunwang.com/archives/140340.

[238] *Ibid.*.; CNCERT/CC, https://www.cert.org.cn/publish/english/index.html.

[239] Song Jingli, "Ant Financial invests in cybersecurity firm Clover Sec," *KrASIA* (April 19, 2019), https://kr-asia.com/ant-financial-invests-in-cybersecurity-firm-clover-sec.

[240] 王潘, 一线｜周鸿祎发内部信：360 未来要投资至少 50 家安全公司, 腾讯科技 (April 14, 2019), https://web.archive.org/web/20220419055337/https:/tech.qq.com/a/20190415/008233.htm.

BugBank (漏洞银行)	Vulnerability research, advanced threat detection	Baidu, TopSec
KnownSec (知道创宇)	Vulnerability research, advanced threat detection	Venustech
SlowMist (慢雾科技)	Blockchain security	
AISec (安赛科技)	Vulnerability research, advanced threat detection	Baidu, Huawei, Qihoo 360
BlockSec	Blockchain security	Alibaba, Qihoo 360
PeckShield (**派盾科技**)	Blockchain security	Qihoo 360
Pwnzen Infotech Ltd. (**犇众信息**)	Vulnerability research, operating system security research, offensive & defensive research	Qi An Xin, Qihoo 360



Tophant (斗象科技)

Founded: 2014

2022 CCIA Ranking: 47

Investors: Eastern Bell Capital, Shenzhen Hui Capital Limited, Cowin Capital, Yinxinggu Capital, Linear Capital, China Electronics Technology Group, Spinnotec, Xiamen C&D Corporation, Zhangjiang Hi-Tech Investment, Qianhai FOF

One of the leading cybersecurity firms in the country, Tophant, offers cybersecurity testing, monitoring, and data analysis for government enterprises and clients in finance, entertainment, e-commerce, and other industries.[241] Prior to starting Tophant, Chen Xie (谢忱), the current CEO, was employed as a Network Security Expert at Alibaba and Baidu, and he now serves as an external expert to the China Academy of Information and Communications Technology, a research institute under the Ministry of Industry and Information Technology (MIIT). Tophant's investors also include the China Electronics Technology Group (CETC), a PRC state-owned company.[242]

Tophant provides support to CNCERT and China's National Vulnerability Database (CNVD), and acts as an Advanced Support Unit for Shanghai's municipal network security system.[243] The firm has collaborated with State ministries, such as the Ministry of Public Security (MPS), to conduct research into vulnerability mining and offensive and defensive techniques.[244] Tophant also hosts Freebuf, an online forum for cybersecurity professionals and hackers.[245]

Pwnzen Infotech Ltd. (犇众信息)

Founded: 2014

Pwnzen Infotech Ltd. was founded by a team of veterans in information security and vulnerability exploitation. Zhengguang Han (韩争光), a cofounder and the current CEO, previously worked for Fortinet, Inc. Xiaobo Chen (陈小波), another cofounder, was a security researcher with Venustech, Intel Security (now McAfee), and FireEye. Yexuan Chen (陈业), the current head of data security and R&D, previously worked at Knownsec (see below).[246] The firm was backed in its early days by Qihoo 360, a behemoth in China's cybersecurity industry, before being acquired by Qi An Xin.[247]

[241] Liya Su, "China Deal Monitor: Cybersecurity Firm Tophant bags over $14m and more," *Deal Street Asi*A (February 24, 2020), https://www.dealstreetasia.com/stories/china-deal-monitor-tophant-176296.

[242] "Cybersecurity firm Tophant gets backing from state defence group CETC," *Intelligence Online* (August 30, 2021), https://www.intelligenceonline.com/surveillance--interception/2021/08/30/cybersecurity-firm-tophant-gets-backing-from-state-defence-group-cetc,109687588-art.

[243] *Ibid*

斗象科技, 公司简介, https://perma.cc/74A8-VY2H.

[244] 公安部第三研究所与斗象科技联合成立"神剑实验室," *China Daily* (July 26, 2021), https://perma.cc/9QDV-L7FC.

[245] Freebuf, https://www.freebuf.com.

[245] *Ibid*

犇众信息, 核心成员, https://perma.cc/V8VX-NE6H.

[247] Pei Li and Cate Cadell, "At Beijing security fair, an arms race for surveillance tech," *Reuters* (May 30, 2018), https://www.reuters.com/article/ctech-us-china-monitoring-tech-insight-idCAKCN1IV0OY-OCATC.

The heart of Pwnzen is its cybersecurity team, Pangu Team (盘古团队), which is well known for its exceptional skill in hacking competitions. The team placed second in the most recent Tianfu Cup, a hacking competition where participants were able to exploit weaknesses in software code—vulnerabilities—to infiltrate Windows 10, Adobe PDF Reader, Ubuntu, Apple iOS 15 and Safari, and Google Chrome, among several other products. The team was awarded the highest cash reward in the competition for their exploit.[248]

Pangu Team, in turn, established Pangu Lab[249] (盘古实验室), which conducts "advanced security research and attack and defense research."[250] The lab made waves in late February 2022 when it published a report linking a 2013 exploit targeting the Linux platform to the U.S. National Security Agency (NSA).[251]

Cyber Kunlun (赛博昆仑)

Founded: 2021

Investors: CICC Capital, Hike Capital, Sequoia Capital China, ZhenFund

Cyber Kunlun is well-known for winning first place in the Tianfu Cup competition, which it also helps organize.[252] Its founder and CEO, Wenbin Zheng (郑文彬, mj0011),[253] formerly served as the Chief Technology Officer of Qihoo 360.[254] During his tenure at Qihoo 360, he established the infamous 360 Vulcan research team, known for their exploits at Pwn2Own, an international hacking competition based in Canada.[255] Xuebin Chen (陈雪斌), Cyber Kunlun's

[248] Davey Winder, "iPhone 13 Pro Hacked: Chinese Hackers Suddenly Break iOS 15.0.2 Security," *Forbes* (October 18, 2021), https://www.forbes.com/sites/daveywinder/2021/10/18/iphone-13-pro-hacked-chinese-hackers-suddenly-break-ios-1502-security/?sh=5a7d80e91fe6.

[249] https://www.pangulab.cn

Pangu Lab, https://www.pangulab.cn.

[250] Pangu Lab, About Pangu Lab (February 20, 2022), https://perma.cc/6GCN-S8P3.

[251] Bvp47 Top-tier Backdoor of US NSA Equation Group. 分析简版-英文 (pangulab.cn).

[252] Eduard Kovacs, "$1.9 Million Paid Out for Exploits at China's Tianfu Cup Hacking Contest," *Security Week* (October. 19, 2021), https://www.securityweek.com/19-million-paid-out-exploits-chinas-tianfu-cup-hacking-contest.

[253] Wenbin Zheng (@mj0011), *Twitter*, https://twitter.com/mj0011sec.

[254] 何帅, 专访中国顶尖黑客 mj0011：其实没有那么多不平凡 (August 15, 2014), https://web.archive.org/web/20220419223219/http://www.heshuai.net/526.html.

[255] John Cusack, "Pwn2Own and 360Vulcan: the interview," *Geek Reply* (March 27, 2015), https://perma.cc/G384-BV4C; 360 安全研究团队, http://www.360.cn/vulreport.html.

Chief Technology Officer, also worked as a director at Qihoo 360's Vulnerability Research institute.[256]

Cyber Kunlun's researchers are at the forefront of vulnerability research. Their stated focus is providing exclusive defense capabilities for zero-day vulnerabilities.[257] Vulnerabilities, according to Zheng, are the core of offense and defense in cybersecurity, as hackers need first to obtain vulnerabilities if they want to attack a company.[258] Zheng notes that supporting affected enterprises by sharing discovered vulnerabilities is "one of [the] key[s] to a good research team."[259] Cyber Kunlun has identified and reported dozens of vulnerabilities in Windows, iOS, Google, open-source, and VMware products. Of Microsoft's 145 vulnerability fixes from April's Patch Tuesday, 36 were reported by Cyber Kunlun, including half of the 10 most significant vulnerabilities.[260]

The firm continues to work with Qihoo 360 and other major tech firms in organizing the Tianfu Cup and has partnered with the aforementioned Pangu Lab to coordinate their respective teams' knowledge in vulnerability mining and protection and advanced threat detection and response to develop new security products and services.[261]

Chaitin Tech (长亭科技)

Founded: 2014

2022 CCIA Ranking: 22

Investors: ZhenFund, Matrix Partners China, Junsan Capital, Qiming Venture Partners, Apple Funds, Didi Global, Peakview Capital (China)

Chaitin Tech's founders have impressive backgrounds. Wenlei Zhu (朱文雷), Kun Yang (杨坤), and Yusen Chen (陈宇森) met as members of the Blue Lotus hacking teams, known for their exemplary performance in the DEFCON CTF competitions before deciding to form a

[256] 刘沙, 赛博昆仑完成新一轮早期融资，半年多融资额共计近 1.5 亿元, *CCW* (December 28, 2021), https://perma.cc/4CWU-KDT4.

[257] Speakers of ZeroCon, *ZeroCon*, https://zer0con.org/#speaker-section.

[258] 真梓, 36 氪首发丨「赛博昆仑」完成近亿元新一轮融资，半年内融资总额近 1.5 亿元, 36Kr (December 12, 2021), https://web.archive.org/web/20220627034126/https://36kr.com/p/1546386100349192.

[259] Ed Targett, "NSA reports 1 bug under attack, Chinese firm 36, as Patch Tuesday lands with 0 days, drama," THE STACK (April 12, 2022), https://web.archive.org/web/20220419222639/https:/thestack.technology/april-patch-tuesday-hyper-v-rce/.

[260] *Ibid.*

[261] 盘古实验室签约赛博昆仑，国内两大白帽天团强强联合, *Freebuf* (July 20, 2021), https://archive.ph/T5IfG#selection-1989.0-2003.0.

business together.[262] Chen now sits on the board of Saitech, a Singapore-based bitcoin mining operation, and also founded Hangzhou Jiao Gei Mao Ba Technology, which specializes in the application of AI to gaming.[263]

Chaitin Tech's team has won multiple domestic and foreign network security competitions and provides infiltration testing and security consulting services to a wide range of customers.[264] It is host to its own CTF competition, with questions designed from the modification of real-world software.[265] This impressive performance has earned its founders the "favor and recognition" of the Cyberspace Administration of China, MIIT, and MPS.[266]

Clients include DiDi Chuxing, Tencent, Bank of China, Agricultural Bank of China, China Merchants Security, Douyin, China Southern Airlines, Unilever, Huawei, Panasonic, Vivo, China Mobile, and VIPKid, among many others. The startup was acquired by Alibaba Cloud in 2019 but has been allowed to continue to operate independently.[267]

BugBank (漏洞银行)

Founded: 2012

Investors: Puhua Capital, SB China Capital, NewMargin Ventures

Bugbank, an internet security service platform under Shanghai Moule Network Technology Co., Ltd., operates an automated vulnerability diagnosis system and has accumulated a database of vulnerabilities following years of research.[268] Its founders, including Xiaonan Bao

[262] 长亭外，陈宇森和他的伙伴们，知乎 (May 17, 2016), https://web.archive.org/web/20220627034759/https://zhuanlan.zhihu.com/p/20915607.

[263] Saitech Limited, "SAITECH Announces Two New Members to the Board of Directors," *Globe Newswire* (December 6, 2021), https://web.archive.org/web/20220627035027/https://www.globenewswire.com/news-release/2021/12/06/2346281/0/en/SAITECH-Announces-Two-New-Members-to-the-Board-of-Directors.html.

[264] 张超, 朱文雷｜从清华学子到胡润榜领袖，一位 90 后学霸的创业之路, 清华交友综总会 (November 1, 2019), https://web.archive.org/web/20220419194604/https:/www.tsinghua.org.cn/info/1953/14218.htm.

[265] 中国经济网, "长亭科技杨坤：学霸团队是如何创业的?" Qianlong (December 1, 2019), http://china.qianlong.com/2019/1201/3456771.shtml.

[266] 张超, 朱文雷｜从清华学子到胡润榜领袖，一位 90 后学霸的创业之路, 清华交友综总会 (November 1, 2019), https://web.archive.org/web/20220419194604/https:/www.tsinghua.org.cn/info/1953/14218.htm.

[267] 长亭科技, 长亭科技被阿里云全资收购，全面升级安全服务能力, 微信 (October 10, 2019), https://web.archive.org/web/20220419195242/https:/mp.weixin.qq.com/s/wrTvo6YapAuVxEZ1p98-Pw.

[268] BugBank, Cybersecurity Excellence Awards, https://cybersecurity-excellence-awards.com/candidates/bugbank/.

(鲍晓南), CTO Xuesong Zhang (张雪松), and CEO Luo Qinglan (罗清篮), developed the database as means to bring together white hat hackers and domestic enterprises in an effort better to coordinate emergency responses to vulnerabilities and exploitation risks.[269] BugBank was designed and operates based on the view that cooperation among actors in the domestic security industry is better for security than competition.[270]

Bugbank employees have strong backgrounds in information security. The BugBank Red Team consists of 30,000 cybersecurity experts with experience in a variety of areas, including "hacking" and "cracking."[271] The founding team, prior to creating Moule, provided vulnerability discovery and detection services for the 2008 Beijing Olympics.[272]

CEO Luo Qinglan personally began hacking at a young age after experiencing the "first hacker war"—an incident in 1999 where American and Chinese hackers exchanged a series of cyber attacks after American bombs intended for a nearby warehouse were aimed at the Chinese embassy in Belgrade, killing three people.[273] As a student in high school and college, he worked as a white hat hacker and won several awards for his work in network security.

The company coordinates with partners at different levels of cooperation. Their strategic partners include departments within the Shanghai government, the Chinese National Vulnerability Database of Information Security (CNNVD), and the Open Web Application Security Project (OWASP). Bugbank also maintains "friendship links" with Baidu and TopSec, among others.[274]

KnownSec (知道创宇)

Founded: 2007

[269] 小微, 漏洞银行希望通过市场化手段"收编"黑客为企业服, CHINA DAILY (October 15, 2015), https://web.archive.org/web/20220421063807/http:/covid-19.chinadaily.com.cn/hqgj/jryw/2015-10-15/content_14259385.html.

[270] 风口浪尖的白帽创业老兵 "漏洞银行"创始人 罗清篮专访, SOHU (August 2, 2016), https://web.archive.org/web/20220421051942/https:/www.sohu.com/a/108759699_184952.

[271] Bugbank Red Team, https://www.bugbank.cn/redteam.html.

[272] 第一财经专访漏洞银行联合创始人鲍晓南：用攻击者视角守护企业信息安全, 中华网 (February 21, 2022), https://web.archive.org/web/20220421063417/https:/hea.china.com/article/20220221/022022_1013524.html.

[273] 沈梦雪，创业让年轻的创业者更有力量 (September 22, 2015), https://web.archive.org/web/20220421045823/http:/app.why.com.cn/epaper/qnb/html/2015-09/22/content_269079.htm. Also https://en.wikipedia.org/wiki/United_States_bombing_of_the_Chinese_embassy_in_Belgrade.

[274] BugBank, https://www.bugbank.cn.

Investors: China Internet Investment Fund, Tencent, Baidu

Wei Zhao (赵伟), one of KnownSec's founders, worked as a security researcher at Venustech and McAfee Security Lab prior to starting the company.[275] The firm has grown to encompass three research and development centers in Beijing, Chengdu, and Wuhan, with branches in several other cities. Over 1,800 employees work for the company in a variety of areas.

KnownSec's brands approach information security from a number of points.[276] The 404 Lab is a relatively well known team that has uncovered several vulnerabilities in network systems, including Microsoft, Oracle[277], and Apple.[278] ZoomEye is an internet-scale network scanner that maps cyberspace.[279] Seebug is a vulnerability database where hackers can submit vulnerabilities for rewards. POCSuite3 is a framework to verify and exploit vulnerabilities. Ceye.IO is a tool for monitoring the Domain Name System (DNS) and "can help security researchers collect information when testing vulnerabilities."[280] KnownSec even hosts its own hacking competition, known as KCon.

Because KnownSec believes that "there is no national security without cybersecurity," the firm has committed to following Party leadership, established a Party branch in 2012, and organized a security team composed of party members. The company website states that "the essence of network security is confrontation, and the essence of confrontation is the ability to compete on both ends of the offensive and defensive."[281]

KnownSec provides services to the Party, government, military, and private enterprises and citizens. Customers include the Cyberspace Administration of China, MIIT, MPS, the State Administration for Market Supervision, China Merchants Group, China Communications Construction Company, China General Nuclear Power, WeChat, Douyin, and Weibo.[282] In 2021,

[275] Wei Zhao, *LinkedIn*, https://www.linkedin.com/in/knownsec/.

[276] Anthony Lai, *Threat Trend, Intelligence and Response*, Knownsec Hong Kong, https://web.archive.org/web/20220421215731/https:/i40.hkpc.org/CyberSec/pdf/Day%201_1400-1440_Mr.%20Anthony%20Lai%20%28new%29.pdf.

[277] KnownSec 404 Team, "Oracle WebLogic Deserialization RCE Vulnerability (0day) Alert (update on April 26, 2019)," *Medium* (April 21, 2019).

[278] "About the Security Content of Safari 15.3," APPLE (January 26, 2022), https://support.apple.com/en-us/HT213058.

[279] *Ibid.*

https://www.zoomeye.org

[280] Introduce, Ceyo.io, http://ceye.io/introduce.

[281] *Ibid.*

[282] *Ibid.*

[283] 我们是谁, 知道创宇, https://www.knownsec.com/#/intro.

KnownSec was selected to serve as a National Network Security Emergency Service Support Unit for CNCERT.

AISec (安赛科技)

Founded: 2012

Investors: Tencent, Qihoo 360

AISec (which stands for Artificial Intelligence Security)[283] was founded by Lin Yujian (林榆坚), who previously worked as a network security researcher at Baidu.[284] The company focuses on research in threat detection technologies, including data analysis, vulnerability mining, and intrusion detection. It is known for its vulnerability scanning product, AIScanner, and WebIDS. A version of AIScanner serves as an Internet vulnerability and intrusion detection system. AISec uses their technology to maintain a platform for analyzing and monitoring advanced persistent threats (APT).

