BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

Preliminary considerations on China's international cooperation in cyber security: legislation, competent authorities, and challenges

Andreea-Maria PIERȘINARU, Ph.D. Student*
*National University for Political and Administrative Studies (SNSPA)
e-mail: andreea_piersinaru@yahoo.com

Abstract

This article addressed general issues regarding the Chinese legislative framework, competent authorities, China's strategic objectives and the challenges in terms of international cooperation in the field of cybersecurity. The main objective of the research is to identify the actors involved in ensuring China's cybersecurity, describe their responsibilities and correlate them with Chinese cyber-security legislation and China Cyber Security Cooperation Strategy. This study traces preliminary considerations for future in-depth analyses of the impact of China's actions in the field of international cybersecurity.

Among the main findings of the study the aspects briefly identified were related to the influences of the policies and narratives of the Chinese Communist Party presented in China's International Cyber Security Cooperation Strategy, as well as to the fact that, despite China's intention to become a cyber power, open to cooperation, international reactions are quite reluctant due to allegations of cyber espionage and domestic surveillance problems existing at the national level, among others.

Keywords:

China; cyber security; cyber sovereignty; cyber espionage; international cooperation; cyber superpower.

Article info

Received: 10 May 2024; Revised: 10 June 2024; Accepted: 13 June 2024; Available online: 5 July 2024

Citation: Pierșinaru, A.M. 2024. "Preliminary considerations on China's international cooperation in cyber security: legislation, competent authorities, and challenges". *Bulletin of "Carol I" National Defence University*, 13(2): 121-141. https://doi.org/10.53477/2284-9378-24-24

Cybersecurity has become an essential part of states' foreign and security policy, due to accelerated globalisation and digitalisation. As one of the world's largest economies and technological powers, China has created a comprehensive strategy for international cooperation in cybersecurity. In recent years, China has stepped up its efforts to participate in global discussions and partnerships, multilateral cooperation being the key to addressing international cyber challenges.
In the reviewed literature some studies approach the Chinese legislative framework regarding cyber security historically and others analytically from the perspective of international cooperation.
Thus, relevant studies on the evolution of cybersecurity legislation in China include Rogier Creemers's study which provides an in-depth analysis of Chinese cybersecurity legislation.

Since the late 1990s, China has adopted a policy of "informatization" – or 信息化 (xìn xī huà), which includes the use of digital technology in economic, social and governmental activities. This policy evolved with the establishment in 2014 of the Central Leading Group for Cybersecurity and Informatisation, chaired by President Xi Jinping. Following this step, during the Xi administration, the "Cyber Power Strategy" or "网络强国战略" (Wǎngluò qiángguó zhànlüè) was developed, with the primary aim to improve China's technological capabilities and modernize state governance, including projects such as judicial informatization and the social credit system (Creemers 2023).

Another landmark study in the reviewed literature is Meirong Guo's "China's Cybersecurity Laws, Their Relevance to Critical Infrastructures and the Challenges They Face". His study brings a new interpretation to the Cybersecurity Law adopted in 2016, which from his perspective was not effectively implemented because cybersecurity was integrated into several laws, or administrative regulations already in place at the departmental level and the law lost consistency. Guo also points out that the People's Republic of China did not have specific legal regulations for cybersecurity before the adoption of the Cybersecurity Law in 2016; nevertheless, he stresses the importance of China's participation in international cooperation in cybersecurity to formulate international technical standards and deal with global cyber threats (Guo 2018).

In this context, China is committed to building extensive cooperative partnerships with all participants of the international community, developing dialogue platforms, and promoting a fair cybersecurity framework for all (MFA CN 2017). China has adopted this approach in its cooperation with ASEAN and the Shanghai Cooperation Organization on network and information security emergency response.
In all normative papers and Chinese leaders' speeches, China declares itself open to cybersecurity cooperation, demonstrating this interest through active participation in World Summits on Information Society and other international or regional cybersecurity-related conferences. China hosted the first World Summit

on Cybersecurity, which was organised by the EastWest Institute in Dallas. This event is mentioned by Chinese leaders in all cybersecurity-related public presentations to position China as a leader in the field and one of the initiators of international cybersecurity dialogue (Chinese Embassy in the UK 2011). China also states that it supports a multilateral, democratic and transparent global internet governance system (MFA CN 2023) and includes supporting the United Nations in its leadership role in global digital governance and rulemaking, stressing the need for an open and fair approach to cyber governance.

Another pillar of China's strategy is cooperation in research and development to enhance cybersecurity through industrial and academic partnerships. This includes collaborating with international research institutions and universities (Zhang, et al. 2022). In this context, China announced, in 2017, a project to 4 to 6 world-renowned cyber security institutes by 2027. These institutes will have the main objectives of training professionals in network security, conducting relevant academic research and cooperation with companies and governmental departments. One of the major objectives of these institutes is international cooperation, which includes the training of key academic staff abroad and the development of academic research collaboration within international consortia (Chinese Ministry of Education 2017).

According to the study published in 2021 by the Center for Security and Emerging Technologies, China established the National Cyber Security Center (NCC) in Wuhan[1], which includes seven research, talent development and entrepreneurship centres. NCC is home to two laboratories focused on governmental cybersecurity research and an incubator to support innovation in the private sector. (Fig.1.) This centre is supported from the highest levels by the Chinese Communist Party (CCP) and aims to reduce dependence on foreign technologies and promote national innovation (Cary 2021).

