Name of Publisher: EVERMIND EDUCATION & RESEARCH
Review Type: Double Blind Peer Review
Area of Publication: Social Sciences (miscellaneous)

Vol. 2 No. 4 (2024)

Journal of Political Stability Archive

Online ISSN 3006-5879
Print ISSN 3006-5860

https://journalpsa.com/index.php/JPSA/about

Cyber Warfare and National Security: Analyzing the Evolving US-China Cyber Rivalry through the Lens of Realism and Its Implications for Global Cyber security Governance

Muneeb Aurangzeb
M.Phil. Scholar Department of International Relations,
Federal Urdu University of Arts, Sciences & Technology, Karachi.
muneeb.ir@fuuast.edu.pk
https://orcid.org/0009-0003-0580-3574

Dr. Syed Shuja Uddin
Assistant Professor Department of International Relations,
Federal Urdu University of Arts, Sciences & Technology, Karachi.
dr.shuja.ir@fuuast.edu.pk
https://orcid.org/0009-0008-8359-9915

Dr. Muhammad Irfan
Assist Professor, Department of Mass Communication,
The Federal Urdu University of Arts, Science & Technology, Karachi
erfanaziz@fuuast.edu.pk
https://orcid.org/0009-0007-9380-6861

Dr. Zubaida Aziz
Assistant Professor, Department of Political Science,
Federal Urdu University of Arts, Sciences & Technology, Karachi.
zubaida.gondal@yahoo.com
https://orcid.org/0009-0007-0971-8659

Abuzar Iqitdar
Lecturer, Department of Political Science,
Federal Urdu University of Arts, Science and Technology, Karachi.
abuzar.iqitdar@fuuast.edu.pk
https://orcid.org/0009-0008-3838-822X

DOI: https://doi.org/10.63468/jpsa.2.4.13

Abstract

The growing use and innovation in information technology and communication in all domains of life has made the world richer but also fragile and it has led to breach of privacy and increased dependence on the internet. Thus cyber security has become one of the major global concerns a growing nontraditional security issue. We can observe that the cyber security discourse of today emphasizes the increasing set of threats ranging from cybercrime, computer viruses, and cyber espionage. Globally cyber terrorism and cyber war are also becoming major issues that are discussed on global platforms. The complexity of the digital world and increased security risk have led to overemphasis that may violate equality, freedom of speech, and fairness. The study aims to highlight the growing paranoia that comes with the growth of cyberspace through the lens of the theory of realism, understanding that the concept of security dilemma also exists in the cyber domain. Just like traditional conflicts, states are engaged in constant power struggles in cyberspace. The study highlights the major concerns related to cyber security and cyber-warfare with its relationship to foreign policy implications for China and the U.S. The methodology applied in this study includes a comprehensive exploration of the landscape of cyber-security and cyber-warfare in China and the U.S. The chapter seeks to analyze the growing landscape of cyber security and cyber warfare and the changing nature of threats with a focus on the foreign policy implications of China and the U.S. about cyber security and warfare. A detailed comparative analysis of China and the U.S. with an understanding of differences and potentials of collaboration and conflict concerning cyber policies. The chapter will contribute to the promotion of international cooperation in addressing this new emerging global challenge of cyber security and warfare. With deep insights to understand this global threat, this research aspires to have a lasting influence on national security considerations with evidence-based suggestions and recommendations. By identifying potential areas for collaboration and examining diplomatic responses to cyber incidents. This chapter seeks to foster a more collaborative approach to secure cyber security and the implication of the phenomenon on the Foreign Policies of China and the U.S. Recognizing that Cybersecurity is entwined with international relations, the research argues that findings extend beyond the specific context of China and the U.S. The chapter aims to contribute to the vast field of international relations by shedding light on the complex between national interest, diplomatic relations, and Cybersecurity. The key argument in this study is to underscore the rapidly evolving nature of cyber warfare tactics and Cybersecurity threats and emphasize the need for an adaptive policy response to effectively counter emerging challenges in both China and the U.S.

Keywords: Cybersecurity, cyber warfare, cyber-attacks, Foreign policy, and international cooperation.