Although their customers are far too many to list, AISec has provided services for large tech companies, government ministries, and information security authorities, including Qihoo 360, Huawei, Baidu, the National Research Center for Information Technology Security, the China Information Technology Security Evaluation Center, CNERT/CC, the China Academy of Information and Communications Technology, the Ministry of Public Security, the Ministry of Culture, the Ministry of Science and Technology, and the Ministry of Industry and Information Technology.[285]

AISec is certified by the Ministry of Industry and Information Technology as a National Information Technology Talent Training Base, a certification established as part of China's strategy to foster domestic talent in critical technologies.[286] The company also serves as a technological support unit for the National Vulnerability Database of Information Security (CNNVD), operated by the China Information Technology Security Evaluation Center (中国信息

AISec, https://www.aisec.com/cn/about.php.

[284] 云海, 获 360 和腾讯投资 "安赛科技"保障企业信息安全 曾服务央行建行, *Pencil News*, https://web.archive.org/web/20220420195856/https:/www.pencilnews.cn/d/17007.html; 邹江, 他是一名来自玉林的 80 后 CEO, 玉林新闻网 (March 14, 2019), https://web.archive.org/web/20220421072011/https:/www.sohu.com/a/301281518_99894401.

AISec, 典型案例, https://www.aisec.com/cn/whouse.php.

[286] AISec, 关于我们, https://www.aisec.com/cn/about.php

安全测评中心), "a state agency that provides cybersecurity services to the PRC government and large Chinese corporations."[287]

SlowMist (慢雾科技)

Founded: 2018

Shareholders: Chenming Zhong, Qi Wu (吴琦/Chairman), Weipeng Huang (黄伟鹏), Bi Huang (黄比)

SlowMist, a blockchain security firm, was founded by former KnownSec VP Chenming Zhong (钟晨鸣, handles: cosine/余弦/evilcos).[288] Zhong is a "well-known hacker" from the xeye team that created KnownSec's ZoomEye, led the 404 team, and founded the company Joinsec.[289] Zhong maintains that the primary values of SlowMist are, in order of importance, don't be evil, don't have a poor attitude, and approach network security with a sense of reverence.[290]

SlowMist quickly became well-known for reporting several previously unknown and undisclosed vulnerabilities during the March 2018 Ethereum Black Valentine's Day event. The company now offers security services to thousands of customers, including security auditing, threat intelligence, and other consulting firms.[291] Their products include anti-money laundering software, a vulnerability scanner, Crypto hack archives, and a smart contract firewall.

SlowMist has worked on a number of projects, including Huobi, Binance, Crypto.com, EOS, and Amber Group, and partnered with international companies such as Amazon Web Services, Cloudflare, Bitdefender, and FireEye.[292]

According to the company website, SlowMist has "actively participated" in promoting blockchain security standards. It was one of the first to join the MIIT working group for the "2018

[287] China Information Technology Security Evaluation Center, "Research Report on the Status of China's Information Security Professionals 2018-2019," Ben Murphy ed., Etcetera Language Group, Inc. trans., (CSET 2020), https://cset.georgetown.edu/wp-content/uploads/t0231_cyber_employment_report_EN.pdf

[287] *Ibid.*, 3.

[288] 从传奇黑客到安全专家 慢雾科技创始人余弦站在区块链安全战争最前线, 金色财经 (March 8, 2021), https://web.archive.org/web/20220423000307/https:/www.jinse.com/news/blockchain/1018008.html.

[289] Ripple, 专访慢雾余弦：区块链安全漏洞引起的资产损失在未来将进一步扩大|算力波, 新浪财经 (October 29, 2019), https://web.archive.org/web/20220421233522/https:/finance.sina.com.cn/blockchain/2019-10-29/doc-iicezzrr5812052.shtml.

[290] *Ibid.*

[291] SlowMist, 关于我们, https://www.slowmist.com/about-us.html.

[292] SlowMist, *About Us*, https://www.slowmist.com/en/about-us.html; SlowMist, Partners, https://www.slowmist.com/en/#partners.

China Blockchain Industry White Paper" and is a member of the "Joint Laboratory of Blockchain and Network Security Technology" in the Guangdong-Hong Kong-Macao region.[293]

BlockSec

Founded: 2021

Investors: Fenbushi Capital, A&T Capital, Qulian, Impossible Finance, Incuba Alpha, Near MetaWeb Ventures

A new company, BlockSec primarily focuses on blockchain security and governance through the development of platforms that help to monitor cryptocurrency and related interactions, such as providing smart contract transaction auditing.[294] BlockSec lists among its clients Amber Group, Ant Group, Burrow, Crypto.com, Impossible Finance, and Tidal Finance.

The firm was founded by Yajin Zhou (周亚金) and Lei Wu (吴磊), who worked at Qihoo 360 as security researchers and who currently work as professors at the School of Cyber Science and Technology and the College of Computer Science and Technology at Zhejiang University.[295] Yajin Zhou's research interests include "software security, operating systems security, hardware-assisted security and confidential computing," particularly in the areas of smart contracts and decentralized finance.[296]

PeckShield (派盾科技)

Founded: 2018

Investors: Gaorong Capital

Another firm focused on blockchain security, PeckShield was founded in 2018 by BlockSec's founder Lei Wu, Xuxian Jiang[297] (蒋旭宪), a former Chief Scientist with Qihoo 360, and Chiachih Wu (吴家志), a senior security researcher at Qihoo 360.[298] Jiang also served as a

[293] MIIT, 2018 年中国区块链产业白皮书 (2018), https://web.archive.org/web/20220421115930/https:/www.miit.gov.cn/n1146290/n1146402/n1146445/c6180238/part/6180297.pdf.4294

[294] BlockSec, https://blocksec.com.

[295] 周亚金, https://person.zju.edu.cn/yajin#0; Lei Wu, LINKEDIN, https://www.linkedin.com/in/lei-wu-1685842a/?originalSubdomain=cn; 吴磊, https://person.zju.edu.cn/lei_wu.

[296] Yajin Zhou, https://yajin.org.

[297] Xuxian Jiang, *LinkedIn*, https://www.linkedin.com/in/xuxianjiang/.

[298] Dfuse, "In the Eyes of a Blockchain Developer: Chiachih Wu from PeckShield," *Medium* (March 6, 2019), https://medium.com/@dfuseio/in-the-eyes-of-a-blockchain-developer-chiachih-wu-from-peckshield-d7740b9a6889.

PhD advisor to Wu, Lei, and Yajin Zhou while working as a professor at North Carolina State University.[299]

PeckShield touts the substantial experience of its employees, who have worked as "seasoned security professionals and senior researchers . . . at companies such as Qihoo 360, Microsoft, Intel, Juniper, and Alibaba" and are known for their achievements in "vulnerability analysis, operating systems, and malware defense."[300] The company aims to use its team's extensive experience in security research to analyze risks in public blockchains in order to develop responses to risks.[301]

To help clients prevent hacking attacks, PeckShield developed a platform, DAppShield, that allows clients to conduct security testing and monitor funds. The firm offers products to manage and monitor digital assets. Clients primarily include blockchain infrastructure vendors, crypto wallets, and exchange companies, such as Bitpie, KuCoin, and Newdex.

[299] 全球顶尖区块链安全公司派盾科技（PeckShield）获高榕资本数千万元天使轮融资, *GeekPark* (June 6, 2018), https://web.archive.org/web/20220421082155/https://www.geekpark.net/news/229781.

[300] *Ibid.*

PeckShield, https://peckshield.com/#about.

[301] https://web.archive.org/web/20220420062746/https://blog.csdn.net/weixin_43891115/article/details/88412870;
https://web.archive.org/web/20220420062746/https://blog.csdn.net/weixin_43891115/article/details/88412870

5. Personnel Recruitment and Operations

According to Xi Jinping, "competition in cyberspace is, ultimately, a competition for talent."[302] China recruited talented hacking personnel by taking advantage of Chinese hackers' patriotism and by co-opting existing criminal hacking collectives. China increasingly has moved towards professionalizing its cybersecurity operations, focusing its attention on developing local talent through elite institutions, integrating military and civil cyber ecosystems, and bolstering the private tech sector while still maintaining close government ties with it.

History

China's first hackers emerged after the Internet was introduced to the country in the late 1990s. Indignant at what they saw as a series of humiliations dealt against China by foreign nations, young Internet enthusiasts online began to form loosely connected nationalist hacking groups.[303] The first of these, the Green Army (绿盟), cut its teeth attacking Indonesian websites during the 1998 riots in Jakarta, during which many ethnically Chinese Indonesians were victims of violence.[304]

Following the May 1999 U.S. bombing of the Chinese embassy in Belgrade, Yugoslavia, the Green Army, as well as the newly formed hacking collective known as the Honker Union (中国红客), launched a series of cyberattacks against U.S. government networks.[305] Hackers also turned their sights to Taiwan and Japan, defacing a number of government sites in objection to Lee Teng-hui's "two-state" theory and accusing Japan of denying the Rape of Nanjing and whitewashing wartime atrocities in China.[306]

In 2001, a reckless Chinese fighter pilot collided with a Navy signals intelligence aircraft, killing the fighter pilot. The damaged American plane was forced to land on the nearby Hainan

[302] 习近平，*在网络安全和信息化工作谈会上的讲话*，新华社 (Apr. 19, 2016), https://perma.cc/JW2N-22BH?type=image.

[303] 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).

[304] Mitch Edwards, "China's Green Army: Capitalism Defeats China's First Hacking Group," *Medium* (March 28, 2018), https://medium.com/@theCTIGuy/chinas-green-army-capitalism-defeats-china-s-first-hacking-group-d4c73631d2ca.

[305] Michelle Delio, "A Chinese Call to Hack U.S.," *Wired* (April 11, 2001), https://www.wired.com/2001/04/a-chinese-call-to-hack-u-s/. It is hard to imagine that the attacks on the U.S. Embassy compound in Beijing and cyber attacks would have taken place without the blessing of the Chinese government.

[306] Ginny Parker, "Japan Wakes Up to Hackers," *ABC News* (January 28, 2001).

Island, where the crew was detained by Chinese authorities.[307] American and Chinese hackers reacted to the incident by targeting websites with cyber-graffiti of flags, photos, and messages.[308] Led by the Honker Union, Chinese hackers declared war on the United States shutting down the White House website, infecting a number of other computer networks with viruses, and disrupting servers with denial of service attacks.[309]

Alarmed by the activity, the People's Daily, the official newspaper of the Central Committee of the Chinese Communist Party, published an editorial decrying "web terrorism" and urging Chinese hackers to cease attacking U.S. sites.[310] The hackers agreed to call off the war, declaring that they had achieved their goals.[311]

Veterans of these hacking collectives formed much of China's early cybersecurity industry. The Green Army began its first venture into more professional strata in 1999, when it hosted the "first known for-profit security conference" in Shanghai.[312] Members became drawn into a legal battle shortly after, torn between forming a non-profit security company or pursuing a for-profit model instead. In the end, commercial interests won out, and the winning members formed the internet security company NSFocus.

Other cybersecurity companies were quick to hire early generation hackers: TopSec, a computer security service, hired the founder of the Honker Union, Lin Yong, while Qihoo 360 brought on Yuan Renguang and Pan Jianfeng, two well-known hackers in the 1990s.[313] Private companies were not the only ones who took notice. The PLA and other Chinese government institutions have recruited early generation hackers from their universities into the PLA and other government institutions.

University Recruitment and Involvement in Cyber Operations

Since 2015, China has implemented policies to replace its criminal hacking groups with professionals cultivated at home.[314] Chinese public officials have long recognized the need to cultivate local expertise in important economic sectors and areas relevant to national security, and improving domestic education plays a central role in cultivating this talent. Chinese universities develop top talent, conduct sensitive research programs in tandem with, or funded by, the

[307] Craig S. Smith, "May 6-12; The First World Hacker War," *The New York Times* (May 13, 2001).

[308] Rose Tang, "China-U.S. Cyber War Escalates," *CNN* (May 1, 2001).

[309] Smith, *May 6-12; The First World Hacker War*, *op. cit.*

[310] Dorothy Denning, "Cyberwar: How Chinese Hackers Became a Major Threat to the U.S.," *Newsweek* (October 5, 2017).

[311] Smith, *May 6-12; The First World Hacker War*, *op. cit.*

[312] Edwards, *China's Green Army, op. cit.*

[313] 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*" *op. cit.*

[314] Dakota Cary, "China's next generation of hackers won't be criminals. That's a problem," *TechCrunch* (2021).

government, and act as recruitment pipelines for the PLA, MSS, and related contractors. Beijing has recruited experts from overseas and retained local talent that might otherwise be interested in studying or working abroad.[315] Chinese universities develop top talent, conduct sensitive research programs in tandem with, or funded by, the government, and act as recruitment pipelines for the PLA, MSS, and related contractors.

China's recruitment efforts in cyber are part of a larger effort to recruit and retain expertise in a variety of critical areas for national security. In 2008, the then head of the CCP's Organization Department, Li Yuanchao, introduced the "Thousand Talents" Plan, an attempt to reverse the brain drain of Chinese scientists and academics who studied and remained overseas by incentivizing them to return to China.[316]

By offering financial and other prestige benefits through this and similar programs, China has been able to recruit Chinese citizens and foreigners to work in high-priority research areas in Chinese companies and universities.[317] Of the 3,600 people offered monetary awards and positions under the Youth Thousand Talents plan, approximately 288 were offered positions at institutions that are part of, or have close relationships with, the defense industry, and more than 500 were offered positions at laboratories managed by the Chinese Academy of Sciences.[318]

First-rate talent, however, will only want to go to first-rate institutions. Realizing that these recruitment drives were insufficient to generate the scope and range of talent that China hoped to entice, the government implemented a series of policies to reform local universities into elite institutions for cyber training. The CAC, in collaboration with the Ministry of Education, generated a plan to develop World Class Cybersecurity Schools (一流网络安全学院) by partnering with universities to develop elite cybersecurity training programs.[319]

[315] Remco Zwetsloot, "China's Approach to Tech Talent Competition: Policies, Results, and the Developing Global Response," *Global China* (April 2020), https://cset.georgetown.edu/publication/chinas-approach-to-tech-talent-competition-policies-results-and-the-developing-global-response/.

[316] David Zweig and Huiyao Wang, "Can China Bring Back the Best? The Communist Party Organizes China's Search for Talent," *The China Quarterly* (September 12, 2013); and John Brown, *Securing U.S. Research Enterprise from China's Talent Recruitment Plans*, Statement before the Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations (November 19, 2019).

[317] https://cset.georgetown.edu/publication/detailed-rules-for-the-thousand-talents-program-high-level-foreign-expert-project/ *Communist Party of China Central Organization Department, Detailed Rules for the "Thousand Talents Program" High-Level Foreign Expert Project, Beijing Institute of Technology* (Ben Murphy ed., Etcetera Language Group, Inc. trans., 2011).

[318] Ryan Fedasiuk and Jacob Feldgoise, "The Youth Thousand Talents Plan and China's Military," *CSET* (August 2020).

[319] 关于印发《一流网络安全学院建设示范项目管理办法》的通知， 中华人民共和国教育部 (2017), http://www.moe.gov.cn/srcsite/A16/s3342/201708/t20170815_311176.html; 国务院, 国务院关于印发统筹推进世界一流大学和一流学科建设总体方案的通知, 中华人民共和国中央人民政府 (Oct. 24, 2015).

Since its launch, the CAC has designated 11 universities as World Class Cybersecurity Schools (WCCS).[320] Students at these universities take courses on AI and big data management, vulnerability analysis, and network attack and defense, among other subjects.[321] The schools' focus on AI and machine learning may provide China's future cybersecurity professionals with an advantage over their U.S counterparts as U.S. CAE-Cyber Operations Degrees lack the multitude of options offered by these programs.[322] These universities produce "graduates capable of attacking and defending networks, regardless of how international firms or assessments rank the institutions."[323]

In addition to implementing first-rate education programs, designated universities also partner with the government. Two of the eleven World Class Cybersecurity Schools, Wuhan University and Huazhong University, have jointly created the National Cybersecurity School at the National Cybersecurity Talent and Innovation Base (国家网络安全人才与创新基地, The National Cybersecurity Center), which also contains two government-program, focused laboratories.[324] Members from the CCP's Cyberspace Affairs Commission oversee the Center. In 2022 alone, 1,300 students are set to graduate from this joint National Cybersecurity School.

University and academic links to China's military and defense industry run deep. As of 2009, the PLA and the State Administration for Science, Technology and Industry for National Defense (国家国防科技工业, SASTIND, a subordinate agency of the MIIT), supervised around 74 national defense science and technology key laboratories (国防科技重点实验室), 39 of which were located in civilian universities.[325] In addition, 36 national defense key discipline labs (国防重点学科实验室) and 53 Ministry of Education defense labs (教育部国防重点实验室) operate out of nonmilitary universities.[326]

Seven universities in particular—Northwestern Polytechnical University, Harbin Engineering University, Beijing Institute of Technology, Harbin Institute of Technology, Beihang University (also a WCCS), Nanjing University of Aeronautics and Astronautics, and Nanjing University of Science and Technology—operate under the direction of the Ministry of Industry and Information Technology through the SASTIND.[327] Known as the Seven Sons of National

[320] 一流网络安全学院建设示范项目高校增至 11 所, 中华人民共和国国家互联网信息办公室 (September 17, 2019).

[321] Dakota Cary, "China's CyberAI Talent Pipeline," *CSET* (2021), https://cset.georgetown.edu/publication/chinas-cyberai-talent-pipeline/.

[322] Cary, *China's CyberAI Talent Pipeline*, *op. cit.*

[323] *Ibid.*

[324] Dakota Cary, *China's National Cybersecurity Center* (Washington: CSET, July 2021).

[325] Alex Joske, *The China Defence Universities Tracker* (Barton: Australian Strategic Policy Institute, November 25, 2019).

[326] *Ibid.*

[327] *Ibid.*

Defense (国防七子), these universities graduate thousands of students who join organizations and companies in defense research every year.