[1] Video about NCC in Chinese language : https://www.bilibili.com/video/BV1Vz411z7gT/?t=0h0m54s

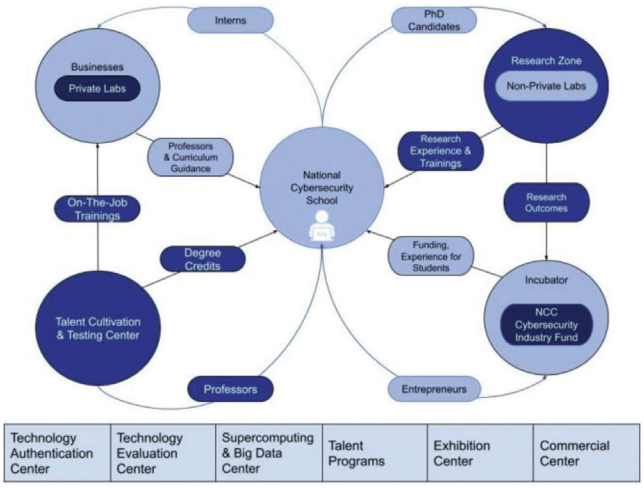

Figure No. 1 National Centre for Security and Emergent Technologies (Cary 2021)

Price Waterhouse Cooper (PWC) notes in a report published in 2023 that, despite public openness to cybersecurity cooperation, international cooperation norms are affecting China's domestic cybersecurity policy, forcing Beijing to implement strict regulations and laws to manage data flows and protect critical infrastructure (PwC Indonesia 2023).
Despite its efforts to become a cyber superpower, China faces significant challenges, such as accusations of cyber espionage and concerns about its domestic methods of surveillance and information control (Julian 2021).

Given China's legislative developments in cybersecurity but also its strategic goal of becoming a cyber superpower during the Xi administration, an introductory study on China's current legislative outlook on cybersecurity was deemed appropriate. The research will include a brief overview of the structures that ensure cybersecurity at the national level given that these were not identified in a unified way in the literature reviewed, but only in the text of the Chinese Cybersecurity Law. Finally, the perspective of the cyber security cooperation strategy and the challenges in implementing the objectives will be briefly analysed.

Methodology and Research Limitations

This study aims to identify the preliminary considerations regarding China's legislation and strategy in cybersecurity and their effects on international cooperation on cybersecurity. This research hypothesises that China's desire to protect its cyber sovereignty and strengthen its position as a cyber superpower has a significant impact on international cybersecurity cooperation. Thus, the following research question emerges: *How does China's cybersecurity legislation affect cooperation with other states?*
In the testing of the hypothesis, quantitative methods were used for data collection and analysis: secondary data analysis (for literature) and content analysis (for legislative texts). Secondary data analysis involves finding answers to new research questions using data that has already been collected from other studies (Fulton Library n.d.).

The article is a brief introduction to China's cybersecurity, which is limited to presenting the most important aspects, from the author's perspective, of the China Cyber Security Act, but also of the Chinese International Cooperation Strategy, as well as identifying some of the challenges that the Chinese Government has in achieving its objectives of international cooperation in the field of cyber security. These preliminary considerations will also refer to the main tasks of the competent authorities dealing with the implementation of the action plan of the cybersecurity strategy according to the law.

All these might open new research opportunities in the field, by in-depth studies using other research methods, which due to the constraint of time, could not be

developed in this article. The elements presented in the study can thus be used as a reference or starting point for future in-depth analyses conducted by researchers interested in the topic, as well as by experts in policy and strategy development in China's international cybersecurity cooperation.

The article is structured into two main sections preceded by a short introduction and this methodology is accompanied by the limits of research. At the end, there are underlined a series of conclusions. The first section is devoted to a brief presentation of the structure of the state apparatus dealing with cybersecurity in the People's Republic of China and the legislative framework on cyber security. As far as the legislative framework is concerned, only China's Cyber Security Act has been examined.

The second section of the article is an introduction to the Strategy of the People's Republic of China for International Cooperation in the field of cybersecurity and the challenges in achieving the objectives set out in the strategy. Regarding China's challenges in achieving the objectives set out in the strategy of international cooperation, three cases of Chinese cyber-spying-related groups were analysed: APT10, APT 31 and APT41.

The findings of the study highlight the importance of the topic and the need to conduct more studies in the field of cybersecurity, especially on the perspectives that come from China for a better understanding of the prospects of international cooperation in cyberspace security.

Brief Overview of the Structure of the State Apparatus in Charge of Cybersecurity in the People's Republic of China and the Legislative Framework for Cybersecurity in China (gov.cn)[2]

[2] The law will be analysed as a whole.

To understand the structure of the state apparatus in charge of cyber security in China, it is necessary to remember that in an autocratic state like China, no governmental structure is independent or functions on its own without the impact of the strategies and narratives of the Chinese Communist Party and its leaders.

So, given this pyramidal structure, the Central Commission for Cyberspace Affairs (CCCA) of the Central Committee of the Communist Party of China is the main body responsible for implementing cyber security policies, founded in 2018 following the 2014 efforts initiated by the Cyber Security and Information Security Working Group. The CCAC is responsible for coordinating the activities of the following subordinate agencies and entities, which communicate and collaborate: Cyberspace Administration

(CAC), Public Opinion Information Center, China DNS Registry managed by China Internet Network Information Center (CNNIC), CNCERT (National Cybersecurity Incident Response Center), TC260- China National Information Security Standardization Technical Committee, and China Cybersecurity Association. The effective coordination of these agencies and entities is essential for implementing cybersecurity policies and promoting integrated cyberspace governance in China. Reflecting the strategic importance that the Communist Party of China gives to cyber control and cybersecurity, Xi Jinping, together with Li Qiang and Cai Qi, chairs the CCAC.

