Assessment
China Cyber Espionage and Cyber Attacks in the US

Does the Chinese government fund and support cyber espionage with the intention of preparing for large-scale cyber attacks in the US?

Key Judgments

We assess that the restructuring of the collection process initiated by Xi Jinping, the increased reliance on technology, and the growing sophistication and scale of recent cyber espionage and cyber attacks conducted by government-sponsored Chinese hackers demonstrate the Chinese government's willingness to expand their cyber espionage capabilities and expose the US military and economy to cyber attacks. These efforts are and will continue to target critical economic and military information that can serve China's long-term strategic plan.

- Prior to Xi Jinping's presidency, the Chinese collection strategy focused more on private companies for businesses or the personal gain of individuals in the People's Liberation Army (PLA) units. However, with the recent crackdown on corruption, **President Xi Jinping has reorganized and strengthened the collection process to focus on China's long-term military and economic strategies.** Of the 224 reported incidents of Chinese cyber-attacks since 2000, 69% of those happened after Xi assumed office.

- **Since the early 2000s, Chinese hackers have infiltrated US agencies' networks to steal sensitive military data including data on nuclear weapons tests, design, aircraft, and the Space Shuttle Discovery program. These incidents undermine national security and provide China with information to conduct damaging future cyber attacks.** These activities have continued for over two decades and only escalated in sophistication and scale. On multiple occasions, Chinese government agencies or PLA units were the direct perpetrators. While on other occasions, there was no definitive evidence of Chinese governments directly ordering such attacks, these classified data provide little benefits for private entities given that private individuals and entities could not mobilize such information for profits other than blackmailing. At the same time, these data are of high-interest for Chinese governments given its military and political entanglements with the US on a global stage. Hence, it is more likely that the Chinese government has at least indirectly funded these cyber espionage campaigns. Additionally, given that China and the US have been on constant tense grounds with military tensions in the South China Sea, the Chinese government's possession of

American military information exposes the US military to critical threats. Some of these incidents can show the potential to escalate into cyber attacks.

- **Chinese hackers have also gained access to important political information on US officials including state officials, senators, the Secretary of Commerce, and US presidential candidates Barack Obama and John McCain.** These cyber espionage incidents pose threats to both public trust in democracy and national security. The fact that foreign powers can access future US presidents' agendas undermine the public trust in privacy and security – key elements of a functioning democracy. These results of cyber espionage are inevitable and, hence, demonstrate China's determination to weaken US image and reliability on a domestic and international level.

- **With regards to economic information, every year, private and public companies in the US have been targeted by Chinese hackers including the New York Times, Google, Coca-Cola, and small-to-medium startups.** While these incidents can be conducted by individuals or private groups, the lack of prosecution and the continuing cyber attacks on large scales targeting US corporations are indicative of the Chinese Communist Party and the Chinese government's support for these cyber attacks.

Background

With the rise of technology and President Xi's reorganization of the intelligence collection process, cyber space have emerged as China's favored area of espionage and attacks

- It is important to differentiate between cyber espionage and cyber attack. The former aims at intelligence gathering while the latter possesses malicious intent to harm.
- China has begun its academic discussion of cyberspace as an area for warfare starting in the 1990s. As early as 1993, the Chinese military revamped its strategic guidelines to include an emphasis on the importance of modern technology in the military.
- In 2013, the Chinese military publicly acknowledged cyberspace as the new war frontier.
- Since 2000, Chinese military or government employees have been charged with or alleged to be directly involved in about 50% of over 224 recorded cyber attacks.
- These espionage and attacks have resulted in what experts estimated to be as high as billions of dollars in economic damages and considerable exposure of American military and political to critical vulnerabilities.
- Private American citizens are also subjected to loss of personal information and involuntary consumption of harmful propaganda.
- These attacks have aimed at acquiring military technologies and information regarding US businesses, private individuals, and high-profile politicians – data that are of high