In 2016, China's defense industry employed 36% of Master's graduates and 51% of Ph.D. graduates from Beihang University.[328] Both Huawei and ZTE are counted among their top employers.[329] China's state-owned defense enterprises recruit from elite universities, particularly graduate students. In 2019, they hired 6,000 graduates from 29 universities, 72 percent of which graduated from the Seven Sons.[330] Many U.S. companies, including Microsoft, Dell, Google, IBM, Intel, Texas Instruments, Honeywell, and Synopsys, have established training programs with the Seven Sons on machine learning, big data, and integrated circuit design, despite their close ties to China's military and defense industry.[331]

In addition to training next generation offensive cyber talent and conducting cutting edge research on behalf of government ministries, Chinese universities have been directly implicated in cyberattacks. Zhejiang University and Harbin Institute of Technology are identified recruitment sources for APTs.[332] Taiwan and the United States have accused a Ministry of Education laboratory at Wuhan University, the Key Laboratory of Aerospace Information Security and Trusted Computing, of conducting cyberattacks on behalf of the PLA against the Pentagon and U.S. Government.

Among the APT1 hackers,[333] originally attributed in 2013 to the PLA Unit 61398,[334] was Mei Qiang (alias Super Hard), linked to the PLA Information Engineering University (PLAIEU).[335] The PLAIEU has multiple professors accused of perpetrating cyberattacks.[336] Members of Unit 61398 were also linked to Shanghai Jiao Tong University and likely recruited graduate students for the Unit from Zhejiang University's College of Computer Science and Technology.[337]

[328] 北航信息公开网， 北京航空航天大学一流大学建设方案, 北京航空航 天大学 (Dec. 29, 2017).

[329] Joske, *The China Defence Universities Tracker., op. cit.*

[330] Ryan Fedasiuk and Emily Weinstein, "Universities and the Chinese Defense Technology Workforce," *CSET* (December 2020).

[331] *Ibid.*

[332] Dakota Cary, *Academics, AI, and APTs*, CSET (March 2021).

[333] *United States v. Wang Dong, et al.,* No. 14-cr-118 (W.D. PA, May 1, 2014). For an analysis of this case and subsequent cases against Chinese hackers see Nicolas Rostow and Abraham Wagner, *Cybersecurity and Cyberlaw* (Durham: Carolina Academic Press, 2020), pp. 758-787.

[334] Dan McWhorter, "APT 1: Exposing One of China's Cyber Espionage Units," Mandiant (2013).

[335] Cyb3rSleuth, *Chinese Threat Actor Part 5,* (February 20, 2013).

[336] Cyb3rSleuth, *Chinese Threat Actor Part 3,* (March 2, 2012).

[337] 中国人民解放军 61398 部队招收定向研究生的通知, 浙江大学计算机科学与技术学院 (May 5, 2004).

China's MSS is charged with conducting cyber espionage and operates two universities in China, the University of International Relations in Beijing and Jiangnan Social University.[338] The MSS works closely with several other universities for training, conducting research, and other cyber activities: professors at Hunan University and Tianjin University have been designated as MSS experts and awarded prizes by the ministry.[339] Southeast University, which has received funding from the MSS to improve China's cyber offensive capabilities, has been linked to a cyber operation against the U.S. healthcare company Anthem.[340] The MSS recruits cyber operators from Harbin Institute of Technology, Beijing University of Posts and Telecommunications, and Zhejiang University.[341]

Xidian University operates a graduate program with Guangdong ITSEC, a security evaluation center under the MSS's 13th Bureau, in its Network and Information Security School. While the university "awards degrees and handles admissions," Guangdong ITSEC provides MSS mentors and hands-on experience to graduate students.[342] Guangdong ITSEC, which is based more than 1000 miles away from Xidian University, is also the managing organization for the threat activity group APT3, although there is no record of any participation in the APT from Xidian University.[343] APT3 (aka UPS, Gothic Panda, TG-011), based in Guangzhou, was first linked to the MSS in 2017 when DOJ indicted three members of the active threat group for computer hacking, trade theft, and identity theft.[344]

The three worked for the Internet security firm Guangzhou Bo Yu Information Technology Company Limited (Bouyusec), which its website says is an active partner of Huawei Technologies and the Guangdong Information Technology Security Evaluation Center. In 2017, APT3 acquired a variant of an NSA-developed cyberweapon known as ETERNAL ROMANCE, perhaps through reverse engineering. Since 2015, APT3 appears to have moved away from targets in the U.S. in favor of focusing on organizations in Hong Kong.

Military Recruitment and Military Civil Fusion

The PLA quickly realized the potential of early hacking collectives and led or conducted most state-sponsored offensive cyber campaigns in the 1990s and early 2000s. With the reorganization of the military in 2015-16, the PLA transferred many of China's cyber operations to the MSS.[345] While the PLA has historically been able to recruit talent directly out of

[338] Joske, *The China Defence Universities Tracker, op. cit.*

[339] *Ibid.*

[340] Cary, *Academics, AI, and APTs*, *op. cit.*

[341] Joske, *The China Defence Universities Tracker*, *op. cit.*

[342] Cary, *Academics, AI, and APTs*, *op. cit.*

[343] *Ibid.*.

[344] *United States v. Yingzhuo*, 17-cr-247 (W.D. PA, 2017)

[345] Paul Mozur and Chris Buckley, "Spies for Hire: China's New Breed of Hackers Blends Espionage and Entrepreneurship," *The New York Times* (August 26, 2021).

universities, it increasingly relies on contractors and military civil fusion, using civilian talent to carry out military missions.

Many of the PLA's earliest recruits were what have been referred to as "young patriotic hackers." Of these PLA's recruits from the hacker community, the most well-known is Tan Dailin (谭戴林), also known as WickedRose, whom the Department of Justice indicted in August 2019 as part of APT41.[346] As a graduate student at Sichuan University, Tan Dailin led a hacking collective founded in his dorm room known as the Network Crack Program Hacker group (NCPH), which began to gain notoriety after allegedly hacking 40% of hacker associations' websites in China.[347] He was first noticed by the PLA after hacking into Japanese computers and was invited to participate in a local security competition.[348]

After winning the event, Tan and his team were invited to participate in an intensive month-long training program that included simulating network intrusion attacks, designing hacking tools, and developing other attack strategies.[349] They subsequently won a larger multi-regional competition organized by the PLA and continued to work with the military long afterward. While funded by the military, the NCPH created a number of programs that used vulnerabilities in Microsoft Office to insert malware that would allow the team to download documents and other files, giving them access to thousands of U.S. government documents.[350]

In early 2018, the SSF commenced public civilian recruitment.[351] The SSF, like its Western counterparts, probably faces challenges to hiring and retaining civilian talent as a result of salary discrepancies and differences in employment cultures. Differences between the SSF and the private sector likely make the SSF a less appealing organization to domestic information security professionals.[352]

The primary method that the PLA has used to circumvent this problem has been through MCF—Military Civil Fusion— a strategy aimed at developing a "world class military" by eliminating "barriers between China's civilian research and commercial sectors, and its military

[346] Department of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally*, (September 16, 2020). *United States v. Lizhi, op. cit.*

[347] Simon Elegant, "Enemies at the Firewall," *TIME* (December 6, 2007).

[348] Alan Paller, *Cybersecurity: Developing a National Strategy*, SANS Institute (April 28, 2009).

[349] 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, op. cit.*

[350] Dunham and Melnick, *"Wicked Rose" and the NCPH Hacking Group*, *op. cit.*

[351] 亓创, 王财寅, 刘思维 & 颜海生, *严！严！严！战略支援部队某部文职人员面试现场直击*, 解放军报记者部 (Nov. 14, 2018), http://www.mod.gov.cn/services/2018-11/04/content_4828604.htm.

[352] Natalie Herbert, *Achieving the PLA's Strategic Support Force talent needs through MCF* (China Aerospace Studies Institute, February 2021).

and defense industrial sectors."[353] This approach aspires to integrate civilian and defense sectors in order better to synchronize technology, resources, and research between the commercial and defense ecosystems.[354]

As part of this effort, the PLA works closely with universities to cultivate talent, conduct research, and exchange resources.[355] For example, the SSF has signed an agreement with nine institutions to train new talent for combat forces: University of Science and Technology of China, Shanghai Jiao Tong University, Xi'an Jiaotong University, Beijing Institute of Technology, Nanjing University, Harbin Institute of Technology, China Aerospace Science and Technology Corporation, China Aerospace Science and Industry Corporation, and China Electronics Technology Group Corporation.[356] Within the SSF, individual units also partner with universities to conduct research.[357]

MCF also encompasses cooperation with private sector companies as well. The PLA has developed strategic agreements with companies such as China Mobile to develop information infrastructure, exchange resources, promote information security, and train talent, among other activities.[358] Qihoo 360, a cybersecurity company known for recruiting legacy hackers, also operates China's first "cybersecurity innovation center" under the guidance of the Central Commission for Integrated Military and Civilian Development.[359] The PLA is host to security competitions of its own in order to attract new talent and evaluate tools that can be used for cyber operations.[360]

The PLA has endorsed recruiting civilians with cyber expertise into a militia reserve force in order to supplement military forces in moments of heightened cyber conflict.[361] While these reserves would likely be limited to providing logistics and conducting espionage, rather than engaging in offensive campaigns, membership allegedly numbers more than 10 million people.[362] Like the early hacker collectives, civilian participation in military cyber operations introduces the risk of such civilians acting erratically. These approaches—military civil fusion and endorsing a

[353] U.S. Department of State. *Military-Civil Fusion and the People's Republic of China* (2020).

[354] Elsa B. Kania and Lorand Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*, (Washington: Center for New American Security, January 28, 2021).

[355] Herbert, *Achieving the PLA's Strategic Support Force talent needs through MCF*, *op. cit.*

[356] 李国利 and 宗兆盾, "Strategic Support Force to Cooperate with Nine Local Organizations to Cultivate High-End Talents for New Combat Forces," *Xinhua*, (July 12, 2017).

[357] Herbert, *Achieving the PLA's Strategic Support Force talent needs through MCF*, *op. cit.*

[358] Alex Stone and Peter Wood, *China's Military-Civil Fusion Strategy* (Montgomery: China Aerospace Studies Institute, June 15, 2020).

[359] Nicholas Lyall, "China's Cyber Militias," *The Diplomat* (March 1, 2018).

[360] Cary, *Testimony before the U.S.-China Economic and Security Review Commission on China's Cyber Capabilities: Warfare, Espionage and Implications for the United States, op. cit.*

[361] 中国国防报, *重点来了！这样推进网信领域军民融合深度发展*, CCTV (December 14, 2016).

[362] *China's Cyber Militias*, *op. cit.*

civilian militia reserve force—help the PLA balance exploiting the capabilities of the civilian and commercial sectors while retaining control over targeted offensive cyber campaigns.[363]

Private Sector Recruitment and Coercion

Historically China prefers to rely on "intermediaries, front companies, and contractors" to conduct state sponsored cyber offensive campaigns, as it allows government ministries to claim plausible deniability when attacks are discovered.[364] These actors are often sponsored but not necessarily managed by the government, leading to a mix of "traditional espionage with outright fraud and other crimes for profit."[365]

Many of these hacking groups began as criminal operations that are co-opted by the State to conduct espionage.[366] Government supervisors, such as the MSS, ignore the groups' illegal activity in exchange for cooperation in reconnaissance.[367] The MSS also may use prior illegal activity to coerce young hackers into conducting espionage operations. In 2021, the United States indicted four members of APT40, who worked with the MSS for several years to steal intellectual property, trade secrets, and other information from entities involved in defense, aviation, chemicals, and maritime activities, among others.[368] The White House also signaled alarm at the PRC's use of criminal contractors who conduct cyber operations for personal profit.[369]

These private sector hacking groups often work with other actors involved in cyberoperations. For example, APT 40 worked under the guise of an internet security start-up, Hainan Xiandun Technology Development Co., in order to hack into Microsoft's Exchange Server.[370] The company, operating under the Hainan State Security Bureau of the MSS, posted

[363] *Ibid.*

[364] Andy Greenberg, "How China's Hacking Entered a Reckless New Phase," WIRED (July 19, 2021).

[365] Mozur and Buckley, *Spies for Hire*, *op. cit.*

[366] Cary, *China's next generation of hackers won't be criminals*, *op. cit.*

[367] 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*" *op. cit.*

[368] *United States v. Xiaoyang, et al,* No. 21-cr-1622 (S.D. CA, 2021). The Advanced Persistent Threat (APT) 40 in the indictment includes BRONZE, MOHAWK, FEVERDREAM, G0065, Gadolinium, GreenCrash, Hellsing, Kryptonite Panda, Leviathan, Mudcarp, Periscope, Temp.Periscope, and Temp.Jumper. See also, *Advanced Persistent Threat Groups*, Mandiant (March 5, 2022), https://www.mandiant.com/resources/apt-groups.

[369] The White House, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*, (July 19, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

[370] "Who is Mr. Gu?," *IntrusionTruth* (January 10, 2020).

several job notices on university websites, and its listed contact was a professor in the Information Security Department at Hainan University.[371]

Other contractors may be recruited through an MSS organization known as the China Information Technology Evaluation Center (中国信息安全测评中心/CNITSEC), known for "conduct[ing] vulnerability testing and software reliability assessments."[372] The organization certifies several security evaluation centers across the country. CNITSEC provides the MSS the opportunity to work closely with cybersecurity companies and researchers, which gives the Ministry intimate knowledge of who is working on potentially useful projects.[373] The MSS may approach contractors under the guise of security evaluations conducted by CNITSEC.[374]

Domestic security conferences offer ideal venues for recruiting, providing a space for government organizations, private companies, established hacking groups, and up-and-coming individuals to network.[375] Sponsored by the government and large technology companies such as Baidu, Alibaba, and Venustech, conferences like XPwn2017 and Tianfu Cup are often used by the PLA and MSS to recruit university students and other individual hackers.[376]

Competitors can earn large rewards for demonstrating exploits in widely used software and hardware.[377] Cyber Kunlun, founded by former Qihoo 360 employees, were the most recent winners of the Tianfu Cup, where participants demonstrated exploits against Windows 10, Adobe PDF Reader, Ubuntu 20, Parallels VM, iOS 15, Apple Safari, and Google Chrome, among others.[378]

Chinese law compels businesses, universities, and other institutions to provide assistance and cooperation to the PRC's national intelligence services wherever they operate.[379] Another

[371] *Ibid.*

[372] Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford University Press, 2015).

[373] 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*" *op. cit.*

[374] *Ibid*.

[375] Patrick Howell O'Neill, "How China turned a prize-winning iPhone hack against the Uyghurs," *MIT Technology Review* (May 6, 2021).

[376] 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*" *op. cit.*

[377] Eduard Kovacs, "$1.9 Million Paid Out for Exploits at China's Tianfu Cup Hacking Contest," *Security Week* (October 19, 2021).

[378] Ravie Lakshmanan, "Windows 10, Linux, iOS, Chrome and Many Others at Hacked Tianfu Cup 2021," *Hacker News* (October 17, 2021).

[379] Article 7 of the National Intelligence Law of the PRC (国家情报法) requires any organization or citizen to support, assist, and cooperate with Chinese intelligence services, either by providing access to data, infrastructure, or other materials necessary to support national intelligence work. Office of the Secretary

provision requires Chinese businesses abroad to provide the same degree of collaboration. [380] In addition, the 2021 Regulations on the Management of Network Product Security Vulnerabilities requires individuals and domestic and foreign entities in China to report zero-day vulnerabilities to the MIIT within two days of discovery. The regulations forbid the same actors from sharing these vulnerabilities with overseas organizations and individuals, other than network product providers.[381]

Private sector companies have also been linked to cyber threat groups that have conducted offensive campaigns against foreign networks. TopSec, a Beijing-based company that helps to organize the Tianfu Cup, allegedly assisted a group linked to the 2015 hack of the U.S. insurance company, Anthem.[382] Chinese media identified the firm, which has partnered with the National Cybersecurity Center in Wuhan, as training PLA hackers.[383]

In 2018, Huawei filed a patent with the Chinese Academy of Sciences for an artificial-intelligence surveillance system that could automatically detect whether or not pedestrians belonged to Uyghur or other ethnic groups.[384] A number of other companies, such as NSFocus, Qihoo 360, and Venustech, are known for hiring early legacy hackers, who moved from illegal hacking activity into contracting work for the PLA and MSS and then into the private cybersecurity sector. It is likely that many of these types of firms continue to work with the CCP conducting espionage, attacks, and training.[385]

of Defense, *Military and Security Developments Involving the People's Republic of China*, (2021).; 中国人民代表大会， 中华人民共和国国家情报法 (2018).

[380] Article 10 allows the law to apply extraterritorially, such that Chinese businesses abroad may be compelled to cooperate with domestic intelligence authorities as well, although some companies have disputed this interpretation. Huawei, *Media Statement: Huawei Technologies Global HQ*, (August 24, 2018).

[381] *工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知*, 中华人民共和国国家互联网信息办公室 (July 13, 2021), https://archive.ph/9cL8j.

[382] O'Neill, "How China turned a prize-winning iPhone hack against the Uyghurs."

[383] Cary, *Testimony before the U.S.-China Economic and Security Review Commission on China's Cyber Capabilities: Warfare, Espionage and Implications for the United States*, *op. cit.*

[384] IPVM Team, "Patenting Uyghur Tracking - Huawei, Megvii, More," *IPVM* (January 12, 2021), https://ipvm.com/reports/patents-uyghur.

[385] 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*" *op. cit.*

6. Open Source Software and the Role of AI

The Role of Chinese AI in Open Source Code

Much of the world's software relies on open source code that is freely available online that may be redistributed and modified. In the midst of a re-galvanized interest in software supply chain security, open source software faces a number of alarming security issues.[386] Maintainers and developers, in China and elsewhere, have deliberately or accidentally corrupted multiple open source libraries.