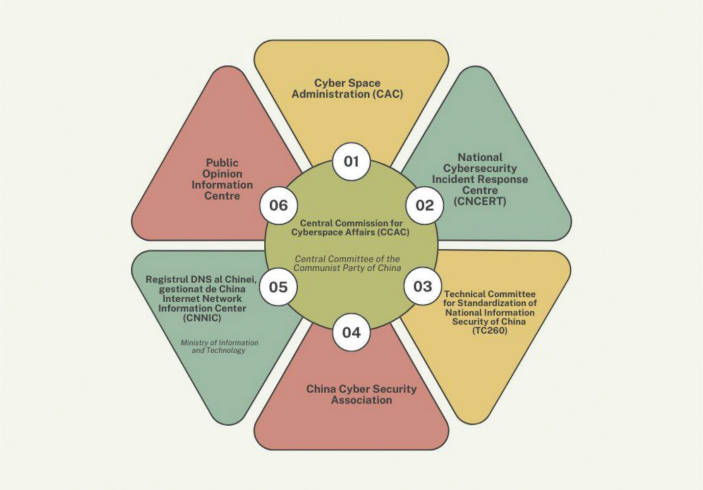

Figure No. 2 Structure of the state apparatus in terms of cyberspace and cybersecurity in China[3]

[3] Personal interpretation following China's Cyber Security Law.

The following diagram, designed by the author, presents the structure of the state apparatus in charge of cyberspace and thus cybersecurity in China for a more precise understanding of the above. After the presentation of the diagram, a brief overview of the tasks of each institution will follow.

The Cyberspace Administration (CAC) is China's national cyber regulation agency. In addition to national cyber regulation, the CAC also deals with cyber censorship and sets specific policies. This entity is vital to China's cyber governance system as it is responsible for overseeing and controlling the internet to ensure that all content published on the internet meets the requirements of the Communist Party of China (CCP). The CAC, through its cyberspace management responsibilities, also sets rules for technology companies and monitors online communication to prevent the spread of information deemed dangerous or destabilizing to the state (CAC n.d.).

In 2019, CAC launched a project to eliminate pornography, violence, gambling, fraud, superstition, parody, threats and the spread of "inappropriate lifestyles" and "bad popular culture" that imposed a high level of online content control, favouring the online positive image of the CCP (Xinhua 2019).
In the same year, CAC issued a regulation stipulating that any behaviour

deemed to be considered a cybercrime will be added to the social credit system – the cyber criminals' punishment being the impossibility of accessing bank credits or other citizen facilities (Dandong 2019).

Another important institution of the state apparatus in the field of cybersecurity is the *Public Opinion Information Centre,* which brings together government efforts of censorship and surveillance of information on the internet, and monitors, and analyses public opinions on the internet. There are references to this centre, only in the text of the law. The study has so far not yet identified any other sources to present or discuss the activities of the Centre.

The structure responsible for managing the DNS Registry of China is the *China Internet Network Information Centre (CNNIC)*. Regarding the management and operation of the top-level domain (TLD), CNNIC is responsible for the ".cn" domains. This includes overseeing domain entries and ensuring that the DNS infrastructure associated with these domains works well. On the other hand, CNNIC has an important responsibility in protecting personal data and cybersecurity: ensuring the security of the DNS infrastructure and protecting users' data. This includes establishing security rules to prevent abuse and cyber-attacks, as well as managing WHOIS data, which contains information about domain owners. To comply with international standards in domain name management, CNNIC works with ICANN and other international internet management organizations. This includes active involvement in global policy processes and implementation of international decisions in China's domain system. Finally, CNNIC encourages the creation and use of internationalized domain names (IDNs), which allow the use of Chinese characters in the domain name. This would facilitate internet access in the native language of Chinese speakers (CNNIC n.d.).

CNCERT (National Cybersecurity Incident Response Center) oversees cyber threat prevention efforts, anticipating and blocking potential attacks before they affect national networks or critical infrastructure, and ensures the fullest and fastest possible recovery after handling an incident, thus restoring affected services and systems. CNCERT works with similar teams in other countries and with international organisations to manage cybersecurity incidents that may affect various countries. CNCERT is a member of the Forum of Security Incident Response Teams (FIRST) and one of the founders of the Asia Pacific Computer Security Incident Response Group (APCERT). CNCERT informs the public and organizations about cybersecurity risks and best practices for protection and collects and distributes data about security vulnerabilities through the China National Vulnerability Database (CNCERT/CC n.d.).

The main objective of *China's Technical Committee for National Information Security Standardization (TC260)* is to create national standards for cybersecurity. This committee is responsible for the establishment and maintenance framework of

standards governing various aspects of cybersecurity in China, such as network products and service security, critical information infrastructure protection and cybersecurity incident management. TC260 works with other government entities and private sector organizations to ensure that cybersecurity standards are consistent and effective. This involves non-government legal entities such as national and international companies' contributions. According to public data published on the organization's official website, TC260 has published about 300 technical cybersecurity standards so far and continues to improve them to meet the ever-changing needs in cybersecurity (TC260 n.d.).

The Cybersecurity Association of China (CSAC) coordinates public-private policies between the private, public and academic sectors. CSAC influences Chinese cybersecurity legislation through its activities. This includes promoting industry best practices and security standards. CSAC argues that the Chinese origins of goods and services improve the country's security, so it recommends using goods and services offered by Chinese companies over foreign competitors. The association works to promote and defend China's cybersecurity interests internationally by participating in discussions and negotiations on international cybersecurity standards and legislation (Cyber Security Association of China (CSAC) n.d.).

China's Cyber Security Act (gov.cn 2016), approved in its first format on 7 November 2016 and entered into force on 1 June 2017, constitutes the legislative frame for cyber security in China. The general objective of the law is to ensure network security, cybersecurity, national security and public interests, protect the rights and legitimate interests of citizens, and promote healthy economic and social digitalisation. The state provides measures to monitor, defend and manage network security risks and threats coming from within and outside China's borders, protects critical infrastructures from potential attacks and menaces, provides penalties for cybercrimes, and is meant to assure order and security in cyberspace. Another important aspect mentioned in the law concerns data localization. In China, the law requires essential personal data and other personal data collected from cyberspace to be stored within the country. Critical infrastructure operators are required to ensure this by law. Article 2, Chapter 1 states:

This Law shall apply to data processing activities, security supervision and regulation of such activities within the territory of the People's Republic of China. If data processing outside the territory of the People's Republic of China harms national security, public interests or the legal rights and interests of persons or organizations in the People's Republic of China, legal liability shall be investigated in accordance with the law. (NPC.GOV.CN 2021)

In addition to the Cybersecurity Law, the Data Security Law was published (2021) that imposes new rules for enterprises interacting with Chinese citizens both at home and abroad, and the influence of domestic legislation migrating to foreign space with implications for China's international cybersecurity cooperation is observed.

