The Influence of China's Political System on Cybersecurity Governance and Strategy

Venencia Paidamoyo Nyambuya
Nirmala Devi Gopal
Department of Criminology & Forensic Studies
University of KwaZulu-Natal
Durban, South Africa

Received: 11 June 2024
Revised:
Accepted: 8 November 2025

Abstract

This article delves into the intricate relationship between China's autocratic system and its cybersecurity landscape, examining the extent to which the former influences the development of frameworks, strategies, and responses to cyber threats. Drawing upon a comprehensive analysis of China's political structure, cybersecurity policies, and historical context, this study investigates how authoritarian governance shapes the nation's approach to cybersecurity. Methodologically, the article adopts a qualitative approach, drawing on a systematic review of scholarly literature, official publications, and case studies of major cyber incidents to identify recurring patterns and insights. By exploring key factors such as government control, censorship mechanisms, and prioritisation of state interests, it sheds light on the unique challenges and opportunities presented by China's autocratic system in safeguarding its digital infrastructure. Additionally, this research assesses the implications of these dynamics on international cybersecurity norms and global cyber governance. Through a nuanced exploration of these interconnections, this article offers valuable insights into the complex interplay between political systems and cybersecurity strategies in an increasingly digitised world.

Keywords: cybersecurity, China, political system, authoritarian governance, cybersecurity governance, cybersecurity strategy.

Introduction

China offers a different socio-political structure that is more influential on the dynamics of cyberspace. The case of China illustrates the importance of socio-cultural factors, the authoritarian, single ruling party structure and their impacts on cybersecurity strategy. The People's Republic of China (PRC) was founded in 1949. It is a socialist State that is governed by the democratic dictatorship of its citizens. Specifically, it is an autocratic or even totalitarian governed State (Wang, 2023). At the end of a 22-year civil war, the Chinese Communist Party (CCP) won the right to the Chinese mainland territory, forcing the Nationalist Party (Kuomintang or KMT) to go into exile to the island of Formosa, which is modern-day Taiwan (Loo, 2021). Both states grew into authoritarian regimes through the second half of the 20th century: The Republic of China in Taiwan favoured a right-wing, capitalist dictatorship backed by the U.S., whereas the People's Republic of China, on the mainland, birthed a Marxist-Leninist communist regime based upon the ideology of its founding father, Mao Zedong (Vochelet, 2021).

China's political system is commonly described as authoritarian, but a more precise understanding situates it within the framework of a Marxist-Leninist single-party state under the Chinese Communist Party (CCP) (Tang, 2016). Unlike liberal democracies, power is highly centralised; the CCP controls the state, military, judiciary, and media, leaving minimal space for political pluralism or opposition

(Cabestan, 2017). Decision-making is top-down, with key policy directions and governance strategies emanating from the Party's leadership bodies, particularly the Politburo Standing Committee (Li & Zhou, 2019). In practice, this structure exhibits characteristics often associated with dictatorships, limited electoral competition, suppression of dissent, and strict control over civil society and the press (Tang, 2016). Zeng (2014) argues that labelling China solely as a dictatorship oversimplifies the system. The CCP combines ideological governance with technocratic management, blending Marxist-Leninist principles of party leadership with pragmatic policy implementation aimed at economic development, social stability, and international influence (Zeng, 2014).

China's political structure directly shapes its approach to cybersecurity and digital governance. Thus, centralised control allows the CCP to implement comprehensive cybersecurity laws, surveillance programs, and data governance frameworks with relative speed and uniformity (Nantieh, 2020). The intertwining of party authority with state institutions ensures that cybersecurity is not merely a technical or defensive concern but a political instrument for maintaining social control, safeguarding state interests, and asserting sovereignty in cyberspace (Wang, 2020). Though popular uprisings struck both countries in the 1980s, their outcomes were different. While the rebellion in Taiwan led the country into the "third wave" of democratisation, the Tiananmen Square uprisings in Mainland China led to a regime reconfiguration (Vochelet, 2021).

A Qualitative Research Approach

This study adopts a qualitative research approach, combining a systematic review of scholarly literature, official government publications, policy briefs, and credible media reports with case-study analysis of significant cyber incidents. Sources were selected based on relevance, credibility, and recency, focusing on developments in China's cybersecurity policies, domestic cybercrime, and transnational cyber threats from the early 2000s to 2023. The inclusion criteria encompassed sources that provided detailed information on China's cybersecurity laws, strategic policies, cyber incidents, and governance practices. Speculative sources, lacked verifiable evidence, or were outside the year 2000 –2024 timeframe were excluded.

Data were analysed thematically, identifying recurring patterns, trends, and insights regarding China's cybersecurity governance, state-driven cyber operations, and the broader geopolitical implications of its strategies. Cross-referencing multiple sources enhanced reliability, while integrating academic perspectives ensured a comprehensive and balanced understanding. This methodology provides a structured lens to examine China's cybersecurity framework while situating it within the global digital governance landscape and ongoing debates on cyber power and state control.

Development of Cyberspace and Cybersecurity in China

Over the past three decades, the CCP has developed one of the world's most sophisticated digital governance systems, the Social Credit System (SCS), which has contributed to making China one of the most controlling authoritarian regimes globally (Hou & Fu, 2024). The SCS centralises vast amounts of data on Chinese citizens, including financial behaviour, social interactions, and online activity, allowing the state to monitor, assess, and influence individual and organisational behaviour (Liang, Das, Kostyuk & Hussain, 2018). While this system has attracted significant criticism from Western democracies and international human rights organisations for its implications on privacy, freedom of expression, and civil liberties, its most striking feature may be the widespread compliance among the Chinese population.

Compliance with the SCS is not merely passive; it reflects a complex interplay of social, political, and psychological factors that reinforce authoritarian resilience (Gilley, 2003). Citizens internalise

the norms promoted by the system, adapting behaviours to align with state expectations and avoiding penalties that could limit access to services, travel, or employment opportunities (Hou & Fu, 2024; Kostka & Antoine, 2020). This dynamic creates a feedback loop in which state surveillance and social incentives mutually reinforce obedience, thereby stabilising the regime and reducing overt opposition.

Moreover, the SCS exemplifies how technology and authoritarian governance intersect: it is not just a tool for monitoring or punishment but a mechanism for shaping societal behaviour in alignment with state-defined goals (Liang & Chen, 2022). It highlights the CCP's ability to integrate ideological control with advanced technological infrastructure, demonstrating that contemporary authoritarian resilience relies as much on data-driven governance and social engineering as on traditional coercive instruments (Baldin, 2022). Understanding the SCS is therefore critical for analysing China's approach to cybersecurity, digital governance, and the broader exercise of power in a highly centralised, Marxist-Leninist system.

Generally, authoritarian resilience can refer to a state's ability to maintain illiberal top-down structures that subjugate its controlled population, further legitimising and reinforcing this hierarchy (Vochelet, 2021). The CCP is the sole governmental party, and it claims leadership on everything in China, meaning it controls state administration, the private sector and civil society (Grünberg & Drinhausen, 2019). In the aftermath, its human rights record has been suspect. According to The Economist Intelligence Unit's Democracy Index (2020: 3), "China experienced a fall of 23 places, landing at 153rd out of 167 countries on the global rating". However, this figure only partially reflects the entrenched authoritarian reality of the Chinese state. Beyond a numerical downgrade, China's low ranking embodies systematic violations of fundamental human rights, including pervasive mass surveillance, extensive censorship, and the arbitrary detention of dissenting voices (Pei, 2024). These practices demonstrate that China's cybersecurity strategy is not a neutral or purely defensive measure, but an extension of state power designed to maintain political control (Hulvey, 2022). In this sense, the global democracy ranking is less a technical measurement than a signal of the deeper erosion of democratic freedoms, situating China's cybersecurity framework in direct conflict with international human rights norms.

For instance, leveraging cyberspace and Artificial Intelligence (AI), the Mainland Chinese State at the turn of this century (in 2014 specifically) deployed the Chinese Social Credit System (SCS) (社会信用体系) as a means of social control of the entire citizenry. The SCS has been described as one of the most sophisticated software systems that has made the People's Republic one of the most controlling existing authoritarian regimes (Vochelet, 2021: 2; Orgad & Reijers, 2020). It is a form of 'cybernetic citizenship', that is, a "mere nodes of sociotechnical networks under corporate or government control" (Orgad & Reijers, 2020). This is software programmes, hinged on the socio-cultural factors and "Asian values", which centralises the majority of Chinese citizens' data to enhance surveillance and deepen the authoritarian grip of the ruling party (Vochelet, 2021: 2).

The SCS, still being developed by the biggest technological companies in China, "aims at centralising big data on all Chinese citizens in one application, offering a detailed profile on many individuals' characteristics, ranging from household information or health profile to credit balance" (Ibid). Through the centralised surveillance system, the State can measure behaviour, social and commercial transactions of individuals through the "social credit score". Those able to pool high scores (1050) are rewarded and showcased as models for others. Others below the benchmark (minus 849) are restricted from basic social benefits – like air travel, train tickets, fast internet access and so on. Citizens who are rated below average (549) are blacklisted "and publicly shamed as bad citizens" (Vochelet, 2021).

Cyberspace and cyber threats in China

The SCS model suggests a centralised State with a firm grip on all citizens, including dissidents and cybercriminals alike. But that position is significantly far from reality. Note that China has the largest internet user demographic and one of the largest internet markets worldwide. The scale and impact of cybercrime in China have grown significantly in recent years. In 2022, the country recorded over 342,800 cyberattacks, affecting sectors ranging from government and military to healthcare, with weekly incidents ranging between 1,300 and 2,400. The economic cost of cyberattacks in China was estimated at USD 1.24 trillion in 2023, and projections indicate it could reach USD 1.79 trillion by 2024 (sci-tech-today.com). In terms of law enforcement, computer crimes increased by 36.2% in 2023, involving roughly 323,000 individuals, while telecom fraud indictments rose nearly 67% to 51,000, and overall arrests related to cybercrime surged 47% to 726,000 (AP News, 2023). These challenges are compounded by China's vast internet user base, which reached 1.123 billion (79.7% of the population) as of June 2025, with 99.7% accessing the internet via mobile devices (CIW News, CNNIC, 2025). These figures highlight both the growing prevalence of cybercrime and the immense scale of China's digital ecosystem, highlighting the complexity of regulating and securing cyberspace in the world's largest internet market.

Interestingly, "apart from extended access to broadband internet connections, mobile internet took up a large share in internet user growth. The share of users accessing the internet via mobile devices had significantly exceeded that of those via desktop in the country. About 99.6 % of Chinese internet users accessed the web via mobile phone" (Thomala, 2023). For comparison, the global average internet penetration rate had resided at about 64.4 per cent as of January 2023. The internet penetration in China had also been above the average rate in the Asia-Pacific countries. However, neighbouring countries such as Japan and South Korea had displayed substantially higher internet penetration rates than China. It is worth noting that the internet usage in the country has faced a large regional disparity. Some of the remote western regions had shown penetration rates of below 45%.

To put things in context, cybercrime in China has two broad perspectives: there are cybercrimes committed in China and other international cybercrimes originating from China, which has been a major diplomatic row discouraging foreign Internet firms from operating in the country (Kshetri, 2013[b]). The country's security and cyberwarfare possibility is assessed to be not as formidable as they would have the world believe. In 2015, there were found to be 126,196 cybersecurity incidents, with 126,424 cases coming from within China. (Qi et al, 2018). Thus, cybercrime in China is framed in the Criminal Law and defined with the following offences: illegally accessing computer systems; illegally accessing or controlling data held on computer systems; providing programmes and tools to access or illegally control computer systems; destroying computer systems; committing financial crimes using a computer (Erqi, 2023). The Chinese law enforcement authorities collaborate and have formed networks with more than 70 countries, as well as Interpol (Calcara, 2020).

According to official disclosure, the scale of the cybersecurity industry in China exceeded 200 billion yuan ($29.23 billion) in 2021 and grew at an annual average of 15% from 2016 to 2020 (van Wyk, 2022). A special report on judicial big data shows that the number of cases involving information network crimes has increased year by year, with fraud accounting for the highest proportion (Ibid). The report noted that the number of cybercrime cases has increased since 2017, and over 40% of the cases involved online fraud. From 2017 to 2021, China's courts handled more than 282,000 cybercrime cases involving a total of 282 different crimes, of which fraud accounted for the highest proportion (36.53%). Online fraud cases mostly focused on fake loans, impersonation, and false recruitment. Over the same period, more than 660,000 defendants were involved in cybercrime cases across the country, with an average of about 2.4 defendants per case. Most of the defendants

were aged between 18 and 40, and the proportion aged between 18 and 28 has increased since 2019, while the proportion of those aged above 29 has decreased (van Wyk, 2022).

According to the special report on judicial big data, there were 72,000 cases involving 143,700 defendants (90% of whom were born after 1980) related to the crime of assisting online criminal activity, such as by providing technical support, including internet access, server hosting, network storage, or by providing advertising, payment, and settlement. This criminal activity took off from 2020 with a year-on-year increase of 34 times and increased by a further 17 times in 2021 (van Wyk, 2022). The report indicates that the number of cybercrime cases filed by the ministry decreased year-on-year for nine consecutive months from June 2021, and 42,000 bank card gangs, as well as 440,000 criminal suspects, have been investigated. The official also revealed that many of the ministry's cybercrime investigations have focused on Chinese nationals operating from neighbouring countries. The ministry has dispatched working groups to countries such as Cambodia, the United Arab Emirates, and Myanmar to carry out cross-border cybercrime investigations and has repatriated around 36,000 suspects from abroad (van Wyk, 2022).

Cybercrimes from China to the world

China has more often than not been on the offensive in its cyber operations. In fact, China was suspected to be the country which had been spying the most in the world (Attenberger, 2022: 53). Experts estimated that between 2005 and 2010, the Chinese were responsible for 60% of all industrial spy activities (Scheidges & Schürmann, 2010). Also, China is criticised for having outsourced its cyber activities to non-state actors, like cybercriminals, who act outside the law or capitalise their activities (Attenberger, 2022). Though the Chinese government commonly blames foreign hackers for cyber-attacks targeting the country, data proxies and indicators from a number of sources across a long time period indicate that substantial cyber-attacks originate in China (Kshetri, 2013[b]). There are a handful of examples to glean from, even in the most recent times.

The February 2023 high-altitude balloon incident illustrates how China's technological and surveillance capabilities extend beyond cyberspace into physical and cross-border intelligence operations (Glebsy & Lackenbauer, 2024; Borger, 2023). While presented as a civilian weather balloon, the device carried equipment consistent with intelligence collection, highlighting the dual-use nature of such technologies. This case reflects a broader pattern in which China integrates advanced technology into mechanisms of state control and information gathering, a strategy that complements its domestic cybersecurity infrastructure. Important to note is that in linking physical surveillance platforms with digital intelligence networks, China's approach exemplifies how state-led cyber and technological strategies are embedded within a framework of political oversight, social control, and strategic influence, both domestically and internationally.

As that was unfolding, the annual global threat report alleged China-linked cyberespionage groups targeting 39 industries on nearly every continent (CrowdStrike, 2023). About a quarter of the hacking was aimed at North America, while most of it targeted China's Asian neighbours, the report found. The techniques China used have become increasingly sophisticated as cybersecurity has improved, the report found. "U.S. officials say China, like the U.S., hacks into the networks of its adversaries to gather intelligence. But they say China also hacks private corporations to steal intellectual property, which the U.S. says it does not do. China consistently denies that, while a top American intelligence official once called Chinese hacking of Western companies "the greatest transfer of wealth in history" (Dilanian, 2023).

Earlier, in 2005 and 2009, China was ranked second behind the U.S. as, of the top countries for originating cyber-attacks (Kshetri, 2013[b]). According to the Anti-Phishing Working Group (APWG),

70% the world's maliciously registered domain names were established by the Chinese to attack domestic businesses (Ibid). In 2011H1, Chinese perpetrators established 11,192 unique domain names and 3,629 .cc subdomains for such attacks, the majority of which attacked Chinese companies, and 8% targeted Taobao.com. Likewise, according to APWG, China had the world's highest malware infection rate of 54.1% in 2012Q1.

There are other instances of insider cybercrimes in the West that have been blamed on China. In 2004, there was the 'Titan Rain' during which hackers entered military and research institutes in the U.S. and Great Britain. About 79,000 attacks were launched, out of which 1,300 were successful. The hacker group is suspected of coming from China because three routers established in the province of Guangdong were identified (Attenberg, 2022: 51). In 2005, a Chinese intern working in Valeo was detained in France for alleged database intrusion aimed at IP theft (Kshetri, 2013[b]). Between 2007 and 2008, there was the ShadyRat attack during which the United Nations, the United States, U.S. corporations, among others, were targets. The anti-virus vendor, McAfee, attributed the attack to China or Russia. The spy network is estimated to have retrieved data of 70 international organisations and corporations in that year (Attenberg, 2022: 52).

Between 2007 and 2009, cyberattacks such as GhostNet and Shadows targeted sensitive information from Tibetan exiles in India, the Dalai Lama, and Indian research and governmental institutions, resulting in the theft of confidential documents (Farwell & Rohozinski, 2011). Given the political context and longstanding tensions between China and the affected parties, these attacks have often been attributed to Chinese actors (Attenberg, 2022, p. 52). In 2009, Operation Aurora marked a significant cyber espionage campaign against major U.S. corporations, including Google and Yahoo, which provoked a diplomatic dispute between the United States and China. In the same year, the Lockheed Martin Corporation suffered data exfiltration that compromised sensitive information related to its military aircraft program (F-35), which has also been linked to Chinese cyber actors (Attenberg, 2022).

Similarly, a 2011 report entitled "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace" suggested that some Chinese companies used ethnic Chinese "insiders" to steal information from Western companies (Kshetri, 2013[b]). In 2011, a Chinese-born scientist was convicted of stealing trade secrets from Cargill and engaging in economic espionage at Dow AgroSciences. Cargill estimated that the information stolen by the scientist was worth US$12 million in R&D (Kshetri, 2013[b]). Similarly, a Motorola employee arrested by U.S. Customs in Chicago allegedly possessed a one-way ticket to China and proprietary information that was worth $600 million in about 1,000 electronic documents (Kshetri, 2013[b]). To take another example, an employee at Valspar Corporation, who was arrested in 2009, allegedly downloaded 160 formulas for paints and coatings, which were estimated to cost the company about $20 million in R&D or about one-eighth of the company's annual profits. Similarly, another chemist at DuPont downloaded data on organic light-emitting diodes, which he allegedly intended to transfer to Beijing University. It was also reported that China-based hackers attacked DuPont's computer networks two or more times in 2009 and 2010. In the same vein, a product manager at Ford Motor Company allegedly made unauthorised digital copies of about 4,000 documents, which would help him to get a job with a Chinese automobile company (Kshetri, 2013[b]).

Cybersecurity policy framework and strategy in China

The Chinese government has been hands-on in creating a large body of cybersecurity legislation to deal with digital crime, though more in an unconventional manner. In 2013, China addressed cybersecurity for the first time holistically (Jinghua, 2019). Three main legislations have since followed suit (van Wyk, 2022): Firstly Cyber Security Law that became active on June 1, 2017. The Law defined the concept of cyberspace sovereignty, and included specific provisions for network

operators, and for data localisation related to foreign companies operating in China. Secondly, the Data Security Law (DSL), effective from September 1, 2021. The Law classified data in terms of its relevance to national security, with implications on how data can be stored and transferred. Thirdly, the Personal Information Protection Law, effective from November 1, 2021. This includes provisions to regulate and promote the protection of personal information. A draft of the Personal Information Protection Law was published on the 21st of October 2020 and seems to be inspired by the European General Data Protection Regulation (GDPR). This draft defines personal information as "all kinds of information" related to identifiable natural persons and excludes information which has undergone anonymisation. It protects the personal information of natural persons handled by organisations and individuals in mainland China, as well as organisations and individuals outside of mainland China that are handling the personal information of natural persons who are physically located in mainland China. It also applies to products or services intended for natural persons in mainland China (Qi, 2021). (4) A fourth piece of legislation is focused on internet telecommunications fraud, and it is currently being reviewed for a third time, and it is expected to be promulgated soon (van Wyk, 2022).

The Cyber Security Law

In 2016, China enacted the Cybersecurity Law of the People's Republic of China to strengthen its cybersecurity framework (Aitel et al., 2022; Xu & Lu, 2021). President Xi Jinping repeatedly emphasised the importance of enhancing cybersecurity legislation as part of the broader national strategy. The law itself states that it seeks "to ensure cybersecurity, to safeguard cyberspace sovereignty, national security, and social and public interests, to protect the lawful rights and interests of citizens, legal persons, and other organisations, and to promote the healthy development of the informatization of the economy and society" (National People's Congress [NPC], 2016, art. 1). Similar to China's National Security Law, the Cybersecurity Law prioritises cyberspace dominion, highlighting the protection of network operations, critical information infrastructure, and online information as central to national security and state control.

The Chinese government plays an active role in international cyber cooperation to maintain cyberspace dominion whilst stimulating the development of the internet economy. A total of 46 international organisations from the USA, Asia, Europe, and Oceanic regions signed a letter to oppose the enactment of the Cybersecurity Law whilst it was in its draft stages, since they were concerned that the law would raise trade barriers. The law does not conform to international trade regulations; however, despite the apprehension by international organisations, and upon consultation with experts, China enacted the law stating that the law will be supplemented with regulations and standards in time, after there was an appeal to suspend the law by the international groups (Qi et al, 2018).

Indeed, the Cybersecurity Law does not solve any specific cybersecurity issues; rather, it provides a general configuration for dealing with cybersecurity concerns, and a means to build China's cybersecurity legal system. This means that supplementary rules and regulations are required to prevent ambiguity and provide more complete legal rules. Cyberspace sovereignty, being such a central principle of both the National Security Law and the Cybersecurity Law, encompasses four rights. These rights are:

(a) The right of jurisdiction, which refers to the nation's right to manage the networks within its territory. All cyber activities that occur within mainland China, despite the nationalities of those carrying out the activities, are subject to the law.

(b) The right of self-defence, which refers to the right of a state in dominion defending itself from threats and cyber-attacks from outside the state.

(c) The right of independence, which essentially means that countries should not interfere in another country's internal affairs and respect sovereignty;

(d) The right of equality refers to all countries having equal impact on the rules and international order of cyberspace, ensuring that no country harms another country's network whilst managing their own (Qi et al, 2018).

However, the cybersecurity laws and policies are not in isolation from the larger economic development and national security plans of the modern Chinese State (see Table 1 below). The autocratic *cum* top-down government has an eye on becoming the global hub for science and technology hub of the 21st century (The State Council of the People's Republic of China, 2006). In "China's Military Strategy", published in 2015, China articulates that its strategic goal is to complete the building of a moderately prosperous society in all respects by 2021 (The State Council Information Office of the People's Republic of China, 2015). Notably, China had defined Information Warfare (IW) as the eyes and ears of the services' military operation systems (Wu, 2006). The concept encompasses electronic warfare, network warfare, Command and Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance (C4ISR) and related matters (Wu, 2006), which in modern-day China would be considered cyber warfare (Jinghua, 2019).

Table 1: Cybersecurity strategy-related documents in China and their approaches

Year	Name of Document	Published by	Approach
2004	China's National Defence	The State Council	Active Defensive
2011	China's National Defence in 2010	Information Office of the State Council	Active Defensive
2013	The Science of Military Strategy	Academy of Military Science	Active Defensive
2015	China's Military Strategy	Information Office of the State Council	Active Defensive
2016	Full text of National Strategy for Security in Cyberspace	Cyberspace Administration	Active Defensive
2019	China's National Defence in the New Era	The State Council Information Office	Active Defensive

Source: Attenberg, 2022: 49-50.

It is fundamental to note that there is a restriction in access to information in China because it is controlled by the government (Wu, 2006; & Attenberg, 2022). However, the State has invested heavily in information warfare resources to further develop the field, engineering innovative weapon systems (Wu, 2006). A White Paper launched in 2004, called "China's National Defence", elaborates that "Informationalisation has become the key factor in enhancing the warfighting capability of the armed forces" (The State Council of the People's Republic of China, 2004). A principal feature on the battlefield would be the confrontation of ICTs (The State Council of the People's Republic of China, 2004). The updated document in 2011 communicated that China plans to build up its Army (The People's Liberation Army, PLA) to win informationised wars (The People's Republic of China, 2011). In order to adapt to the international and national security environment, China communicates in both strategies, its adherence to an overall active defensive military strategy (Attenberg, 2022).

Most of the related information scholars have about Chinese cybersecurity and national defence framework has been sourced through the West (Attenberg, 2022). In 2013, China addressed cybersecurity for the first time holistically (Jinghua, 2019). The Chinese Academy of Military Science (2013) composed a strategy called "The Science of Military Strategy", published by the Federation of American Scientists. China itself published only in 2015 a similar holistic strategy, called "China's Military Strategy" (The State Council Information Office of the People's Republic of China, 2015). China announces that they would not attack, but counterattack in case of an attack, referring to their active defence position (Attenberg, 2022: 46), "being one of the major victims in hacker attacks" (The State Council Information Office of the People's Republic of China, 2015:29). The "cyberspace has become a new pillar of economic and social development, and a new domain of national security" (The State Council Information Office of the People's Republic of China, 2015).

At the end of 2016, China announced it to publish a cybersecurity strategy (The State Council of the People's Republic of China, 2016), and it left no one in doubt of its intention. The strategy communicates a variety of strategic objectives, among them to "defend vigorously, respond effectively, promote peace, security, cooperation and order in cyberspace" (Creemers, 2016 & Attenberg, 2022: 47). "Wordings, such as "defend vigorously" and "respond effectively", point out that China is willing to hack back in case it gets attacked. It is an active defensive approach" (Attenberg, 2022: 47).

China's Cybersecurity Strategy: Ambitions, Threats, and Vulnerabilities

China has made its ambitions as a global cyber power unmistakably clear, aiming to establish itself as a cyber-hegemon. Persistent cyber threats within its borders, however, suggest ongoing vulnerabilities in its cyber defences, challenging the perception of an infallible system often portrayed in Western analyses. Allegations of state-linked cyber operations indicate that China pursues an active defensive posture, yet domestic and transnational cybercrime remains difficult to fully control.

China's Great Firewall, while effective at regulating domestic internet access, primarily challenges individual users attempting to bypass restrictions and is less effective as a deterrent against sophisticated cybercriminals. The management of cross-border cybercrime presents additional challenges, including the vastness of cyberspace, widespread use of VPNs, proxy services, and encryption technologies, and the complexities of coordinating with multiple jurisdictions with differing laws, languages, and procedural protocols. The increasing professionalism of cybercriminal networks, operating as coordinated "dark industry chains," further complicates law enforcement efforts (UNODC, 2022).

Transnational cyberattacks illustrate the practical limitations of China's cybersecurity governance. For example, in 2017, the WannaCry ransomware worm exploited Microsoft Windows vulnerabilities to infect hundreds of Chinese government agencies, universities, and businesses. More recently, during the COVID-19 pandemic, a range of malware attacks targeted Chinese institutions. Vietnamese hackers distributed Metaljack malware to Wuhan shortly after China alerted the World Health Organisation in January 2020, while Emotet malware was reportedly delivered under the guise of safety emails from a "Singaporean specialist." Subsequent attacks included Denial of Service operations on epidemic prevention units, phishing attacks targeting medical groups in India, and the global circulation of malware such as CXK-NMSL ransomware, AZORult, Dharma/Crysis, and MBR Wiper, often disguised as COVID-19-related communications (Lallie et al., 2020). Other attacks exploited applications and promotional offers to steal payment and login credentials, demonstrating the adaptability and creativity of cybercriminals in exploiting global crises.

Despite its active legal and regulatory measures, including the Cybersecurity Law and subsequent data protection frameworks, China continues to face structural challenges in controlling cybercrime. The United Nations Office on Drugs and Crime (UNODC, 2022) has highlighted three key limitations: (1) difficulty attributing and identifying perpetrators due to encryption, proxies, and VPN usage; (2) obstacles in international cooperation required for transnational evidence collection; and (3) increasing organization and sophistication of cybercrime networks, which operate collaboratively from planning through execution and revenue distribution. The UNODC recommends that China strengthen cross-border collaboration rather than rely solely on active defensive measures, which may inadvertently exacerbate collective threats.

Overall, while China demonstrates significant ambition and capability in cyber governance, the persistence of both domestic and transnational cyber threats highlights the complexity of balancing state control, cybersecurity defence, and international norms. The evidence underscores that China's cybersecurity strategy is not solely a technical endeavour but also an instrument of political oversight and social regulation, operating within the broader context of authoritarian governance and the challenges of global cyber interdependence.

Conclusion and Policy Implications

This study has examined China's cybersecurity framework, highlighting the intricate ways in which authoritarian governance shapes both domestic and international cyber strategies. China's approach reflects a dual objective: defending cyberspace against external threats while consolidating internal political control. While these strategies demonstrate significant technical and organisational capacity, persistent cyber vulnerabilities and transnational cyber threats highlight the limits of state-driven cybersecurity efforts.

The findings have several implications for policymakers, international organisations, and civil society.

- For China, enhancing transparency, aligning cybersecurity practices with international norms, and strengthening cross-border cooperation could reduce global tensions and improve the effectiveness of cybercrime prevention.
- For the international community, governments and multilateral organisations should develop frameworks to engage with China on cybersecurity standards, data governance, and threat mitigation, while safeguarding open internet principles and human rights.
- Civil society actors should monitor the deployment of surveillance technologies and advocate for digital rights, particularly in contexts where state-driven cyber governance is being exported.

The Global South, and African states in particular, face both opportunities and risks in adopting Chinese digital technologies through initiatives such as the Belt and Road Digital Silk Road (Eguegu, 2022). While these partnerships may enhance infrastructure and digital capacity, they also carry the potential for exporting digital authoritarianism, undermining democratic governance, and creating dependencies on surveillance-centric technologies. Policymakers in these countries should carefully assess these risks, invest in cybersecurity capacity-building, and implement safeguards to protect citizens' privacy and digital rights.

Finally, China's model is shaping international norms around data sovereignty, cross-border cybercrime, and internet governance. As the global debate over the rules of cyberspace continues, the Chinese approach offers both a case study and a challenge to open, multilateral internet governance. Its growing influence necessitates critical engagement from global actors to ensure that emerging cyber norms balance security, economic development, and the protection of fundamental

rights. In sum, understanding China's cybersecurity strategies is essential not only for assessing its domestic governance but also for anticipating their implications for the international cyber order and digital governance in the Global South.

References

Aitel, D., d'Antoine, S., Bulazel, A., DeSombre, W., Garcia-Camargo, I., Garwin, T., Roos, I., Rostow, N. and Wagner, A., 2022. China's Cyber Operations.

Baldin, B., 2022. Beyond authoritarianism: AI-based surveillance systems for social and security management. The Chinese Social Credit System.

Cabestan, J.P., 2017. The Party runs the show: How the CCP controls the state and towers over the government, legislature and judiciary. In *Routledge Handbook of the Chinese Communist Party* (pp. 75-91). Routledge. https://doi.org/10.4324/9781315543918-5

Calcara, G., 2020. A transnational police network cooperating up to the limits of the law: examination of the origin of INTERPOL. *Transnational Legal Theory*, *11*(4), pp.521-548. https://doi.org/10.1080/20414005.2020.1793282

Creemers, R. 2016. Disrupting the Chinese state: new actors and new factors. *Asiascape: Digital Asia*, 5, 169-197. https://doi.org/10.1163/22142312-12340094

CrowdStrike. 2023. CrowdStrike 2023 Global Threat Report: executive summary. Available: https://www.crowdstrike.com/resorurces/reports/global-threat-report-executive-summary-2023/ [Accessed: 13 May 2024].

Dilanian, K. 2023. Forget the spy balloon. China-linked hackers collect far more information, report says. *NBC NEWS*[Online]. Available: https://www.nbcnews.com/news/forget-chinese-spy-balloon-china-linked-hackers-collect-far-information-rcna72583 [Accessed: 13 May 2024].

Erqi, G., 2023. The Legal Governance on Cybercrime through the Lens of Positive Criminal Law. *Mod. L. Rsch.*, *4*, p.14.

Farwell, J.P., & Rohozinski, R. 2011. Stuxnet & the future cyber war. *Survival*, 53(1), 23-40. https://doi.org/10.1080/00396338.2011.555586

Gilley, B., 2003. China's Changing of the Guard: The Limits of Authoritarian Resilience. *Journal of Democracy*, *14*(1), pp.18-26. https://doi.org/10.1353/jod.2003.0008

Glesby, N. and Lackenbauer, P.W., 2024. Balloons, NORAD, and the Defence of North America: Reflections on the February 2023 Incidents Concerning.

Hou, R. and Fu, D., 2024. Sorting citizens: Governing via China's social credit system. *Governance*, *37*(1), pp.59-78. https://doi.org/10.1111/gove.12751

Hulvey, R.A., 2022. Cyber sovereignty: How China is changing the rules of internet freedom.

Jinguah, L. 2019. *What are China's cyber capabilities and intentions?* New York: IPI Global Observatory.