In 2020, for example, a Senior Security Engineer at Huawei published a commit to the open source Linux Kernel Self-Protection Project, claiming that it was a security patch. This patch was filled with introduced security vulnerabilities. Huawei denied responsibility for the commit, stating that the vulnerabilities were the act of the individual working alone.[387] In 2021, an Alibaba engineer found a severe vulnerability in the open source library Log4j that allowed any individual remotely to control systems running Log4j,[388] and reported it to Apache. Instead of rewarding the engineer, however, the Chinese government suspended Alibaba Cloud's information sharing agreement with China's Ministry of Industry and Information Technology for six months[389] for not sharing the vulnerability with the government within two days of disclosure.[390]

Open source software (OSS) development solicits input from its community of users via technical standards meetings, code submissions, and online community discussions. These typically small communities are ripe targets for adversarial influence campaigns and software supply chain attacks.[391] There exists no established trust metric by which the open source community can vet accounts or individuals that submit code based on code artifacts, commit quality, historic community influence, and affiliations. An attacker may contribute to popular

[386] See *Readout of White House Meeting on Software Security*, January 13, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/

[387] Catalin Cimpanu, "Huawei denies involvement in buggy Linux kernel patch proposal," *ZDNe*t (May 12, 2020), https://www.zdnet.com/article/huawei-denies-involvement-in-buggy-linux-kernel-patch-proposal/.

[388] Issie Lapowsky, "Researchers warn of a 'very, very scary' bug affecting major apps," *Protocol* (December 10, 2020), https://www.protocol.com/bulletins/log4j-bug.

[389] Jonathan Greig, Chinese regulators suspend Alibaba Cloud over failure to report Log4j vulnerability," *ZDNet* (December 22, 2021), https://www.zdnet.com/article/log4j-chinese-regulators-suspend-alibaba-partnership-over-failure-to-report-vulnerability/.

[390] Zeyi Yang, "Beijing punishes Alibaba for not reporting Log4j loophole fast enough," *Protocol* (December 22, 2021), https://www.protocol.com/bulletins/alibaba-cloud-log4j.

[391] Patrick Howell O'Neill, "The internet runs on free open-source software. Who pays to fix it?" *MIT Technology Review* (December 17, 2021), https://www.technologyreview.com/2021/12/17/1042692/log4j-internet-open-source-hacking/.

libraries and submit deliberately vulnerable code or even functional backdoors that will be exploited after the code is incorporated into the product.

In addition, distracting core contributors, through useless change commits, flame wars (hostile online comments or exchanges), or other activities, may lead to a failure thoroughly to vet patches or bug reports, leaving vulnerabilities in the code. Throughout all of this, China, a primary adversary in cyberspace, has developed a robust open source community that can be utilized to chip away at the security of U.S. software.

China and Open Source: A History

China has embraced Linux and the open source community since the early 2000's. As early as 2002, the Beijing Science and Technology Commission[392] called Linux "China's most important chance to improve its software industry." This commission recommended that the Chinese government adopt Linux as an operating system for new computers and encouraged private sectors and universities to contribute to Linux and other open source software.[393] In 2010, the CCP's 10th Five Year Plan outlined a need to "develop the software industry, strengthen the development of the information infrastructure, and apply digital and network technologies extensively . . . so that industrialization and the information revolution go hand in hand."[394]

Two other factors further pushed China's adoption of open source technologies and Linux in particular: the 2008 global financial crisis slashed IT costs across Chinese companies, resulting in more firms seeking out free and open source software, and the 2011 launch of Android smartphones in China exposed additional individuals to the Android OS and Linux.[395]

Chinese government bodies and businesses see Linux and other open source software as appealing for multiple reasons. First, taking advantage of premade software and existing technical knowledge allows China to focus capabilities on leapfrogging[396] to more advanced technologies. In 2008, the MIIT stated that in order to reach industry development goals for the next 5 to 15 years, China would need to learn from the advanced experience of international information technology development, improve technical capabilities, and speed up scientific research and

[392] James Andrew Lewis, et al, *Government Open Source Policies*, (Washington: Center for Strategic and International Studies, April 16, 2010), https://www.csis.org/analysis/government-open-source-policies.

[393] *Ibid*.

[394] Zhu Rongji, "Report on the Outline of the Tenth Five-Year Plan for National Economic and Social Development," The National People's Congress of the People's Republic of China (March 5, 2001), http://www.npc.gov.cn/zgrdw/englishnpc/Special_11_5/2010-03/03/content_1690620.htm.

[395] Rebecca Arcesati and Caroline Meinhardt, "China bets on open-source technologies to boost domestic innovation," *Merics* (May 19, 2021), https://merics.org/en/short-analysis/china-bets-open-source-technologies-boost-domestic-innovation.

[396] Kaveh Waddell, "China is playing next-generation leapfrog with the West," *Axios* (February 9, 2019), https://www.axios.com/china-ai-leapfrog-eba53d3b-1f47-49d9-bb4c-e638d96bfcb2.html.

development in a cycle of "digesting and re-innovating" ("消化再创新").[397] This cycle fits well with creating a domestic open-source community that learns from well-respected international code repositories, as well as from fellow domestic contributors.

Second, China circumvents an overreliance on proprietary western software by utilizing open source alternatives. After the Trump administration sanctioned Huawei in 2019, Huawei was barred from importing most U.S.-made chips and components[398] and was no longer able to use the Android operating system in its phones.[399] The United States has also prevented U.S. investment in Huawei, Hikvision, and 57 other Chinese companies due to their connections to Chinese defense and related materiel sectors.[400]

Information technology is already a central part of the CCP's Made in China 2025 Plan, a national strategy aimed to reduce China's reliance on foreign technology imports while investing heavily in its own innovations.[401] As fewer funds are being transferred from the West to Chinese firms, and now that Chinese firms can no longer reliably depend on Western technologies for fear of having them stripped away through sanctions, open source technologies provide an appealing alternative: it is freely available online and not subject to export control.

China and Open Source Today

In the last decade, China has become an open source powerhouse, both domestically and abroad. The China Academy of Information and Communications Technology (CAICT) stated that approximately 87% of Chinese companies use open source software in 2020.[402] GitHub, one of the primary platforms for open source worldwide, featured a large number of Chinese

[397] 《信息产业科技发展"十一五"规划和 2020 年中长期规划纲要》——保障措施, 科技司 (September 1, 2008), https://wap.miit.gov.cn/jgsj/kjs/ghzc/art/2020/art_d7700b69dbed4001a126a098ed3787d0.html.

[398] Graeme Wearden, "Trade war: China blasts US over Huawei blacklisting – as it happened," *The Guardian* (May 16, 2019), https://www.theguardian.com/business/live/2019/may/16/trade-war-markets-huawei-us-blacklist-donald-trump-china-business-live?page=with:block-5cdcffc18f088c3e913d730b#block-5cdcffc18f088c3e913d730b.

[399] Chris Welch, "Google addresses Huawei ban and warns customers not to sideload apps like Gmail and YouTube," *The Verge* (February 21, 2020), https://www.theverge.com/2020/2/21/21147919/google-addresses-huawei-services-ban-android-trump-sideload-apps.

[400] "FACT SHEET: Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China," White House (June 3, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/03/fact-sheet-executive-order-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/.

[401] *Made in China 2025 Explained*, (Cambridge: Harvard University, China Innovation Project, January 31, 2022), https://perma.cc/W6L5-RVPN.

[402] Arcesati and Meinhardt, "China bets on open-source technologies."

repositories in their 2020 Insight Report, stating that most of the major open source projects are supported by large Chinese technology companies.[403]

Alibaba, PingCAP, Baidu, Tencent, JD, and Huawei are the top 6 active Chinese enterprise accounts on the GitHub platform. GitHub specifically calls out Baidu's open source deep learning platform PaddlePaddle and its autonomous driving platform Apollo as highly active open source communities.[404] GitHub states that Alibaba is incredibly active on GitHub's platform. In addition, China has the second-largest number of GitHub users and contributors after the United States.[405]

More importantly, the number of Chinese firm and individual contributions to Western open source software has skyrocketed. In 2021, Huawei beat out Intel as the top contributor to the Linux Kernel—software that is the baseline of Western technologies like Google's Android, NASA's satellite software,[406] and the U.S. Army's Common Operating Environment.[407] This contribution activity coincided with Huawei's release of its own open source Linux distribution platform, openEuler, in September 2021.[408]

Huawei also has contributed code to more than 40 mainstream Western technical communities, including Kubernetes, OpenStack, Hadoop, TensorFlow, httpd, and MySQL.[409] These packages are being deployed now in sensitive applications where the insertion of malicious code could have disastrous consequences for U.S. national security.[410]

Artificial intelligence is an emerging technology that has melded well with China's open source ecosystem. China's AI strategy has linked AI to military and civilian use-cases and stresses innovation in the space: China's State Council has set a goal of making China the world leader in

[403] Shengyu Zhao et al, "GitHub 2020 Digital Insight Report," *X-lab* (2021), http://oss.x-lab.info/github-insight-report-2020-en.pdf.

[404] *Ibid.*

[405] "The 2021 State of the Octoverse", *GitHub* (Accessed August 18, 2022), https://octoverse.github.com/.

[406] "30 Big Companies and Devices Running on GNU/Linux," *TecMint* (January 7, 2015), https://www.tecmint.com/big-companies-and-devices-running-on-gnulinux/.

[407] The Red Hat Public Sector Team, "Red Hat's Decade of Collaboration with Government and the Open Source Community," *Red Hat Blog* (May 11, 2012), https://www.redhat.com/en/blog/red-Hats-decade-of-collaboration-with-government-and-the-open-source-community.

[408] Sean, "Huawei to launch new openEuler OS on September 25," *Gizmochina* (September 23, 2021), https://www.gizmochina.com/2021/09/23/huawei-launch-new-openeuler-os-september-25/.

[409] 曾响铃, "华为啃下硬骨头，窥视多样计算的未来," *OFweek* (October 22, 2020), https://ee.ofweek.com/2020-10/ART-8110-2818-30465438.html.

[410] See Katie Bo Lillis, "FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications," *CNN* (July 25, 2022).

AI by 2030,[411] and the CCP consistently frames AI as a crucially important technology at the heart of its future economy.

Chinese military leaders clearly want to use AI for offensive cyber purposes. An analysis of 343 AI-related equipment contracts made by PLA procurement in 2020 shows that the PLA is focused on procuring AI for intelligence analysis, predictive maintenance, information warfare, and navigation and target recognition in autonomous vehicles.[412] Chinese military academics speculate about the uses of AI for stealth, scale, and adaptability in information operations, and hyper-targeted phishing attacks.[413] At the same time, many large-scale tactical gains have occurred in the realm of non-military organizations and open source software.

How do AI and open source software fit together? Xi Jinping's stated goals in AI—to pursue both world leadership and self-reliance in AI technology[414]—is in line with use of open source technologies. Open source is featured in China's AI innovation plans: the MIIT New Generation AI Innovation Key Task List from 2018 explicitly contained a task on "Open source, open platforms,"[415] looking to use open source to expand the number of data sets, models, and users for machine learning technologies. Western firms have taken note, as a study from the National Intelligence University states that both U.S. and Chinese AI efforts appear to depend on open-source coding and development platforms like GitHub.[416]

Most of the large companies that contribute to open source are developing large scale and state-of-the-art AI projects with the government. China's "National Team of AI" recommends plans for AI projects, infrastructure, and training, and recruiting new talent, to the government, frequently working with MOST, Ministry of Finance, Ministry of Education, MIIT, and the Chinese Academies of Science.[417] The 15 companies comprising the "National Team" that also are top enterprise contributors on GitHub are: Baidu, Alibaba, Tencent, Huawei, JD, and Xiaomi.[418]

[411] Ashwin Kaja and Yan Luo, *Covington Artificial Intelligence Update: China's Vision for The Next Generation of AI* (New York: Covington & Burling, March 24, 2018) https://www.insideprivacy.com/artificial-intelligence/chinas-vision-for-the-next-generation-of-ai/.

[412] Ryan Fedasiuk, Jennifer Melot and Ben Murphy, *Harnessed Lightning: How the Chinese Military is Adopting Artificial Intelligence* (Georgetown: Center for Security and Emerging Technology, October 2021) https://cset.georgetown.edu/publication/harnessed-lightning/.

[413] John Chen, *Chapter 11 Cyber and influence operations*, SOSi. (forthcoming, 2022)

[414] Gregory C. Allen, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security* (Washington: Center for New American Security, February 2019) https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

[415] Richard Uber, *China's Artificial Intelligence Ecosystem* (Washington: National Intelligence University, 2021) https://ni-u.edu/wp/wp-content/uploads/2021/08/Uber_Monograph_DNI2021_02261.pdf.

[416] *Ibid.*

[417] *Ibid.*

[418] *Ibid.*

In implementation of this strategy, Chinese firms have open sourced large and impressive AI related projects—although many of these projects are documented in Chinese and thus largely inaccessible to Western audiences.[419] In addition to PaddlePaddle, Baidu also open-sourced LinearFold, its linear-time AI algorithm to increase the speed to predict RNA spatial structure of coronavirus and empower epidemic prevention and control.

Chinese AI in the Linux Kernel

The most alarming and prevalent area in open source software touched by Chinese AI systems may actually be the Linux kernel: the main component of a Linux operating system (OS) and the core interface between a computer's hardware and its processes. As noted, a large amount of proprietary Western software depends on the Linux Kernel. When, in 2021, Huawei beat out Intel as the Linux kernel's top contributor, a large share of these commits gave reporting credits to the "HULK" bot—Huawei's Unified Linux Kernel robot.[420]

According to interviews with Wei Yongjun (魏勇军) a principal engineer at Huawei Cloud[421] and HULK bot's creator,[422] the "HULK" robot is a complex distributed system with a massive test set and a series of advanced automated testing and problem detection methods.[423] According to Wei, "Huawei precisely mines the defects of the Linux Kernel, guarantees a high-quality and sustainable Linux Kernel, and supports the commercial use of various solutions."[424] As reported in technical blogs, HULK integrates big data machine learning and semantic analysis technology, as well as fuzzing technology based on scene semantics, system-wide function-level fault injection and precise coordination.[425] This makes the HULK robot an efficient, accurate and scalable testing system to find issues in code that other maintainers can fix.

Wei Yongjun further adds that Huawei "has spent a lot of time and energy in the maintenance of the Kernel because of the development of the openEuler distribution." Based on multiple open-source developer forums, the HULK robot has not just been used by Huawei

[419] Kevin Xu, "Open Source in China: The Players," *Interconnected*, (May 7, 2020) https://interconnected.blog/open-source-in-china-the-players/

[420] 曾响铃, "华为啃下硬骨头，窥视多样计算的未来."

[421] "Yongjun Wei," *ZoomInfo* (accessed August 18, 2022), https://www.zoominfo.com/p/Yongjun-Wei/-1617531087.

[422] 老王, "寻找为 Linux 内核贡献数千补丁的"超能力者," Linux 中国 (June 8, 2021), https://linux.cn/article-13468-1.html.

[423] *Ibid.*

[424]

ttps://webcache.googleusercontent.com/search?q=cache:xTXzjggcRpAJ:https://bbs.saraba1st.com/2b/forum.php%3Fmod%3Dviewthread%26tid%3D2011200%26extra%3Dpage%253D12%26ordertype%3D1%26page%3D1+&cd=2&hl=en&ct=clnk&gl=us

[425] "Linux Kernel 5.8 发布，华为在内核代码贡献上排名第二," PC18 (September 3, 2020), https://www.pc18.net/thread-4866-1-1.html.

developers to find code issues in the Linux Kernel, but also in the Android OS,[426] Red Hat Linux,[427] and Tegra Linux.[428] Because HULK robot is an internal Huawei product trained on and developed in tandem with Huawei's openEuler Linux distribution platform, it is likely that Huawei is primarily using the HULK robot to find bugs in their openEuler distribution platform first, then running the software on other distribution platforms to find similar bugs.

Using automated systems to find vulnerabilities or poor code in open source is not new: Google's syzbot, automated testing (fuzzing) software was the second-most credited reporting system for the Linux Kernel in 2021.[429] Huawei has, however, been accused of industrial espionage against T-Mobile,[430] been linked to a 2012 cyber-espionage campaign in Australia stemming from a Huawei backdoored software update,[431] been labeled a security threat by both the U.S. and Australian governments,[432] and violated international sanctions by selling telecommunications equipment to Iran.[433] In addition, HULK robot's reporting credits were three times that of syzbot's in 2021, dwarfing other reporting contributions.[434]

This abundance of committed code and bugs found by HULK robot, especially in the hands of a company like Huawei, provide two distinct opportunities for malicious activity. First, Huawei engineers can place deliberately vulnerable code into the Linux Kernel, hiding under the noise of HULK robot's commits. A Huawei engineer has already been accused of placing vulnerable code in the Linux Kernel in 2020, while other Huawei engineers have been accused of creating numerous "KPI-grabbing" changes in 2021—changes that are incredibly minor, reported by

[426] Baokun Li, "Commit dd8b865cc40832d32bbf912a65c657483533fdd4," *Google Git* (June 8, 2021), https://android.googlesource.com/kernel/common/+/dd8b865cc40832d32bbf912a65c657483533fdd4.

[427] Paul Moore, "[PATCH -next] audit: Use list_move instead of list_del/list_add" (June 9, 2021), https://listman.redhat.com/archives/linux-audit/2021-June/msg00038.html.

[428] Yue Haibing, "[-next,25/36] spi: s3c24xx: use devm_platform_ioremap_resource() to simplify code," OZ Labs (September 4, 2019), https://patchwork.ozlabs.org/project/linux-tegra/patch/20190904135918.25352-26-yuehaibing@huawei.com/.

[429] Jonathan Corbet, "Statistics from the 5.4 development cycle, *LWN* (November 7, 2019), https://lwn.net/Articles/804119/.

[430] Laurel Wamsley, "A Robot Named 'Tappy': Huawei Conspired to Steal T-Mobile's Trade Secrets, Says DOJ," *NPR* (January 29, 2019), https://www.npr.org/2019/01/29/689663720/a-robot-named-tappy-huawei-conspired-to-steal-t-mobile-s-trade-secrets-says-doj.

[431] Jordan Robertson and Jamie Tarabay, "Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack," *Bloomberg* (December 16, 2021) https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack

[432] Kate O'Flaherty, "Huawei Security Scandal: Everything You Need to Know," *Forbes* (February 26, 2019), https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/?sh=7b4b7f3973a5.

