The Chinese Conception of Cybersecurity:

A Conceptual, Institutional, and Regulatory Genealogy

ABSTRACT by Eng. Ami Rotter Elazari MBA LLM

How does the Chinese government define cybersecurity? Security in the digital realm has gained increasing prominence in recent years, both within China's domestic policy landscape and in its participation with global digital governance. However, the Chinese conception of this term is different from the Western one, and is embedded within the country's distinctive political, economic and technological context. Drawing on Chinese government documents, this paper will trace the evolution of how successive generations of Chinese leaders have identified digital security concerns, and how they have deployed institutional, regulatory and policy tools to respond to them.

The authoring agencies that the Author **Eng. Ami Rotter Elazari** sources include National Security Agency (NSA), The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canadian Cyber Security Centre (CCCS), and New Zealand's National Cyber Security Centre (NCSC-NZ)

PARK JIN HYOK
"Kim Hyon Woo" Alias Accounts
https://www.justice.gov/usao-cdca/press-release/file/1092951/download

Introduction

How does the Chinese definition of cybersecurity inform policy practice? In the Western world, cybersecurity has predominantly been preoccupied with hacking, the unauthorized intrusion into networks to acquire information, disrupt their functioning or cause material real-world effects. It has come with a particular aesthetic, either images of shady individuals wearing hoodies or Guy Fawkes masks, depicted in shades of 'hacker blue', overlaid with Matrix-inspired columns of 0s and 1s. In the national security realm, cybersecurity has also come to be associated with 'bad actors', such as Russia and China, who hack election processes or the valuable intellectual property of innovative businesses. These Western depictions reflect central elements of the post-Cold War global order in which they emerged, including the low cost of cyber attacks in comparison to physical and kinetic means of attack, as well as the vulnerability of highly digitized society to these,Footnote[1] but also the dominance of most notably the technical, economic and political dominance of the US in the digital realm.Footnote[2] Over time, the concept of cybersecurity has also expanded from protecting technical networks to maintaining a particular vision of the Internet, and an envisioned global order in which it is embedded.

In China, too, cybersecurity (*wangluo anquan*) has become a top priority. In 2014, Xi Jinping announced China would become a 'cyber power' (*wangluo daguo*), an objective comprising economic and technological elements and the capabilities to secure them. Cybersecurity would be a key enabler for this ambitious agenda.Footnote[3] By the end of 2017, Beijing had published a national cybersecurity strategy,Footnote[4] an international cyber cooperation strategy,Footnote[5] and the Cybersecurity LawFootnote[6] that became a cornerstone of a still-expanding regulatory regime.Footnote[7] It has participated ever more in international governance processes such as the UN Group of Governmental Experts (GGE) on state conduct in cyberspace and the Open-Ended Working Group (OEWG) on ICTs in international security. It is investing heavily in educational and training facilities, as well as industrial policy for the cybersecurity sector.

What animates and informs these policy, regulatory, institutional and industrial moves? Which ideas, visions, histories and perceptions have infused the Chinese approach to cybersecurity? As securitization scholars have long argued, security concerns are constructed through narratives.Footnote[8] In order to deal with complex situations, humans develop clusters of stories to explain the world, and provide a framework for intervention.Footnote[9] These select and encode what constitutes a threat, prioritize some concerns over others, and offer tools for response. The construction of security concerns is this heavily context-sensitive and embedded in pre-existing social, economic and political visions and realities. They also shape reactions to material developments creating new potential forms of harm. To invent the car means inventing the car accident and thus the necessity for speed limits. In recent decades, no development has been more impactful in this regard than digitization and the concomitant emergence of cybersecurity as priority concern. This means this paper does not itself define cybersecurity as a term, or delineate its policy implications. Instead, it seeks to understand how the Chinese leadership has done so, and how this has evolved over time.

Drawing on official and semi-official government documents, including policy, legal and regulatory documents, leaders’ speeches and publications by government-affiliated research and technical bodies, this paper traces the evolution of the securitization of digital affairs in China. It pays particular attention how cybersecurity considerations are embedded in political and material contexts. The most important one is the Leninist nature of China’s political system, which demands a total monopoly on political power for the Chinese Communist Party (CCP) and a governance model enabling the Party leadership to realise its programme and maintain order. Its primary perceived threat is subversion by domestic or foreign hostile powers. Consequently, maintaining regime integrity and stability will be a dominant factor of China’s cybersecurity vision. However, China’s regime type is not the only important consideration. Its engagement with digital technology is also profoundly shaped by its near-total absence in the emergence and popularization of the initial generation of digital technologies, and the international frameworks set up to govern them. China’s undeniable technological progress in a range of fields notwithstanding, the succession of US sanctions, the dominance of US operating systems on China’s market, and its relative secondary role in global governance organizations demonstrate the extent to which China remains far more dependent on the West than the other way around. In other words, where the West sees itself as the progenitor, and thus rule-setter, of the digital world, the Chinese perception is that it started from far behind and must gain greater capabilities and influence. Lastly, the context in which China’s cybersecurity vision develops is not static. Beijing’s policies were often responses to successive external circumstances, including growing digitization inside China, the increased technological and commercial sophistication of digital devices and economies, and worsening international relations. In turn, the outside world has responded to Beijing, with this mutual escalation culminating in the current ‘tech Cold War’.Footnote[10]