China's cybersecurity law also provides perspectives on international cooperation, governance of cyberspace, research in network technology and setting standards for combating cybercrime. It also stresses China's commitment to building a secure and open cyberspace as secure that reflects the values of transparent, democratic and multilateral governance, as stipulated in the text of the law (gov.cn 2016). In addition, the Chinese Government is encouraging the adoption of various skills training policies in the field of cybersecurity, encourages international talent exchanges and supports companies and research institutions to participate actively in the national network security standards' design. Regarding this process, the China Cyber Space Administration (CAC) is responsible for authorizing and testing all network products before they are marketed, ensuring that they meet the strict security standards imposed nationally (Cyberspace Administration of China 2017).

On 12 September 2022, major amendments to the China Cyber Security Act were introduced. These amendments introduced new fines and penalties for breaches of general network security rules. In addition, the administrative penalties for cybercrimes committed by critical infrastructure operators have been reviewed and several administrative sanctions and prohibitions for other illegal acts not mentioned in the previous administrative legislation have been added. The amendments to the Cyber Security Act underline China's commitment to strengthening cybersecurity and responding dynamically to emerging challenges in the field (gov.cn 2016).

Thus, the cybersecurity legislative framework as well as the CACC's objectives, through all subordinate agencies and entities, are meant to strengthen China's ability to control and regulate the national cyberspace. These structures not only enforce policy but also influence the cyber landscape, targeting both domestic and international audiences. It is important to reflect on the role these structures play in promoting cyber security as well as censoring online content, with a significant impact on freedom of expression and human rights in the digital age, especially when references are made to China's international cooperation in the field of cyber security. The following section will discuss some relevant introductory issues and themes, from the author's perspective, on China's strategy for international cybersecurity cooperation.

People's Republic of China's Strategy for International Cybersecurity Cooperation – Short Presentation of the Key Points and Challenges in Achieving the Strategy's Goals

China's Strategy for International Cooperation in Cyberspace (launched in 2015 but updated on a regular basis - last update: 2022) (Xinhua News Agency 2017) is in line with President Xi Jinping's belief that countries are interconnected, have common interests and must cooperate to achieve common goals of maintaining peace and security. Therefore, promoting openness and cooperation in cyberspace are common

interests, but also responsibilities of the entire international community.
The Chinese model of international cooperation (as it appears, officially, in all normative acts and especially in the speeches of Chinese leaders) is the promotion of a new kind of cooperation in international relations: *win-win*. This model is also present in the Chinese strategy for international cooperation in cyberspace.

In the text of the strategy, the phrase 网络强国 (*wǎngluò qiángguó*) is frequently found, which can be interpreted as an expression of the main objective of the strategy: the Chinese pathway to become a "cyber superpower" or "a national power in cyberspace", and among the secondary objectives of the strategy there is identified the need for a state to control and govern its own cyberspace (Xinhua News Agency 2017).

There are six objectives of the Chinese Strategy for International Cybersecurity Cooperation:

1. Defending national sovereignty and security in cyberspace.
2. Developing a system of new international rules and norms for cyberspace.
3. Promoting fair Internet governance: it advocates for fair and equitable international Internet governance.
4. Protecting the legitimate rights and interests of citizens: it focuses on protecting the rights and interests of individuals in cyberspace.
5. Promoting cooperation in the digital economy: it aims to strengthen cooperation in the digital economy at the international level.
6. Building relevant platforms for cultural cyberspace exchange: it emphasizes the importance of cultural exchanges in cyberspace (Xinhua News Agency 2017).

The strategy states that the Chinese state promotes international cooperation based on the principles stipulated in the UN World Summit on Information Society (WSIS) format: building an inclusive, people-centred and development-oriented information society (Sustainable Development 2016).

China's concrete initiatives in international cooperation in cyberspace, according to the strategy's action plan, include (Xinhua News Agency 2017):

- Promoting fair Internet governance: China has advocated for fair and equitable international Internet governance.
- Deepening cyber cooperation with other countries: China has worked to deepen cyber cooperation with the UN, US, Russia and the EU (joint activities, expert-level meetings and development of cooperation projects through digital economy initiatives).
- Cyberspace trade rule formulation and policy coordination: China has expressed support for the formulation of cyberspace trade rules and effective policy coordination between states.

- Enforcement of international law in cyberspace: China aims to enforce international law in cyberspace to strengthen its position in the global digital order.
- China will continue to organise the annual Wuzhen Summit (World Internet Conference) and other international conferences and forums: the Conference on Interaction and Confidence Building Measures in Asia (CICA), the Forum on China-Africa Cooperation (FOCAC), the China-Arab States Cooperation Forum, the Forum of China and the Community of Latin American and Caribbean States and the Asian-African Legal Consultative Organization.
- Discussions and consultations in the China-Japan-Korea format, ASEAN Regional Forum and Boao Forum on cyber policies will continue.
- China is promoting cooperation on cybersecurity within the Shanghai Cooperation Organization (SCO) and BRICS.

Nevertheless, in terms of advanced technologies, China aims to become a world leader in the field. This goal has a significant impact on global cyberspace. The article will further highlight China's strategic goals in the development of processors and other high technologies, as well as their effects on global cyberspace. To become a world leader in advanced technologies, China is advancing in reducing dependence on foreign technology products, especially those coming from the United States and other Western countries. This refers to the creation of domestic software and processors to replace imported products. So, an important step in this endeavour was to ban the use of Intel and AMD processors on government computers and servers (Zulhusni n.d.).