[433] Matt Burgess, "Is China really using Huawei to hack the world's communications?" *Wired* (January 25, 2019), https://www.wired.co.uk/article/huawei-5g-uk-security.

[434] Corbet, "Statistics from the 5.4 development cycle."

automated systems, and take more time for the maintainers of the kernel to review than for an engineer to commit the change.[435]

Second, and harder to catch, presuming that Huawei first runs HULK bot and other tools on its internal openEuler system before patching the original open-source Linux Kernel, and that the Chinese government has expressed wishes that vulnerabilities in open source software are reported internally as soon as possible, at least some vulnerabilities found in the Linux Kernel by Huawei may not be reported to Linux.

[435] Thomas Claburn, "Huawei dev flamed for 'useless' Linux kernel code contributions," *The Register* (June 26, 2021), https://www.theregister.com/2021/06/26/linux_kernel_contributor_from_huawei/.

7. Social Cyber Data Analysis – Tools for Threat Description, Localization, and Preemption

The research team has developed a set of artificial intelligence (AI) tools to assist with its analysis of China's cyber operations. They have permitted a preliminary analysis of personnel who engage in open source development in China and Russia, North Korea, and Iran as well. Looking at data collected involving the interactions of these individuals, these tools identify specific code contributions within the Linux Kernel and elsewhere and identify the authors through their email addresses and other identifiers.

An analysis of open source software and social media has been shown to be a useful way to identify suspicious cyber activity and potentially malicious cyber operations stemming from China. The present analytical effort uses novel AI techniques to create an analysis pipeline of Chinese cyber operations and the actors involved, localizing suspicious contributors and events for further inspection. Earlier analyses of open source development lacked the tools necessary to uncover suspicious behavior and malicious faith contributions and did not have access to the large body of data collected in the present effort.

The following examples merely scratch the surface of what will be possible with these tools in providing resources for open-source development communities to protect their processes and government and representatives of user organizations to assess the likelihood that the codebase has been compromised and by whom. They show that data inherently produced by the open source development process confirms and deepens understanding of the Chinese cyber ecosystem that was developed through traditional open source research methods discussed above. The methodology can be applied to other cyber ecosystems.

The work so far has focused on social cyber analysis of the Linux Kernel. As an introduction to the report on that effort, it is useful to summarize broader uses of the data analysis to show the breadth of what can be learned through application of these methods.

Increasing Chinese Role in Linux System Software Development for Microprocessors

As a matter of national security, the United States is properly concerned about the dangers of dependence on Chinese supply chains and China's aim to dominate important technological sectors using national resources to that end. In the past, U.S. policy focused on limiting dependence on foreign strategic minerals and controlling exports of high-technology items such as airframes, aircraft engines, and advanced lithography equipment for semiconductor production in advanced weapon systems. Such approaches are difficult to apply to emerging technologies in the 21st century.

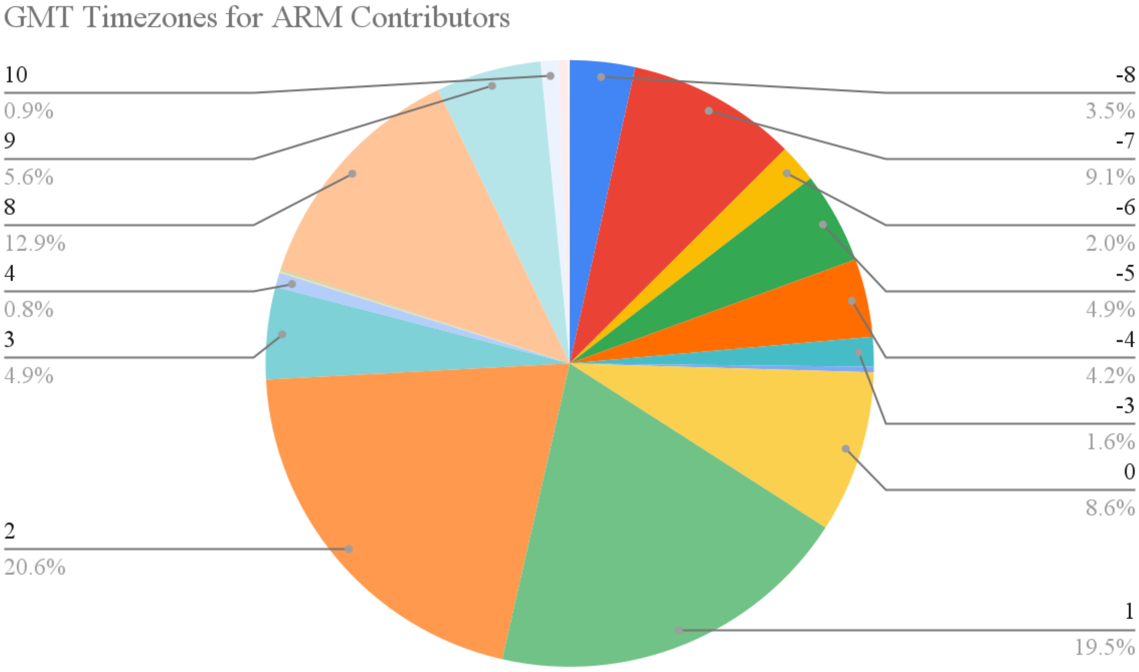
The technology supply chains, including microelectronics, software, and cyber are extremely complex. Those that depend on embedded software can change much more quickly than the hardware technologies that dominated the 20th century. Analysis of vulnerabilities in open source and proprietary software reveal the reality of these supply chains. For example, the data show that development of foundational software is already much more globally intertwined than is commonly understood. The common image of competition between the United States and China pits U.S. developments against Chinese attempts to catch up and surpass the United States.

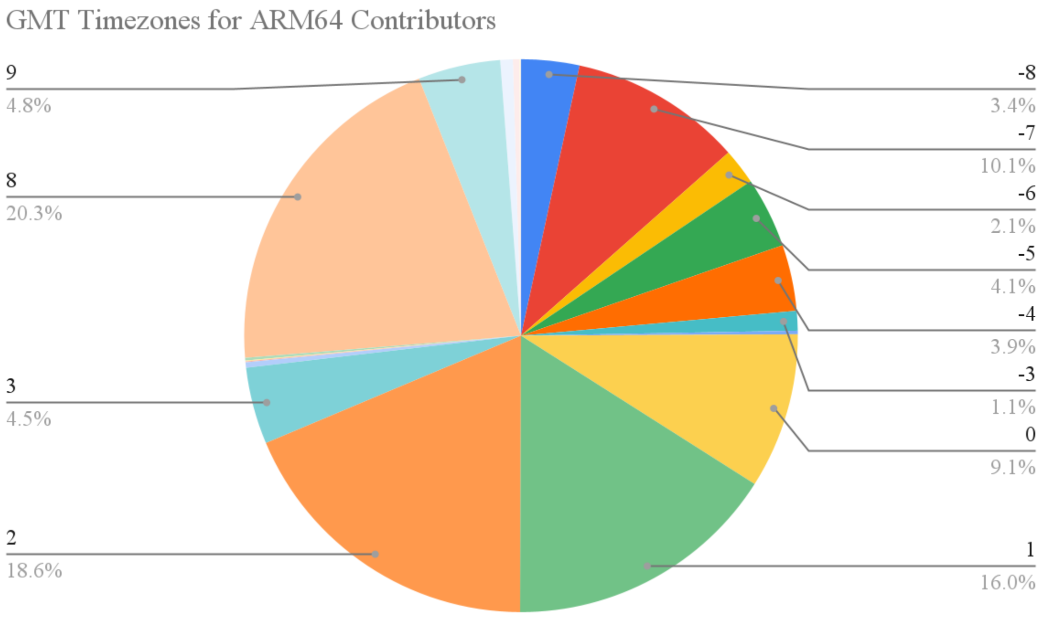
The image perhaps applies to TikTok threatening to overtake and dethrone Meta's Instagram, causing panic at Facebook. But in the 21st century the more typical pattern is various firms drawing from and contributing to an intertwined technology base to produce products and services.

Social Cyber Analysis of Linux Kernel Developer Time Zones

Invented in the United Kingdom, ARM microprocessors are extremely energy efficient. This architecture now dominates mobile devices including Apple iPhones, iPads, and the M1 and M2 chips in current Apple laptops, as well as the Raspberry Pi single board computers that are increasingly embedded in all sorts of products. For this reason, understanding the development system for these chips and the system software that runs on them is of great interest.

A preliminary analysis, summarized in the charts below, displays the number of users from each time zone contributing to the Linux Kernel specializations for ARM and the more powerful ARM64 processors. It is not weighted based on the volume of contributions from those users, but it is implicitly weighted to some extent by the algorithm which identifies contributions as being relevant to ARM.

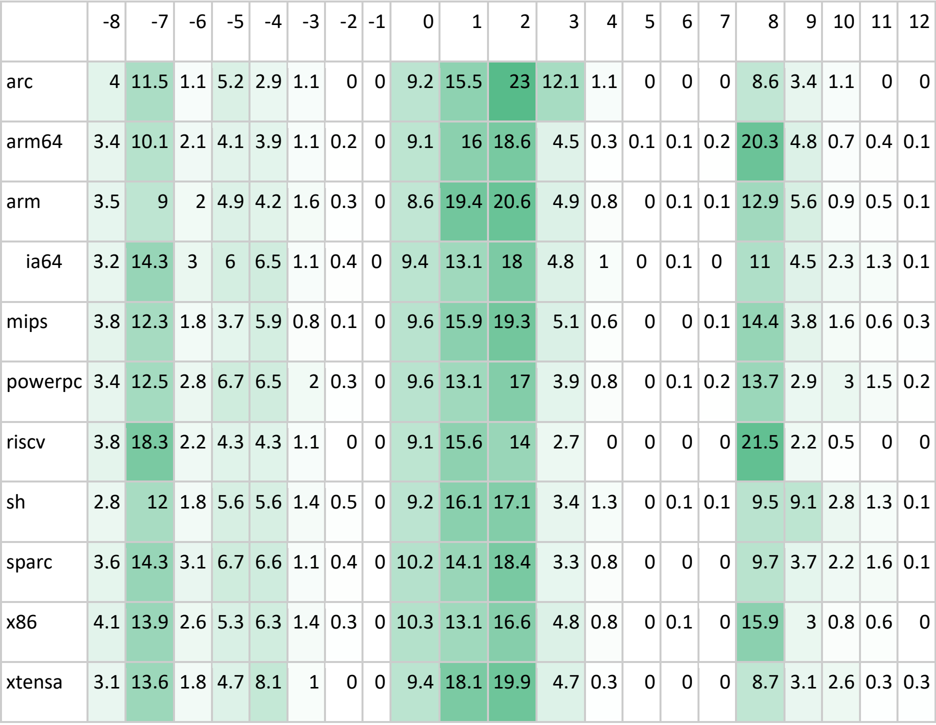




This graph depicts the time zone distribution of commits to ARM file communities from all time. Just under half of the commits for the ARM and 43% of the commits for the newer, more advanced ARM64 come from time zones GMT+0 through GMT+2, corresponding to Europe and Eastern Europe. While ARM Holdings is based in London, the GMT time zone only contributes 9% of the ARM and ARM-64 commits. China's time zone (GMT+8) has contributed 13% of the commits for ARM and 20% for ARM64.

Contributors using emails from Huawei, a company the United States identified as a threat to its national security, are the largest single group contributing to this selection of ARM64-related Linux kernel code elements from the time zone that includes China. In other words, the data suggest that development of the Linux Kernel for ARM processors development is already globalized, with Chinese contributors a substantial presence.

The following chart shows the data for other processors as well. Of particular note is the 22% rate of Chinese contributions for the RISC-V architecture. RISC-V is a next-generation architecture originally developed at the University of California at Berkeley. The data are preliminary and based on systems under development. They are included here to show what is possible rather than as verified information.



	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12
arc	4	11.5	1.1	5.2	2.9	1.1	0	0	9.2	15.5	23	12.1	1.1	0	0	0	8.6	3.4	1.1	0	0
arm64	3.4	10.1	2.1	4.1	3.9	1.1	0.2	0	9.1	16	18.6	4.5	0.3	0.1	0.1	0.2	20.3	4.8	0.7	0.4	0.1
arm	3.5	9	2	4.9	4.2	1.6	0.3	0	8.6	19.4	20.6	4.9	0.8	0	0.1	0.1	12.9	5.6	0.9	0.5	0.1
ia64	3.2	14.3	3	6	6.5	1.1	0.4	0	9.4	13.1	18	4.8	1	0	0.1	0	11	4.5	2.3	1.3	0.1
mips	3.8	12.3	1.8	3.7	5.9	0.8	0.1	0	9.6	15.9	19.3	5.1	0.6	0	0	0.1	14.4	3.8	1.6	0.6	0.3
powerpc	3.4	12.5	2.8	6.7	6.5	2	0.3	0	9.6	13.1	17	3.9	0.8	0	0.1	0.2	13.7	2.9	3	1.5	0.2
riscv	3.8	18.3	2.2	4.3	4.3	1.1	0	0	9.1	15.6	14	2.7	0	0	0	0	21.5	2.2	0.5	0	0
sh	2.8	12	1.8	5.6	5.6	1.4	0.5	0	9.2	16.1	17.1	3.4	1.3	0	0.1	0.1	9.5	9.1	2.8	1.3	0.1
sparc	3.6	14.3	3.1	6.7	6.6	1.1	0.4	0	10.2	14.1	18.4	3.3	0.8	0	0	0	9.7	3.7	2.2	1.6	0.1
x86	4.1	13.9	2.6	5.3	6.3	1.4	0.3	0	10.3	13.1	16.6	4.8	0.8	0	0.1	0	15.9	3	0.8	0.6	0
xtensa	3.1	13.6	1.8	4.7	8.1	1	0	0	9.4	18.1	19.9	4.7	0.3	0	0	0	8.7	3.1	2.6	0.3	0.3

Time Zone Analysis for Specific RISC Processors

Social Cyber Analysis of the Linux Kernel

Linux is omnipresent in a wide variety of devices and is foundational to modern systems, including those central to U.S. national security. Any country or company that develops a new processor or subsystem must ensure that the Linux Kernel, or a version of it, accommodates their hardware or provides hooks for their software.

As a result, strong incentives exist for the dispersion of kernel development. The analysis pipeline consists of a technology stack that ingests the Linux Kernel Mailing List (LKML) and the Linux Git repository, annotates the data, and transforms the annotated data into graph form so that analysts may search it. The data contain emails from the LKML and all associated email metadata, as well as individual commits to the Linux Kernel repository, tagged with metadata such as author, commit comments, timestamp, and author time zone.[436]

The Linux Kernel relies on a lieutenant system that designates responsibility for regions of code by maintainers in the maintainers file. Leveraging machine learning analysis that groups *commits* to *multiple files* generates a heuristic approach to defining key maintainers beyond those identified by the traditional leaders of the Linux community. This approach considers actual contributions by software developers as opposed to perceived contributions by high-ranking

[436] Email metadata includes the email hash, any cc'd / sender/ recipient email addresses, the headers and body of the email, the email subject line, the date the email was sent, time zone of the email author, and the toxicity and sentiment score of the email body itself.

individuals. The analysis then looks at these communities to determine changes in ownership over periods of time regardless of explicitly defined changes in the kernel maintainers file.

The Kernel repository metadata has been further enriched to contain whether an author's email has been found in the *HaveIBeenPwned* database (indicating that the email likely belongs to a real person), the pagerank of an individual author (indicating that the author is a common contributor to the kernel) and what Linux Kernel community (i.e., series of files often committed to by similar sets of individuals) the commit belongs to.

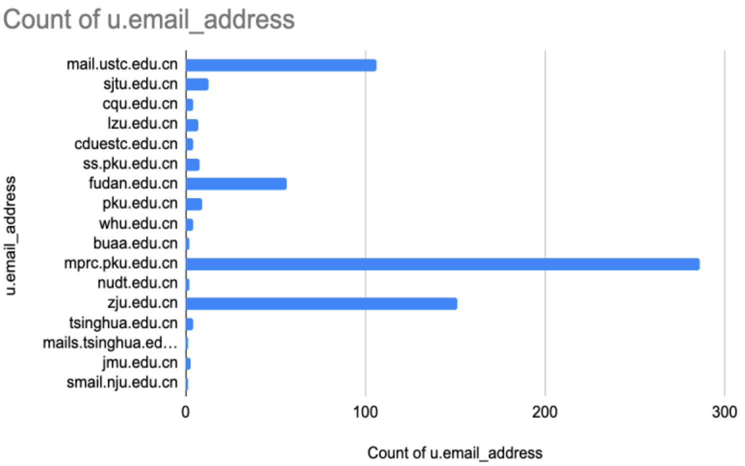
To provide additional context, the contributions database is being expanded to cover other forms of social media and open source platforms, such as Twitter, GitEE (China's version of GitHub), and other datasets. For now, the imported data are not dynamically updated, but provide insight into historical relationships up until the last day that the data were examined. Obviously, this analysis could be extended to real-time indications and warning in the future.

The analysis pipeline has been used to examine the behavior of the 36,000 contributors in the Linux Kernel. It has located 30 individuals exhibiting suspicious behavior. Several of these 30 were already known to have submitted "hypocrite commits" that introduced exploitable vulnerabilities to the Kernel project, but this knowledge was not used in the data analysis. In other words, the evaluation confirms that the data analysis is valid, though further work would be required to characterize the accuracy in terms of sensitivity and selectivity of the analysis.

Other individuals highlighted by the algorithm developed in the research exhibiting the same type of behavior as the known bad actors, likely engaged in malicious cyber activity. The platform allows analysts to explore this behavior in great detail. As other patterns or signatures typical of malicious code insertion are identified, the data can be reanalyzed to tag additional suspicious contributors and incidents.

Analysis of Linux Kernel Contributions from Chinese Educational Institutions

Analysis of the data on contributions to the Linux Kernel confirms the results described above regarding the activity of coders associated with key Chinese educational institutions.