Kostka, G. and Antoine, L., 2020. Fostering model citizenship: Behavioural responses to China's emerging social credit systems. *Policy & Internet*, *12*(3), pp.256-289. https://doi.org/10.1002/poi3.213

Kshetri, N. 2023b. Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers. *Crime, Law and Social Change*, 60(1), 39-65. https://doi.org/10.1007/s10611-013-9431-4

Lallie, H.S., Shepherd, L.A., Nurse, J.R., et al. 2021. Cybersecurity in the age of COVID-19: a timeline analysis of cybercrime and cyber-attacks during the pandemic. *Computers & Security*, 105. https://doi.org/10.1016/j.cose.2021.102248

Li, L. and Zhou, W., 2019. Governing the "Constitutional Vacuum"–Federalism, Rule of Law, and Politburo Politics in China. *China Law and Society Review*, *4*(1), pp.1-40. https://doi.org/10.1163/25427466-00401001

Liang, F. and Chen, Y., 2022. The making of "good" citizens: China's Social Credit Systems and infrastructures of social quantification. *Policy & Internet*, *14*(1), pp.114-135. https://doi.org/10.1002/poi3.291

Liang, F., Das, V., Kostyuk, N. and Hussain, M.M., 2018. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, *10*(4), pp.415-453. https://doi.org/10.1002/poi3.183

Loo, J., 2021. *Free Formosa: The Beginning*. Xlibris Corporation.

Loo, J., 2021. *Free Formosa: The Beginning*. Xlibris Corporation.

Nantieh, P., 2020. *How the Ccp Employs Ai Surveillance Tools to Track and Control Citizens and Their Inherent Cybersecurity Risks* (Master›s thesis, Utica College).

Orgad, L., & Reijers, W. 2020. *How to make the perfect citizen? Lessons from China's model of social credit system*. Fiesole: European University Institute. https://doi.org/10.2139/ssrn.3586503

Pei, M., 2024. *The sentinel state: Surveillance and the survival of dictatorship in China*. Harvard University Press-T. https://doi.org/10.2307/jj.10860939

Qi, A., Shao, G., & Zheng, W. 2018. Assessing China's cybersecurity law. *Computer Law & Security Review*, 34(6), 1342- 1354. https://doi.org/10.1016/j.clsr.2018.08.007

Qi, G., Yating, Z., Youlin, Y et al. 2018. A direct current-voltage measurement method for smart photovoltaic modules with sub-module level power optimizers. *Solar Energy*, 167, 52-60. https://doi.org/10.1016/j.solener.2018.03.082

Tang, W., 2016. *Populist authoritarianism: Chinese political culture and regime sustainability*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190205782.001.0001

The Economic Intelligence Unit. 2020. Democracy Index 2020: in sickness and in health? Available: https://www.eiu.com/n/campaigns/democracy-index-2020/ [Accessed: 13 May 2024].

The State Council Information Office of the People's Republic of China. 2015. PRC State Council China's Military Strategy. *USC US-China Institute* [Online]. Available: https://china.usc.edu/prc-state-council-chinas-military-strategy-2015-may-26-2015 [Accessed: 14 May 2024].

The State Council of the People's Republic of China. 2004. Vigorously promoting a comprehensive strategic partnership between China and the European Union. *Mission of the People's Republic of China to the European Union*[Online]. Available: https:// www.eu.china-mission.gov.cn/eng/more/Topics/200405/t20040512_8303627.htm[Accessed: 14 May 2024].

The State Council of the People's Republic of China. 2011. China's peaceful development. *English.Gov.CN*[Online]. Available: https://english.www.gov.cn/archive/white_paper/2014/09/09/content_281474986284646.htm [Accessed: 14 May 2024].

The State Council of the Republic of China. 2016. Report on the work of the government. *English. Gov. CN*[Online]. Available: https://english.www.gov.cn/premier/news/2016/03/17/content_281475309417987.htm [Accessed: 14 May 2024].

Thomala, L.L. 2023 Internet penetration in China 2000-2022. *Statista*[Online]. Available: https://www.statista.com/statistics/255136/internet-penetration-in-china/ [Accessed: 13 May 2024].

UNODC.2022. Cybercrime. *UNODC Romena* [Online]. Available: https://unodc.org/romena/en/cybercrime.html [Accessed: 14 May 2024].

Van Wyk, B. 2022. China's cybercrime problem is growing. *The China Project* [Online]. Available: https://thechinaproject.com/2022/08/23/chinas-cyber-crime-problem-is-growing/ [Accessed: 13 May 2024].

Wang, A., 2020. Cyber sovereignty at its boldest: A Chinese perspective. *Ohio St. Tech. LJ*, *16*, p.395.

Wang, F.L., 2023. *The China Record: An Assessment of the People's Republic*. State University of New York Press.

Wang, F.L., 2023. *The China Record: An Assessment of the People's Republic*. State University of New York Press.

Wu, G. 2006. Conceptualizing and measuring the perceived interactivity of websites. *Journal of Current Issues and Research in Advertising*, 28(1), 87-104. https://doi.org/10.1080/10641734.2006.10505193

Xu, M. and Lu, C., 2021. China–US cyber-crisis management. *China International Strategy Review*, *3*(1), pp.97-114. https://doi.org/10.1007/s42533-021-00079-7

Zeng, J., 2014. *The Chinese Communist Party's capacity to rule: legitimacy, ideology, and party cohesion* (Doctoral dissertation, University of Warwick).