INTRODUCTION

Cyberspace is an expanding aspect of the digital world that includes social, military, and business communications. The emergence of the internet and digital life has shrunk boundaries and made communications easier in unimaginable ways. Although technological innovation has made life and communications easier, it also raised vulnerabilities and threats

that most were not ready for. Thus, technological tools used by individuals and companies or states are threatened to be invaded by groups seeking to disturb the security of the system. To relate the concept to a theory realists view cybersecurity as the new battlefield and a new domain for warfare, similar to air, sea, land, and space. States may launch cyber-attacks that will disrupt the social stability and critical infrastructure thus securing the cyberspace of their states has become a major priority. The core concept of realism; a security dilemma can be applied to cyber security as well as one state increases its cyber capabilities, other states may feel threatened and are seen to be doing the same.

DEFINING CYBER SECURITY AND CYBER WARFARE

Cybersecurity practice of protecting computer systems, networks, and data from theft, damage, unauthorized access, or any form of cyber-attack. It involves implementing a range of measures, technologies, processes, and best practices to safeguard digital information and ensure the confidentiality, integrity, and availability of computer systems and data.

Cyberwarfare use of digital techniques, tools, and tactics in warfare or conflict. It involves both offensive and defensive operations in the digital realm, where nations or state-sponsored entities employ cyber capabilities to achieve strategic, political, or military objectives. Unlike traditional warfare, cyber warfare domain of cyberspace, which includes computer networks, systems, and the internet.

Historical Development of Cyber Capabilities of China and the U.S

The cyber capabilities of the U.S. and China have been through a complex process of technological developments, strategic policies, and political agendas.

THE 1970S-1990S

In the 1970s, the U.S. and China started to explore their digital potential and its application in military and intelligence. The 1980s marked the establishment of the National Computer Security Center U.S. with heavy investments for research in the field while China focused on defensive capabilities and warfare strategies. The 1990s was a time for revolutionary global connectivity for both the U.S. and China for which they recognized the potential of cyber espionage and cyber-attacks. China established the National Computer Network Emergency Response Team (CONCERT) and began the development of offensive cyber tools.

2000s-2010S THE RISE OF CYBER THREATS AND WARFARE

In the 2000s, the U.S. established the Department of Homeland Security and Cyber Command which focused on defending critical infrastructure and conducting offensive operations while China continued to develop offensive capabilities to cope with major U.S. companies such as Google. In 2010, the Stunt attack on Iran's nuclear facility highlighted the potential of cyberwarfare to disrupt critical infrastructure. At the same time, both states were engaged in a series of cyber-attacks and espionage campaigns against one another.

2020s-2021s

Since 2020 cyberwarfare has become the most recognized domain of warfare, U.S and China continue to invest heavily in cyber capabilities.

CYBER SECURITY IN THE 21ST CENTURY

The 21st century has witnessed an unprecedented explosion in technology and communications. Internet and digital devices have become a crucial part of our lives, at times making survival uneasy. Our dependence on technology in most areas such as communication, business, and entertainment has created a vulnerable platform for cyber-attacks, making cybersecurity an important global issue.

We have become highly dependent on technology; our data from pictures to educational info to contact info is stored online. This dependence makes us more vulnerable to cyber-attacks. With time, cyber-attacks have evolved and become more sophisticated. Cybercriminals are constantly developing new tools and techniques to exploit digital systems, malware attacks, phishing, ransomware, and data breaches are some examples. Such developments have led to the rise of nation-state cyber-crimes as well. Nation-states are increasingly using cyber-attacks as a tool for espionage, sabotage, and warfare. These attacks can target critical infrastructure, military systems, and even civilian populations making it a national security threat.

THE EVOLVING LANDSCAPE OF CYBER SECURITY

The cyber-world is ever-expanding, with innovations and developments the cyber threat has become much more dangerous and frequent. The birth of new technologies such as AI (artificial intelligence), the Internet of Things (IoT), and cloud computing have given rise to vulnerabilities. Cybercriminals and attackers are increasingly using AI-powered tools, social engineering, and detection. Our heavy dependence on devices has fastened the attack surface and made it easy for these criminals to find a way to enter.

As more and more data is being produced and stored in large volumes with increased connectivity on the internet the attack surface has become exploitable with criminals and nation-state hackers taking advantage.