interest to the Chinese government and potentially impossible to use by private companies or individuals.
- However, academic and investigative reports have shown differing viewpoints on clear-cut evidence of Chinese-government-backed cyber attacks.
- Admittedly, the Chinese government has routinely denied allegations of supporting or directly involving in cyber attacks on the US.
- However, Chinese-sponsored cyber espionage to steal sensitive military and potential information has raised the alarms of the intelligence community.
- Additionally, China's technological capabilities have improved significantly in recent years with 2023 seeing one of the largest cyber espionage against the US conducted by a Chinese group in which American critical infrastructures, ranging from power and water facilities to transportation hubs, were targeted.
- The prevalence and over-reliance of the American economy and military on AI technology also provide a new frontier for exploitation by high-skilled hackers.

Substantiation

The Chinese government is currently conducting and will continue to conduct cyber espionage with the intention of preparing for cyber attacks on the US through directly and indirectly funding and ordering the People's Liberation Army, other government agencies, and private groups.

The perpetual espionage on reliable news outlets including the New York Times and the Wall Street Journal and the hacking of politicians including state officials, high-profile politicians, and presidential candidates shake the public trust and undermine democracy.

- Cyber espionage as part of the larger intelligence collection apparatus is common practice across many nations and groups. However, targeting news outlets and influencing public opinions should be categorized or at least considered to be indicative of cyber attacks.
- Such targets demonstrate the interest and the groups behind the attacks to install a sense of fear in the public and disrupt critical pillars of a society.
- Attacking the fourth branch of the government demonstrates a capability and interest in attacking democracy and potentially influencing public opinions and elections, bordering on an encroachment of American sovereignty.
- The knowledge of the public regarding their state officials and representatives being subjected to cyber espionage can severely increase distrust among voters and citizens.

Cyber espionage on critical military information ranging from attacking satellites and infiltrating nuclear facilities is indicative of the ability and the possession of information that can lead to effective attacks on the US.

- The target being military information is not new to government-sponsored espionage.
- However, with recent talks on a potential mutual agreement to ban the use of AI technology in nuclear facilities stalled, espionage on military facilities can turn disastrous as it allows the Chinese government to access key elements vulnerable to cyber attacks, opening areas for Chinese control of dangerous US military infrastructure.
- The infiltration of military facilities and stakeholders including US government defense contractors is likely to be the work of the Chinese government given that such information is more valuable to a state actor as compared to private entities.
- In 2013, the Chinese military also publicly acknowledged their view of cyberspace as a new warfare frontier.

The recent attack on a critical facility exposes the US public and government to not just cyber espionage but cyber attacks that can be destructive to national security.

- Microsoft and Western intelligence agencies alleged that Volt Typhoon, a state-sponsored group, has been spying on a variety of US critical infrastructure from telecommunications to transportation hubs.
- Espionage on this scale requires substantial resources that are likely provided or at least sponsored by the Chinese government.
- While hacking emails and phone calls are not new, a large-scale infiltration of transportation hubs shows the vulnerabilities of US transit security that can allow hackers to gain access to infrastructure and launch attacks.

While espionage to steal trade secrets from small-to-medium US companies and occasionally larger companies can be solely attributed to private Chinese entities, the scale of these attacks and the inaction of the Chinese government as well as their view on cyberspace demonstrate their support for these cyber activities.

- Cyber espionage targeting private businesses to gather trade secrets and invade personal information of individuals using services provided by these businesses, including hotel chains and commercial banks, can constitute cyber attacks given that it undermines the operations and customer trust in these companies.
- The sheer frequency of these attacks to steal competitive trade information and the continual denial of accusations by the Chinese government show the government's support for cyber espionage and cyber attack missions.
- These activities also constitute cyber attacks since these incidents have cost US businesses billions in dollars and further disrupt companies' business operations.
- As Xi Jinping assumed office and reconstructed the intelligence collection process to prevent intelligence officers from conducting cyber espionage for personal gains, the Chinese government's strategy showed a commitment to carrying out cyber espionage for long-term gain, namely to gain military and market supremacy on a global stage.

Outlook

The Chinese government, through sponsoring private groups, will continue to conduct large-scale cyber espionage and escalate these efforts to launch cyber attacks on the US.