This paper proceeds as follows. First, it reviews the emergence of security concerns in the early days of China's connectivity with the global Internet in the 1990s and 2000s. Subsequently, it discusses how these concerns have gradually become integrated, culminating in the establishment of the unified 'cybersecurity and informatization' bureaucracy in 2014 and the publication of the CSL in 2016. Subsequently, it examines how the rapidly worsening tensions with the US have fostered new cybersecurity concerns over the past few years. It concludes with a reflection on the implications of China's cybersecurity vision for scholarly and policy considerations. Lastly, a lexical remark is necessary. The Chinese term '*wangluo anquan*', usually translated as cybersecurity, literally refers to 'network security'. It is a relatively new term that replaced the previous dominant concept of 'information security' (*xinxi anquan*) in the early 2010s. This shift recognises that security concerns could emerge from other sources than harmful information, and that the entire networked world became a risk vector. While this paper uses the translation 'cybersecurity' for the sake of readability, and because this is how Beijing translates it itself, readers should bear in mind that the word has different semantics in Mandarin.

The Emergence of ICT Security Concerns: 1994–2003

China only gained full connectivity to the global Internet in 1994, relying previously on technical facilitation from Germany.Footnote[11] Over the next few years, several thousand people, mostly scholars and researchers, went online.Footnote[12] Perhaps the most basic functionality, technical support for Chinese characters, was sketchy. Different character formats meant websites and applications didn't display well from one computer to the next.Footnote[13] Yet this situation would soon change. The first of the 'Golden Projects', major government initiatives to digitize fields including public security, taxation and customs, were announced in 1993, and commercial Internet services became available in 1995. By the turn of the century, the number of Internet users had skyrocketed to 7 million, and would exceed a billion by the end of 2021.Footnote[14]

In contrast to the relatively light-touch approach of Western governments, Chinese authorities nearly immediately started identifying and responding to digital security concerns. The State Council issued its first decree on the security of 'computer information systems' in 1994,Footnote[15] focusing primarily on systems in 'State affairs, economic construction, national defence construction, and frontier science and technology'. Indicating how digital security policy was embedded in Leninist thinking from the start, going far beyond mere technical concerns, it prohibited the use of computers systems to harm the national interest, the collective interest, citizens' rights and interests, or the security of computer systems themselves. The Ministry of Public Security (MPS) gained primary responsibility over several mandates: creating a hierarchical protection system enabling differentiated management of higher and lower priority networks, registering internationally connected networks, managing incidents and cybersecurity duct sales, and prevention of 'computer viruses and other harmful data endangering social and public security'.

The leading concern was the unchecked production, dissemination and acquisition of online information. Peking University's *Weiming BBS* was shut down in 1996 already, on the grounds of disseminating politically sensitive content, while forums and blogs came under scrutiny at the same time.Footnote[16] Authorities introduced regulations to impose direct control over the various components of the communication architecture. State control was implemented over internationally connected networks, online information services and network access. 1996 rules on internationally connected networks required all international gateways to be managed by the Ministry of Post and Telecommunications (MPT), and all existing cross-border networks to be brought under the control of the MPT, the Ministry of Electronic Industry, the State Education Committee or the Chinese Academy of Science. State Council approval would be required for the construction of new cross-border connections and networks using those connections had to obtain approval from their respective regulatory authorities.Footnote[17] From 2000 onwards, commercial online service providers had to apply for business licences with the newly-established Ministry of Information Industry (MII), and non-commercial service providers had to register.Footnote[18] Internet connections could only be obtained after a lengthy administrative process involving real identity verification, and similar requirements were rapidly introduced for the operators of Internet cafésFootnote[19] and their visitors.Footnote[20]

The MPS itself issued the first dedicated regulations on Internet security at the end of 1997, addressing both hacking and online content-related security concerns.Footnote[21] They introduced a list of prohibited content nearly directly lifted from existing regulations for traditional media, covering concerns including subversion of the “basic principles established in the Constitution to obscenity, violence, defamation and ‘superstition and heresy’.Footnote[22] They also prohibited unauthorized intrusion into networks, altering the functions of networks, tampering with data on networks, or disseminating malicious software. Ironically, they protected ‘users' freedom to communicate and communication confidentiality” from interference. Lastly, they created wide obligations for the operators of international gateways to accept ‘supervision, inspection and guidance’ from public security bodies. This formed the first regulatory basis for the content management system that become known as the Great Firewall of China (GFW), a term coined in *Wired* magazine in 1997.Footnote[23]

The provisional keystone of this regime was a 2000 Decision of the National People's CongressFootnote[24] which explicitly criminalized four categories of online activities. The first consisted of hacking into military and high-tech computer systems, distribution of malware and cyber-attacks, and obstructing the functioning of networks. The second addressed national security and social stability, including the distribution of rumours, subversive content, or state secrets, inciting ethnic hatred or organising ‘heretic groups’. Third, the NPC sought to maintain order in the marketplace, and criminalized the use of the Internet to sell counterfeit or inferior products, damage the reputation of businesses or their products, violate intellectual property rights, manipulate financial markets through false information, or distribute pornography. Fourth, in the area of private users' rights, the Decision criminalized online defamation, seizure of communication, or online fraud.