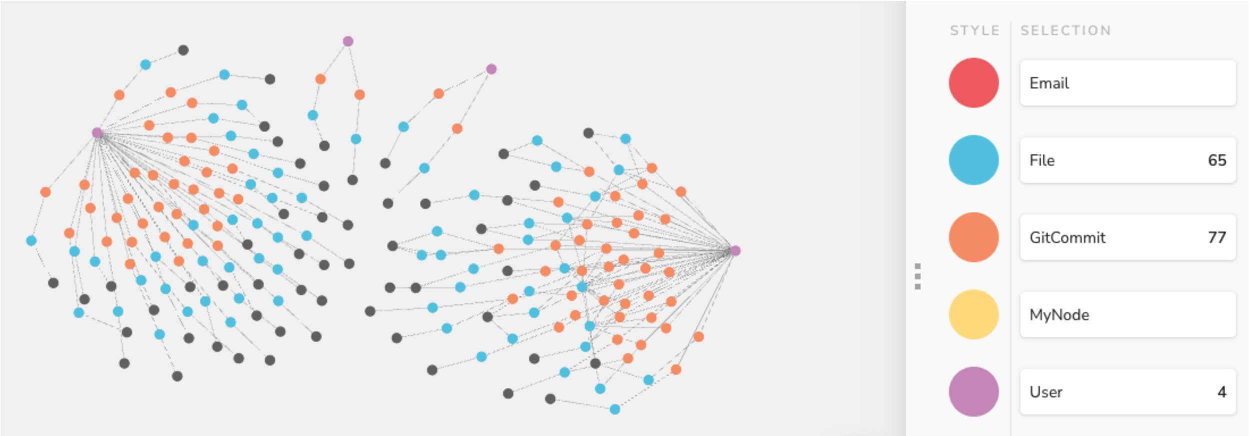


Total volume of contributions to the Linux Kernel from Chinese educational institutions.

The vast majority of the contributions from the time zone GMT-7 (Denver) come from the University of Science and Technology of China (USTC), which is often referred to as the Caltech of China.[437] The toolset allows the analysis to go a step further and determine which regions of code students from USTC are contributing as well as the nature of those commits.

Community ID	Top Files within Community
101187	"arch/x86/boot/boot.h,arch/x86/boot/string.c,arch/x86/boot/memory.c"
15955	"net/core/neighbour.c,include/net/neighbour.h,include/trace/events/neigh.h"
449261	"drivers/net/ethernet/cisco/enic/enic_main.c,drivers/net/ethernet/cisco/enic/enic.h,drivers/net/ethernet/cisco/enic/vnic_dev.c"
687636	"drivers/ipack/carriers/tpci200.c,drivers/ipack/ipack.c,include/linux/ipack.h"
336560	"drivers/net/ethernet/qualcomm/emac/emac.c,drivers/net/ethernet/qualcomm/emac/emac-mac.c,drivers/net/ethernet/qualcomm/emac/emac-sgmii.c"

Areas of the Linux Kernel contributed to by USTC Students - Primary files within the community.



The vast majority of these contributions came from two users in particular. Wu Fengguang, (wfg@mail.ustc.edu.cn) shown on the right, and Lv Yunlong, (lyl2019@mail.ustc.edu.cn). Two

[437] Yangyang Cheng, "Science vs. the state: a family saga at the Caltech of China," *MIT Technology Review* (December 19, 2018), https://www.technologyreview.com/2018/12/19/138217/science-vs-the-state-a-family-saga-at-the-caltech-of-china/.

other users made substantially fewer contributions. From this analysis it is possible to determine that Wu Fengguang and Lv Yunlong worked on separate projects and were not collaborating with each other and that they made similar volumes of contributions to their respective regions of code.

While this example does not depict explicitly malicious behavior on the part of these students, it shows a capability to examine contributions from institutions that may not be acting in good faith. In 2020, President Trump suspended entry to the United States of Chinese students whose schools have ties to the Chinese defense industry.[438] Of these schools, both Beihang and Nanjing University have been seen making contributions to the Kernel.

Inspection of these contributions makes it possible to assess that they were not malicious in nature. It was, however, possible to observe an additional contribution from a student at the National University of Defense Technology (NUDT), which made a minor bug fix to the eCryptfs disk encryption subsystem of the Linux Kernel. The commit in question was made in 2012.[439] In 2015, the Commerce Department added NUDT to the U.S. BIS Entity List.[440]

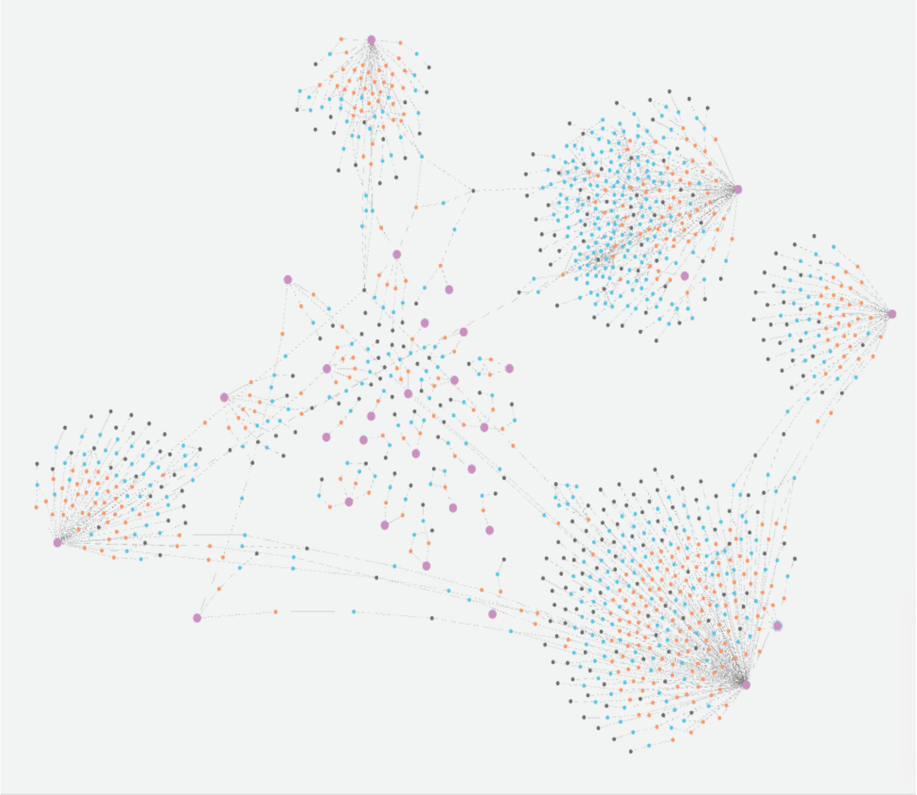
This analysis permits insight into, and understanding of, not only what contributions are being made from risky organizations, but also what *technologies* those organizations use. For example, in the diagram below, all contributions from Chinese educational institutions are plotted against each other in a graph. The large purple dots are users, which are linked to commit nodes (orange), which are linked to file nodes (blue), which are then linked to respective community nodes (black).

This graph makes it possible to show when files are committed that belong to the same community, and we end up seeing small instances of collaboration between users that otherwise may have had nothing to do with each other. At a glance, it is possible to assess that certain users contribute far more than others (purple dots with larger clouds of commits around them), that some of these users have interacted in the same regions of code as others, but in a fairly limited capacity (lines between clouds), and that when these users make contributions they tend to touch a wide area of the Kernel—they do not necessarily focus in one place as can be seen by the many black dots in each cloud.

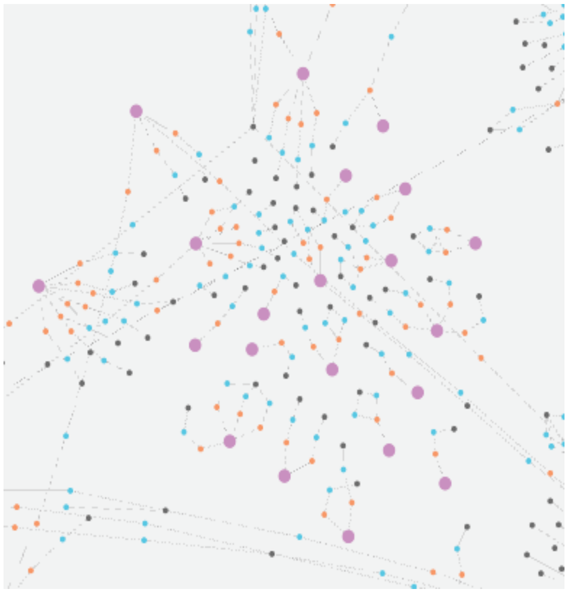
[438] "Executive Order 10043 of May 29, 2020, Suspension of Entry as Nonimmigrants of Certain Students and Researchers From the People's Republic of China," *Code of Federal Regulations* (2020): , https://www.federalregister.gov/documents/2020/06/04/2020-12217/suspension-of-entry-as-nonimmigrants-of-certain-students-and-researchers-from-the-peoples-republic.

[439] Linus Torvalds, Linux, (2012), GitHub repository, https://github.com/torvalds/linux/commit/684a3ff7e69acc7c678d1a1394fe9e757993fd34.

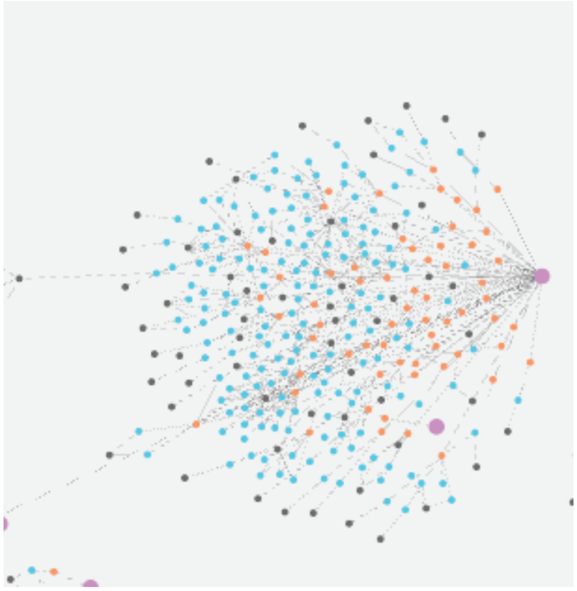
[440] Joske, *The China Defence Universities Tracker, op. cit.*



A normal contributor to the Kernel might be working on a side project, find a bug, and decide to offer up a fix to the community. This sort of behavior can be seen as being depicted as small, one-off contributors with not a lot of commits to their name. Illustrated below is a selection of this type of behavior from the original graph.

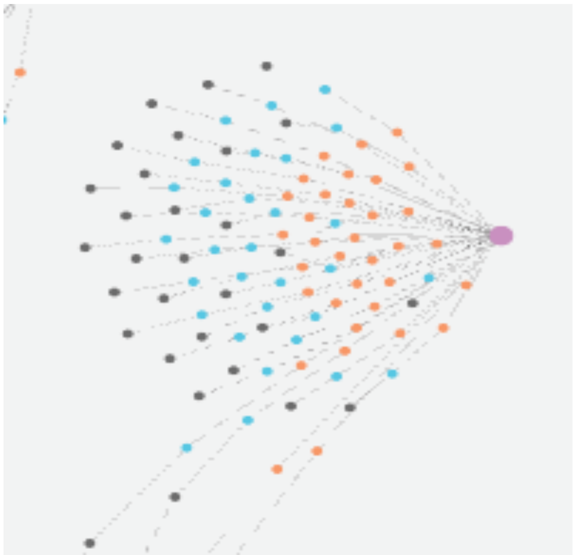


Another type of contributor is a user that is active in the Kernel and tends to focus on a community or cluster of files. Here this type of behavior is depicted as well in the top center cloud (depicted below). It is possible to see communities (black dots) being surrounded by a multitude of files (blue dots), to which the same user is contributing.



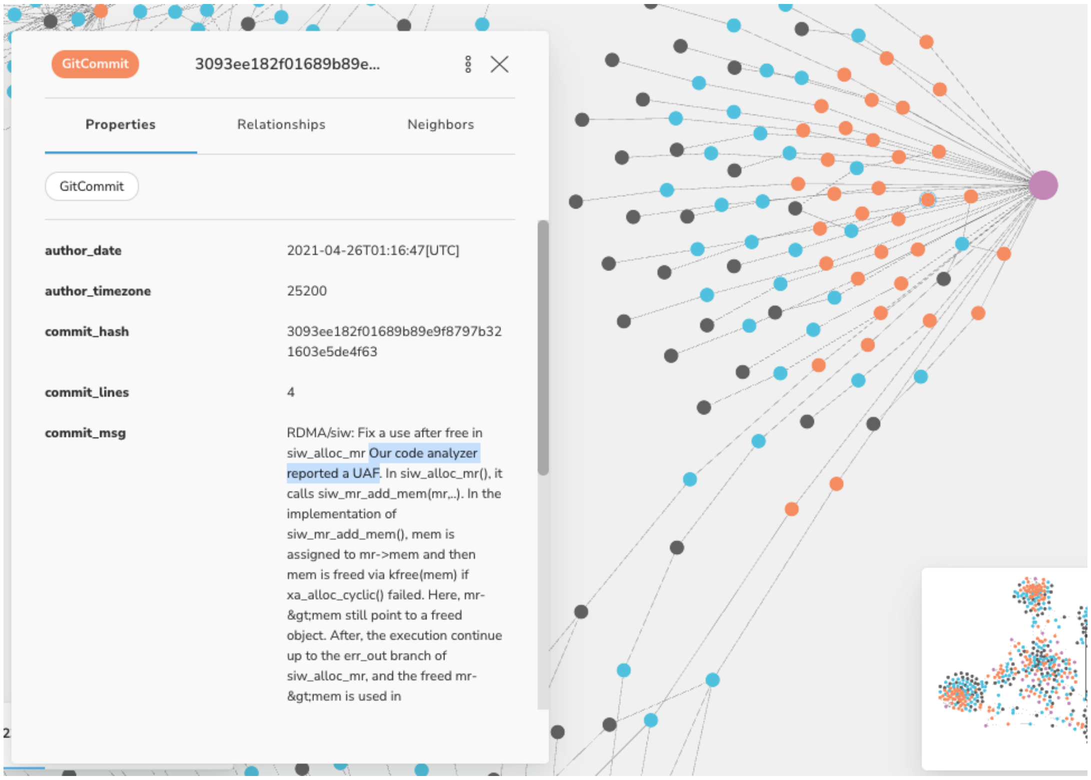
One of the most interesting types of behavior that can be seen through this graph is automated bug finders. Automated bug finders used by organizations in China in the Linux kernel have previously been explored and reported at length by the research team.[441] While a normal user might make contributions based on a particular interest in a given region of code, or because it happened across a bug and wanted to contribute a fix to the open source community, automated bug discovery is characterized by a large volume of fixes that occur across the entire open source project. This phenomenon shows up in the graph as a large volume of commits to files that do not belong to the same community. In other words, lots of communities (black dots) with single files (blue) attached to them. The example below shows this type of behavior.

[441] Winnona DeSombre, Dave Aitel, and Ian Roos, *Watching the Watchers*, (New York: *Margin Research*, April 5, 2022), https://margin.re/media/watching-the-watchers.aspx.



It is also possible to confirm that this behavior is automated by exploring the commit messages related to contributions from this user. As shown below, this individual is using a code analyzer that detects memory corruption vulnerabilities like Use-After-Frees which can be leveraged in the development of offensive cyber capabilities. Searching for scholarly articles by this user yielded a research paper titled "Goshawk: Hunting Memory Corruptions via Structure-Aware and Object-Centric Memory Operation Synopsis."[442] This automated capability gives China a tactical edge when it comes to the generation of offensive cyber capabilities. The analytical tools developed in this project help uncover proliferation of these capabilities within the Linux Kernel.

[442] Yunlong Lyu et al., Goshawk: Hunting Memory Corruptions via Structure-Aware and Object-Centric Memory Operation Synopsis," *2022 IEEE Symposium of Security and Privacy* (2022), https://web.archive.org/web/20220623100707/https://lijuanru.com/publications/sp22-again.pdf.



author_date	2021-04-26T01:16:47[UTC]
author_timezone	25200
commit_hash	3093ee182f01689b89e9f8797b32 1603e5de4f63
commit_lines	4
commit_msg	RDMA/siw: Fix a use after free in siw_alloc_mr Our code analyzer reported a UAF. In siw_alloc_mr(), it calls siw_mr_add_mem(mr,..). In the implementation of siw_mr_add_mem(), mem is assigned to mr->mem and then mem is freed via kfree(mem) if xa_alloc_cyclic() failed. Here, mr-&gt;mem still point to a freed object. After, the execution continue up to the err_out branch of siw_alloc_mr, and the freed mr-&gt;mem is used in

Limitations of the Present Analysis

The analyses reported here are based on methodologies that are still under intensive development; the results should be understood as indicating what is possible rather than currently verified using other tools. There are ways, including seeding the data set with synthetic data representing both malign and benign behavior, of testing the system to understand better the accuracy of the results and the sensitivity and specificity of detection of various sorts of incidents.

While the results suggest that social cyber data analysis of open source software development can yield useful information, it is in the nature of such behavioral data that people who become aware that they are the focus of data analysis may change their behavior. For example, contributors might use distinct emails for different open source development systems or even within the same system, use emails that obscure their professional affiliations, or take steps to obscure the time zone from which they operate. Thus, social cyber analysis systems must be under continual development to keep ahead of changes in systems and behavior.

Social Cyber analysis has shown to be highly promising as a complement to more traditional methods in characterizing the scope and nature of national software capabilities and efforts. It provides unique and significant information on the activities of developers in maintaining and improving open source software products. It also confirms the conclusions of the painstaking survey of Chinese software development and hacker ecosystems presented in this report. It shows great promise in characterizing the scope and nature of potential threats to the open source software and in localizing and identifying those threats. Such information allows open source software development organizations, intelligence organizations, and other interested parties to take steps to preempt operations aimed at inserting malicious code into open source software.

8. Conclusions

China has greatly expanded its cyber capabilities with respect to intelligence collection, espionage, misinformation, as well as cyber warfare and now poses the greatest threat to the United States in the cyber arena. China has developed a cyber strategy consistent with CCP values. China's dominance of domestic information, population control, and pursuit of global control of significant economic sectors in the cyber landscape enhance military freedom of action with regard to Taiwan and other potential military objectives.