The Chinese government is investing substantially in emerging technologies such as artificial intelligence (AI), and *quantum computing*, among others. For example, China began building open-source RISC-V processors and launched quantum communications satellites. These processors are used in various industries, such as autonomous vehicles and artificial intelligence (Goswami 2023; Cheung 2023).

By exporting technology, its own standards, and promoting cyber sovereignty, China is seeking to increase its global influence. This also includes promoting the standards that support China's Internet governance model and active involvement in international standardisation organizations (Cary 2023). Thus, integrating Chinese technology into the vital infrastructures of other states can cause vulnerabilities, which can later lead to cyber espionage activities (Pleil 2023).

China's international cybersecurity cooperation strategy promotes the establishment of a world order in cyberspace, based on rules agreed upon by all members of the international community, highlights the need for expanded partnerships in cyberspace, supports international cooperation in combating cyber terrorism and cybercrime, and promotes reform of the global governance system of the internet. (Xinhua News Agency 2017).

Within the text of the strategy, special attention is attributed to public opinion and its presence in the online space. It is considered that the online presence of public opinion has become the most important task of Chinese propaganda, and as such, the need to maintain a "positive energy" online and offline is emphasized to "keep things under control" as mentioned in the text strategy (Xinhua News Agency 2017). Positive online advertising must be stronger than ever so that the Party's ideas always become the strongest voice in cyberspace. An important feature of China's cyber security is the Chinese government's strict control and supervision of the internet, as reflected also in Art.12, Chapter 1 of the PRC Cyber Security Law:

Any person and organization using the internet must comply with the Constitution and laws of the country, respect public order and social morality; must not jeopardize cyber security and may not use the internet to engage in activities that endanger national security, national honour and national interests; must not undermine national sovereignty, overthrow the socialist system, incite separatism, break national unity, support terrorism or extremism, promote ethnic hatred and ethnic discrimination, disseminate violent, obscene or sexual information, create or circulate false information to disrupt economic or social order or information that violates the reputation, confidentiality, intellectual property or other legitimate rights and interests of others and other such acts.

To ensure the successful implementation of Art.12, Chapter 1 cited above, China has developed the control and monitoring system known as the "Great Firewall". It involves monitoring users' online activity and blocking access to numerous international websites. By preventing the spread of information considered subversive or harmful, this centralised and comprehensive method seeks to maintain political and social stability. China monitors and censors the content that appears on the internet: it blocks or censors sensitive information about the government or human rights, users are monitored in detail for all their online activities, including browsing history, messages and posts on social networks; personal information such as phone numbers or identity cards are collected by internet service providers; Chinese websites are obliged to censor content deemed inappropriate, as well as to collaborate with authorities to track and report suspicious activities (Stanford n.d.).

Regarding international cooperation with other regions, China uses the BRICS platform (Brazil, Russia, India, China and South Africa, Iran, Egypt, Ethiopia and the United Arab Emirates) to promote cooperation in the field of cybersecurity. China has sought within this group to collaborate on joint projects to combat cybercrime and improve information security. In a broader approach, these efforts are part of a goal linked to building a network of alliances with developing countries and counterbalancing Western influence on global internet governance (Li 2018).

China has also made significant steps in cybersecurity cooperation with Thailand to create a safer cyberspace and protect citizens from malicious activities. This

collaboration includes information sharing, best practices and technological innovations to combat cyber threats (Saffa 2024).

In East Asia, countries such as India, Vietnam, Japan and South Korea consider China an aggressive cyber power, despite China's efforts to position itself as a leader in cyber cooperation through BRICS. These nations are concerned about China's ability to exploit cyber power for surveillance and espionage purposes, a situation that has generated regional tensions and spurred initiatives to strengthen cybersecurity (Wagner 2019).

Following this context, Vietnam and Japan have signed a cybersecurity agreement to combat China's aggressive cyber-attacks. This agreement is a consequence of both countries' concerns about China's cyber activities in the Indo-Pacific area (Yamaguchi 2021). Nonetheless, in January 2024, Vietnam discovered that China-supported advanced persistent threat groups (APTs), such as APT31, APT41, Grayling, Mustang Panda and SharpPanda, were involved in cyber espionage activities on Vietnamese governmental agencies. Japan has also intensified cyber defence cooperation with the United States, Australia and others, participating in NATO cyber exercises and signing cyber security agreements, in addition to that with Vietnam Singapore and Indonesia. Japan has regularly protested the presence of the Chinese Coast Guard near the Japan-controlled, but China-claimed Senkaku Islands, indicating a constant concern about China's cyber and military activities in the region (Truong 2024).
Unlike East Asian states, which are reluctant to cooperate on cybersecurity with the PRC, the Russian Federation and the Solomon Islands, as well as Thailand, are open to cooperation with China and have already taken steps in this direction.

As for the relationship with the Russian Federation, since 2017, the Chinese Cyber Space Administration (CAC) has been working with Roskomnadzor, the Russian internet regulatory and censorship authority. This cooperation demonstrates that the two states share similar views on internet control and surveillance. It is also part of a broader effort to promote cyber sovereignty and counter Western influence in terms of governance of international cyberspace (Kremlin 2017).
In 2023, China and the Solomon Islands signed a cooperation agreement in the fields of cybersecurity and police. This agreement is part of China's efforts to expand its influence in the South Pacific by providing technical assistance and training in cybersecurity (Smith 2023).

Regarding cooperation in the field of cybersecurity between China and the EU, although there have been several discussions on cooperation on cyberspace between the EU and China, so far, there is still no real cooperation between the Union and China. In the negotiating process on cooperation, efforts have been for cooperation in the digital field, including the development of a common framework for the governance of electronic data (EIAS 2023). These efforts are the result of mutual

recognition of the potential benefits of collaborating in combating cybercrime, promoting digital commerce and protecting critical infrastructures (European Commission 2019).
The difficulty of China-EU cooperation is also caused by China's malicious cyber activities, carried out by state actors against the EU, which will be detailed further in this section. As a result of these incidents, the EU has asked China in 2021 to take adequate measures to stop these activities. (European Council 2021).