In short, in a brief few years, Chinese authorities created a regulatory environment for the Internet that addressed content regulation, required the identifiability of users and operators, set technical requirements, and had started to create the necessary enforcement mechanisms and the technical tools. This rapid proliferation reflects a rise in the prominence of digital security. The number of references to digital security in official media outlets increased drastically around the turn of the century, covering both technological concerns such as viruses and other malware and socio-political concerns.Footnote[25] The focus on content reflects a broader context of strengthening media control. Less than a decade after Tiananmen, blamed in official documents on American 'peaceful evolution' operations,Footnote[26] the Internet presented a new channel for the spread of potentially destabilizing or subversive foreign content. In January 1999, a Shanghainese software entrepreneur, Lin Hai, gained the dubious distinction of being the first person sentenced to prison for online content-related offences. He had provided over 30.000 Chinese addresses to Li Hongkuan, a New York-based intellectual who circulated a newsletter called *Da Cankao*, containing censored articles and other political news.Footnote[27] Another dissident, Wang Youcai, used the attention garnered by an upcoming state visit by Bill Clinton to register a new political organization called the China Democracy Party, posting its manifesto to thousands of *Da Cankao* recipients.Footnote[28] He too was swiftly arrested and convicted. Yet perhaps the greatest impetus to policing foreign content came with the crackdown against Falun Gong from 2001 onwards. Under the leadership of the engineer Fang Binxing, the 'National Computer Network and Information Security Management Centre', an alter ego for the national computer emergency response team CNCERT/CC, started constructing the technical systems of the GFW, enabling efficient blacklisting of foreign websites.Footnote[29] This initially used functions in network infrastructure components supplied by companies such as Cisco, originally designed to enable corporate customers to monitor and control traffic in and out of their own networks. The GFW would eventually block most of the world's leading media outlets and social media platforms, and has become more sophisticated technologically. It would even be used for an attack against software sharing platform GitHub in 2015, dubbed the 'Great Cannon'.Footnote[30]

Institutional adjustments occurred as well. In 1998, the MPT and the Ministry of Electronics Industry merged into the new Ministry of Information Industry (MII), which gained authority over China's digital infrastructure and informatization programmes, as well as over the China Internet Network Information Centre (CNNIC). This was established the year before, partly to act as the Chinese registrar for the Domain Name System (DNS). This brought a level of government control over domain names that was largely absent in other major jurisdictions, where the DNS was seen as predominantly a private affair. Regulations soon followed that required DNS registrars to register with MII, and expanded content control provisions to cover domain names.Footnote[31] Institutional consolidation moved further forward with the establishment in 1996 of the Advisory Committee for State Informatization (ACSI) which grouped scientific and technical experts as well as corporate officials to assist in policymaking, and the State Informatization Work Leading Group in 1999. This was a coordinating body, chaired by then-Vice Premier Wu Bangguo, with its working office residing in MII. Its membership consisted of viceministers from the Party and state bodies involved with information technology, ranging from the MPS and the Ministry of State Security to the Central Propaganda Department and the Ministry of Foreign Trade. Its first stated task was 'organizing and coordinating major matters in the areas of the national computer network and information security management'.Footnote[32] This was a significant shift from previous informatization coordination work, which had largely focused on economic development issues.Footnote[33] In 2001, the Leading Group was raised in bureaucratic rank to the Premier level. It was also renamed, becoming the State Informatization Leading Group (SILG)

WANNAMINE
MONERO
https://www.crowdstrike.com/blog/cryptomining-harmless-nuisance-disruptive-threat/

Initial but Incomplete Consolidation: 2003–2010

The new SILG promptly issued policy proposals on improving information securityFootnote[34] that still form the core of the cybersecurity regime today. The problems it identified included weak emergency response capabilities, a lack of talent and critical technical prowess, low industrial competitiveness, an underdeveloped regulatory environment, low information security awareness in society and lacklustre information security management. A factor the document did not mention was the fact that the vast majority of computers in China ran counterfeit copies of foreign operating systems, mostly Windows. In the SILG's view, these problems contributed to the proliferation of online harmful information, cyber attacks and malware, loss or disclosure of online confidential information, cybercrime, as well as "domestic and foreign hostile forces' attacks and destructive activities against radio and television satellites, cable television and terrestrial networks, and their use of information network to conduct reactionary propaganda activities". In short, security in the digital realm was defined as being a full-spectrum concern, including defence against ordinary criminal activities as well as dissidents and adversarial state actors that would undermine the CCP's rule—most significantly the United States and its allies.

In response, the document argued for a comprehensive and systematic upgrade of information security protection efforts. First, it called for the implementation of the multi-level protection system, which had already been mentioned in some of the first related regulations in 1994. Subsequently, it advocated the use of encryption technology to enhance online trust and the security of e-government and e-commerce applications. Control systems were to be established in regulatory authorities and network operators to respond to cyberattacks, with the support of a State-run national information supervision and control system. In support of these substantive goals, the document highlighted the need to strengthen technological research and development, supporting the growth of the information security industry, enhancing regulatory structures and technical standards, improving education and training as well as information security awareness among ordinary Internet users. This document also contained the first high-level mention of the term ‘indigenous and controllable’ (*zizhu kekong*), referring to perceived security improvements offered by using domestically produced technologies. This term, which would expand to ‘secure and controllable’ (*anquan kekong*) later, demonstrates that Chinese authorities were already aware of the potential vulnerability resulting from reliance on foreign technologies. Illustratively, the document put forward the long-term goal of ‘a structure where basic information networks and important information systems are mainly composed of indigenous and controllable equipment’, and indicated that State-funded informatization projects should adopt homegrown software, hardware, and services where possible. Lastly, the document called for the promulgation of an ‘Information Security Law’.