According to Check Point's recent report, cyber-attacks increased by 7% during in first half of 2023. The Check Point also showed that 1 in 31 organizations internationally experienced a weekly ransomware attack in the first quarter of 2023. Recent examples have shown the use of AI Software Chat GPT code generation that may help new threat actors in cyber-attacks. Adding to this malware statistics for 2023 are adding difficulties to cybersecurity. The estimate shows that 560,000 new malware are detected every day. Hacking has become easier which is a big concern. Day to day they are finding ways to cover their malevolent plots as legal websites. According to the Independent public breach tracker, almost 340 million people were affected by data breaches in the first 3 months of 2023.

LISTED BELOW ARE SOME OF THE MAJOR TRENDS OF 2023 THAT DEPICT THE CYBER THREAT

Ransomware: This type of cyber-attack has become dominant, with attackers targeting critical **infrastructure**, healthcare, and other high-value organizations.

Phishing: A common and effective attack vector. Attackers are becoming more adept at designing believable emails and tricky websites to reveal sensitive software.

Supply Chain Attacks: These attacks target vulnerabilities in software or hardware supply chains to compromise a large number of organizations at once.

Zero-day Attacks: These attacks exploit vulnerabilities that are unknown to software vendors, making them difficult to defend.

Deep Fakes: The most dangerous forms of A. Fake videos and audio recordings that can be used for blackmailing and disinformation campaigns.

The constantly developing landscape of digital innovation and emerging technologies gives rise to both opportunities and challenges. The swift growth of emerging technologies such as 5G and generative A. I am creating more opportunities for cyber-attacks and data breaches to happen. Such emerging technologies include Quantum Computing, 5G networks, and Cloud Computing. Quantum Computing is a threat to frequently used encryption algorithms that harm the privacy of sensitive data including personal information and financial transactions. The feature of 5G birthed vulnerabilities that affect illegal access and data breaches.

AI has given many opportunities and made things easier for example, such technologies automate threat detection and response. AI-powered tools can analyze large amounts of data to identify patterns and predict future attacks; however, they also pose challenges. The ability of A. I generate man-like responses to spread misinformation; AI algorithms may collect biased data that might result in discriminatory outcomes.

RECENT CYBER ATTACK CASES

In October 2023, Vietnamese hackers attempted to install spyware on the communication devices of U.N Officials, journalists, the chairs of the House Foreign Affairs Committee, and Homeland Security. This attempt extracts calls and texts from infected devices. The attempt was a negotiation between American diplomats and Vietnamese regarding the growing influence of China over the region, however, the attempt remained unsuccessful.

In September 2023, Indian hacktivists attacked Canada's military and Parliament webs with DDoS (distributed denial of service), i.e. when bots swarm the website-slowed system for hours. This attempt Justin Trudeau's open accusation against India for assassinating Sikh Activist Hardeep Singh Nijjar. In the same month, Iranian hackers attempted a cyber-attack against Israel's railroad network. Russian cyberattackers breached the International Criminal Court's IT System during the Russian war crimes in Ukraine.

In November 2023, Toyota Financial Services warned their customers of a data breach revealing that sensitive data leaked. The company confirmed that unauthorized access systems in Africa and Europe. A ransomware attempt in which the company demanded 8,000,000$, failure of payment will result in data being uploaded on the dark web. Customer data including name, residential address, contact information, and IBAN revealed compromised. Another company faced a similar situation, 23andMe; a genetic testing powder faced multiple lawsuits in October due to an attack that led to the theft of customer data.

In August 2023, hackers made X, previously known as Twitter, offline in several states to pressurize owner Elon Musk to bring Star Link to Sudan. This led to the disability of over 20,000 accounts in the U.K., U.S., and other states.

Such attempts reveal that cyber threats are stronger than ever, and attackers are not far away from political secrets and information. It also depicts that once our data is online it's never safe, no matter how strong the password is or how secure the website is, our data is on the verge of theft at any given moment.

China's Cyber Security Strategies

In terms of technology and cyberspace, China has always stood out with its approach to espionage, governance, and increased military focus. China firmly believes that the West poses too much influence in shaping the internet's future, due to which China supports internet governance based on sovereignty which means allowing states to regulate cyberspace according to their preferences. China's view of information is based on using it as a strategic tool for advantage and it also recognizes the potential threat if these are not kept under control.

