IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

# CHINA'S CYBER THREATS AGAINST EAST ASIA

**Akshita Pant* and Prof (Dr.) Nagalaxmi M. Raman****

* Research Assistant, Master's in International Relations, Amity Institute of International Studies, Amity University Uttar Pradesh.

**Director and Head, Amity Institute of International Studies, Amity University Uttar Pradesh, Noida

## ABSTRACT

Cyber-attacks by China against East Asian states are accelerating. The issue of personal information and privacy being hindered is affecting not only individual data but state security and sovereignty. China's AI advancements are becoming a threat to nations like Taiwan, Japan, and South Korea, who are already anxious over China's heavy military and economic dominance in the region. Now, their nations' cyber security is also under threat. This article provides insight into China's developments in cyberspace and its capabilities. The Chinese government has been spying on its neighbors and is behind numerous malicious attacks that have led to these nations being alert in safeguarding their secret government information that could be vital for their security. Japan has been the victim of many cyber-attacks by China, mainly in 2021, similarly, Chinese hackers have carried out malicious attacks on South Korea and their academic institutions over the years. More recently Taiwan has been the one to face these attacks a lot more. This article goes through the instances of these cyber security infringements by China and how it is affecting these states. The importance of strong cyber governance and how East Asian nations could unite to form a safe cyber security institution to protect themselves from Chinese attacks.

## INTRODUCTION

Security is one of the most crucial elements in any state's policies and plans. But Cyberspace has turned out to be a modern security realm that has been not governed adequately by the international order. With the new trends that follow the 21st century comes digital space's positive and negative outcomes. Any state could use it for its benefits and advancements and could also use it for malign intentions. China has been under scrutiny for conducting countless cyber attacks on numerous states. The advancement of technologies that China acquires is unknown but the way, it hacks the government data and steals the information of states. It could be stated that China's artificial intelligence is evolving at a fast speed. Ironically China itself is depending itself on information networks in almost all aspects, for trade and commerce, for advancements in artificial intelligence, and also in defense.

As the allegations are not proven and the states are not sure if the Chinese intentions as they mentioned over their cyberspace and artificial intelligence are based on their defensive and non-destructive social unrest to spread, which could lead to large-scale social and political instability.[1]

For that reason, Governance of Cyberspace is vital right now, the information, privacy, and data of individuals, organizations, and states need to be secured. But it is also necessary to know how an individual views Cyberspace security if they see it being governed as a state-centric device and then their rules and security regulations or if they need an international independent organization for the cyber security moderation. A third way of finding a solution could be giving your trust to a private independent company to supervise these security issues, to lay out similar ground rules, where they could raise awareness the people using the internet, and different cyberspaces and to educate people about hackers with malicious intent who are persistently testing their skills to seek out private and discreet intelligence and information. Cyberspace is not easy to govern as it lacks sovereignty and borders, everyone owns the internet and nowadays billions of people have access to cyberspace and its various platforms. It is difficult to align cyberspace governance with modern-day security threats as variations.[1] One aspect of cyberspace that creates tensions and mistrust among individuals is its complexity and ever-changing dynamics. We never know what shape a new cyber threat will take to breach privacy.

## CHINA'S AI AND CYBER CAPABILITIES

State-sponsored cyberterrorism by Chinese highly equipped hackers has carried out endless attacks. The place where the citizens are under surveillance 24/7 and there is little to no privacy China is the land of fastly growing Artificial Intelligence and highly advanced Cyberspace. The cyber espionage carried out by China is also claimed to be highly advanced and secretive. It is hard to detect the cyber tools that it uses in order to take our important information about governments. China has made significant advancements in artificial intelligence (AI) over the past few years, particularly in computer vision, natural language processing, and autonomous systems. This AI