This document fostered both regulatory and institutional developments. The most important one was the multi-level protection system (MLPS) for information security. Having already been called for in 1994, a first plan for its construction finally emerged in 2004, under the lead of the MPS.Footnote[35] The basic principle of this system was that all information systems had to be categorized into five tiers, depending on their importance and relevance to national security, social stability, economic development and the public interest. Higher tiers came with higher protection requirements, inspections and regulatory constraints. Implementing regulations, published in 2007, incorporated several existing technical standards and required that all second tier and higher networks had to be registered with local public security bodies. The document also contained dedicated rules on State secrets and encryption.Footnote[36] Separately, the MPS published rules on technical measures for online security protection, which required Internet service providers and companies using the Internet to take steps to prevent malware, create disaster-proof backups, record and preserve user records, and monitor the operational status of networks. They also had to be able to identify and cease the transmission of unlawful information, prevent defacing of webpages, and prevent spam.Footnote[37] The Network and Information Security Coordinating Group, operating under the SILG, released overarching policies on security risk assessment by companies, which required the combination of enterprise self-management and government inspections, calling for the regularization of security protection in companies and the formulation of underpinning technical standards.Footnote[38] The Ministry of Industry and Information Technology, as MII was renamed after merging with the State Administration for Science, Technology and Industry for National Defence and the State Council Informatization Office, issued regulations on cybersecurity protection in telecommunications networks, equally imposing requirements for regular security audits and risk assessments.Footnote[39]On the institutional side, a new National Technical Committee for Information Security Standardization, also known as Technical Committee 260 (TC260) saw the light in 2002 under MIIT, and a National Network and Information Security Coordination Group in 2003 under the SILG. Zhao Zeliang, who would become Chief Engineer of CAC and director of TC260, was deputy head of this Group for a year.Footnote[40] The beginnings of indigenous cybersecurity review took shape with the establishment of a national information security product certification and licensing system in 2004Footnote[41] with a dedicated

certification body, the China Cybersecurity Review Technology and Certification Center following in 2006.

To summarize, the 2000s saw Chinese authorities incrementally consolidate different facets of digital security, including content control and countering cybercrime to mitigating China's reliance on foreign technologies and prioritizing the protection of more sensitive and important network systems. Content control was shared between the MPS, which mostly focused on news and current affairs, and the censorship authorities which had expanded their existing pre-publication licensing and review system to the online sphere. The MPS had also started to build up the MLPS, creating greater compliance requirements network administrators. MIIT was moving ahead in technical standards and the protection of telecommunications infrastructure. Where security protection in Western countries remained very much an afterthought in the design of digital products and the operation of online services,Footnote[42] it became increasingly built into China's emerging regulatory architecture. Even so, the development of digitization rapidly outpaced the ability of authorities to turn those aspirations into reality, while China's relatively weak technological capabilities and institutional corruption would continue to bedevil the cybersecurity environment.

2010–2016: Cybersecurity Goes Global, While the Domestic Digital Economy Mushrooms

Despite the gradual evolution of the information security regime the leadership continued to play catch-up as its challenges continued to expand. Digital adoption continued to expand rapidly. The increased sophistication of digital technologies, and particularly the rapid popularization of mobile devices, had a transformative impact on the online circulation of information, the creation and processing of data and the functioning of digital economic and governmental processes, all the while making the Internet ever more of an essential conduit for daily life. The Chinese government did not crack down on these evolutions, and facilitated the emergence of large, private, online platform companies.Footnote[43] Yet as Chinese citizens took to social media and e-commerce in their millions, risks increased as well. Although Chinese authorities were enthusiastic proponents of increased connectivity, every new netizen, every new online business and every new e-government application also added to the potential vulnerability surface. In addition, the new social media platforms, such as Weibo, provided easy access to mass communication and organization tools that were used to political effect. An early social media service, Fanfou, had been taken offline in 2009 after violent riots in Urumqi.Footnote[44] Subsequently, a steady stream of political scandals, often enriched with smartphone-enabled imagery, became public on Weibo. These ranged from garden-variety corruption among local officials to an alleged attempt to cover up evidence after a major high-speed railway crash.Footnote[45] The run-up to the 18th Party Congress, which would anoint Xi

Jinping as General Secretary, was marred by rumours about a military coup (Benney 2014). Nearly immediately after the Congress, a major debate broke out on social media about constitutional reform in China, a critical challenge to regime integrity.Footnote[46] Neither traditional media control departments nor MPS and MIIT seemed to be able to effectively handle these challenges, particularly in view of the rapid speed at which information could circulate, defying the relatively slow methods adopted by these departments.

Furthermore, companies also exhibited very dubious behaviour, often with considerable security implications. In one famous case emerging in 2010, security company Qihoo's software detected that Tencent's popular QQ instant messaging app would scan irrelevant files of users' drives, effectively spying on users. It announced a new programme, Privacy Guard, to deal with the issue. Tencent accused QQ of disseminating false information, denying the accusations. Furthermore, Tencent disabled its instant messaging app on devices running Qihoo's security software, meaning users had no choice but to switch it off to continue messaging their contacts. This incident demonstrated that companies were willing to play fast and loose with the safety of their users if money could be made. MIIT forced both companies to apologise and end their public spat. It also issued new regulations on the online services market, effectively becoming the digital competition regulator, a task for which its resources were severely limited.Footnote[47] Internal journals increasingly revealed concerns about the ability of the CCP to survive its increasing integration with a network society.Footnote[48]

Cybersecurity issues also increasingly gained an international element. 2010 marked an inflection point in the relationship between China and its prime digital counterpart, the United States. Early that year, Google ended its Chinese operations. Although it had abided by censorship regulations, authorities' growing demands for the disclosure of Gmail information and a series of attacks against its systems attributed to China, drove the company to pack up and leave. Several days later, then-Secretary of State Hillary Clinton launched the 'Open Internet AgendaFootnote[49]', a move Beijing interpreted to target China. A decade earlier, almost to the day, her husband, then-President Bill Clinton, had derided Chinese Internet control efforts as an attempt 'to nail jello to the wallFootnote[50]'. Chinese leaders had never needed much convincing that the US sought to effect regime change in Beijing, but the Internet gave those concerns new urgency. China's immediate response was an official White Paper, in which the term 'cybersovereignty' (*wangluo zhuquan*) received its first high-profile outing. This White Paper not only defended and justified China's approach to Internet management, it also argued that China had the sovereign right to govern its digital space, in contrast to the Western notion that cyberspace superseded national boundaries and was subject to universal values. Furthermore, its section on internet security prioritized the role of national governments in securing information flows, combating cybercrime and hacking.Footnote[51]

By the end of 2011, the line of the Hu administration had become that 'hostile foreign powers are intensifying strategies and plots to Westernize and divide our country, and the ideological and cultural sphere is the focus sphere in which they conduct long-term infiltrationFootnote[52]'. A later internal communiqué, the infamous Document 9, was even more candid, stating that ‘mistaken thinking trends and viewpoints exist in large numbers in foreign media and reactionary publications, and permeate into the borders through the Internet and underground channels; they are also disseminated to a certain extent on domestic online forums, battle line-ups and microblogs […]’. It also listed a litany of infiltration activities conducted by ‘Western anti-China forces and domestic “dissidents”’, ranging from human rights dissemination activities and the disclosure of official corruption to support for protest movements in Tibet and Xinjiang. Moreover, it accused them of ‘pointing the spearhead’ of ‘colour revolutions’ at China.Footnote[53] Washington’s pivot to Asia,Footnote[54] in which the US rebalanced its foreign policy towards the ‘Asia-Pacific’, further strained the relationship, as Beijing saw it as a thinly veiled attempt at containment.

Technical security concerns also gained greater prominence. One of the Edward Snowden’s 2013 revelations was that from 2009 onwards, the NSA conducted an operation codenamed ‘Shotgiant’ against the emerging Chinese telecommunications vendor Huawei. It gained access to customer lists, training documents and product manuals, as well as the source code of individual products. The ostensible goal for these operations was surveilling Huawei customers in Iran, Afghanistan, Pakistan, Kenya and Cuba, but also to better gauge China’s own plans, intentions and capabilities.Footnote[55] CAC deputy director Wang Xiaojun pointed at Stuxnet as an example of how critical or strategic facilities could be harmed.Footnote[56] A lively debate broke out in security and defence circles, as well as official state media, about novel forms of Chinese vulnerability,Footnote[57] including US dominance of the Domain Name System (DNS) and the associated constellation of root servers.Footnote[58] Defence scholars voiced worries about technologies to circumvent the Great Firewall, for instance through Google’s ‘Project Loon’, which used drone balloons to enable wireless Internet coverage without terrestrial infrastructure.Footnote[59] MIIT Chief Engineer Zhang Feng cited Microsoft’s decision to discontinue security support for Windows XP as a case of vulnerability to corporate decisions taken abroad.Footnote[60] Illustratively, the use of the term ‘cybersovereignty’ in Chinese academic papers and the top State newspaper *People’s Daily* skyrocketed from zero in 2010 to 132 and 44 respectively in 2016, when the Cybersecurity Law was issued.Footnote[61] The proportion of People’s Daily article framing cybersecurity in foreign relations terms rose from 2% between 2000 and 2009 to 30% subsequently.Footnote[62]

This rapid proliferation of challenges and concerns led the recently appointed General Secretary Xi Jinping to prioritize cybersecurity ever more. At first, these efforts were firefighting responses to specific issues. The State Internet Information Office, a small department of the State Council Information Office, was given independent leadership in the person of Lu Wei, hitherto propaganda chief in Beijing. There, he had developed tactics to manage raucous social media landscape, which he now deployed at the national level.Footnote[63] Tackling online celebrities and the possibility of information virality on public social media, the Supreme People’s Court imposed criminal liability and possible imprisonment for the publication of false information online, if retweeted 500 times or viewed 5000 times.Footnote[64] Faced with rife incidents of data theft and illegal data trading, the NPC Standing Committee issued a resolution on online information protection which formed the nucleus of the future data protection regime.Footnote[65] Reflecting the expansion of digital concerns far beyond information and content, the hitherto dominant term 'information security' (*xinxi anquan*) was gradually replaced by 'cybersecurity' (*wangluo anquan*).Footnote[66]