Like other states, China relies heavily on technology, making the government highly involved with the developments regarding the internet. The Chinese have always seen unrestricted data as a threat to their regime for which they have maintained political control over the internet while keeping economic gains obtainable. In China, the concept of the internet is based on controlling information through censorship that contradicts the view of the West. Such regulations Great Firewall of China, which monitors all Chinese Cyberspace and helps in categorizing several websites for better surveillance. Not just internal obstruction through information, the Chinese government fears the information coming from foreign sources as well. Chinese networks are still receiving a large part of data from the West, which makes them concerned believing that such data is equipped with loopholes and Trojan horses that will leak sensitive Chinese data to them. To counter these fears Chinese government has enforced hefty controls over information and security controls.

Open discussion regarding the nature and future of cyberspace on a global level is not something new; it has been in discussion since 2013. At that time, the United Nations Group of Governmental. Experts, which included representatives from China, also discussed that International Law and the UN Charter apply to the behavior of the state in the domain of cyberspace. China offered an alternative approach through the Shanghai Cooperation Organization in UNGA, with Russia and other Central Asian states in 2015. A mutual belief in SOC states was that the importance of the nation passed into cyberspace. A report published by the US-China Security Review Commission enables China to consider two ideas; firstly both domestic and foreign citizens in a state's territory using cyberspace shall be controlled by the host state which contradicts the Western liberal approach of respecting human rights, thus showing that for China maintain social order is more important than individual privacy.

Secondly, China is a lot concerned about controlling its cyber sovereignty and does not want any interference from outside sources, even though they have mentioned international law in UNGA, they suggest each state make its own cyber rules.

CHINA'S MILITARY CYBER CAPABILITIES AND THEIR POTENTIAL APPLICATION

China's military and cyber capabilities have grown as a major concern for the global community in the past years. China has invested heavily in developing its capabilities aimed at achieving dominance in the cyber domain. Stories regarding the cyber threat that China poses. Most argue that China uses cyber power to rise and win global supremacy, there are also

allegations that China is behind many malevolent cyber activities. The Military Strategy of China describes the cyber capabilities objectives that include:

a. Cyber awareness
b. Cyber Defense

SUPPORT OF COUNTRY'S UNDERTAKINGS IN CYBERSPACE INTERNATIONAL COOPERATION

The strategy aims at stemming major cyber crises, ensuring information security, and maintaining social stability and national security. From these major focus is planted on national security and social stability as several incidents including the Arab and London riots in 2011, depict that social media plays a pivotal role in planning and organizing movements or protests. Thus, the Chinese government monitors the internet and social media to prevent platforms that can spread such information leading to social unrest. China has developed dedicated cyber warfare units within the People's Liberation Army (PLA), which is responsible for offensive and defensive cyberspace operations.

POTENTIAL APPLICATIONS

China can utilize its cyber capabilities to gather intelligence, spread misinformation, and disrupt enemy communications to gain an advantage in military conflicts leading to warfare. The threat that they create adversaries by taking steps that seem unfunfavorable to Chia. China's cyber-surveillance capabilities monitor and control its citizens and information to maintain stability. The People's Liberation Army (PLA) established its 5th branch; The People's Liberation Army Strategic Support Force (PLASSF) which is responsible for cyber, space, electronic and political warfare, as a part of China's military reform. The PLASSF enhenhancese PLA's power display in cyberspace and aerospace and improves the army's capability to fight nontraditional conflicts.

Rear Admiral Yin Zhuo of the PLA Navy has stated that:

The main mission of PLASSF is to provide support to combatant operations so that the PLA can increase control of the regional advantages in cyber warfare and space warfare. The main objectives include target acquisition, undertaking daily navigation operations, management of satellites, countermeasures, and so on.

CONCERNS FOR CHINA'S GROWING CYBERSPACE

China's emerging cyber capabilities have raised concerns globally specifically regarding their involvement in cyber-attacks and espionage. Numerous states including the U.K., U.S., and Canada have accused China of their involvement in cyber espionage trying to steal sensitive information; these accusations are evidence. American security experts have called the U.S. defense against cyber-attacks weak and irrelevant, while China keeps pouring money into its cyber program. Cyber-attacks attempted by China towards the U.S. have been compared to the 9/11 attacks, stating they take Chinese threats seriously. In 2007, an attempt American Nuclear Arms laboratory alerted U.S. security more. It was unknown how much data, leaked but the attack was back to China. A document from M15 in the U.K. containing 14 pages revealed that a U.K.-based company had a threat from Chinese espionage. German Chancellor, Angela Merkel's office was hacked and very sensitive was breached; the attack was

later traced and found to be connected to China. Such incidents show that China's growing cyber strength can harm the security of numerous states, which makes them concerned, and alert.