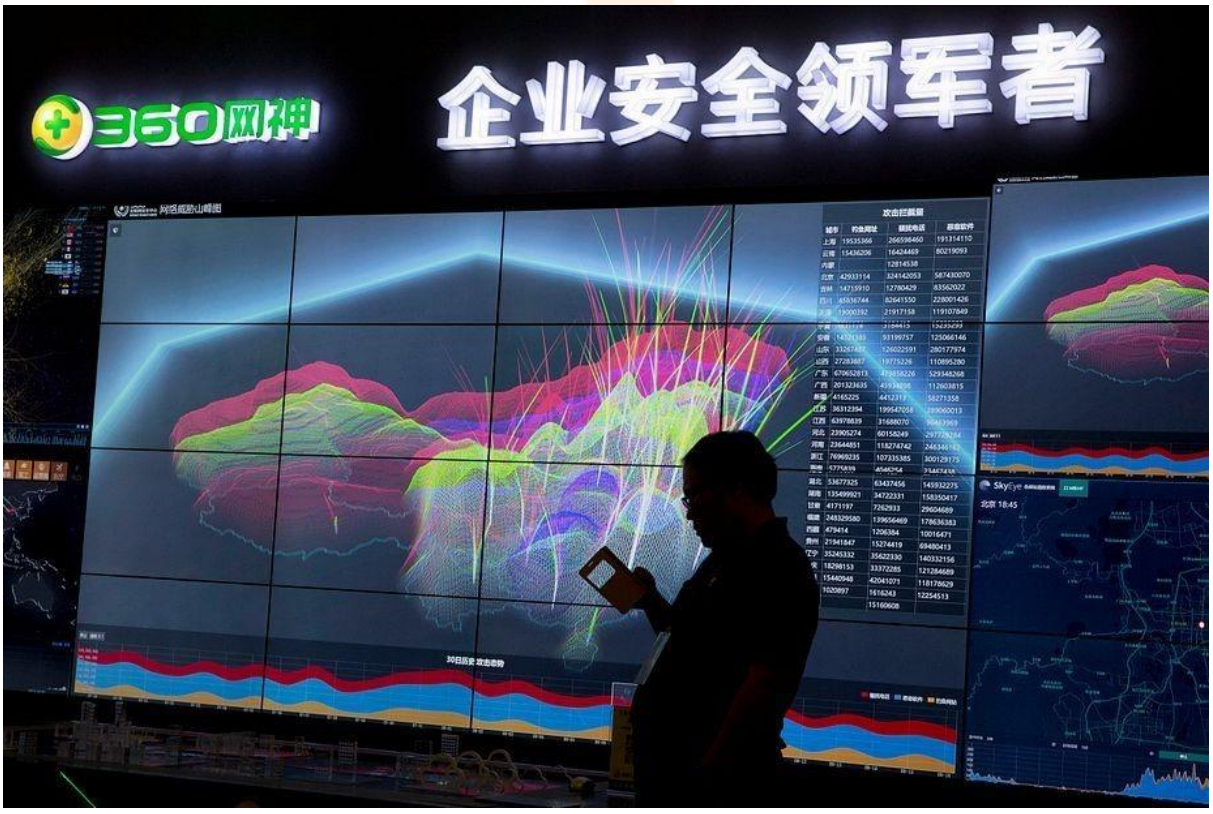


Image Source: Ng Han Guan/ The Diplomat

**Figure 1** A Chinese worker showcasing live visualization of fraudulent phone calls and phishing all across China during the 4th China Internet Security Conference in Beijing.

growth is helpful to carry out different types of cyber-attacks. One of the modern hacking tools used by China is the Microsoft Exchange Server vulnerability 2021 used to access and attack email servers. Scientific development, research, and modernization of AI have become the scapegoat for acquiring intellectual property, secret non-disclosed research, or placing Chinese interests in a favorable economic position.[2]

Defending and safeguarding critical information infrastructure is the utmost priority of any state and for that reason, governments use high technologies to protect the information of their nations. China is relying heavily on intellectual property and knowledge too, so no state is safe from cyber-attacks and invasion of privacy. Dependence on information networks in all aspects, including in defense, could make China more reliable on advanced artificial intelligence.

The key to the success of artificial intelligence in China could be the reliance on the quality of data and cheap labor. Megvii and SenseTime, two of the world's most valued startups to exist in today's time, both worth billions of dollars, are Chinese Artificial intelligent companies specializing in the field. In closer inspection and learning more about Artificial intelligence we could easily identify the more important components i.e., software, powerful computers, and data, famously stated as the new trinity of artificial intelligence.[3] China's government encourages and promotes surveillance technology and cyber functions abroad. This benefits and make up diplomatic ties and dialogue cooperation of law enforcement, and also develop training strategies in the Global South states. This not only helps in the promotion of cyber tools and surveillance technologies but also supports the state's goals with interest to international rules and regulations and in enhancing multilateral and regional institutions.[4]

Daxin is said to be one of the best malware in cyberspace and it took 10 years to detect it. It is a form of remote access trojan ( RAT ) which can provide hackers access to an infected system. The latest power tool by China hijacks all legitimate and authorized connections to disguise its communications in normal network traffic. Daxin is mainly distributed through phishing emails, malicious attachments, or software downloads from untrusted sources. Once installed on a victim's computer, it can perform various malicious actions, such as stealing sensitive information, recording keystrokes, taking screenshots, and executing arbitrary commands.[5]