Once the most immediate concerns had been managed, attention turned towards institutional overhaul, with the creation of a comprehensive new bureaucracy for digital affairs. The successful crackdown on social media had created momentum for the SIIO, and its director would turn it into a sprawling bureaucratic empire. The department was renamed, becoming the Cyberspace Administration of China (CAC).Footnote[67] To bring the coordination of digital policy to the highest level of political seniority, the SILG and its information security subordinate were merged into a new body, the Central Leading Group for Cybersecurity and Informatization (later renamed Central Commission for Cybersecurity and Informatization), chaired by Xi Jinping personally. CAC hosted this Leading Group's secretariat. It gained primary responsibility for all online content control,Footnote[68] and took over several departments from MIIT, including cybersecurity coordination and the related oversight over TC260. It also took over authority over CNNIC and, in 2018, over CNCERT/CC. However, it did not gain the MPS' cybersecurity powers, creating a situation where MPS and CAC would remain at loggerheads over cybersecurity competences for years to come.

Almost simultaneously, the NPC started drafting the CSL.Footnote[69] This involved lengthy debates on how to reconceptualize cybersecurity, manage its relationship with technological and economic development, and address the international ramifications. In 2016, Xi Jinping laid down conceptual parameters at a national work conference on cybersecurity and informatization. First, cybersecurity was 'holistic', or closely embedded within broader national security concerns. Second, it was dynamic and not static, requiring flexibility in policy and regulation. Third, cybersecurity was 'open', necessitating greater foreign interaction and exchange, as well as the import of advanced technology. Fourth, cybersecurity was relative and not absolute, meaning it is necessary to prioritize and act selectively rather than aim for perfection. Fifth, cybersecurity is 'shared', and thus needs joint participation of non-governmental actors, including businesses, social organizations and individuals.Footnote[70] On this basis, Xi outlined that, outside of legislation and regulation, cybersecurity would also require a significant build-up of capabilities, particularly relating to critical information infrastructure. This would result in an 'all-weather, omnidirectionally sensing cybersecurity posture', including threat identification, reporting and information sharing mechanisms, as well as on strengthened defensive and deterrence capabilities in which intrusion into potential targets would be far more difficult or retaliation more costly.

Subsequently, the CAC issued the National Cyberspace Security Strategy (NCSS),Footnote[71] a succinct review of the circumstances the authorities perceived in cyberspace, the objectives they wished to obtain, the principles they intended to uphold, and the specific tasks they planned to address. The Strategy emphasised the importance of digital technology for the dissemination of information, for economic development and people's daily lives, for social governance and interaction, and as an extension of the national sovereign sphere. Yet these opportunities were threatened by grave challenges. Its first concern was that ‘cyber penetrations harm political security’, as countries interfere in other countries’ domestic affairs, attack their political systems, incite social unrest or political subversion, or engage in cyber espionage. Subsequently, it listed threats to economic security, such as damage to critical infrastructure through cyberattacks, to cultural and ideology security, for instance through ‘online rumours and degenerate culture’, and to social security, through online terrorism and extremism, as well as through fraudulent and criminal activities targeting both individuals and businesses. Lastly, the Strategy noted an increasing degree of international competition in cyberspace, to control strategic resources and acquire norm-setting power, another veiled criticism of the US. With the publication of this strategy and the passing of the Cybersecurity Law, attention would now turn to implementing the tasks laid down in the CSL and the NCSS.

2016–Current: Implementing the CSL, Iterating the Cybersecurity Concept

Reflecting the comprehensive conception of cybersecurity, the 2016 CSL included a range of mandates for line ministries to implement. First of all, the CSL codified a legal basis for content control, highlighting the enduring centrality devoted to maintaining the Party’s ideological and cultural dominance. This not only governs content itself, but also the means by which it can be created and disseminated, such as AI-generated ‘deep fakes’ and algorithmic recommendation respectively.Footnote[72] The CSL also demonstrated the rapidly growing importance of data security. The Law itself contained only a few rudimentary provisions on data, but these burgeoned into a comprehensive new regime founded on twin pieces of legislation: the Personal Information Protection LawFootnote[73] and the Data Security Law.Footnote[74] The former started out as a response to recurrent abuses of personal information, but grew to regulate large online platforms’ data-enabled business models. The latter, in contrast, seeks to protect national security and the public interest from harm emanating from the abuse of any kind of data, personal or otherwise.Footnote[75] In both cases, subsequent implementing regulations have devoted specific attention to data export as well as sector-specific concerns. Of these, smart vehicles have been the most prominent, reflecting evident concern with the purposes to which data these vehicles gather might be put. Illustratively, Tesla cars are no longer permitted in Chinese government compounds and military facilities, as well as in the town of Beidaihe when the leadership holds its annual summer vacation there.Footnote[76]