US's Cyber Security Strategies and Capabilities

United States' approach towards cyber security has gone through significant changes since the emergence and growth of the digital age. Each administration has adopted different and revamped strategies keeping in view the evolving nature of cyber threats. Since the 1990s, the U.S. has focused on protecting critical infrastructure and protection of economic security. The Computer Security Incident Response Team (CERT) in 1988 at Carnegie Mellon University after the outbreak of a computer worm was discovered. CERT was a trademarked acronym of the organization.

ANALYSIS AND CLASSIFICATION OF CYBER CRIMES

Recommendations for response and preventing risk.

The National Infrastructure Protection Center (NIPC) established in 1998, is a unit of the U.S. federal government responsible for protecting computer and information systems. The current mission of provide a focal point for gathering data on threats to the infrastructure. After the attack of 9/11, a great focus has cyber terrorism and national security. Department of Homeland Security in 2002 that consolidated cybersecurity efforts under one roof. Information sharing and international collaboration are emphasized as well.

With the evolution and sophistication of cyber trends and development-increased attention to defensive and offensive cyber capabilities. A major focus protecting critical infrastructure and intellectual property from threats and criminal organizations. The Cyber Security Information Sharing Act in 2015 encouraged companies to share data to avoid security breaches. A National Cyber Strategy drafted in 2018 that outlined a wide-ranging approach to cybersecurity. This strategy identifies that collaboration between private and public sectors is crucial for securing the cyber domain. It highlights a significant point that the responsibility of cyber security falls both on individuals and organizations thus cooperation between industry and society is crucial to secure the cyber space. Joe Biden's administration revised the National Cyber Strategy in 2023 aiming at resilience, collaboration, and risk management. Continued investments in in-depth research and innovation in the field of cyberspace and AI.

US CYBER COMMAND (USCYBERCOM)

USCYBERCOM is a special operation command and the U.S. military's fundamental organization for offensive and defensive digital activities. General Paul Nakasone of the U.S. Army is the current command of the organization and serves as the Director of NSA (National Security Agency) both organizations work in collaboration. Both NSA and Cyber Command work respectively according to Title 10 and Title 50 of the U.S. code. USCYBERCOME in 2010 as a sub-command under U.S. strategic command. President Trump elevated it as a fully unified command in 2018. From being reliant on the NSA for people and resources, Cyber Command has grown into an independent and robust organization over 12 years.

USCYBERCOMD consists of a wide range of missions, from observing the Department of Defense's network and supporting them to defend critical infrastructure to conducting defensive and offensive operations. The major role of the organization is to guarantee DOD's (Department of Defense) capability to operate in times when the world is becoming highly dependent on cyber. To date, Cyber Command has three major responsibilities:

a. To assure the DoD by directing operations and assisting its capabilities
b. Protect the U.S from threats and protect the National Interest
c. Assisting the combatants to accomplish their missions through cyberspace
d. The responsibilities are crucial for assuring the success of the national defense any loophole may compromise US military services.

THE EFFECT OF A GROWING LANDSCAPE OF THE CYBER WORLD ON THE FOREIGN POLICIES OF CHINA AND THE U.S

The growing landscape of cyberspace has made states paranoid and conscious of their security and social stability. China sees itself as a target of cyber-attacks from different actors, which include state actors as well. Such paranoia has led to increased focus on growing their cyber capabilities and strengthening security. The Chinese government is investing heavily in developing cyber defense structures, offensive cyber capabilities, and stricter regulations for the industrial sector. Cyberspace has become the new battleground for the U.S. and China; both states accuse one another of cyber war and spying which is resulting in tensions and a cyber-race between both.

To understand how China perceives cyberspace it is important to analyze the statements given by General Secretary Xi. He has often emphasized his aspiration of making China a cyber superpower and viewing cyberspace as the scene for global strategic competition. As said by Xi often, the term cyber superpower is a strategic concept as well as a political catchphrase. The term Cyber superpower depicts the achievement of uniformity with powers like the U.S. in the aspect of cyber capability and influence on global internet governance; the definition encompasses the grand ambition of the Chinese government and Communist Party plan. As a strategic concept, the term inculcates plans related to security, innovation in technology, digital economy, and influence on global cyber governance. The term appears in essential documents of China such as the 14th five-year plan. China's objective was to gain superiority in cyberspace in the belief that targeting the enemy's most treasured digital system in the early phases of a conflict would bring a swift victory.