Although in 2015, during the Obama administration, the US and China reached an important agreement by which they pledged to refrain from cyber economic espionage in both states (The White House 2015), China is still involved in numerous cases of cyber espionage targeting government and private companies. The APT10, APT31 and APT41 groups are recognized for their complex attacks on critical infrastructure and theft of intellectual property in the US and Europe. The following are some cases of Chinese cyber espionage that have a major impact on China's international cooperation in the field of cyber security and represent another facet of the challenges China faces in international cybersecurity cooperation.

The Chinese state-sponsored cyber espionage group, APT10, also known as Cicada or Stone Panda, has been active for over a decade, with the main objective of spying on technology and defence companies in the US and Europe. The "Operation Cloud Hopper" (2014-2018) campaign is an example of this regard, targeting the Managed Service Providers (MSPs) in several countries, such as the United States, Japan, Canada and Australia. APT10 penetrated MSP customer networks and stole technology and business secrets (CYWARE 2022; Vijayan 2017).

Several cyber security reports and official sources have confirmed the link between China's State Security Ministry and the APT10 cyber-attack group. The first report was made in 2018 by an anonymous group of researchers named Intrusion Truth who published a report about Zhu Hua and Zhang Shilong as members of the APT10 group and linked to China's State Security Ministry. Nevertheless, cybersecurity company CrowdStrike has confirmed this fact, too (O'Donnell 2018). The U.S. government subsequently accused this group of infiltrating the networks of more than 45 US technology companies and government agencies and stealing private data, including information about U.S. Navy personnel (Office of Public Affairs 2018). In December 2018, the United Kingdom and its allies publicly revealed that the APT10 group acted on behalf of China's State Security Ministry (MSS) to launch large-scale cyber campaigns targeting intellectual property and commercial sensitive data in Europe, Asia and the United States (National Cyber Security Centre 2018).

Besides APT10, other hacking groups are believed to be linked to China's Ministry of State Security, such as APT31 and APT41.
APT31 (Zirconium, Judgment Panda, Bronze Vinewood, Red Keres) is a hacking group notorious for stealing sensitive data and intellectual property. This group

has been involved in cyber-attacks targeting journalists, politicians, academics and governmental institutions, as well as security companies and public institutions. The US and UK have claimed that APT31 is a weapon of China's Ministry of State Security - used by the Security Department of Hubei Province, Wuhan and was developed to detain critics of the Chinese regime and compromise government institutions (gov.uk 2024; US Department of the Treasury 2024).

In 2021, APT31 attacked the UK Electoral Commission's systems, obtaining the personal data of around 40 million voters (Yerushalmy 2024) and was involved in attacks on critical US infrastructure (defence and energy). APT31 was accused, also of hacking Microsoft Exchange email server software and the personal emails of campaign staff working for Joe Biden in 2020 (Office of Public Affairs 2024).
As a result of these attacks, the US and UK governments have sanctioned individuals and organizations related to the APT31 group, including Wuhan Xiaoruizhi Science and Technology Company Limited, which facilitated the MSS cyber operations (UK GOV 2024; US Department of the Treasury 2024).

Another Chinese cyber-espionage group, APT41, also known as Double Dragon, combines state-sponsored espionage with cybercrime for financial purposes. This group has worked in many industries such as telecommunications, high technology and health (Fraser, et al. 2019).
A high-profile case of APT41's actions is the attack that targeted the software company NetSarang in 2017. Back then, the group injected malicious code into a software update package that was signed with a legitimate NetSarang certificate. Hundreds of businesses around the world were affected by the attack (Mandiant 2022).

The United States Department of Justice filed charges against seven APT41 members in 2020 for cyber-attacks targeting technology, telecommunications and health companies, as well as for theft of intellectual property and sensitive data (Office of Public Affairs 2020). Nonetheless, in March 2021, in the case of the cyber-attack that targeted Microsoft's email software, attackers used a previously undetected vulnerability to gain remote access to email boxes. NATO, the European Union, Australia, New Zealand and Japan have officially attributed the attack to state-sponsored Chinese actors, the group known as Hafnium (GMF 2021).

Given the above, one can see the complexity of assuming the fulfilment of all the objectives set out in China's strategy for international cooperation in the field of cybersecurity. China claims that every nation has the right to have control over its national cyberspace and uses this discourse internationally intending to protect national interests and the state from external influence, due to geopolitical conflicts with the United States and other Western countries (Shen 2016). At the opposite pole, to ensure an open and free cyberspace, the European Union is advocating a multi-stakeholder cyber governance model, such as public-private cooperation with NGOs and international academic institutions.

Conclusions

The study responded to the research question launched following the hypothesis and shows that China's desire to protect its cyber sovereignty and to strengthen its super cyber power position, as well as domestic legislation based on both internal and external monitoring of databases belonging to Chinese citizens, have a major impact on the strategy of international cyber security cooperation. Nonetheless, challenges arise in meeting the objectives proposed in the strategy of international cooperation in the field of cybersecurity, such as cyber espionage carried out by Chinese state actors.

China's goal of protecting critical infrastructures and personal data of Chinese citizens is highlighted by the China Cyber Security Act, the Personal Data Protection Act and the recent amendments to the two laws. Although these acts were essential to creating an atmosphere of international collaboration, along with the International Cyber Security Cooperation Strategy, some countries in East Asia, the US and Europe have expressed concern about China's objectives, accusing China of cyber espionage and excessive surveillance.