- These attacks will focus on military facilities and trade secrets with the capacity to enhance market advantages for China.
- Attacks on critical American industries, especially transportation will allow China to add to its arsenal another area of potential large-scale attacks.

American platforms and outlets for public information and public discords including large tech companies such as Google and Meta and news outlets such as the New York Times and the Washington Post will continue to be important targets as the Chinese government aims to undermine democracy in the United States. Moreover, these espionage will further allow China to influence the opinions of the US public.

- Large public companies will continue to see hacking attempts on their employees' personal emails and the organization's central networks but will do so on a larger scale.
- US state officials and political candidates will continue to see their agenda and personal information as targets of espionage and attacks. This is extremely worrisome as the US are expecting highly contested election cycles. These politically charged times will enable China to conduct large-scale espionage as a larger plan to influence US election.
- The public's trust in the democratic process will decrease as evidence of cyber espionage and attacks by a rival foreign government come into light.

As the tension between the US and China escalates alongside the increased fragmentation of the relationship between NATO and the China-Russia alliance, the current global conflict climate that surrounds proxy war might cede to give way to cyberwars in which cyber attacks ordered by the two countries can intensify to inflict physical damage.

- In 2023, a state-sponsored Chinese hacking group carried out one of the largest cyber attacks against American critical infrastructure ranging from telecommunications to transportation hubs. While the capabilities of groups responsible for this attack are unknown, their target being transportation raises alarm on potential physical damage.
- Additionally, cyberspace is proven to be able to escalate into cyber attacks and cyber warfare. The Stuxnet virus case wherein the US and Israel allegedly used a cyber virus named Stuxnet to attack Iran's nuclear facilities demonstrates the current technological capabilities of cyberwar as well as the willingness of nations to resort to cyberattacks as a form of war.

The significant improvement in sophistication and efficiency of AI poses technological vulnerabilities of the US military and economy to espionage and attacks.

- With no solid pledge to ban the use of AI in nuclear weapons command and control as well as autonomous weapons, there is a high possibility that future espionage can exploit AI technology in the military.
- Additionally, with AI becoming increasingly central to the future of businesses in America, the technology can be exploited through multiple fronts.
- Firstly, China-backed hackers can use AI to tailor phishing malware to infiltrate small start-ups which are using AI at a much higher rate to minimize costs in their businesses. These small companies, however, do not possess a high cyber security system.
- Secondly, hackers supported or enabled by the Chinese Communist party can target the cloud computing and chip infrastructure that are critical to the AI industry through corrupting datasets and data centers that feed AI technology.

Citation

"China's Cyberattack Strategy Explained." *Booz Allen*, Booz Allen Hamilton, 16 Nov. 2022, www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html. Accessed 15 Dec. 2023.

"The Chinese Groups Accused of Hacking the US and Others | Reuters." *Reuters*, 21 July 2023, www.reuters.com/world/china/chinese-groups-accused-hacking-us-others-2023-07-21/. Accessed 16 Dec. 2023.

Furchtgott-Roth, Diana. "China Abandons Paris Agreement, Making U.S. Efforts Painful and Pointless." *The Heritage Foundation*, 26 July 2023, www.heritage.org/global-politics/commentary/china-abandons-paris-agreement-making-us-efforts-painful-and-pointless. Accessed 15 Dec. 2023.

Goodman, Peter S. "The Rise and Fall of the World's Most Successful Joint Venture." *The New York Times*, 14 Nov. 2023, www.nytimes.com/2023/11/14/business/us-china-economy-trade.html. Accessed 15 Dec. 2023.

Goswami, Rohan. "Microsoft Warns That China Hackers Attacked U.S. Infrastructure." *CNBC*, 24 May 2023, www.cnbc.com/2023/05/24/microsoft-warns-that-china-hackers-attacked-us-infrastructure.html. Accessed 15 Dec. 2023.