Cyber activities such as economic espionage play a vital role in China's foreign policy by subsidizing its technological and economic development. Cyber capabilities China's military modernization efforts as cyberwarfare is seen as a key component of its military strategy. China also actively engages in cyber diplomacy to shape international norms and regulations related to cyberspace.

United States of America

The United States of America has always seen cyber-space as an opportunity to grow and connect but with growing developments and threats the U.S. has become eager to protect its infrastructure and make the internet a safe, secure, and reliable space for its citizens. The U.S. believes that its critical infrastructure is at continued risk from threats of cyberspace that

may harm its social stability. Threats are constantly evolving with developments in cyber such as the emergence of AI; this made the U.S eager to address these effectively to use the internet for growth rather than a hurdle.

The major priorities of the U. S administration in terms of cybersecurity include the protection of the state's critical infrastructure, improving their ability to counter cyber threats and incidents to respond quickly, promoting international cooperation to cyber a secure place, and designing a workforce that is cyber aware and technologically advanced.

RECOMMENDATIONS

a. Moderating cyber risks requires an inclusive approach that must include the government, international collaboration, and the private sector. Following are some policy recommendations:
b. Developing and implementing an inclusive national cybersecurity strategy that may include priorities, aims, and actions that will enhance cyber security in different domains.
c. Establishing a regulatory framework with clear and practicable rules that will help in standardizing security. Penalties and rewards for complete compliance.
d. Motivating private and public partnerships for information sharing for timely response and prevention.
e. Continuous research is essential in cyber technologies to understand the phenomenon. Developing innovative solutions in AI and machine learning to enhance capabilities.
f. Investing in cybersecurity educational programs at different levels to create skilled professionals.
g. Engaging on international platforms to establish cyber norms, working together globally to enhance cybersecurity programs.
h. Continuous monitoring for early threat detection and ensuring compliance with standards.
j. To better save the world from the disaster of this new growing threat, dialogue and trust-building between the U.S. and China is crucial. Both these states need to work in cooperation and not against one another to counter the growing threats of cyberspace. Open dialogue and meetings will help clear misunderstandings and build trust. The U.S. and China are forefront of the cyber race and if they keep accusing each other rather than cooperating; a cyber-cold war may escalate.

FINDINGS

The growing popularity of cloud computing and the Internet of Things (IoT) increases the chances of cyber-attacks and amplifies the need for swift cybersecurity solutions. The increased use of AI and machine learning in cyber-attacks necessitates the development of innovative strategies. Raising awareness about cybersecurity threats and the promotion of best practices among individuals and organizations is crucial for building a resilient cyberspace. International cooperation is essential in combating cyber-attacks and cyber-terrorism. Both the U.S. and China are involved in developing strong cybersecurity systems to counter the

threat of the cyber world. They are also developing their A. I computing systems are threatened by each other.

CONCLUSION

By analyzing the data collected, it is evident that cyber threats and cyberwarfare are stronger than ever. The innovations and developments in the areas of A. Technology is bringing societies to a stage that was not witnessed before. Thus to stay sane in this evolving landscape of the cyber world states need to establish frameworks, develop their systems, and keep updated in the domain of the digital world. U.S. and China both are involved in a cyber race; each is paranoid about attacks from the opposite side but lacks collaboration. From the findings, it is evident that China has an upper hand in the cyber domain and has been involved in numerous cyber-attacks in different states. The technological rivalry between the U.S. and China is intensifying; each of them is investing heavily in technological developments and revamping their cyber capabilities.

REFERENCES

Kimberly Hsu. Craig Murray (2014). China and International Law in Cyber Space. U.S. and China Economic and Security Review Commission Staff Report. https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf

Lyu Jinghua (2019, April 1). What are China's Capabilities and Intentions? Carnegie Endowment for International Peace.

Magnus Hjortdal. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. Journal of Strategic Studies, Vol 4, (2), 1-24. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss

MikkRaud. (2016). China and Cyber: Attitudes, Strategies, and Organization. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf

U.S.-China Economic and Security Review Commission. (2022). Chapter 3, Section 2: China's Cyber Capabilities. Retrieved from https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf

White House. (2023). National Cybersecurity Strategy 2023. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf