MANDIANT
YOUR CYBERSECURITY ADVANTAGE

TESTIMONY BEFORE THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

PANEL II: CHINA'S GOALS AND CAPABILITIES FOR CYBER ESPIONAGE

China's Capabilities for State-Sponsored Cyber Espionage

KELLI VANDERLEE
SENIOR MANAGER, STRATEGIC ANALYSIS
MANDIANT THREAT INTELLIGENCE

FEB. 17. 2022

Executive Summary

- Following China's military and intelligence restructuring, Mandiant Threat Intelligence believes the technical tradecraft used by Chinese cyber espionage groups since 2016 has steadily evolved to become stealthier and more agile, while taking measures to complicate attribution.
- Chinese cyber espionage operators' use of vulnerability exploitation, third party compromise, and software supply chain compromise exemplify both the scale of Chinese state-sponsored threat activity and the strategic evolution in use of tactics to maximize efficiency and impact.
- In 2020 and 2021, we believe Chinese cyber espionage activity has demonstrated a higher tolerance for risk and is less constrained by norms or diplomatic pressures.

Chinese Cyber Espionage Distinguished by Interests and Scale

Threat clusters attributed to China exhibit a range of skill levels and employ tactics, techniques, and procedures (TTPs) common to many cyber threat groups.[i] Following China's military and intelligence restructuring, we believe the technical tradecraft used by Chinese cyber espionage groups since 2016 has steadily evolved to become stealthier and more agile, while taking measures to complicate attribution. For example, using software supply chain and third-party compromises to collect data makes detecting and preventing intrusions more difficult for victims.

Chinese cyber espionage malware use appears to have evolved to operate on a wider variety of operating systems, focus on modular code families, and increasingly incorporate malware only executed in memory. Actors also leverage a combination of publicly and non-publicly available tools to accomplish operations. We believe that Chinese threat groups have become increasingly likely to use publicly available malware and other widely used tactics, particularly in early stages of a compromise, in an effort to blend in with other threat activity.

The primary elements that distinguish Chinese cyber espionage activity from that of groups we track linked to other states are national interest and scale. Beijing has specific and unique intelligence collection requirements that are unlikely to overlap with other nations, for example in Hong Kong, Tibet, and the Uyghur community. In terms of scale, Chinese cyber threat activity is simply bigger. Based on Mandiant observations, there are more Chinese state-linked threat groups conducting more compromises, exploiting more zero-days than other nations – and this remains true even after the volume of Chinese cyber threat activity we observed declined by at least half from 2013 to 2016.[ii,iii]

Initial Infection Vectors: A Journey of a Thousand Miles Begins with a Single Step

Chinese cyber espionage actors use a variety of initial access vectors to gain a foothold in targeted environments including email phishing and other social engineering, strategic web compromise, and SQL injection. While not unique to Chinese groups, Chinese activity sets have used several tactics with distinction. For the purposes of this testimony, I would like to focus on Chinese cyber espionage operators' use of vulnerability exploitation, third-party compromise, and software supply chain compromise, as these reflect both the scale, and the strategic evolution in use of tactics to maximize the efficiency and impact of Chinese cyber espionage.

Vulnerability Exploitation

Malicious actors exploit flaws or vulnerabilities in software for a variety of purposes ranging from obtaining information about a targeted device that should not have been accessible, to causing a device to stop working, to convincing a targeted device to run attacker commands. Many of the vulnerabilities we see threat actors exploit are vulnerabilities that vendors have disclosed and patched. These are sometimes called n-day vulnerabilities. Zero-day vulnerabilities are vulnerabilities that were exploited before the vendor was aware of the issue to release a patch, and before consumers had the option to update their software and fix the problem.

Chinese cyber espionage actors have made effective use of both n-day and zero-day vulnerabilities in 2020 and 2021.[iv] Significantly, in Mandiant analysis of zero-day exploitation from 2012 to mid-2021, of the vulnerabilities we were able to attribute, Chinese state-linked groups exploited more than any other nation.[v]

APT41 Exploits Multiple N-Day Vulnerabilities in Early 2020

In early 2020, Mandiant observed APT41[1] conduct a large-scale campaign leveraging vulnerabilities in enterprise networking and endpoint management devices from Citrix, Cisco, and Zoho, that affected more than 75 Mandiant customers.[vi] These organizations spanned 20 nations including the United States, and a variety of sectors, from aerospace and defense, to pharmaceuticals, to energy and utilities.

Despite the wide aperture of the campaign, we found evidence that the activity was targeted. For example, observed attempts to exploit Cisco devices were only sent to Cisco devices, suggesting that the attackers had identified a list of internet accessible devices before commencing operations. APT41 is one of the most prolific Chinese cyber espionage groups that we track, and this campaign further underscores the apparent high operational tempo and wide collection requirements for APT41.[vii]

Multiple Chinese Activity Sets Exploit Microsoft Exchange "ProxyLogon" Vulnerabilities

From January to March 2021, we documented many threat groups using the so called "ProxyLogon" zero-day vulnerabilities to gain access to targeted networks, including at least five activity sets we attribute to China.[viii] While three of these clusters appeared to carefully select their targets before an attempted exploitation of these vulnerabilities, others conducted widespread scanning and compromised tens of thousands of servers in virtually every vertical and region.

The progressive adoption of the same exploit code among Chinese espionage groups prior to the release of a public patch potentially indicates the existence of a shared development and logistics infrastructure and possibly a centralized coordinating entity. Mandiant research dating back to 2013 has likewise suggested a logistical support function supporting Chinese cyber espionage groups.[ix]

The widespread impact of this activity prompted an unprecedented international response: in July 2021, governments and intergovernmental organizations in North America, Europe, and Asia issued coordinated statements condemning the ProxyLogon exploitation activity as well as other cyber espionage directed by the Chinese government.[x,xi,xii]

Pulse Secure VPN Zero-day Exploitation

Mandiant investigated multiple intrusions in the defense, government, high-tech, transportation, and financial sectors in the U.S. and Europe that occurred between August 2020 and March 2021. We suspect these incidents began with exploitation of several vulnerabilities in Pulse Secure VPNs, including one zero-day. We attribute this activity to two Chinese activity clusters, one of which we suspect of having ties to APT5. Associated with this activity, we are tracking at least 16 malware families specifically designed to manipulate Pulse Secure devices.[xiii]

Both activity sets associated with this campaign took steps to preserve operational security and stymie forensic investigations, such as clearing logs, cleaning up evidence of data staged for exfiltration, and

[1] Mandiant defines APT groups as activity clusters we believe to be state sponsored and primarily focused on espionage.

changing file timestamps. The actors demonstrated detailed knowledge of the targeted appliances and victim networks.

Third Party Compromise

Third-party compromise exploits the inherent trust that users and administrators place in relationships with other legitimate businesses, as well as genuine products and services that enter their organization through expected avenues. Malicious actors frequently target professional service providers, such as lawyers or accountants, and technology service providers, such as managed IT, managed service providers (MSPs), or cloud infrastructure providers to gain access to client data and networks. Third-party compromises afford tactical and operational advantages to attackers compared to direct targeting: a single compromise can facilitate access to multiple potential targets, and victims may be less likely to detect, and have fewer options to prevent, an intrusion that abuses a trusted channel.

APT10 MSP Compromises

In April 2017, PricewaterhouseCoopers (PwC) reported on APT10 activity targeting MSPs to conduct third-party compromises against additional victims in "Operation Cloud Hopper."[xiv] According to PwC, APT10 initially compromised MSPs, then used this access to infect downstream customers by exploiting the trusted access to systems required for the MSP to conduct its services. Data stolen from these customers was then often compressed and sent back to the MSP for eventual exfiltration.

This is consistent with Mandiant observations.[xv] For example, we investigated cases in which APT10 accessed victims through MSPs in North America and Europe. A notable infection involved a SOGU backdoor that was set to communicate with its command and control (C&C) server through a server belonging to the victim's MSP, likely indicating a foothold on the MSP's network. The tactic also masks malicious C&C and exfiltration traffic and make it appear innocuous.

A U.S. indictment, unsealed in December 2018, and other open-source reporting further corroborates APT10's use of MSP third-party compromise to gain access to additional victims, including telecommunications companies.[xvi,xvii]

APT41 and MESSAGETAP

During a 2019 incident response investigation at a telecommunications network provider, Mandiant identified a malware family dubbed MESSAGETAP that we attribute to APT41.[xviii] Specifically, MESSAGETAP was discovered within a cluster of Linux servers responsible for routing Short Message Service (SMS) messages to an intended recipient or storing them until the recipient has come online.

MESSAGETAP is designed to work with configuration files providing parameters for collection: keywords of geopolitical interest to China, as well as international mobile subscriber identities (IMSI) and phone numbers identifying specific devices for potential monitoring, see Figure 1. If SMS content sent or received by one of the identified devices also matched the keyword list, the contents of the message would be saved for later collection by the threat actors. Sanitized examples of keywords include the names of political leaders, military and intelligence organizations, and political movements at odds with the Chinese government.

The deployment of MESSAGETAP at a telecom demonstrates Chinese strategic intelligence collection efforts to move "upstream," collecting information closer to the backbone of global communications. Instead of targeting individual devices for SMS data, the detected APT41 campaign captures such information at the telecom, many degrees removed from the end user. This type of compromise would leave no forensic evidence on targeted users' devices or other signs that the messages had been intercepted.

Software Supply Chain Compromise

A specialized subset of third-party compromise, supply chain compromise, occurs when attackers gain unauthorized access to legitimate infrastructure or tools and implant malicious code to be delivered by the legitimate vendor or repository via the same trusted distribution methods that users would normally use to obtain the legitimate hardware, software, open-source package, or updates.

In Mandiant analysis of software supply chain compromise incidents from 2013 to 2020, of the incidents we were able to attribute to state sponsored actors, Chinese threat groups conducted nearly double the number of Russian and North Korean-attributed incidents combined.

APT41 is well known for several large-scale software supply chain compromises targeting video games as well as common enterprise software, such as the 2018 campaign affecting the ASUS live update utility, dubbed Operation ShadowHammer by Kaspersky.[xix] Open-source reporting suggests that more than 50,000 systems installed the malicious update.[xx] See Figure 2 for information about APT41 software supply chain compromises.

In 2019 and 2020, we observed evidence of at least four examples of suspected Chinese software supply chain compromises which involved trojanizing or including suspicious functionalities in software provided, and in some cases, required by government authorities. Three of these cases involved Chinese government software and appear to have been intended to gather intelligence on foreign businesses operating in China as well as Chinese citizens.[xxi, xxii, xxiii] One instance affected a Vietnamese government digital signature verification software.[xxiv]

Chinese Military and Intelligence Restructuring Informs MSS and PLA Cyber Threat Activity

Since taking power in 2012, Xi Jinping has sought to consolidate domestic power and maintain China's regional hegemony through political and military modernization.[xxv] Mandiant Threat Intelligence believes the restructuring of China's military and civilian intelligence agencies significantly impacted cyber espionage operations in terms of active actors, tempo of operations, and observed TTPs, particularly from 2014 to 2016 when several substantial changes were enacted, see Figure 3.[xxvi]

Mandiant recently conducted a focused study of Chinese cyber threat activity from 2017 to 2020 and found that observed cyber threat activity appears to be consolidating into patterns reflective of the new structure and operational mandates of the People's Liberation Army (PLA) and the Ministry of State Security (MSS).

Building on this research, we suggest that MSS activity can be differentiated from that of the PLA based on geographic scope and alignment of operations and victims to each organization's mission mandate. While threat groups we believe to be affiliated with PLA Theater Commands, such as Tonto Team and TEMP.Overboard, appear to focus operations on regions within the areas of responsibility of their respective Theater Commands, MSS-affiliated groups, such as APT41, APT5, and APT10, discussed above, demonstrate a much broader geographic scope. We also believe that MSS groups are more likely to target the United States and regions outside of China's direct sphere of influence, such as Europe, Latin America and the Caribbean, and North America. This geographic spread likely reflects MSS responsibilities to conduct domestic counterintelligence, non-military foreign intelligence, and support aspects of political security.[xxvii]

Indictments, Sanctions, Diplomatic Agreements No Longer Significantly Constrain Cyber Espionage

Mandiant Threat Intelligence believes Chinese cyber espionage activity has demonstrated a higher tolerance for risk and is less constrained by norms or diplomatic pressures than previously characterized, mirroring bolder rhetoric and policy in other arenas.

Public Exposure and Indictments of Cyber Threat Operators

Evidence suggests that public exposure and indictments of Chinese cyber espionage operators has become less effective at deterring threat activity over time.

Public exposure and indictments of APT1 and APT3 in 2014 and 2017, appeared to result in those groups ceasing operations.[xxviii,xxix,xxx] In contrast, while we did not observe new APT10 activity for approximately two years after the 2018 indictment, the group has since resumed threat activity.[xxxi] Similarly, following the indictments against APT41 operators and affiliates announced in September 2020, we noted only a lull in activity with resumed operations observed by summer 2021.[xxxii]

Diplomatic Agreement to Cease Commercial-Application IP Theft

Indictments released in 2020 and 2021 further indicate that Chinese threat groups continued to steal commercial application intellectual property (IP) after the September 2015 agreement between Presidents Obama and Xi was established.[xxxiii]

Following the early 2021 ProxyLogon exploitation campaign, the U.S. Department of Justice (DOJ) unsealed an indictment against members of APT40, alleging that the indicted individuals worked for front company Hainan Xiandun established and directed by the Hainan Province MSS branch.[xxxiv] One of the most significant accusations in the indictment, Act 52, indicates that APT40 stole commercial application intellectual property (IP) in October 2015, one month after the Obama-Xi agreement was forged. In December 2018, Mandiant independently identified APT40 headquarters in Hainan via technical analysis of an operation targeting Cambodian elections.[xxxv,xxxvi]

Similarly, in July 2020, the DOJ filed an indictment against two Chinese nationals accused of conducting cyber threat activity for personal financial gain as well as "with the acquiescence" and assistance of officers assigned to the Guangdong branch of the MSS.[xxxvii] The defendants allegedly demonstrated an interest in COVID-19 vaccines as well as IP from high-tech, defense, manufacturing, pharmaceutical, healthcare research, construction and engineering, energy, and media and entertainment sectors throughout the globe. This activity may also constitute a violation of the Obama-Xi agreement, though the actors' status as freelancers could complicate that argument. Mandiant has been tracking this cluster of threat activity since 2012 as UNC302,[2] although we have evidence these actors have been active since at least 2009.

Following the Obama-Xi agreement, Mandiant continued to observe Chinese cyber espionage groups steal military and dual-use IP, for example during the Pulse Secure vulnerability exploitation campaign described above. We also see Chinese state sponsored actors regularly target organizations where commercial IP theft is a plausible objective, including intrusions at universities as well as entities in the technology, construction and engineering, transportation, and biotechnology sectors. In some cases, we discovered evidence of data staging, but often the available forensic artifacts are insufficient to confidently identify the nature of files of interest or whether data left a compromised environment. As noted above, many Chinese cyber espionage actors have demonstrated greater attention to operational security in recent years and have taken steps to cover their tracks, such as clearing logs.

Direct theft via cyber means is only one avenue for acquiring desired intellectual property, and we have also noted evidence of Chinese state initiatives supporting forced technology transfer, insider threat, talent recruitment, and acquisitions, partnerships, and joint ventures.[xxxviii] Open sources indicate Chinese interest in acquiring IP from key sectors persists, though the means used to obtain it have not always involved cyber threat activity. For example, a DOJ indictment suggests that from 2010 to 2015, APT26 conducted cyber threat activity against several companies to acquire IP related to commercial aircraft engines. A separate indictment alleges that from 2016 to 2018, an insider at a U.S. aerospace company conspired with a Chinese national to steal proprietary technology related to aviation and turbine technologies.[xxxix] The indictment further alleges that the Chinese Government provided financial support and facilitated the creation of research

[2] Mandiant creates UNC or "uncategorized" groups to track newly discovered clusters of activity and artifacts. As we collect additional related evidence over time, we expand our understanding of an UNC group.

agreements between Chinese turbine parts manufacturing companies set up by the indicted individuals and Chinese state-owned institutions working to develop turbine technologies.[xl]

Technology to Tradecraft: How Emerging Technologies Support Chinese Espionage

Mandiant Threat Intelligence assesses that innovative technologies such as 5G, quantum computing, and artificial intelligence (AI) will provide new and improved means for Chinese intelligence to capture, transfer, decrypt, and process data. With the vast amount of data already collected through Chinese cyber operations, more processing power and faster data transfer will help to turn this stolen data into actionable intelligence for future espionage activity. Significantly, the Chinese Government has also called out 5G, quantum computing, and AI as particular areas of focus for investment and development.[xli] See Figure 4.

5G

5G improves the performance, capacity, reliability, and speed of the network and decreases latency compared to 4G and other previous generations of networks, likely facilitating data collection and processing power. Vulnerabilities or backdoors can potentially be built into Chinese 5G products and allow state-sponsored espionage actors to eavesdrop, steal information, and conduct network exploitation. Malicious functionalities do not need to be included from the beginning and can feasibly be introduced by a software update.

There is some precedent for this type of activity. In November 2016, open sources, citing an internal report by the U.S. Joint Chiefs of Staff Directorate for Intelligence (J2), claimed that Boyusec, which Mandiant and the U.S. government linked to Chinese espionage actors APT3, was collaborating with Huawei to install backdoored security products onto computer and telephone equipment manufactured in China.[xlii,xliii,xliv]

Quantum Computing

Quantum computing will have significant implications for the threat landscape and cyber espionage capabilities, primarily due to quantum key distribution, its effect on cryptographic systems, and the growth in processing power. Using quantum key distribution guarantees that the data encrypted by quantum keys are transferred securely. Quantum computers can defeat many public-key cryptographic algorithms. The increased computation power of quantum computers can theoretically be used in large data analytics and optimization problems, helping China to analyze troves of data faster.

Artificial Intelligence

The Chinese State Council plans to make the nation an AI superpower by 2030 by investing in this emerging technology at home and abroad.[xlv] The country has already begun leveraging AI-based tools for surveillance and law enforcement purposes, as well as influence operations.[xlvi, ,] We assess with moderate confidence that Chinese intelligence services will use machine learning applications to help identify potential individuals for recruitment and social engineering.

Machine Learning

Machine learning is a subfield of AI that trains on data to build models to process large amounts of data in shorter periods of time. In machine learning, models learn from previous calculations and adapt to new environments to perform trend analysis, make predictions, examine behaviors, and perform other actions that illuminate relationships in the dataset. For Chinese intelligence, this technology could facilitate categorization and processing of the millions of records stolen in breaches so that it becomes actionable.

Shifting the Cost-Benefit Equation

Mandiant Threat Intelligence suggests that Chinese cyber espionage activity in 2020 and 2021 has demonstrated a higher tolerance for risk and is less constrained by norms or diplomatic pressures, mirroring bolder rhetoric and policy in other arenas.[xlix] This includes limited signs that China may be willing to engage in disruptive and destructive cyber attacks.[l,li,lii] The activity trend indicates that despite a variety of U.S. efforts to signal and enforce its perspective on Chinese cyber threat operations, Chinese policymakers view the rewards for continuing this activity as outweighing the risks of persisting in this activity.

Support Private Sector Defense and Resiliency

One significant avenue to respond to the challenge of Chinese cyber espionage against the private sector could be to explore ways to support private sector cyber defensive measures and resiliency in the event of a compromise. There are a number of forms this could take, for example:

- Incident reporting: Incentivizing private sector victims to report incidents to government authorities would help the government to collect additional evidence about Chinese cyber threat activity and better understand the scope, objectives, and techniques of these operations.
- Information Sharing: In 2021, the U.S. government noticeably increased efforts to issue public advisories about active campaigns, including details such as exploited vulnerabilities and mitigation recommendations. The government has also increased socializing best practices, for example, with public announcements about deadlines for when Federal agencies are required to patch certain exploited vulnerabilities. These announcements can inform organizations' planning around when and how they should react or take proactive steps to improve cyber security.

Other creative actions, such as using a search warrant to remove webshells that Chinese cyber espionage actors had installed on private sector servers during the ProxyLogon campaign, may also support private sector defense and resiliency.[liii,liv]

Discourage Cyber Crime, Disruptive and Destructive Attacks

If the United States and its allies seek to reduce the frequency and impact of foreign state-sponsored cyber threat activity, a beneficial foundational step would likely be to have clear definitions separating cyber espionage from cybercrime and acts of war, and to reinforce these definitions in international bodies and treaties until they become recognized and enforceable norms. Significantly, China and other nations are also actively pursuing norm-setting.[lv]

Encourage Partnership

Chinese cyber espionage activity affects not only the United States, but also many allies and partners across the globe. It is possible that coordinated announcements to condemn significant threat activity as well as encouraging other nations to release information about active campaigns could increase the cost of conducting this activity for China and reduce plausible deniability. International law enforcement cooperation may also help the U.S. and its international partners to gather data about active Chinese cyber espionage campaigns, and potentially identify ways to interrupt them.

It may also be worthwhile to explore potential avenues for the U.S. and its allies and partners to find common ground with China on cyber issues, for example on ransomware.[lvi]

Acknowledgements

Thank you to Mandiant colleagues including but not limited to: Scott Henderson, Emily Cranston, Sarah Jones, Dan Perez, Fred Plan, Nalani Fraser, Michelle Cantos, Parnian Najafi.

Appendix

Figure 1: Overview Diagram of MESSAGETAP

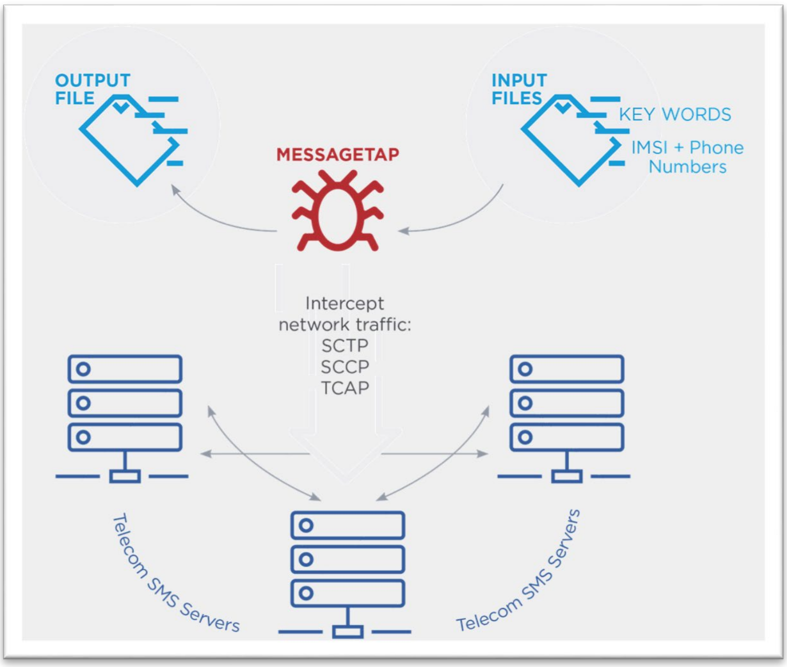


Figure 2: APT41 Supply Chain Compromises

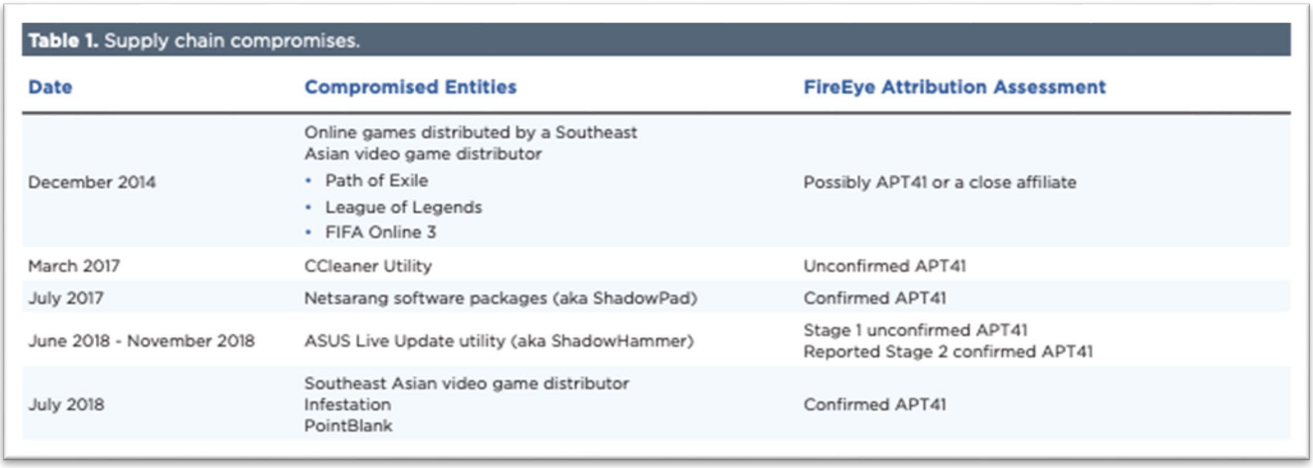


Table 1. Supply chain compromises.

Date	Compromised Entities	FireEye Attribution Assessment
December 2014	Online games distributed by a Southeast Asian video game distributor • Path of Exile • League of Legends • FIFA Online 3	Possibly APT41 or a close affiliate
March 2017	CCleaner Utility	Unconfirmed APT41
July 2017	Netsarang software packages (aka ShadowPad)	Confirmed APT41
June 2018 - November 2018	ASUS Live Update utility (aka ShadowHammer)	Stage 1 unconfirmed APT41 Reported Stage 2 confirmed APT41
July 2018	Southeast Asian video game distributor Infestation PointBlank	Confirmed APT41

Figure 3: Active Network Compromises by China Based Groups

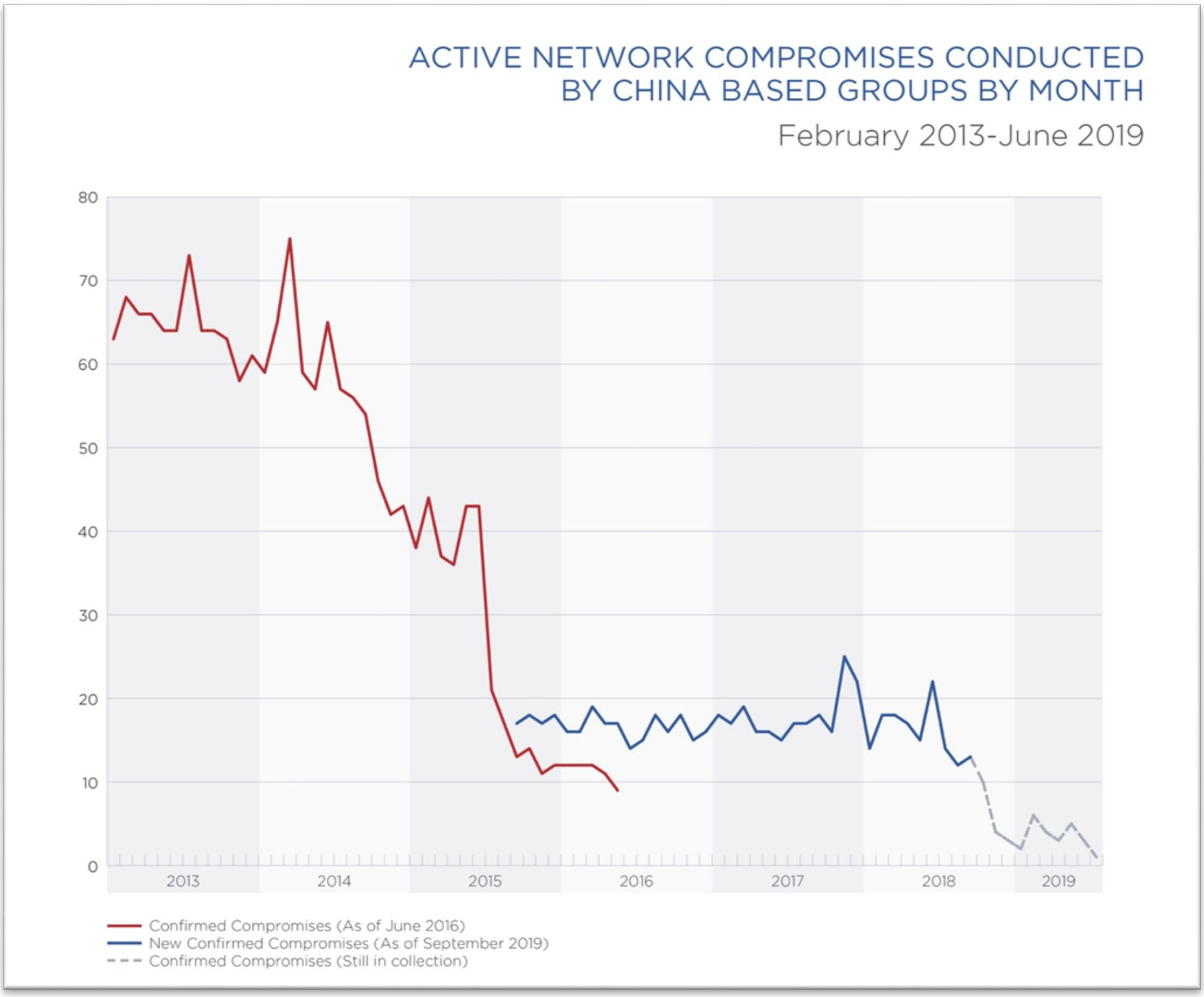
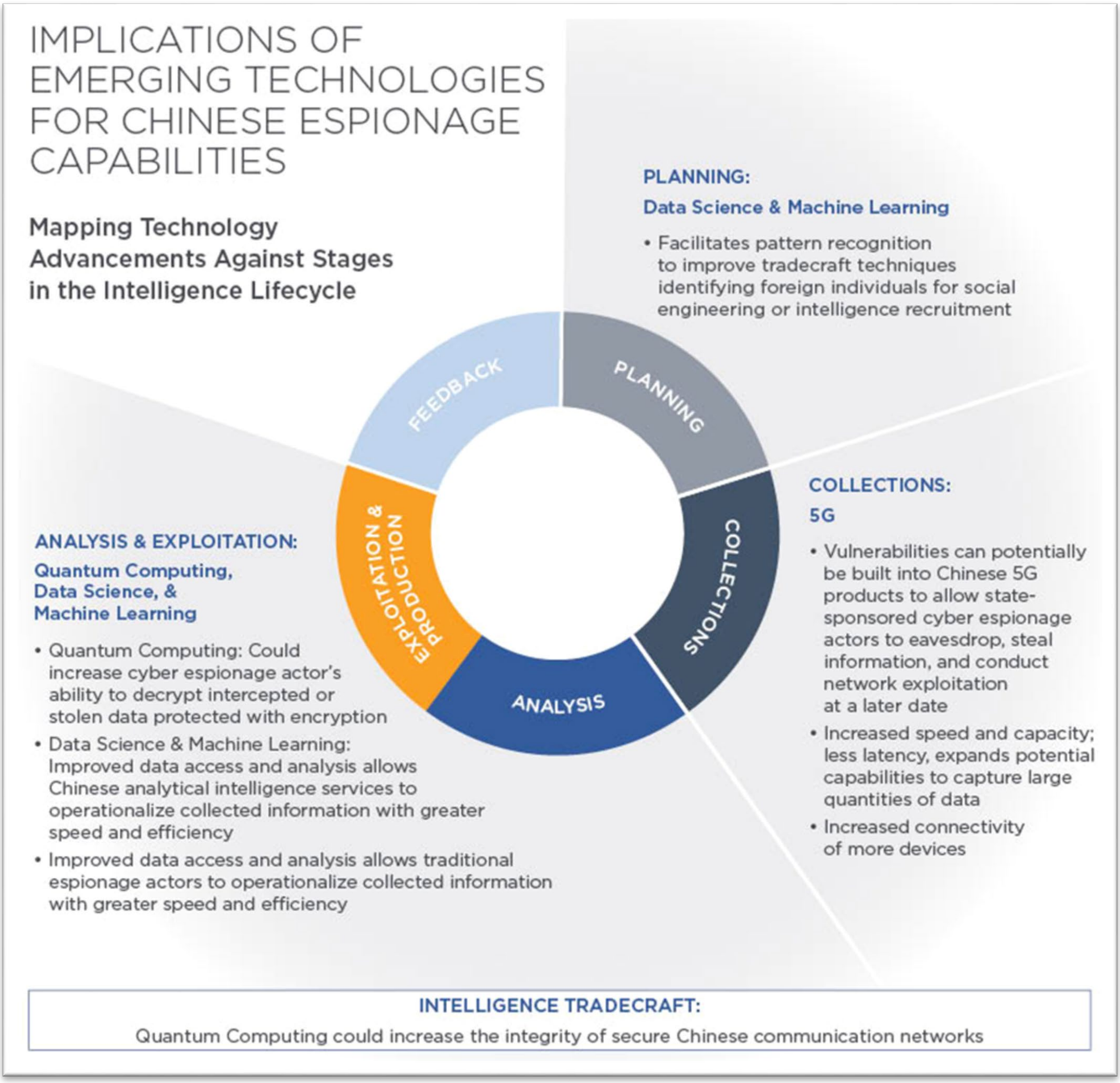


Figure 4: Use Cases for Emerging Technologies Mapped to the Intelligence Lifecycle



IMPLICATIONS OF EMERGING TECHNOLOGIES FOR CHINESE ESPIONAGE CAPABILITIES

Mapping Technology Advancements Against Stages in the Intelligence Lifecycle

PLANNING:
Data Science & Machine Learning

- Facilitates pattern recognition to improve tradecraft techniques identifying foreign individuals for social engineering or intelligence recruitment

COLLECTIONS:
5G

- Vulnerabilities can potentially be built into Chinese 5G products to allow state-sponsored cyber espionage actors to eavesdrop, steal information, and conduct network exploitation at a later date
- Increased speed and capacity; less latency, expands potential capabilities to capture large quantities of data
- Increased connectivity of more devices

ANALYSIS & EXPLOITATION:
Quantum Computing, Data Science, & Machine Learning

- Quantum Computing: Could increase cyber espionage actor's ability to decrypt intercepted or stolen data protected with encryption
- Data Science & Machine Learning: Improved data access and analysis allows Chinese analytical intelligence services to operationalize collected information with greater speed and efficiency
- Improved data access and analysis allows traditional espionage actors to operationalize collected information with greater speed and efficiency

INTELLIGENCE TRADECRAFT:
Quantum Computing could increase the integrity of secure Chinese communication networks

[i] "Chinese State-Sponsored Cyber Operations: Observed TTPs," Cybersecurity & Infrastructure Security Agency, July 19, 2021, https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/1/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF

[ii] "Redline Drawn: China Recalculates its Use of Cyber Espionage," Mandiant, June 2016, https://www.mandiant.com/resources/red-line-drawn-china-recalculates-its-use-of-cyber-espionage

[iii] Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," FireEye Cyber Defense Summit, October 10, 2019, https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

[iv] "Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities," National Security Agency, October 20, 2020, https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF

[v] Kathleen Metrick, Parnian Najafi, and Jared Semrau, "Zero-Day Exploitation Increasingly Demonstrates Access to Money, Rather than Skill – Intelligence for Vulnerability Management, Part One," Mandiant, April 6, 2020, https://www.mandiant.com/resources/zero-day-exploitation-demonstrates-access-to-money-not-skill

[vi] Christopher Glyer, Dan Perez, Sarah Jones, Steve Miller, "This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits," Mandiant, March 25, 2020, https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-exploits

[vii] Nalani Fraser, Fred Plan, Jacqueline O'Leary, Vincent Cannon, Raymond Leong, Dan Perez, and Chi-En Shen, "APT41 (Double Dragon): A Dual Espionage and Cyber Crime Operation", Mandiant, August 7. 2019, https://www.mandiant.com/resources/apt41-dual-espionage-and-cyber-crime-operation

[viii] Matt Bromiley, Chris Digiamo, Andrew Thompson, Robert Wallace, "Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities," Mandiant, March 4, 2021, https://www.mandiant.com/resources/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities

[ix] Ned Moran and James T. Bennett, "Supply Chain Analysis,: From Quartermaster to Sunshop," Mandiant, November 2013, https://www.mandiant.com/resources/supply-chain-analysis-from-quartermaster-to-sunshop

[x] "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," White House Press Statement, 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/

[xi] "UK and allies hold Chinese state responsible for a pervasive pattern of hacking," UK National Cyber Security Centre, July 19, 2021, https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking

[xii] "China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory," Council of the European Union, July 19, 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/

[xiii] Dan Perez, Sarah Jones, Greg Wood, Stephen Eckels, Emiel Haeghebaert, "Re-Checking Your Pulse: Updates on Chinese APT Actors Compromising Pulse Secure VPN Devices," Mandiant, May 27, 2021, https://www.mandiant.com/resources/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices

[xiv] "Operation Cloud Hopper," Pricewaterhouse Coopers, April 2017, https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf

[xv] "APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat," Mandiant, April 6, 2017, https://www.mandiant.com/resources/apt10-menupass-group

[xvi] "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," U.S. Department of Justice, December 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[xvii] Jack Stubbs, Joseph Menn, and Christopher Bing, "Inside the West's failed fight against China's 'Cloud Hopper' hackers," June 26, 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

[xviii] Raymond Leong, Dan Perez, and Tyler Dean, "MESSAGETAP: Who's Reading Your Text Messages?" Mandiant, October 31, 2019, https://www.mandiant.com/resources/messagetap-who-is-reading-your-text-messages

[xix] "Operation ShadowHammer: a high-profile supply chain attack," Kaspersky, April 23, 2019, https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/

[xx] "ShadowHammer: Malicious updates for ASUS laptops," Kaspersky, March 25, 2019, https://www.kaspersky.com/blog/shadow-hammer-teaser/26149/

[xxi] Catalin Cimpanu, "FBI warns US companies about backdoors in Chinese tax software," *ZDNet*, July 24, 2020, https://www.zdnet.com/article/fbi-warns-us-companies-about-backdoors-in-chinese-tax-software/

[xxii] Lily Hay Newman, "Facebook Moves Against 'Evil Eye' Hackers Targeting Uyghurs," *Wired*, March 24, 2021, https://www.wired.com/story/facebook-moves-against-evil-eye-hacking-group-targeting-uyghurs/