China's desire to protect its cyber sovereignty is a key component of its international cyber security cooperation strategy. China is seeking to strengthen its position as a cyber superpower and to protect its interests by implementing a transparent and multilateral Internet governance system. Contrary to China's desire, many states and international organizations do not trust China's efforts to build a global Internet governance system. Accusations of using technology for internal surveillance, regularly conducting cyber-attacks as a state actor or concerns about domestic intelligence monitoring and control practices have affected China's objectives in international cybersecurity cooperation, as potential partners are reluctant to the Chinese government's intention of openness and sincere collaboration.

In this brief introductory study, in addition to references to the legislative framework on cybersecurity in China, a presentation was made of the governmental structures dealing with cyberspace security in China. The study concluded that all those structures are interdependent and coordinated hierarchically by the Central Commission for Cyber Space Affairs (CCAC) of the Communist Party of China. Therefore, the CCP committee governs the activities of cyber-related agencies and entities (CAC, CNNIC, CNCERT, TC260 and CSAC) and traces the priority lines for the implementation of strategies in the field.

This hierarchical structure influenced by the CCP has also caused the reluctance of foreign countries to identify increasing threats from Chinese state-controlled groups, such as APT10, APT31 or APT41, which mainly aim at cyber espionage of critical and national-interest infrastructures in areas such as military, telecommunications, health or energy, according to the cyber security reports mentioned throughout the article.

In conclusion, China is in an extensive process of demonstrating its cyber superpower capacity, to contribute to the creation of a safer cyberspace, but with the clear objective at the same time of maintaining a secure cyberspace at the national level that positively reflects all the actions of the CCP.

References

ABC News. 2015. *US and China Reach Agreement to Stop Commercial Cyber Espionage.* https://abcnews.go.com/US/us-china-reach-agreement-stop-commercial-cyberespionage/story?id=34041002.

Atlantic Council. 2023. *The 5×5—China's cyber operations.* https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/.

CAC (Cyberspace Administration of China). n.d. **中央网**络安全和信息化委员会办室. https://wap.cac.gov.cn/.

Carolan, Ciara. 2024. *Europe and Belgium are 'unresponsive' in the face of Chinese cyber-attacks, says hacked MP.* https://www.brusselstimes.com/983253/europe-and-belgium-are-passive-in-the-face-of-chinese-cyber-attacks-says-hacked-mp.

Cary, Dakota. 2021. *China's National Cybersecurity Center. A Base for Military-Civil Fusion in the Cyber Domain.* https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/.

—. 2023. *Community watch: China's vision for the future of the internet.* https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/.

CCTV News. 2023. *Strategy for International Cooperation in Cyberspace.* https://news.cctv.com/2023/11/07/ARTILliq1FlQi0B7msdoKsBn231107.shtml.

Cheung, Sunny. 2023. *Examining China's Grand Strategy For RISC-V.* https://jamestown.org/program/examining-chinas-grand-strategy-for-risc-v/.

Chinese Embassy in UK. 2011. *China's Perspective on Cybersecurity.* http://gb.china-embassy.gov.cn/eng/ambassador/dsjhjcf/2011lr/201106/t20110602_3386103.htm.

Chinese Ministry of Education. 2017. *Management Measures for the Demonstration Project of Building a First-Class Cibersecurity College.* http://www.moe.edu.cn/srcsite/A16/s3342/201708/t20170815_311176.html.

CNCERT/CC (National Computer network Emergency Response technical Team/Coordination Center of China). n.d. **国家互**联网应急中心. https://www.cert.org.cn/publish/main/34/index.html.

CNNIC (China Internet Network Information Center). n.d. **中国互**联网络信息中心. https://www.cnnic.com.cn/.

Consiliul de Stat al Chinei. 1994. *Regulations of the People's Republic of China on Computer Information System Security Protection.* https://www.gov.cn/gongbao/content/2011/content_1860849.htm.

Creemers, Rogier. 2023. *Cybersecurity Law and Regulation in China: Securing the Smart State.* https://brill.com/view/journals/clsr/6/2/article-p111_001.xml.

Cyber Security Association of China (CSAC). n.d. 中国网络空间安全协会. https://www.cybersac.cn/.

Cyberspace Administration of China. 2017. 关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告 *[Announcement on the release of the "Catalogue of Critical Network Equipment and Network Security Special Products (First Batch)"].* https://www.cac.gov.cn/2017-06/09/c_1121113591.htm.

CYWARE. 2022. *APT10: A Chinese Threat on a Global Espionage Mission.* https://cyware.com/resources/research-and-analysis/apt10-a-chinese-threat-on-a-global-espionage-mission-56fe.

Dandong, Han. 2019. *Legal Daily.* http://epaper.legaldaily.com.cn/fzrb/content/20190729/Articel04004GN.htm.

EIAS. 2023. *EU Digital Dialogue and Cooperation with China: The Way Forward?* https://eias.org/publications/op-ed/eu-digital-cooperation-with-china-the-way-forward/.

European Commission. 2019. "EU-CHINA - A Strategic Outlook." https://commission.europa.eu/system/files/2019-03/communication-eu-china-a-strategic-outlook.pdf.

European Council. 2021. *China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory.* https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/#:~:text=We%20continue%20to%20urge%2.

Fraser, Nalani, Fred Plan, Jacqueline O'Leary, Raymond Leong Vincent Cannon, Dan Perez, and Chi-en Shen. 2019. *APT41: A Dual Espionage and Cyber Crime Operation.* https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation.

Fulton Library. n.d. *Quantitative Research Methodologies.* https://uvu.libguides.com/methods/quantitative.

GMF. 2021. *NATO, EU, and allies attribute email intrusion to Chinese state-backed hackers.* https://securingdemocracy.gmfus.org/incident/allies-attribute-email-hack-to-china-backed-hackers/.

Goswami, Namrata. 2023. *China Prioritizes 3 Strategic Technologies in Its Great Power Competition.* https://thediplomat.com/2023/04/china-prioritizes-3-strategic-technologies-in-its-great-power-competition/.

gov.cn. 2016. 中华人民共和国网络安全法_滚动新闻_中国网 *[Cybersecurity Law of the People's Republic of China].* https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.

gov.uk. 2024. *UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity.* https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity.

Guo, Meirong. 2018. "China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces." *International Journal of Critical Infrastructure Protection* vol. 22: pp. 139-149. doi:10.1016/j.ijcip.2018.06.006.

Handler, Simon. 2023. *Atlantic Council.* https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/.

Hmaidi, Antoni. 2023. *"Here to stay" – Chinese state-affiliated hacking for strategic goals.* https://merics.org/en/report/here-stay-chinese-state-affiliated-hacking-strategic-goals.

Julian, Nicholas. 2021. *United States' and China's Cybersecurity Policies: Collaboration or Confrontation?* https://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation.

Kremlin. 2017. *Russia and China Enhance Cybersecurity Cooperation.* https://www.kremlin.ru/events/president/news/55842.

Li, H. 2018. "BRICS and the Internet: Building a New Global Consensus." *International Affairs* 94 (5): 1125-1145.

Mandiant. 2022. *APT41 (Double Dragon): A Dual Espionage and Cyber Crime Operation.* https://www.mandiant.com/resources/reports/apt41-double-dragon-dual-espionage-and-cyber-crime-operation.

MFA CN (Ministry of Foreign Affairs of the People's Republic of China). 2017. *Ministry of Foreign Affairs Holds Briefing for Chinese and Foreign Media on President Xi Jinping's State Visits to Russia and Germany and Attendance at 12th G20 Summit.* https://www.fmprc.gov.cn/mfa_eng/topics_665678/2017zt/XJPDEDFWBCXGEODSECFH/201707/t20170704_703649.html.

—. 2023. *Proposal of the People's Republic of China on the Reform and Development of Global Governance.* https://www.fmprc.gov.cn/eng/wjbxw/202309/t20230913_11142010.html.

National Cyber Security Centre. 2018. *APT10 continuing to target UK organisations.* https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations.

NPC.GOV.CN. 2021. "Data Security Law of the People's Republic of China." http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html.

O'Donnell, Lindsay. 2018. *APT10 Under Close Scrutiny as Potentially Linked to Chinese Ministry of State Security.* https://threatpost.com/apt10-under-close-scrutiny-as-potential-chinese-ministry-of-state-security-contractor/137139/.

Office of Public Affairs. 2024. *Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians.* https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived.

—. 2020. *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally.* https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

—. 2018. *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information.* https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

Pleil, Helen. 2023. *Being a Cyberpower – China's Ambitions in Cyberspace.* https://www.techpolicy.press/being-a-cyberpower-chinas-ambitions-in-cyberspace/.

PwC Indonesia. 2023. *A comparison of cybersecurity regulations: China.* https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html.

Saffa, Azizah. 2024. *Thailand and China Strengthen Cybersecurity Cooperation.* https://opengovasia.com/2024/05/29/thailand-and-china-unite-for-cyber-resilience/.

Shen, Yi. 2016. "Cyber Sovereignty and the Governance of Global Cyberspace." *Chinese Political Science Review* vol. 1: pp. 81-93. https://doi.org/10.1007/s41111-016-0002-6.

Smith, J. 2023. *China and Solomon Islands Sign Security Pact.* https://www.theguardian.com/world/2023/apr/12/china-and-solomon-islands-sign-security-pact.

Stanford. n.d. *Free speech vs Maintaining Social Cohesion.* https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.

Sustainable Development. 2016. *World Summit on the Information Society (WSIS).* https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170.

TC260 (National Cybersecurity Standardization Technical Committee). n.d. 全国网络安全标准化技术委员会. https://www.tc260.org.cn/.

The White House. 2015. *U.S.-China Cyber Agreement.* https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/us-china-cyber-agreement.

Thomas, Nicholas. 2009. "Cyber Security in East Asia: Governing Anarchy." *Asian Security* 5 (1): 3-23.

Truong, Sylvie. 2024. *Chinese espionage campaigns and cyberattacks on critical infrastructure in Southeast Asia.* https://thereadable.co/chinese-espionage-campaigns-and-cyberattacks-on-critical-infrastructure-in-southeast-asia/.

UK GOV. 2024. *UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity.* https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity.

US Department of the Treasury. 2024. *Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure.* https://home.treasury.gov/news/press-releases/jy2205.

Vijayan, Jay. 2017. *China-Based Threat Actor APT10 Ramps Up Cyber Espionage Activity.* https://www.darkreading.com/cyberattacks-data-breaches/china-based-threat-actor-apt10-ramps-up-cyber-espionage-activity.

Wagner, B. 2019. "Cybersecurity in East Asia: Government Policies and Sectoiral Responses." *Journal of Cyber Policy* 4 (1): 55-72.

Xinhua. 2019. http://www.xinhuanet.com/yuqing/2019-01/04/c_1210030391.htm.

Xinhua News Agency. 2017. 网络空间国际合作战略 *[Cyberspace International Cooperation Strategy]*. http://www.xinhuanet.com/politics/2017-03/01/c_1120552767.htm.

Yamaguchi, Mari. 2021. *Japan, Vietnam Look to Cyber Defense Against China.* https://thediplomat.com/2021/11/japan-vietnam-look-to-cyber-defense-against-china/.

Yerushalmy, Jonathan. 2024. *China cyber-attacks explained: who is behind the hacking operation against the US and UK?* https://www.theguardian.com/technology/2024/mar/26/china-cyber-attack-uk-us-explained-hack-apt-31.

Zhang, Duanhong, Wenjia Ding, Yang Wang, and Siwen Liu. 2022. *Exploring the Role of International Research Collaboration in Building China's World-Class Universities.* https://doi.org/10.3390/su14063487.

Zulhusni, Muhammad. n.d. *China's new tech policies challenge Intel and AMD in a shifting landscape.* https://techwireasia.com/03/2024/chinas-tech-shift-what-it-means-for-the-future-of-intel-and-amd/.