Last year Chinese hackers used zero-day vulnerabilities the most to carry out malicious attacks on cyberspace these are the cyber attacking tools that the attackers use to exploit vulnerabilities without the knowledge of the software developer, just like in 2020, a Chinese hacking group known as APT41 was found to be exploiting multiple zero-day vulnerabilities in a popular software product to conduct cyber attacks. [6]

## EAST ASIA: VICTIM OF THE CYBER-ATTACKS

China's dominating presence in East Asia and its historical linkages with the region is evident. But in current times China's advancements in not just military and economic capabilities but also in its cyberspace and artificial intelligence development have turned out to be another threat to East Asian states. Just like any Global superpower trying to dominate every sector to signify its relevance, it can be stated that China is advancing its cyber power using it to rise and ultimately acquire global dominance and it could be easily speculated that the Chinese government is sponsoring the non-state actors and hiring professionally skilled hackers to conduct many malicious cyber activities. It can be theorized that many of the allegations focus on the back-and-forth power struggle between China and the United States regarding cyber espionage and it is claimed by the professionals that these actions are unlikely to cause any armed conflict or any economic instability in the international order. Each state should vary from the other since almost all capable state actors are alleged to conduct cyber espionage.

> **"Cyberspace undeniably reflects some form of geography."** Sandra Day O'Connor, SC U.S.

Regardless of the differences in opinions, it is clear that China's influence in cyberspace in East Asia has been a topic of concern for many years as China has been conducting many hacks in the East Asian states mainly Taiwan, Japan, and South Korea. China's size and economic power have made it a significant player in the region, its influence, and impact in all areas whether it is economic, military, or cultural should not be taken lightly and now China's technological advancements have enabled it to exert influence in cyberspace too. China has been accused of engaging in various cyber-attacks in East Asian states, and these have been under heavy scrutiny after the Russia- Ukraine war and crisis all the cyber-attacks have come into the limelight as China has its eagle eyes on Taiwan and the alleged "spy balloons" sent by the Chinese government again alarms the region as Japan and South Korea also fears for their security and their territory being hampered. China's cyber-attacks in these three states include intellectual property theft, espionage, and hacking. Gathering intelligence, disrupting political opponents, and controlling the information flow of other states both domestically and abroad are some of China's cyber capabilities that it has been using to gain critical information.

In addition to these cyber threats and cyber-attacks, accusations are made against China for using social media and other online platforms to spread propaganda and shape public opinion. This has raised concerns about the potential for China to manipulate elections, influence public opinion, and sow discord in the region. It's important for governments and organizations to develop effective cybersecurity strategies and to work together to combat cyber threats to address these concerns properly. Investment in cybersecurity research should be increased with the development, and sharing of threat intelligence, and the promotion of international cyber-issued cooperation.

**TAIWAN:** Tsai Ing-wen Taiwan's President stated that "Information security is national security". At the time when Taiwan has spotted dozens of spy balloons and in recent years has been suspected of Chinese military aircraft in its airspace.[7] China's influence in cyberspace in Taiwan has been a significant concern for the Taiwanese government and the international system. "One China "ideology of China considers Taiwan a part of its territory still and it has been known to use its cyber capabilities and recent advancements to exert political and economic pressure on Taiwan even though the military of China is hovering over Taiwan's border. Taipei-based organization Doublethink Lab tracking has documented over 2,900 instances of disinformation targeting Taiwan and hacking for various information since Pelosi's visit towards the November elections. After the Russia- Ukraine war it is evident that Taiwan has been alerted and the U.S. lawmaker and the strategic community has warned Taiwan to be more conscious as China is likely to target more of their cyber intelligence to seek crucial information regarding their defense and security.[8]

Allegations on China of using cyberattacks to gather intelligence, steal intellectual property, and disrupt the operations of Taiwanese businesses and government agencies. Again, in Taiwan's case, China has been using social media sites and platforms to sway public opinion of them.

Pentagon is to expand cybersecurity cooperation with Taiwan against China's growing aggression tend to address these challenges, the Taiwanese government has been working to enhance its cybersecurity capabilities, including developing cybersecurity legislation, increasing investment in cybersecurity research and development, and promoting international cooperation on cyber issues. Taiwanese government statistics estimated that it faced 20 to 40 million Chinese cyberattacks every month in 2019 and from that point forward the cyber-attacks have just escalated. It has become one of the primary factors for safeguarding Taiwan's cyberspace as the Russia- Ukraine war escalated. Nancy Pelosi's visit has made China tenser about its stance on Taiwan's sovereignty. Taiwanese businesses and individuals have also been encouraged to take proactive measures to safeguard themselves from continuous cyberattacks, by using strong passwords that are hard to crack or decoded, keeping software updated and using anti-virus, and being observant and careful about phishing scams.

The evolving nature of cyber threats and the importance of safeguarding intellectual property with the ongoing rise in cyber attackers means that the fight against cyber threats is ongoing in Taiwan and that it requires constant attention from not only the Taiwanese government but also assistance from other states and international; community as well with the necessary adaptation of newer tools to keep pace with new threats and vulnerabilities.

**JAPAN:** Japan has been a victim of cyberattacks by China for a long time and there have been several high-profile cyber-attacks on Japanese targets at have been attributed to Chinese state-sponsored hackers have been targeting sensitive information related to military, economic, and political matters. One of the most famous examples of the cyber threat was the long going cyber-attack targeting Japanese organizations conducted by the Chinese APT group coded named "Cicada," it was exposed by the U.S.-based cybersecurity firm Symantec in 2020.[9] These attacks have included the theft of sensitive information from Japanese defense contractors, the disruption of the operations of Japanese critical infrastructure, and the compromise of Japanese government agencies and diplomatic missions. It was revealed by LINE, a Japanese messaging platform in 2021 that subcontractors from China had access to their servers which contained the personal information of 86 million users, and the information was outsourced to a Chinese-based firm with monitoring functions. With the security threat increasing Japan has extended its strategy to a multilateral level and has started engaging in collective cooperation and dialogues for safer cyberspace with other states and international institutions.

The Quadrilateral Security Dialogue (Quad), the group comprising the United States of America, Japan, Australia, and India is planning to make an operative platform as an alliance of cybersecurity to cooperatively counter the threats and cyber-attacks from China.

The QUAD has launched a Cyber challenge to advance cyber security among the countries. QUAD plans to focus on improving and building technical defenses, promoting international norms and standards for responsible behavior in cyberspace, and strengthening cooperation and information sharing between nations.[10]

**South Korea:** China is well aware of and intimidated by the close relations between South Korea and the United States Of America. The most infamous Cyber threat to the South Korean website of South Korea's Lotte Duty-Free was crashed by China in 2016 which was assumed to be retaliation for Lotte's decision to provide land for the deployment of the U.S (THAAD) system which was in response to the North Korean missile threat at the time. The "Dark Seoul" Attack in 2013 media outlets and banks in South Korea were targeted and both North Korea and China were accused of the attack.[11]

In January 2023, Korea Internet and Security Agency (KISA) stated that a group of hackers carried out a cyberattack, and most academic and research institutes were affected. South Korea is already affected by continuous cyber threats by North Korea and is working towards strengthening its cyber security and governance. South Korea- U.S. cooperation could lead to the advancement of their cyberspace. ASEAN-Korea Cyber Security Cooperation Project, includes capacity building, joint research projects an exchange of information for the best security result. The ASEAN Cyber Shield launch was also announced by KISA for better research, planning, and technical research in the area. NATO and South Korea's cybersecurity collaboration is evident as the attacks by China can prove to be more dangerous than they seem as China has been keeping its eye on its neighborhood countries and their allies.

The South Korean government has openly expressed concern about the threat of Chinese cyber-attacks and has taken necessary measures to advance its cyber defenses, which includes not only increased cooperation with the United States but also with other states and organizations as well. In recent years, there have been reports of joint military exercises and information-sharing agreements that could safeguard the cyberspace between South Korea, the U.S., and Japan aimed at countering cyber threats from China and North Korea even though Japan and South

Korea have complicated relations, they can come together to defy a common threat. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is joined by South Korea's National Intelligence Service for better security of cyberspace.[12]

## DILUTING THE CYBER DOMINANCE OF CHINA IN EAST ASIA

East Asian states, especially Taiwan, Japan, and South Korea, no matter how complicated and complex their historical and present relations are, need to engage in and continue to work on partnerships and initiatives in regional cyber security and governance. Cyber-attacks should not be taken lightly, these are serious threats to their territory and ultimately sovereignty and safety. The dominating influence China wants to preserve in the region is indisputable. East Asian states in this day and age should collectively form a structured and governed cyber governance with a multi-stakeholder foundation for peace and security. Governance of Cyberspace on a much wider level is needed to safeguard this region from China's fast-paced hard-track artificial intelligence and cyberspace growth at this moment in time, the new trends in cyber threats have led to fear in people that have further led to their mistrust of using any apps and even less trust in the government with their private information. If the state leaders think about the basics of setting up rules and regulations in a cyberspace setting up standardized norms and international processes is one of the fundamental elements for the governance of cyber security. Another alternative that the East Asian nations and international system collaboratively could work on is a capacity-building framework for international cybersecurity that reflects the actual practice and can be used in international negotiations on stability in cyberspace. Still, international law and its analysis play a vital role in the framework for responsible state behavior in cyberspace which again needs constant monitoring. These possible actions could solve the upcoming complex threats and challenges and create a step towards security in all forms and the citizens and the state simultaneously. The organization and companies need to work together with the states and the international system to build a safer and more trustworthy operation and structural governance that holds the culprits and the hackers accountable to ensure safety among the people of the world. Naming cyberspace a global commonality should mean that the international world needs to safeguard it all together and limit its misuse as much as it can with the help of multilateral cooperation.

---

**REFERENCES**

[1] Liaropoulos, A. N. (2017). Cyberspace Governance and State Sovereignty. In Springer eBooks (pp. 25–35). Springer Nature. https://doi.org/10.1007/978-3-319-52168-8_2

[2] Shandler. (2023). The 5×5—China's cyber operations. Atlantic Council. https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/\

[3] Defence technology | Jan 29th 2022. (n.d.). The Economist. Retrieved April 24, 2023, from https://www.economist.com/technology-quarterly/2020/01/02/chinas-success-at-ai-has-relie

[4] How China built a one-of-a-kind cyber-espionage behemoth to last. (n.d.). MIT Technology Review. Retrieved April 24, 2023, from https://www.technologyreview.com/2022/02/28/1046575/how-china-built-a-one-of-a-kind-cyber-espionage-behemoth-to-last/#:~:text=It%20works%20by%20hijacking%20legitimate

[5] eliasgroll. (2023, March 20). Chinese-linked hackers deployed the most zero-day vulnerabilities in 2022, researchers say. CyberScoop. https://cyberscoop.com/mandiant-zero-day-vulnerabilities-china/

[6] Zheng, S. (2023, February 14). Worse Than Spy Balloons? Taiwan Is More Concerned With Chinese Hacking. Bloomberg.com. https://www.bloomberg.com/news/newsletters/2023-02-14/spy-balloons-no-match-for-china-s-cyber-attacks-suggests-taiwanarah

[7] Nanda, P. (2023, February 12). 'Assault On Taiwan Has Begun': US Links Taiwan To Ukraine, Says US Cyber Forces Must Be Ready For War With China. Latest Asian, Middle-East, EurAsian, Indian News. https://eurasiantimes.com/assault-on-taiwan-has-begun-us-links-taiwan-to-ukraine/

[8] Katz, J., & Katz, J. (2023). New legislation would push Pentagon cybersecurity cooperation with Taiwan. Breaking Defense. https://breakingdefense.com/2023/04/new-legislation-would-push-pentagon-cybersecurity-cooperation-with-taiwan/#:~:text=The%20legislation%20would%20authorize%20the,stop%20further%20attacks%20from%20China.

[9] The Diplomat. (2021, October 16). How Will Japan's Cybersecurity Posture Impact its Relations With China? https://thediplomat.com/2021/10/how-will-japans-cybersecurity-posture-impact-its-relations-with-china/#:~:text=As%20such%2C%20Japan%20has%20conducted,to%20cooperate%20further%20in%20cybersecurity.&text=At%20the%20political%20level%2C%20greater,significantly%20worsen%20current%20bilateral%20relations.

[10] Brajesh, T. (2023, February 4). Quad plans cybersecurity alliance amid China threat - The Sunday Guardian Live. The Sunday Guardian Live. https://sundayguardianlive.com/news/quad-plans-cybersecurity-alliance-amid-china-threat

[11] Brajesh, T. (2023, February 4). Quad plans cybersecurity alliance amid China threat - The Sunday Guardian Live. The Sunday Guardian Live. https://sundayguardianlive.com/news/quad-plans-cybersecurity-alliance-amid-china-threat

[12] Little, J. W. (2023). Combating Chinese Cyber Threats in South Korea. Blogs of War. https://blogsofwar.com/chinese-cyber-threats-against-south-korea-defense-and-collaboration-strategies/#:~:text=China%20has%20also%20been%20accused,have%20been%20involved%20as%20well.