[xxiii] "China's Study the Great Nation app 'enables spying via back door'," *BBC News*, October 14, 2019, https://www.bbc.com/news/technology-50042379

[xxiv] Ignacio Sanmillan and Matthieu Faou, "Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia," ESET, December 17, 2020, https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/

[xxv] Timothy R. Heath, "The Consolidation of Political Power in China Under Xi Jinping: Implications for the PLA and Domestic Security Forces," Rand, April 11, 2019, https://www.rand.org/content/dam/rand/pubs/testimonies/CT500/CT503/RAND_CT503.pdf

[xxvi] Cristiana Brafman Kittner and Benjamin Read, "Red Line Redrawn: China APTs Resurface," FireEye Cyber Defense Summit, October 2018, https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-executive-s05-redline-redrawn.pdf

[xxvii] "China's Intelligence Services and Espionage Operations," Hearing Before the U.S.-China Economic And Security Review Commission, June 9, 2016, https://www.uscc.gov/sites/default/files/transcripts/June%2009%2C%202016%20Hearing%20Transcript.pdf

[xxviii] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[xxix] Dan McWhorter, "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 18, 2013, https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

[xxx] "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," U.S. Department of Justice, November 27, 2017, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

[xxxi] "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," U.S. Department

of Justice, December 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[xxxii] "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally," U.S. Department of Justice, September 16, 2020, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

[xxxiii] "FACT SHEET: President Xi Jinping's State Visit to the United States" White House Press Statement, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[xxxiv] "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," U.S. Department of Justice, July 19, 2021, https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

[xxxv] Fred Plan, Nalani Fraser, Jacqueline O'Leary, Vincent Cannon, Benjamin Read, "APT40: Examining a China-Nexus Espionage Actor," Mandiant, March 4, 2019, https://www.mandiant.com/resources/apt40-examining-a-china-nexus-espionage-actor

[xxxvi] Scott Henderson, Steve Miller, Dan Perez, Marcin Siedlarz, Ben Wilson, Ben Read, "Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally," Mandiant, July 10, 2018, https://www.mandiant.com/resources/chinese-espionage-group-targets-cambodia-ahead-of-elections

[xxxvii] "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research," U.S. Department of Justice, July 21, 2020, https://www.justice.gov/opa/press-release/file/1295981/download

[xxxviii] Sean O'Connor, "Howo Chinese Companis Facilitate Technology Transfer from the United States," May 6, 2019, U.S.-China Economic and Security Review Commission, https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf

[xxxix] "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," U.S. Department of Justice, October 30, 2018, https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

[xl] "Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets," U.S. Department of Justice, April 23, 2019, https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

[xli] Rogier Creemers, Hunter Dorwart, Kevin Neville, Kendra Schaefer, Johanna Costigan, and Graham Webster, "Translation: 14th Five-Year Plan for National Informatization – Dec. 2021" DigiChina Project, Stanford University, January 24, 2022, https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021

[xlii] Bill Gertz, "Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service" *The Washington Free Beacon*, November 29, 2016, https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/

[xliii] Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," FireEye Cyber Defense Summit, October 10, 2019, https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

[xliv] "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," U.S. Department of Justice, November 27, 2017, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

[xlv] Paul Mozur, "Beijing Wants A.I. to Be Made in China by 2030," *New York Times*, July 20, 2017, https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html

[xlvi] Lily Kuo, "Chinese surveillance company tracking 2.5m Xinjiang residents," *The Guardian*, February 18, 2019, https://www.theguardian.com/world/2019/feb/18/chinese-surveillance-company-tracking-25m-xinjiang-residents

[xlvii] Amy B. Wang, "A suspect tried to blend in with 60,000 concertgoers. China's facial-recognition cameras caught him." *The Washington Post*, April 13, 2018, https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/

[xlviii] Philip Tully and Lee Foster, "Repurposing Neural Networks to Generate Synthetic Media for Information Operations," Mandiant, August 5, 2020, https://www.mandiant.com/resources/repurposing-neural-networks-to-generate-synthetic-media-for-information-operations

[xlix] Zhiqun Zhu, "Interpreting China's 'Wolf-Warrior Diplomacy',"*The Diplomat*, May 15, 2020, https://thediplomat.com/2020/05/interpreting-chinas-wolf-warrior-diplomacy/

[l] Georgi Gotev, "Belgium suffers major cyberattack," *Euractiv*, May 5, 2021, https://www.euractiv.com/section/politics/short_news/belgium-suffers-major-cyber-attack/

[li] Charlie Osborne, "Taiwan's major oil refineries struck by malware, causing chaos at gas stations," The Daily Swig, May 6, 2020, https://portswigger.net/daily-swig/taiwans-major-oil-refineries-struck-by-malware-causing-chaos-at-gas-stations

[lii] "Description of the investigation into the ransomware attack on important domestic enterprises [國內重要企業遭勒索軟體攻擊事件調查說明]," Taiwan Ministry of Justice, May 15, 2020, https://www.mjib.gov.tw/news/Details/1/607

[liii] "Justice Department announces court-authorized effort to disrupt exploitation of Microsoft Exchange Server vulnerabilities," U.S. Department of Justice, April 13, 2021, https://www.justice.gov/usao-sdtx/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft

[liv] "Motion to Partially Unseal Search Warrant and Related Documents and [Proposed] Order," U.S. Department of Justice, April 13, 2021, https://www.justice.gov/opa/press-release/file/1386631/download

[lv] Allison Peters, "Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime," Foreign Policy, September 16, 2019, https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/

[lvi] Daniel Gordon, "With Friends Like Xi's: China's Ransomware Headache," Seriously Risky Business, January 12, 2022, https://srslyriskybiz.substack.com/p/srsly-risky-biz-thursday-january-39c