Gramer, Robbie, et al. "China's Building Projects in Africa Are a Spymaster's Dream." *Foreign Policy*, 21 May 2020, foreignpolicy.com/2020/05/21/china-infrastructure-projects-africa-surveillance-spymaster-dream/. Accessed 15 Dec. 2023.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security*, vol. 4, no. 2, Summer 2011, pp. 1–24, doi:10.5038/1944-0472.4.2.1.

Holt, Alexander. "A Brief History of US-China Espionage Entanglements." *MIT Technology Review*, 3 Sept. 2020, www.technologyreview.com/2020/09/03/1007609/trade-secrets-china-us-espionage-timeline/. Accessed 15 Dec. 2023.

Honrada, Gabriel. "US, China at Critical Odds on Future of Military AI - Asia Times." *Asia Times*, 17 Nov. 2023,

asiatimes.com/2023/11/us-china-at-critical-odds-on-future-of-military-ai/. Accessed 16 Dec. 2023.

Jensen, Benjamin. “How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy.” *CSIS*, 19 Oct. 2023, www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy. Accessed 15 Dec. 2023.

Krekel, Bryan. Northrop Grumman Corporation, McLean, Virginia, 2009, *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation Prepared for the US-China Economic and Security Review Commission* .

Lindsay, Jon R., et al. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press, 2015.

Maizland, Lindsay. “China’s Fight against Climate Change and Environmental Degradation.” *Council on Foreign Relations*, 19 May 2021, www.cfr.org/backgrounder/china-climate-change-policies-environmental-degradation. Accessed 15 Dec. 2023.

Nakashima, Ellen, and Joseph Menn. “China’s Cyber Army Is Invading Critical U.S. Services.” *The Washington Post*, 11 Dec. 2023, www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/. Accessed 16 Dec. 2023.

Pettis, Michael. “What Will It Take for China’s GDP to Grow at 4–5 Percent over the Next ...” *Carnegie Endowment for International Peace* , 4 Dec. 2023, carnegieendowment.org/chinafinancialmarkets/91161. Accessed 16 Dec. 2023.

Schmid, Jon. “Rethinking Who’s Winning the U.S.-China Tech Competition | Rand.” *RAND Corporation*, 16 Aug. 2023, www.rand.org/pubs/commentary/2023/08/rethinking-whos-winning-the-us-china-tech-competition.html. Accessed 16 Dec. 2023.

Segal, Adam. “The Code Not Taken: China, the United States, and the Future of Cyber Espionage.” *Bulletin of the Atomic Scientists*, vol. 69, no. 5, 1 Sept. 2013, pp. 38–45, doi:10.1177/0096340213501344.

Siddiqui, Zaba, and Christopher Bing. “Microsoft Says New Breach Discovered in Probe of Suspected ... - Reuters.” *Reuters*, 25 May 2023, www.reuters.com/technology/microsoft-says-new-breach-discovered-probe-suspected-solarwinds-hackers-2021-06-25/. Accessed 16 Dec. 2023.

"Significant Cyber Incidents: Strategic Technologies Program." *CSIS*, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 15 Dec. 2023.

Tian, Yew Lun. "China Draws up List of 100 Instances of U.S. 'Interference' in Hong Kong." *Reuters*, 25 Sept. 2021, www.reuters.com/world/china/china-draws-up-list-100-instances-us-interference-hong-kong-2021-09-24/. Accessed 16 Dec. 2023.

Walton, Calder. "China Has Been Waging a Decades-Long, All-out Spy War." *Foreign Policy*, 28 Mar. 2023, foreignpolicy.com/2023/03/28/china-has-been-waging-a-decades-long-all-out-spy-war/#:~:text=China%20was—and%20remains—the,information%20obtained%20during%20security%20clearances. Accessed 15 Dec. 2023.

Yoachimik, Omer, and Jorge Pacheco. "DDoS Threat Report for 2023 Q3." *The Cloudflare Blog*, 26 Oct. 2023, blog.cloudflare.com/ddos-threat-report-2023-q3/. Accessed 15 Dec. 2023.