Information Dominance and China's Cyber Strategy

China's cyber strategy and institutions supporting it have evolved consistently with the Xi Jinping government's restrictions on expression, increased technological surveillance and control of the population, and increasing international assertiveness and expressions of hostility toward the West. Especially a matter of concern is the marriage of China's antagonism to the West and technological prowess and unequalled role in global supply chains for commercial information and communications products, and, increasingly, related software. While China's own scientific and technology capabilities are significant, its technological progress has been hastened by extensive theft of intellectual property from Western companies and governments, including through state-supported cyber operations.

Cyberspace strategy forms a central part of China's approach to international relations and the goal of an international order more compatible with China's political culture. China prefers a system in which the strong dominate than one in which a rule of law dominates; China has no recent history in which the rule of law has played an important role.

In the last decade, China has benefitted from embedding globally developed open source software in its products and further participating in open source software development customized for its own products. Open source software has permitted China to leap-frog stages of software development and has enabled China to progress in the information, computerization, and nano-technology environment at enviable speed. This participation means that China has a substantial base of coders with access to advanced global open source software development processes.

This access provides opportunities to insert malicious code into systems in daily use in civilian and military systems throughout the West. Being alert to this vulnerability and managing the resulting threat will require fine-grained understanding of both open-source software development processes and China's cyber capabilities and organizations.

China's Cyber Industry

China's cyber industry is robust, substantial, and controlled. It cannot operate without government blessing because China's internal security arrangements ensure a lack of freedom in the cyber field. China's cyber industry is intertwined with the PLA and other government bodies, which were reorganized in the last decade to enhance China's cyber power. China is thus protectionist toward its own cyber industry while simultaneously pushing it to be innovative and to maintain access to Western technology and systems.

Until now, interdependence between industry and government has been more a source of strength than weakness, although the extent of corruption may prove to be an important factor as it has proved to be in the case of Russia's military capabilities on display in Ukraine.[443] The impulse for government domination and controls on access to open development channels ultimately may limit innovation. As in Russia, nationalism and antagonism toward the West, fueled by government propaganda, have helped mobilize popular support for a government.

China foresees competition and perhaps military conflict with the United States and its allies. It has growing confidence that its cyber capabilities will contribute to military success or, even better, to deter the United States and others from daring to oppose future Chinese military actions with regard to Taiwan and the South China Sea, for example. China sees competition with the United States and its allies in the economic, diplomatic, and military realms as continuing to have a substantial cyber component where information dominance in the cyber realm will be crucially important to victory.

Despite the apparent coherence and strength of this strategy, there are risks. China has grown rich through global interdependence. By making its technology firms agents of a hostile government, China has provoked a Western backlash and moves to reestablish at least some balance and separation in the China-West economic competition. China's anti-Western "no limits" alliance with Russia has further alienated influential parts of the West and increased support for Taiwan's *de facto* independence.

Domestic Surveillance and Control

Xi's domestic surveillance state and near totalitarian control of the population during the Covid pandemic have reduced China's economic attractiveness. China's confiscatory approach to foreign technology partners has dramatically reduced China's incentives for Western investment. Looking to the future of China's cyber strategy, it is possible to see an increasingly hostile posture. Chinese government and industry collaboration likely will tighten, accelerating the present trend to split Chinese and Western information economies.

It is possible that the course of Russia's invasion of Ukraine probably gives China's leaders significant concerns. Prior to the invasion, the conventional wisdom was, not only that the Russian military would deliver a rapid success in Ukraine, but also that Russia's vaunted "hybrid warfare" capabilities would be decisive. So far, reality has been different. Much of the discrepancy between prediction and reality is the result of "defense forward" operations by Ukraine and hardening of Ukrainian infrastructure, along with shortfalls in Russian capabilities compared to expectations. China may be too confident to believe that its actions will prove immune to the kind of problems that have surfaced for Russia in the Ukraine war.

[443] It is notably difficult to gather sufficient information about the extent of corruption to be able to assess its impact. See, for example, Wayne Chen, *Corruption in China: How Bad is It?* (Washington: Carnegie Endowment for International Peace, February 2007).

It is also not possible to know the extent to which China's *de facto* alliance with Russia will deepen and threaten its economic access to Western markets. For years, the political control of the CCP has been based on rapid economic growth making the population rich and docile. With Covid and the inherent problems of an export economy transitioning to a more balanced one, there is an immediate prospect that growth will not be maintained. Most likely the government will react with further clampdowns and greater hostility toward the West. Yet the possibility may exists that China's leadership will face conditions that induce some sort of grand re-negotiation of the issues between China and the West, including cyber rules of the road.

Continued Vulnerability of U.S. Critical Infrastructure

Russian failure to meet cyber expectations reflects a success of the U.S. government cyber strategy of Defend Forward. Defend Forward only partly addresses the much greater challenge of China's economic and technological prowess and concerted cyber strategy. The U.S. open economy and vital critical infrastructure remain vulnerable to Chinese cyber operations. The United States relies to too great an extent on supply chain components made in China. Dependence on non-Chinese overseas suppliers also brings risk.

Taiwanese suppliers, for example, are vulnerable to China cyber infiltration short of outright attack or takeover. China's penetration of western technology companies is extensive and a source of Chinese cyber strength and corresponding western weakness. Defend Forward is not a balanced strategy; it relies too much on law enforcement. Alternative programs and approaches are needed as they are in the field of counter-terrorism. Information sharing among trusted allies would be one important measure.

Reducing the Attack Surface

Increased attention to increasing U.S. technological self-reliance and reducing the U.S. cyber "attack surface" is essential to U.S. security. Devices running open source software have become an increasingly large part of this attack surface. Vulnerabilities abound, partly as a result of global participation in the development of this software. Reducing them requires technological, organizational, and legal steps. One promising approach is actively to monitor open source software development processes using "social cyber" tools to detect developer and user organizations indications and malicious code insertion.

Other elements of national and international power and influence and should be deployed in concert to influence how aggressively China may behave in the cyber realm. A clearer policy of deterrence and incentives could supplement Defend Forward operations in making the stakes clear to China. Economic levers beyond the often self-defeating and blunt instrument of tariffs might be used in addition to deterrence within the cyber realm.[444] Given the current trend in U.S.–Chinese relations, American leaders need to pay close attention to opportunities to influence the

[444] On deterrence of cyber attacks, see Abraham Wagner, Thomas Garwin, Nicholas Rostow, Sophia d'Antoine and David Aitel, *Cybersecurity Policy and Planning: Technologies for Keeping the Nation Safe,* (Los Angeles: Center for Advanced Studies on Terrorism, May 2018).

future course of the relationship. After the 20th Party Congress in 2022, China's leadership may take even bolder, anti-U.S. steps than seen so far.

Continued Data Collection and Analysis

Without question, China's cyber operations will continue to pose an increasing threat to U.S. infrastructure, elections, supply chains, and network security. It is essential that the United States make a drastic commitment to understanding and responding to the Chinese threat. Without such a commitment the nation can never hope to deter malicious and potentially catastrophic cyber attacks.[445]

The type of open source data collection effort accomplished in this study needs to become an ongoing operation within the national security community. The AI tools developed in the present effort need to be applied to the evolving data and further developed to meet the needs of a growing challenge. Contractor teams, such as those engaged in the DARPA Social Cyber effort, should be developed and supported to meet this challenge. To the extent possible, their work should be integrated with related efforts by the Intelligence Community.

Offensive Cyber is Essential to U.S. Strategy

Offensive cyber activities are always grounded in the real world; as a result, they are tied to the geopolitical realities that prompt states to act. Understanding China's national cyber strategy and the narratives that justify it is therefore an important prerequisite o development of an effective U.S. cybersecurity strategy. Looking at China's historical trajectory and development in the cyber area and public statements, provides insight into the PRC's overarching method to information communication technologies and how it has changed over time. Understanding China's strategy for information dominance throughout cyberspace can help build a better understanding of how and why China's makes the cyber decisions it does.

Recognizing and Reacting to Deception and Misinformation

China has increasingly utilized the cyber infrastructure to engage in deception and misinformation operations. This is an essential element of China's cyber strategy and uses modern technology. While the United States and its allies are now more inclined to recognize these types of operations, a major challenge remains to structure collection and analytical operations to identify and react to them on a timely basis.

It is increasingly essential to anticipate and deflect the China's strategic use of deception and misinformation. These tactics have been employed throughout China's history, but most governments have yet to seriously address them. This failure inflates China's ability to succeed in those areas in which it decides to compete, and use of deception and misinformation area multiplies China's political and economic advantages.

[445] See John Ratcliffe and Abraham Wagner, *U.S. Needs New 'Manhattan Project' to Avoid Cyber Catastrophe*, NEWSWEEK (May 18, 2022), https://www.newsweek.com/us-needs-new-manhattan-project-avoid-cyber-catastrophe-opinion-1706557. The Office of the Director of National Intelligence echoed this concern in its 2022 Annual Report, calling China "the broadest, most active, and persistent cyber-espionage threat to U.S. Government and private sector networks."

Knowing that China undertakes these types of operations and uses of cyber technologies to accomplish this does not itself enable the U.S. to effectively combat them. A new approach is needed and will draw on the technology base to detect deception activities and misinformation on a timely basis and develop creative solutions to countering them.

References

Agence France-Presse in Beijing, "China passes new national security law extending control over internet," *The Guardian* (July 1, 2015)

Aitel, Dave, *An OSINT look at the Chinese Offensive Cybersecurity Community* (2019)

Allen-Ebrahimian, Bethany, "The American blog pushing Xinjiang denialism," *Axios* (August 11, 2020)

Allen, Gregory C., *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security* (Washington: Center for New American Security, February 2019)

Allison, Graham, Alyssa Resar, and Karina Barbesino, *The Great Diplomatic Rivalry: China vs the U.S.,* (Cambridge: Harvard Belfer Center, August 2022)

Austin, Greg, *Cybersecurity in China: The Next Wave* (Cham: Springer International Publishing, 2018)

Baker-White, Emily, "Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China," *Buzzfeed* (July 17, 2022)

Bakken, Børge, *The Exemplary Society: Human Improvement, Social Control, and the Dangers of Modernity in China* (Oxford: Clarendon Press, 2020)

Balke, Liudmyla, "China's New Cybersecurity Law and US-China Cybersecurity Issues, SANTA CLARA LAW REVIEW (2018)

Beecroft, Nick, *The West Should Not Be Complacent About China's Cyber Capabilities* (Carnegie Endowment for International Peace, July 6, 2021)

Blum, Susan D., *Lies That Bind: Chinese Truth, Other Truths* (Lanham: Rowan & Littlefield, 2007)

Bolsover, Gillian, *Computational Propaganda in China: An Alternative Model of a Widespread Practice*, Samuel Woolley and Philip N. Howard, Eds. Working Paper (Oxford: Project on Computational Propaganda, November 2017)

Brandt, Jessica and Torrey Taussig, *The Kremlin's disinformation playbook goes to Beijing: China has abandoned its low profile for a high-stakes strategy*, (Washington: The Brookings Institution, May 19, 2020)

Bostrom, Nick, *Superintelligence: Paths, Dangers and Strategies* (Oxford; Oxford University Press, 2014)

Brown, John, *Securing U.S. Research Enterprise from China's Talent Recruitment Plans*, Statement before the Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations (November 19, 2019)

Cary, Dakota, *Academics, AI, and APTs: How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research* (Washington: Center for Security and Emerging Technology, March 2021)

Cary, Dakota, *China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain* (Washington: Center for Security and Emerging Technology, 2021)

Cary, Dakota, "China's next generation of hackers won be criminals: That's a problem," *TechCrunch* (November 12, 2021)

Cary, Dakota, *Robot Hacking Games: China's Competitions to Automate the Software Vulnerability Lifecycle* (Washington: Center for Security and Emerging Technology, September 2021)

Cary, Dakota, *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)

Chang, Gordon G., *The Great U.S.-China Tech War* (New York: Encounter Books, 2020)

Cheng, Dean, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Denver: Praeger Publishers, 2017)

Chen, Dingding and Wang Lei, "Where Is China-US Technology Competition Going?" *The Diplomat* (May 2, 2022)

Cheung, Tai Ming, "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities," *Journal of Cyber Policy* (2018)

China State Council, *New Generation Artificial Intelligence Development Plan* (新一代人工智能发展规划) (Beijing, July 2017)

Chinese Tactics, Army Techniques Publication (ATP) 7-100.3 (August 9, 2021)

Congressional Research Service, *Artificial Intelligence and National Security* (November 10, 2021)

Congressional Research Service, *Emerging Military Technologies: Background and Issues for Congress* (November 10, 2021)

Congressional-Executive Commission on China, *China's State Organizational Structure* (accessed August 19, 2022)

Cordesman, Anthony, *China's New 2019 Defense White Paper* (Washington: Center for Strategic and International Studies, July 24, 2019)

Cordesman, Anthony, *China: The Civil-Military Challenge (Rev.)* (Washington: Center for Strategic and International Studies, January 4, 2022)

Cordesman, Anthony, *Chinese Strategy, Military Forces, and Economics: The Metrics of Cooperation, Competition and/or Conflict* (Washington: Center for Strategic and International Studies, September 18, 2018)

Cornish, Paul (ed.), *The Oxford Handbook of Cyber Security* (Oxford: Oxford University Press, 2021)

Corruption in China: How Bad is It? (Carnegie Endowment for International Peace, February 2007).

Costello, John and Joe McReynolds, *China's Strategic Support Force: A Force for a New* Era (Washington: National Defense University Press, 2018)

Cox Committee (House Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China), 105th Congress, 2d Session, Report 105-851, March. 25, 1999)

Creemers, Rogier, *China's Cybersecurity Regime: Securing the Smart State* (Leiden University, 2022).

Creemers, Rogier, *China's Cyber Governance Institutions*, Leiden Asia Centre (January 2021)

Creemers, Rogier, Paul Triolo and Graham Webster, *Translation: Cybersecurity Law of the People's Republic of China* (New America, June 29, 2018)

Creemers, Rogier, "The Pivot in Chinese Cybergovernance: Integrating Internet Control in Xi Jinping's China," *China Perspectives* (2015)

Creemers, Rogier, "China's Conception of Cyber Sovereignty: Rhetoric and Realization" in Broeders, Dennis and Bibi van den Berg, *Digital Technologies and Global Politics* (Lanham: Rowman and Littlefield, 2020)

Cybereason Nocturnus, *Operation CuckooBees: Cybereason Uncovers Massive Chinese Intellectual Property Theft Operation* **(**Cybereason, May 4, 2022)

Cybersecurity Administration (网络安全管理局) of the PRC Ministry of Industry and

Information Technology (MIIT; 工业和信息化部; **工信部**) *Open Solicitation of Opinions on the Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021-2023)*

de Liedekerke, Arthur and Michael Zinkanell, *Deceive and Disrupt: Disinformation as an Emerging Cybersecurity Challenge* (Vienna: Austrian Institute for European and Security Studies, June 2020)

Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (Washington: January 15, 2019)

Delio, Michelle, "A Chinese Call to Hack U.S.," WIRED (April 11, 2001)

Denning, Dorothy, "Cyberwar: How Chinese Hackers Became a Major Threat to the U.S.," NEWSWEEK (October 5, 2017)

Department of Homeland Security (CISA), *Chinese Cyber Threat Overview and Actions for Leaders* (July 19, 2021)

Department of Homeland Security (CISA), *China Cyber Threat Overview and Advisories* (July 2021)

Department of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally*, (September 16, 2020)

Department of State, *People's Republic of China Efforts to Amplify the Kremlin's Voice on Ukraine* (May 3, 2022)

DeSombre, Winnona, Dave Aitel, and Ian Roos, *Watching the Watchers*, (New York: *Margin Research*, April 5, 2022)

Dwoskin, Elizabeth, "China is Russia's most powerful weapon for information warfare," *Washington Post* (April 8, 2022)

Economy, Elizabeth, "Xi Jinping's New World Order," *Foreign Affairs* (January 2022)

Edwards, Mitch, "China's Green Army: Capitalism Defeats China's First Hacking Group," MEDIUM (March 28, 2018)

Erie, Matthew, and Thomas Streinz, "The Beijing Effect: China's Digital Silk Road as Transnational Data Governance," *New York University Journal of International Law and Politics* (2021)

Fedasiuk, Ryan, Jennifer Melot and Ben Murphy, *Harnessed Lightning: How the Chinese Military is Adopting Artificial Intelligence* (Washington: Center for Security and Emerging Technology, October 2021)

Fedasiuk, Ryan and Jacob Feldgoise, *The Youth Thousand Talents Plan and China's Military*, (Washington: Center for Security and Emerging Technology, August 2020).

Feigenbaum, Evan, *China's Techno-Warriors* (Stanford: Stanford University Press, 2003)

Goldsmith, Jack, "The Internet and the Abiding Significance of Territorial Sovereignty," *Indiana Journal of Global Legal Studies* (1998)

Goldsmith, Jack and Robert D. Williams, "The Failure of the United States' Chinese-Hacking Indictment Strategy," *Lawfare* (December 28, 2018)

Greenberg, Andy, "How China's Hacking Entered a Reckless New Phase," *Wired* (July 19, 2021)

Griffiths, James, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet* (London: Bloomsbury, 2021)

Hanson, Fergus, Emilia Currey, and Tracy Beattie. "The Chinese Communist Party's Coercive Diplomacy." (Aspi.org.au, 2020)

Harold, Scott W., Nathan Beauchamp-Mustafaga, and Jeffrey W., Hornung, *Chinese Disinformation Efforts on Social Media* (Santa Monica: The RAND Corporation, 2021)

Hassid, Jonathan, "China's Responsiveness to Internet Opinion: a Double-Edged Sword," *Journal of Current Chinese Affairs* (2015)

Heath, Timothy R., *U.S. Strategic Competition with China: A RAND Research Primer*, (Santa Monica: The RAND Corporation, November 16, 2021)

Henderson, Scott, *The Dark Visitor: The Inside World of Chinese Hackers* (Scott Henderson, 2007)

Herbert, Natalie, *Achieving the PLA's Strategic Support Force talent needs through MCF* (China Aerospace Studies Institute, February 2021)

Hjortdal, Magnus, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* (2011)

Hoffman, Samantha and Elsa Kania, "Huawei and the ambiguity of China's intelligence and counter-espionage laws," *The Strategist* (September 13, 2018)

Horsley, Jamie P., *Behind the Facade of China's Cyber Super-Regulator* (Stanford University, DIGICHINA, August 8, 2022)

Huang, Aaron, *Combatting and Defeating Chinese Propaganda and Disinformation* (Cambridge: Harvard Belfer Center, 2021)

Information Office of the State Council of the People's Republic of China, *China's National Defense in 2004* (December 2004).