One key element of the Data Security Law is its division of data into three hierarchical categories: normal, important and 'core national' data. This tactic of prioritization stems from the Multi-Level Protection System that currently remains under overhaul, and is also applied in the protection system for 'critical information infrastructure'. Prioritization not only entails stricter regulatory requirements, but also mandated security audits by certified third-party bodies and limitations on the software and hardware that can be used. The CSL mandate for cybersecurity review originally focused on 'important network products and services', and have increasingly come to encompass supply chain reliability following the escalation of US sanctions against Chinese technology companies from 2018 onwards. Yet cybersecurity review also illustrates the difficulties and trade-offs confronting the Chinese government's efforts to secure its digital space. In 2017, a rare public debate on whether a dedicated version of Windows for government system should be allowed on the Chinese market or not, as voices prioritizing 'indigenous and controllable' technology argued. The counterargument of a high-level engineer at an approved third party security evaluator, the China Information Technology Security Evaluation Centre (CNITSEC) claimed domestic alternatives would entail high switchover costs with no tangible increase in security.Footnote[77] In 2021, the remit of cybersecurity review was stretched to include reviewing overall corporate conduct. A case was launched against CNKI, China's largest academic repository, ostensibly over how it might be used by foreign researchers, journalists or intelligence services.Footnote[78] The most impactful case, however, concerned ride hailing giant Didi, which listed on the New York Stock Exchange after having received explicit warnings from the CAC not to. After an investigation, the CAC imposed an 8 billion RMB fine, alleging Didi had engaged in data processing activities that 'seriously affected national security'. These included illegally collecting 12 million screenshots from users' mobile phone photo libraries, 107 million facial recognition data points and 8.3 billion data points from users' clipboards. Moreover, it had failed to store certain information securely and to notify users of certain data collection.Footnote[79] These concerns with Chinese companies listing on foreign (usually American) stock exchanges and exporting information reflect ever greater worries about how foreign parties might gain access to Chinese data and use it for harmful purposes. An accelerant may have been the US 'Holding Foreign Companies Accountable Act', which requires greater auditing access to Chinese corporate information.Footnote[80]

A further expansion of the CSL is the introduction of regulations for the management and disclosure of technical vulnerabilities. According to regulations issued jointly by MIIT, MPS and CAC, companies must establish vulnerability reporting interfaces and are encouraged to establish bug bounty programmes. Moreover, the regulations avow the existence of several national threat and vulnerability databases. The publication of vulnerability was prohibited, except after it was patched, and even then subject to conditions. Publication can, for instance, not take place around major national events, as hackers might take advantage of systems that remain unpatched at times of political sensitivity.Footnote[81] Similarly, cybersecurity incident response plans have been drawn up. A National Cybersecurity Emergency Office, housed within CAC, directly coordinates responses to incidents ranging from equipment failures and natural disasters to malware, cyberattacks and content-related incidents.Footnote[82]

These regulatory and institutional developments notwithstanding, China still lacks cybersecurity experts in the numbers necessary to realize them. Internal numbers suggest a shortfall of 1.5 million specialists. To remedy this, a National Cybersecurity Centre was established in Wuhan, which is intended to train over 70.000 full-time graduates as well as part-time early- and mid-career professionals. In 2018, China also started its own hacking competition, the Tianfu Cup, after Chinese security researchers were prohibited from participating in international contests.Footnote[83] A draft three-year plan for the development of the cybersecurity industry was published in 2021.Footnote[84] Although it has hitherto not been formally adopted, it gives an indication of the direction policy and regulation is likely to take. Amongst others, it sets the goal that core tech sectors will need to devote 10% of investment into cybersecurity, creating a significant market for security services at a stroke. Together with increasing regulatory compliance requirements, this tactic generates the income streams that make cybersecurity an attractive commercial proposition.

The breadth of the CSL on its own terms, augmented by further expanding regulatory approaches, has created a situation in which 'cybersecurity' now covers the entirety of security concerns that involve the Internet and digital technologies in some way or another. It has become one of the several security categories that comprise the 'comprehensive national security conceptFootnote[85]', which has become a central policy pillar in the 20th Party Congress report.Footnote[86] This evolution also shapes China's engagement in global digital governance and diplomacy circles. As a relative newcomer China has needed some time to acquire working knowledge of processes and terminology,Footnote[87] and much of its activity in the UN and other global governance forums is shaped by its self-perception as a relatively weaker player in comparison to the USs and other Western states.Footnote[88]

In the UN GGE, China has sought primarily to prevent the imposition of strong substantive norms that would constrain Beijing's space for manoeuvre, while selectively achieving certain aims such as the inclusion of sovereignty in the 2015 consensus report. Illustratively, it has consistently opposed norms around attribution, claiming that cyberattacks are difficult to attribute and that doing so is a political act.Footnote[89] This stance now seems to be shifting, as Chinese companies and State-affiliated entities have published their own attributions. In February 2022, the cybersecurity firm Pangu Lab attributed a decade-old exploit to an NSA-affiliated hacking group named 'The Equation Group'.Footnote[90] Later that year, the State-affiliated Computer Virus Emergency Response Centre accused the NSA's Office Tailored Access Operations of having breached the systems of the Northwestern Polytechnical University, a leading aerospace research institute.Footnote[91] These attributions are nowhere near as technically sophisticated as those regularly published concerning Chinese cyber operations,Footnote[92] but these activities do signal a significant turn. As China believes its capabilities are gaining increasing parity with leading Western actors, and as tensions with the US grow deeper, it is gradually showing greater assertiveness in the digital domain.