Appendix

A. Redefining KIQ

Prior KIQ: How does the intelligence community combat the exploitation of commercial spyware and surveillance by authoritarian and democratic regimes to influence public discord, suppress freedom of information, and undermine democracy? In addition, how are these efforts played out in the United States?

Current KIQ: Does the Chinese government directly and/or indirectly conduct cyber espionage with the intention of preparing for large-scale cyber attacks in the US?

The prior KIQ is too broad of a question to be efficiently answered. Firstly, the question separates two main groups of players: authoritarian and democratic regimes. However, since these are umbrella terms and countries can fall into different areas on the spectrum of political ideologies, the sheer number of countries that should be investigated is quite overwhelming. Additionally, since there are a vast variety of political regimes, their approach to the use of commercial spyware and surveillance would significantly differ. Hence, attempting to research the community's efforts to combat these regimes's exploitation of commercial spyware is unattainable for a short-term project.
The updated KIQ focuses exclusively on China's cyber attack efforts and campaigns. More specifically, the question looks into how China's efforts impact the United States. However, the question still retains an in-depth scope given that it investigates the nature of the Chinese government's cyber activities in the US, not just limited to intelligence collection and surveillance . The Chinese government and Chinese government-backed hackers also target different industries and operate with a variety of goals in their attacks against the US.

B. Key Assumption Check

Key Assumption	Assessment
Chinese hackers, backed by US governments, are stealing trade secret to benefit Chinese industries	Highly likely given that there are incidents wherein Chinese individuals were accused and indicted on charge of intellectual property theft. This information also went from a US firm to a Chinese firm. However, the Chinese government might not be directly ordering or backing these efforts rather they might just be turning a blind eye against these offenses. **(SUPPORTED)**
Chinese hacking group such as Volt Typhoon, APT 41, APT 27, and many others are backed by Beijing	Highly likely, given their resources and levels of attacks. However, there is still a chance that these groups are private since some attacks are directly towards businesses and not just government organizations. **(CAVEATED)**
Chinese hackers, under direct command of the PLA and the Chinese government, are hacking critical military infrastructure to obtain information	Highly likely since in the past 23 years, there are multiple incidents per year wherein the networks of US government agencies and leading companies have been infiltrated by hackers. **(SUPPORTED)**
Technological infrastructure built by China in African countries allow China to perform surveillance	More information needs to be published to demonstrate how these stolen data and surveillance efforts can be played out in real life. **(CAVEATED)**
China's cyber espionage efforts in foreign nations expose US officials to vulnerabilities	US embassies, agencies, and companies abroad still use their own secure networks that are monitored more by the US. Hence, computers and infrastructure built in nations where US officials work may not be what US officials or personnels use for their daily operations. **(CAVEATED)**
One of the goal of China's cyberattack is to target freedom of press in the United States	The US is built on the values of freedom of speech and the press is the public's champion of the First Amendment Right. Hence, cyber espionage efforts targeting the press undermine the public trust and sense of security. However, their attempts to hack newspapers can also be the result of China's concern over US coverage of Chinese policies and how such coverage can find its way to Chinese citizens. **(CAVEATED)**

China is interfering in US democratic processes	There are reports that Chinese hackers accessed information on future agendas of 2008 presidential candidates alongside many government officials. There are also reports on propaganda efforts orchestrated by the Chinese government to influence US elections. However, the Chinese government's priority might concern more with gaining information on future political moves rather than substantially influencing US election results. **(CAVEATED)**
Chinese hackers possess the capabilities and potential capabilities to hack AI technology in the US	There are recorded incident of Chinese hackers corrupting data sets and data centers critical to AI technology as well as infiltrating US start-ups that use AI technology **(SUPPORTED)**
Chinese hackers possess the ability to conducted cyber attacks in the US that can inflict real physical harm	Recent large-scale hacking efforts by Chinese hackers to gain access to water and power facilities as well as telecommunications and transportation hubs raise warnings about their ability to control these systems. However, there are no reports of real physical harm being inflicted due to cyber attacks. **(CAVEATED)**

C. Outside-In Thinking

Societal

- Unfavorable portrayal of the US and its political and economic machines as posing a threat to Chinese society on Chinese media leads to an unfavorable view of the Chinese public on America.
- The public has admirable feelings towards individuals who pursue a career in tech.
- Popular culture places a strong emphasis on the incredibility and prestige of those possessing the ability to infiltrate cyber security as seen through movies and TV shows
- Mainland Chinese's hostile view towards the US's diplomatic relationships with Taiwan and Hong Kong, viewing this as a potential area for escalation in conflict. These reports also anger the Chinese public who have a strong sense of patriotism.

Technological

- In recent decade, China has emerged as a global tech leader with mogul companies such as Tencent and advanced technology possessing immense power to infiltrate sophisticated cyber security system
- China, like many other nations, view tech as the new frontier that determines the power of a nation on the global stage
- Technology reaches into all parts of China with applications such as WeChat that acts as social media, banking, transportation, and news outlet platforms. Hence, the public sees tech as one of the most important infrastructure.
- The increased use of AI in businesses and, subsequently, the rise in training for AI for students and individuals.

Economic

- China has seen continued and sustained GDP growth. However, in recent years, China has slowed down its GDP growth.
- China and the US have a tense and dependent economic relationship.
- The recent trade war between the US and China has resulted in job loss in China as American manufacturers moved their factories to other countries.

Environmental

- China sees Western countries, especially the US, as contributors in its worsening environmental problems.
- China is the world leading emitter of greenhouse gas. Its climate policies have affected the lives of its citizens.
- China has announced a halt in its adherence to the Paris Climate Agreement citing unfair treatment given that developed nations such as the US has had its fair share of polluting the environment for economic development.

Political

- The Chinese Communist Party (CCP) enforces a high level of government censorship on news coverage as well as social media activities, especially those with opinions or reports on Chinese government conduct.
- Xi JingPing and the CCP wield immense power in monitoring public discord.
- China's persistent view of the US as its top enemy when it comes to the US's assistance and diplomatic relationships with Taiwan and Hong Kong.
- China views America as a geopolitical rival undermining its power abroad and its sovereignty given the US's interference in the South China Sea, Taiwan, and Hong Kong

Military

- Immense technological advancement in its military operations.
- China has always demonstrated its military poweress on a global stage.
- China persistently shows military intention towards countries such as Taiwan who are allies with America
- China sustains continual hostility towards the South China Sea is an area of contention between the US and China's diplomatic relationship.

Psychological

- China has a strong determination to rise as global leader in technology and economy
- Chinese citizens have concerns over American manufacturers moving to other countries in the region.

D. What if

What if China is only conducting cyber espionage and view gaining access to US military and business networks as a defense for future offense

- China will continue to conduct large scale cyber espionage
- The public trust in private and public infrastructure will still decrease
- The American economy will still see losses in earning
- Private Chinese hackers will continue to steal American trade secrets
- Other countries might use China's information on American facilities to conduct malicious attacks of their own.

E. Analysis of Competing Hypotheses

Analysis of Competing Hypotheses			
Evidence	**Chinese government are sponsoring cyber espionage against the US with the intention to steal intellectual property and prepare for cyber attacks**	**The Chinese government is not responsible for cyber espionage against the US. Private Chinese companies and individuals are conducting these attacks for personal gains and business-only purposes**	**Chinese government are sponsoring cyber espionage against the US with no intention to conduct offensive cyber attacks, only for defense purposes**
Chinese military acknowledged cyberspace as the new frontier for cyber warfare	C	?	I
Chinese hackers have routinely targeted sensitive US military data including espionage against the Department of Defense, the US Naval War College, Pentagon computer servicing the Secretary of Defense, National Nuclear Security Administration, US defense contractors, and others.	C	I	?
Chinese hackers have disrupted US infrastructure including satellites owned by NASA and USGS and military and civilian operations the South China Sea wherein US companies were involved in maritime satellite systems, aerospace, and defense contracting	C	I	?
Chinese hackers routinely stole personal information of US nations, ranging from their locations to banking information	C	?	I
Chinese government-linked hackers targeted US coronavirus research efforts and 2020 saw	C	I	I

a surge in healthcare related attacks			
Chinese hackers persistently conduct cyber attacks against news outlets and compromise the privacy of journalists' email accounts	C	I	I
Multiple incidents in which hackers, allegedly linked to Chinese government stole significant amount of money from US government agencies and business	C	I	?
Tech companies and intelligence agencies alleged state-sponsored hacking group Volt Typhoon of infiltrating US critical infrastructure organizations ranging from telecommunications to transportation hubs	C	I	I
Chinese hackers stole trade secrets from the US Chamber of Commerce, government agencies, and other private businesses.	C	?	?
Networks of companies in chemical, defense and other industry faced intrusions lasting for six months originated from China-based computers.	?	?	C
Chinese hackers targeted US-based activists.	C	?	I
Chinese government denied allegations of cyber attacks in the US	I	C	I
China's Military Strategy defined primary objectives of cyber capabilities as to only strengthen cyber defense and participate in	I	C	I

international cyber cooperation alongside increase cyberspace situation awareness and support China's endeavors in cyberspace			

C=Consistent, I=Inconsistent, ?=Ambiguous

F. Indicators and Signposts for Change

Tracking the types and scale of cyber espionage and cyber attacks done by Chinese hackers in the US															
Topics	**Indicators**	**2024**	**2025**				**2028**				**2030**				
			I	II	III	IV	I	II	III	IV	I	II	III	IV	
The scale of cyber espionage on US businesses	Increase in the scale of cyber espionage on small-to-medium businesses														
	Increase in the duration the espionage														
	Increase in the extensiveness of attacks on large organization														
The scale of cyber attacks against US businesses	Increase in cyber attacks to steal trade secrets that can result in significant financial loss for US businesses														
	Increase in malicious intention behind cyber espionage against businesses														
The scale of cyber espionage on US critical infrastructure	Increase in cyber espionage against commercial banks														
	Increase in cyber espionage against telecommunications facility														
	Increase in cyber espionage against transportation facilities														
	Increase in cyber espionage against power facilities														
	Increase in cyber espionage against water facilities														
The scale of cyber attacks on US critical infrastructure	Increase in sophistication in cyber attacks against American critical infrastructure														
	Increase in attacks aim to take control or allow for future control of American critical facilities, especially transportation hubs.														

The scale of cyber espionage on US military facilities	Increase in the number of attacks against US Department of Defense													
	Increase in the number of attacks against US defense contractors													
	Increase in the number of attacks against NASA													
	Increase in the number of attacks against military complexes													
	Increase in the number of attacks against military colleges													
	Increase in the number of attacks against US military facilities overseas													
	Increase in the number of attacks against the US power and water facilities													
The scale of cyber attacks on US military facilities	Increase in the level of sophistication of attacks against nuclear facilities													
	Employing more AI technology in attacks													
	Increase in the number of attacks against military infrastructure, especially nuclear facilities, that use AI technology.													
	Increase in the number of attacks that allows for control of military facilities rather than just intelligence collection													
The nature of cyber attacks	Increase in financial loss due to cyber attacks													
	Decrease in the public trust for government and organizations													
	Increase in the number of attacks using AI technology or targeting companies who use AI technology													
The long-term strategy of the	Increase in investment towards technological capacity													
	Increase in emphasis on the cyberspace as the next frontier for war													

Chinese government	Increase in military funding towards strengthening facilities used towards cyber attacks													
	Increase funding for private hacker groups													
Political climate	Increase tension in the South China Sea													
	Increase influence or perceived influence of the US in the South China Sea													
	Increase influence or perceived influence of the US in Taiwan													
	Increase overall political tension between the US and China													
Economic Competition between the two countries	The US impose tax on Chinese imports													
	The renewal of the US-China trade war													
	US new financially lucrative technological innovation													
Exhibition of Military power in proxy war	US new innovation in military infrastructure													
	China’s perception of growing US military power													