Jinghua, Lyu, *What Are China's Cyber Capabilities and Intentions?* (Washington: Carnegie Endowment for International Peace, April 1, 2019)

Jisi, Wang "The Plot Against China? How Beijing See the New Washington Consensus," *Foreign Affairs,* (July/Aug. 2021).

Joske, Alex, *The China Defence Universities Tracker* (Barton: Australian Strategic Policy Institute, November 25, 2019)

Kahn, Lauren, What the Defense Department's 2021 China Military Power Report Tells Us About Defense Innovation," *Lawfare* (February 15, 2022)

Kaja, Ashwin and Yan Luo, *Covington Artificial Intelligence Update: China's Vision for The Next Generation of AI* (New York: Covington & Burling, March 24, 2018)

Kania, Elsa B., *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power* (Washington: Center for New American Security: November 28, 2017)

Kania, Elsa B. and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," THE CYBER DEFENSE REVIEW (2018).

Kania, Elsa B. and Lorand Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy* (Washington: Center for New American Security, January 28, 2021)

Kans, Michael, "Data Brokers and National Security," *Lawfare* (April 29, 2021)

Keller, Perry, "Sources of Order in Chinese Law," *American Journal of Comparative Law* (1994)

Kharpal, Arjun, "Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice," *CNBC* (March 5, 2019)

Kinetz, Erica, "Army of fake fans boosts China's messaging on Twitter," *Associated Press* (May 11, 2021)

King, Gary, Jennifer Pan, and Margaret E. Roberts," How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* (May 2013)

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument." *American Political Science Review* (2017)

King, Gary, Jennifer Pan, and Margaret E. Roberts, "Reverse-engineering censorship in China: Randomized experimentation and participant observation," *Science* (2014)

Klyman, Kevin, "China's Tech Crackdown Could Give It an Edge," *The Diplomat* (April 30, 2022)

Kohn, Miriam, "Clearview AI, TikTok, and the Collection of Facial Images in International Law." CHICAGO JOURNAL OF INTERNATIONAL LAW, (June 1, 2022).

Konaev, Margarita, et al, *Headline or Trendline? Evaluating Chinese-Russian Collaboration in AI* (Washington: Center for Security and Emerging Technology, August 2021)

Kovacs, Eduard, "$1.9 Million Paid Out for Exploits at China's Tianfu Cup Hacking Contest," *Security Week* (October 19, 2021).

Kozy, Adam, *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)

Lakshmanan, Ravi, "Windows 10, Linux, iOS, Chrome and Many Others at Hacked Tianfu Cup 2021," *The Hacker News* (October 17, 2021)

Lammbrau, Michael, "Intelligence Expert: Is TikTok China's Trojan Horse?" *Newsweek* (August 8, 2022)

Lampton, David, "Xi Jinping and the National Security Commission: Policy Coordination and Political Power," *Journal of Contemporary China* (2015)

Lee, Jyh-An., "Hacking into China's Cybersecurity Law," WAKE FOREST LAW REVIEW (2018)

Lee, Kai-Fu, *AI Superpowers, China, Silicon Valley and the New World Order* (Boston: Houghton Mifflin, 2018)

Li, Pei and Cate Cadell, "At Beijing security fair, an arms race for surveillance tech," *Reuters* (May 30, 2018)

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford University Press, March 2, 2015)

Lu, Shen "A report detailed the tech gap between China and the U.S. Then it disappeared," *Protocol* (February 9, 2022)

Lyall, Nicholas, "China's Cyber Militias," *The Diplomat* (March 1, 2018)

Maizland, Lindsay, *Hong Kong's Freedoms: What China Promised and How It's Cracking Down* (New York: Council on Foreign Relations, May 19, 2022)

Mandiant Threat Intelligence, *Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance* (June 28, 2022)

Maranto, Lauren, *Who Benefits from China's Cybersecurity Laws* (Washington: Center for Strategic and International Studies, June 25, 2020)

Marczak, Bill et al., *An Analysis of China's "Great Cannon,"* 5th USENIX Workshop on Free and Open Communications on the Internet (FOCI 15) (2015)

Masaaki, Yatsuzuka, "China's Efforts to Seize Control of Discourse Power in Cyberspace," *Asia-Pacific Review* (March 18, 2022)

McReynolds, Joe (ed.), *China's Evolving Military Strategy* (Washington: Brookings, 2016)

McWhorter, Dan, *APT1: Exposing One of China's Cyber Espionage Units* (Mandiant, 2013)

Miao, Weishan, and Rongbin Han, "Modernization Planner, Authoritarian Paternalist, and Rising Power: Evolving Government Positions in China's Internet Securitization," *Journal of Contemporary China* (2021)

Mearsheimer, John, J., "The Inevitable Rivalry: America, China, and the Tragedy of Great-Power Politics," *Foreign Affairs*, November/December 2021

Metcalf, Mark, *Deception is the Chinese Way of War* (U.S. Naval Institute, February 2017)

Mattox, John Mark, "The Moral Limits of Military Deception," *Journal of Military Ethics* (2002)

Momoi, Yuri, "China's rewrite of Hong Kong's history 50 years in the making," *Nikkei Asia* (July 2, 2022)

Mozur, Paul and Chris Buckley, "Spies for Hire: China's New Breed of Hackers Blends Espionage and Entrepreneurship," *The New York Times* (August 26, 2021)

National Security Agency, *Chinese State-Sponsored Cyber Operations: Observed TTPs* (July 2021)

National Security Commission on Artificial Intelligence, *Final Report* (March 2021)

National Security Institute, "Don't Trust TikTok's Plan to Secure Americans' Data," *The SCIF* (June 30, 2022)

Nimmo, Ben, Ira Hubert, I., and Yang Cheng, "Spamouflage Breakout Chinese Spam Network Finally Starts to Gain Some Traction," *Graphika* (February 2021)

Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the Peoples Republic of China 2021* (October 2021)

Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*, (2021)

O'Neill, Patrick H., "How China built a one-of-a-kind cyber-espionage behemoth to last." *MIT TECHNOLOGY REVIEW* (February 28, 2022)

O'Neill, Patrick H, "How China turned a prize-winning iPhone hack against the Uyghurs," *MIT TECHNOLOGY REVIEW* (May 6, 2021).

Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035) 中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要

Paller, Alan, *Cybersecurity: Developing a National Strategy*, SANS Institute (April 28, 2009)

Perlroth, Nicole, "How China Transformed Into a Prime Cyber Threat to the U.S.," *The New York Times* (July 19, 2021)

Pillsbury, Michael, *The Hundred Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt & Co., 2015)

Pollpeter, Kevin L., Michael S. Chase, and Eric Heginbotham, The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations (Santa Monica: The RAND Corporation, 2017)

Pye, Lucian W. and Nathan Leites, *Nuances in Chinese Political Culture* (Santa Monica: The RAND Corporation, November 1970)

Pye, Lucian W., *Spirit of Chinese Politics* (Cambridge: MIT Press, 1968)

Pyo, Grace, "An Alternate Vision: China's Cybersecurity Law and its Implementation in the Chinese Courts," *Columbia Journal of Transnational Law* (2021)

Qi, Aimin, Guosong Shao, and Wentong Zheng, "Assessing China's Cybersecurity Law," Computer Law & Security Review (2018)

Ratcliffe, John and Abraham Wagner, "U.S. Needs New 'Manhattan Project' to Avoid Cyber Catastrophe," Newsweek (May 18, 2022)

Robertson, Jordan and Jamie Tarabay, *Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack* (Bloomberg, December 16, 2021)

Ruan, Lotus and Gabrielle Lim, "Balancing Reality and Fear: Why an Alarmist Take on Chinese Influence Operations Is Counterproductive," *Just Security* (July 21, 2021)

Sanchez, Linda, Bolstering *the Democratic Resilience of the Alliance Against Disinformation and Propaganda* (NATO Parliamentary Assembly, October 10, 2021)

Saunders, Philip C., "Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Nuclear Forces," USCC (June 10, 2021).

Schroeder, Emma, Stewart Scott, and Trey Herr, *Victory reimagined: Toward a more cohesive US cyber strategy,* (Washington: Atlantic Council, June 14, 2022)

"Section 3: Chinese Intelligence Services and Espionage Threats to the United States," *USCC* (2019)

Segal, Adam, "The Coming Tech Cold War With China," *Foreign Affairs* (2020)

Seib, Philip, *Information War: Journalism, Disinformation and Modern Warfare* (Cambridge: Polity Press, 2021)

Serabian, Ryan and Daniel Kappellman Zafra, *"HaiEnergy" Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites* (Mandiant, August 4, 2022)

Shihab, Mohammed, "Expanding Cyber Demands Embolden China's Homegrown Cybersecurity Darlings: China is building a welcoming ecosystem for its homegrown tech darlings," *The Diplomat* (September 23, 2019)

Silva, Christiana and Elizabeth de Luna, "It Looks like China Does Have Access to U.S. TikTok User Data," *Mashable* (July 2, 2022)

Simonite, Tom, "For Superpowers, Artificial Intelligence Fuels New Global Arms Race," *Wired* (August 8, 2017)

Small, Jalen, "U.S. Intel, Google Warn of Cyberattacks from China, Russia, North Korea," NEWSWEEK (April 28, 2022)

Solis, Gary D., *The Law of Armed Conflict* 3rd Edition (Cambridge: Cambridge University Press, 2022)

Starosielski, Nicole, *The Undersea Network* (Durham: Duke University Press, 2015)

State Council Information Office, *Tenth Five Year Plan for National Economic and Social Development, Informationization Key Point Special Plans* (Beijing, October 18, 2022)

Stockton, Paul, *Defeating Coercive Information Operations in Future Crises* (Baltimore: Johns Hopkins University Applied Physics Laboratory, 2021)

Stokes, Mark A. and L.C. Russell Hsiao, *Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests* (Project 2049 Institute, October 29, 2012)

Stone, Alex and Peter Wood, *China's Military-Civil Fusion Strategy: A View from Chinese Strategists* (Montgomery: China Aerospace Studies Institute, June 15, 2020)

Sun Tzu on the Art of War, translated by Lionel Giles (London: Luzai & Company, 1910)

Swaine, Michael, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor* (2013)

Tai, Katharin, and Yuan Yi Zhu, "A historical explanation of Chinese cybersovereignty," *International Relations of the Asia-Pacific* (2022)

Tan, Zixiang Alex, Milton Mueller, and Will Foster, "China's New Internet Regulations: Two Steps Forward, One Step Back," *Communications of the ACM* (2021)

Tarabay, James and Sarah Zheng, "Chinese Firm That Accused NSA of Hacking Has Global Ambitions," BLOOMBERG (May 31, 2022)

The Chinese Offensive Cyber Landscape (New York: Margin Research, April 2022)

The Longer Telegram: Toward a new American China strategy, (Washington: Atlantic Council (January 28, 2021)

Thomas, Timothy L., *The Chinese Way of War: How Has it Changed*. (McLean: The MITRE Corp, 2020)

Tianliang, Xiao, *Zhanluexue* [Science of Military Strategy] (National Defense University Press 2015)

Uber, Richard, *China's Artificial Intelligence Ecosystem* (Washington: National Intelligence University, 2021)

United States v. Lizhi, et al, No. 20-cr-158 (D.C. DC, May 7, 2020)

United States v. Wang Dong, et al., No. 14-cr-118 (W.D. PA, May 1, 2014)

United States v. Zhang Zhang-Gui, et al., No. 18-cr-3132 (S.D. CA, October 25, 2018)

United States v. Wu Zhiyong, et. al., No. 20-cr-046 (N.D. GA, January 28, 2020)

United States v. Zhu Hua, et al., No. 18-cr-891 (S.D.N.Y. December 17, 2018)

United States v. Ding Xiaoyang, et al., No. 21-cr-1622 (S.D. CA, May 28, 2021)

United States v. Fujie Wang et al., No. 19-cr-153 (S.D. IN, May 7, 2019)

United States Senate, Permanent Subcommittee on Investigations*, Report China's Impact on the U.S. Education System,* (February 2019)

"U.S. Accuses Two Hackers of Stealing Secrets from American Firms for China: Alleged hackers tested defenses at four U.S. companies working on coronavirus treatment," *Wall Street Journal* (July 21, 2020)

Vatanparast, Roxana, "The Infrastructures of the Global Data Economy: Undersea Cables and International Law," HARVARD INTERNATIONAL LAW JOURNAL (2020)

von Carnap, Kai and Valarie Tan, "Tech Regulation in China Brings in Sweeping Changes," *The Diplomat* (December 21, 2021)

Wagner, Abraham**,** *Chinese Cyber and Intelligence Initiatives: Critical Elements of a Grand Strategy* (forthcoming, 2022)

Wagner, Abraham, Thomas Garwin, Nicholas Rostow, Sophia d'Antoine and David Aitel, *Cybersecurity Policy and Planning: Technologies for Keeping the Nation Safe* (Los Angeles: Center for Advanced Studies on Terrorism, 2018)

Wagner, Abraham and Nicolas Rostow, *Cybersecurity and Cyberlaw* (Durham: Carolina Academic Press, 2020)

Waldie, Bradford, "How Military-Civil Fusion Steps Up China's Semiconductor Industry," *DigiChina* (April 1, 2022)

Waltzman, Rand, The *Weaponization of Information: The Need for Cognitive Security* (Santa Monica: The RAND Corporation, April 2017)

Wang, Yuhua, and Carl Minzner, "The Rise of the Chinese Security State," *The China Quarterly* (2015)

Webster, Graham and Paul Triolo, "Translation: China Proposes 'Global Data Security Initiative'," *New America* (September 7, 2020)

Weinbaum, Cortney, Caolionn O'Connell, Steven W. Popper, M. Scott Bond, Hannah Jane Byrne, Christian Curriden, Gregory Weider Fauerbach, Sale Lilly, Jared Mondschein, and Jon

Schmid, *Assessing Systemic Strengths and Vulnerabilities of China's Defense Industrial Base* (Santa Monica: The RAND Corporation, 2022)

Weiping, Zheng and Liu Minfu, *Discussion on the Military's New Historic Missions* (Beijing: People's Armed Police Publishing House, 2005)

Weiss, Jessica Chen and Jeremy L. Wallace, "Domestic Politics, China's Rise, and the Future of the Liberal International Order," *International Organization* (February 2021)

Whaley, Barton, *Stratagem: Deception and Surprise in War* (Boston: Artech House, 2007)

Wong, Chun Han, "China Insists Party Elites Shed Overseas Assets, Eyeing Western Sanctions on Russia," WALL STREET JOURNAL (May 19, 2022)

Wong, Edward, Matthew Rosenberg, and Julian Barnes, "Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say," *New York Times*, (April 22, 2020)

Work, J.D., *China Flaunts Its Offensive Cyber Power* (War on the Rocks, October 22, 2021)

Wuthnow, Joel and Philip C. Saunders, Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications (Washington: National Defense University Press, March 2017).

Xu, Kevin, *Open Source in China: The Players,* (Interconnected, May 7, 2020)

Yang, Jianli and Nick Monaco, "Why the US Must Take China's Disinformation Operations Seriously," *The Diplomat* (January 28, 2022)

Yang, Sheng and Chen Qingqing, "China's national intelligence authority introduces itself in high-profile manner, showing confidence in shaping the image," *Global Times* (January 10, 2021)

Yang, Zeyi, "How Chinese tech companies took over the world in 2021," *Protocol* (December. 29, 2021)

Yu, Miles Maochun, *Understanding China's Strategic Culture Through Its South China Sea Gambit* (Stanford: Hoover Institution, May 2011)

Zhang, Linda, "How to Counter China's Disinformation Campaign in Taiwan." *Military Review* (September-October 2020)

Zhanluexue [Science of Military Strategy] (National Defense University Press 2013)

Zweig, David and Huiyao Wang, *Can China Bring Back the Best? The Communist Party Organizes China's Search for Talent*, *The China Quarterly* (September 12, 2013)

Zwetsloot, Remco, "China's Approach to Tech Talent Competition: Policies, Results, and the Developing Global Response," *Global China* (April 2020)

List of Abbreviations

AI—Artificial Intelligence

APT—Advanced Persistent Threats

BIS—Bureau of Industry and Security (U.S. Commerce Department)

BRI—Belt and Road Initiative

CAC—Cyberspace Administration of China

CAE-Cyber Operations—National Centers of Academic Excellence in Cyber Operations Program (U.S.)

CCAC--Central Cyberspace Affairs Commission (also CCCI)

CCCI—Central Commission for Cybersecurity and Informatization (also CCAC)

CCIA—China Cybersecurity Industry Alliance

CL—Cybersecurity Law

CNCERT/CC—National Computer Network Emergency Response Technical Team / Coordination Center of China

CNITSEC—China Information Technology Security Evaluation Center

CNNVD—Chinese National Vulnerability Database of Information Security

CNVD—China National Vulnerability Database

CTF—Capture the Flag (a type of hacking contest)

DNS—Domain Name System

DSL—Data Security Law

DSR—Digital Silk Road

GAD—General Armament Department

GSD—General Staff Department

ICT—Information and Communications Technology

MCF—Military Civil Fusion

MIIT—Ministry of Industry and Information Technology

MPS—Ministry of Public Security

MSS—Ministry of State Security

NSA—National Security Agency (U.S.)

OSS—Open Source Software

OWASP—Open Web Application Security Project

PLA—People's Liberation Army

PLAIEU—PLA Information Engineering University

PIPL—Personal Information Protection Law

SAMR—State Administration for Market Regulation

SASTIND—State Administration for Science, Technology and Industry for National Defense

SSF—Strategic Support Force

WCCS—World Class Cybersecurity Schools