China has also supported initiatives at the UN to broaden participation in cyber diplomacy processes, diluting the preponderance of the US and its like-minded partners. It has consistently advocated to bring ICANN, the operator of the global DNS, under the control of the International Telecommunications Union,Footnote[93] instead of first the US Department of Commerce and currently a multistakeholder governance construction. This reflects concerns about the potential use of American control over ICANN to disable the Chinese Internet. It was no coincidence that the director of the newly established CAC chose an ICANN conference in London for his first major overseas engagement.Footnote[94] ICANN's decision to not cut off the Internet in Russia after it invaded Ukraine in 2022Footnote[95] will likely have assuaged some of Beijing's worst concerns. In 2018, it supported a Russian UN General Assembly resolution to establish an 'Open-Ended Working Group' (OEWG) for cyber affairs, competing with the more exclusive GGE format. Both institutions worked side-by-side in the subsequent years. This OEWG became the venue where China proposed its first substantive norm. Following increasing US sanctions against Chinese technology companies, Beijing sought to enshrine that states could not exploit national security pretexts to limit market access and export of technology productsFootnote[96] – matters solidly within the sovereign control of states. China will be increasingly presented with this conundrum: its insistence on autonomy, self-determination and a strict interpretation of sovereignty leave it vulnerable when other countries act in similar ways.

Conclusion and implications

The evolution of China's notion of cybersecurity contains clear continuities, which evolve and grow more complex over time. Reflecting China's usual approach of 'relentless gradualism', the concerns that animated Beijing in the late 1990s are still the core of the Chinese risk and threat perception today: digitally enabled threats to the integrity of the regime and the ability to fulfil its political programme, and vulnerabilities stemming from relative Chinese technological and commercial dependence and backwardness. As such, China's cybersecurity narrative is deeply embedded in, and a manifestation of, its broader national security vision. The major change that has emerged across three decades of digitization is one of urgency and priority. China has become far more digitally capable and connected, but that creates new sources of insecurity in and of itself. Moreover, the relatively benign international environment that China experienced in the 1990s has given way to escalating tensions with the United States—tensions with the digital realm at their core.

This evolution in Chinese perceptions has largely been event-driven. Domestically, major shifts have taken place in response to both domestic trends, such as the proliferation of illegal data trading, as well as international events, such as the Snowden revelations. Yet there is a curious difference between these two levels. In contrast to its ambitions for wholesale socio-economic transformation stemming from its monopoly on political power at home, its international ambitions are far more limited. China does not have an explicit substantive agenda for the global realm. Its declared foreign policy objectives are largely intended to create a benign and conducive international environment for the realization of domestic goals. Cybersovereignty serves to ensure the undisturbed and unchallenged authority of the CCP from externally imposed norms and obligations, while its proposed norm for the non-use of technological sanctions and export controls fits with the avowed importance of the digital economy in China's overall development agenda.

A greater understanding of China's conception of cybersecurity opens avenues for scholarly inquiry and policy implications. First and foremost, as a key component of China's vision of Internet governance, it will have a significant role to play as the current structures of Internet governance come under increasing pressure.Footnote[97] This pressure not just comes from China itself, but from a range of countries in the global South that at least partly share its anti-hegemonic instincts and its rejection of US dominance. A better understanding of China may assist in the development of better policy or, at least, the avoidance of unnecessary mistakes. Second, it allows China to be subject to comparative study. It is, for instance, often named in one breath with Russia as the two major threats to the Western vision of the Internet. To be sure, there are ample similarities between Chinese and Russian approaches to digital technology, particularly in terms of what they want to avoid.Footnote[98] However, unlike Russia, China is an enthusiastic adopter of digital technologies as part of a comprehensive programme for socio-economic development, and has fostered a world-class digital industry. This generates both different policy options and research parameters. Lastly, as a leader in cybersecurity regulation, China possibly may become a model for third countries emulating its approach, resulting in a 'Beijing EffectFootnote[99]' analogous to the EU's 'Brussels Effect'. As such, Beijing's approach will have impacts far beyond its own borders, of which policy professionals and researchers should take note

Hackers Make the First-Ever Ransomware for Smart Thermostats
HACK
PLANET

Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
bitcoin
Check Payment
Decrypt

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

China Own Government Cyber Companies

Lazarus Group

is a cybercrime group made up of an unknown 100 number of individuals. ... At the time, two other groups going by the personas

″ New Romanic Cyber Army Team “

and “ WhoIs Team″, ...

Parent organization: **Reconnaissance General Bureau**

Methods: Zero-days, spear phishing, malware, disinformation, backdoors, droppers

Affiliations: Unit 180, Andriel (group)

Official language: Chinese

PLA **APT 40 & APT 1**

PLA Unit 61398 (also known as **APT 1**, “**Comment Crew”** , “**Panda”** , “**GIF89a”**,

and “**Byzantine Candor”**)
(Chinese: 61398**部**队,
Pinyin: 61398 ***bùduì***)
is the Military Unit Cover Designator (MUCD)[1] of a People's Liberation Army advanced persistent threat unit that has been alleged to be a source of Chinese computer hacking attacks.
[2][3][4]
The unit is stationed in Pudong, Shanghai.[5] Shanhai air port province

People's Liberation Army Unit 61398

61398**部**队

source AMI ELAZARI PRIVET