LEIDEN ASIA CENTRE
Partners in Research and Knowledge

Universiteit Leiden

China's Cyber Governance Institutions

Dr. Rogier Creemers | January 2021

Summary

In order to fulfill its ambitions to become a "cyber power", the Chinese government has created a new institutional governance architecture to cover cybersecurity and informatization. Led, at the top, by Xi Jinping personally, this new administrative system consists of numerous Party and State bodies, associated think tanks and technical entities, sectoral associations and industrial alliances. In pursuit of the same general objective, this system must reconcile the differing, and sometimes conflicting needs of serving the needs of a rapidly expanding digital sphere with maintaining strong central control over a policy area of the utmost strategic importance. This report reviews the structure, scope and background of the entities composing this system, discusses the complex and often conflicting relationships between them, and provides a few recommendations to interested parties outside of China for more effective engagement.

Introduction

Since 2011, the political priority given to digital technology in China has increased significantly. Both in response to perceived foreign challenges and domestic issues, the leadership completely overhauled its digital policies, embarking on what became known as the "cyber power strategy" (*wangluo qiangguo zhanlüe*)[1][2]. This policy called for a new "top-level design" that not only encompassed policy substance, but also envisioned a comprehensive reorganization of the institutional landscape for digital policy.

Previously, this policy area was fragmented across numerous ministry-level bodies, including the Ministry of Industry and Information Technology, which mainly covered technical questions, the Ministry of Public Security, which dealt with information security issues, and the propaganda bureaucracy, in charge of managing online content. This fragmentation meant that authorities were not always prepared for the cross-cutting ramifications of rapid technology adoption. In particular, the meteoric rise of China's online giants, in areas ranging from e-commerce to social media, caught them by surprise. Propaganda departments, for instance, had organized online content largely in line with the approach used for traditional media. The advent of user-generated content, and social media most notably, fueled greater political discourse online, including political scandals and what the leadership described as harmful rumors. Taming this raucous online sphere became the first priority of the institution that later became the Cyberspace Administration of China (CAC). Moreover, greater Internet penetration led to increased societal relevance and political priority of cross-cutting questions concerning consumer and data protection, in response to greater incidence of online fraud and swindles.

Simultaneously, China's vulnerability through reliance on foreign technology, as well as its relatively weak position in global cyber governance and the worldwide digital economy also increasingly became matters of concern. The Snowden revelations about the capabilities of US intelligence services reinforced pre-existing beliefs that the United States would use digital means to target the stability and integrity of China's political structure. Microsoft's announcement to discontinue security support for Windows XP in 2011 –

[1] Segal, Adam. "China's Pursuit of Cyber Power." *Asia Policy* 15, no.2 (2020): 60-66.
[2] Creemers, Rogier. "How China intends to become a "cyber power." *Hérodote* 177-178, no. 2. (2020): 297-311.

which powered over two thirds of computers in China at that time – underlined how corporate decisions taken abroad could have a major impact on the security of domestic systems. Chinese businesses were, in many areas, not able to substitute or compete with foreign technologies. At the diplomatic level, processes concerning norms for state conduct in cyberspace started to gain speed, but China's inexperience in these processes meant it had little impact or influence.

With the cyber power strategy, the leadership sought to integrate these various strands of what it would come to call "cybersecurity and informatization" (*wangluo anquan he xinxihua*). Between 2013 and the present, it created an entirely new *xitong* (system) to deal with this policy area. A *xitong* is best understood as a sector-specific bureaucratic cluster of Party and State institutions[3]. *Xitong* cross both horizontal and vertical lines. On the one hand, they involve central-level departments as well as provincial and local-level units. On the other hand, they have institutions forming the core of the system, and entities that are more involved at the peripheral level. For instance, the People's Bank of China plays a very central role in the financial *xitong*, but a more peripheral one where it comes to cybersecurity and informatization. At the heart of all *xitong* lies a core coordinating organization, often called a "central commission" (*zhongyang weiyuanhui*) or "central leading group" (*zhongyang lingdao xiaozu*). This is led by a highly senior official, with a membership grouping high-level functionaries from all member institutions. This organization is primarily in charge of making major policy decisions on the basis of interdepartmental consultation, and acts as an interface between the top leadership and the *xitong's* members. For more detailed policy drafting work, overseeing implementation and providing feedback, this core organization is assisted by an office, usually housed within a permanent Party or State body. Next in line, the *xitong* contains the national-level ministries and administrative departments in charge of drafting and implementing specific pieces of regulation. At the local level, government agencies with responsibilities mirroring those at the central level sometimes draft local ordinances within the scope of their responsibilities and dispose of the majority of resources for daily management and enforcement. Supplementing formal government departments are specialized technical and research bodies, as well as intermediary organizations. The former includes think tanks affiliated with government departments, who provide expertise and analysis for policymakers, as well as specialized departments generating technical input, while the latter consist of Party-led sectoral alliances connecting the policy landscape with industry.

[3] Saich, Tony. *Governance and Politics of China* (New York: St Martin's Press, 2015), 107 – 140.

The leadership itself describes its envisioned model as "concentric circles", with Part-state entities at the core, and extending into all relevant areas of technology development and use, including industry, education, research and application[4]. As such, the cybersecurity and informatization *xitong* also feeds into universities and research centers, providing guidance on new academic courses to be developed, as well as the direction of academic, scientific and corporate research. It is in constant communication with China's burgeoning digital economy, striving to ensure that businesses are aware of their place in the greater scheme of things as they pursue their own growth and innovation strategies. Lastly, the leadership explicitly calls for a greater awareness concerning digital issues among ordinary technology users, amongst others through mechanisms of "social supervision" of technology businesses.

All protestation concerning "top-level design" notwithstanding, it should not be assumed that *xitong* are monolithic entities or harmoniously operating collectives. Interagency strife and turf battles are as present within the Chinese Party-state as they are in any polity. Every member of a *xitong* brings in its own departmental incentives, objectives and concerns, and pursues their interests as much as possible. As considerable efforts are made to present a façade of unity, their presence can usually only be gleaned indirectly, for instance through contrasting approaches presented by government departments in official media, obvious compromises or overlaps in the definition of regulatory powers, or through delays in the promulgation of announced laws and regulations. Such signs, however, can be very useful for China observers, as well as for diplomatic or commercial purposes.

This report will present a brief overview of the most important members of the cybersecurity and informatization *xitong*. It will describe their history and development, key functions and responsibilities, and main interests. It will also propose several recommendations for more effective engagement with this regime.

The Central Commission for Cybersecurity and Informatization (CCCI)

The CCCI forms the pinnacle of the cybersecurity and informatization pyramid. It was established in 2014, named

[4] "Xi Jinping's Speech at the National Cybersecurity and Informatization Work Conference," *China Copyright and Media*, April 22, 2018, https://chinacopyrightandmedia.wordpress.com/2018/04/22/xi-jinpings-speech-at-the-national-cybersecurity-and-informatization-work-conference/

"Central Leading Group for Cybersecurity and Informatization". At its foundation ceremony, Xi Jinping – who chaired the new body personally – laid down the foundations of China's "cyber power" strategy. The core of this strategy was to integrate previously fragmented bureaucratic structures and policy areas. As Xi stated in his speech: "cybersecurity and informatization are two wings on one body, and two wheels on the same cart". Unified leadership and "top-down design" (*dingceng sheji*) were called for to address China's vulnerabilities with greater efficacy[5].

Reflecting these priorities, the new Leading Group largely integrated the functions, as well as the membership of two previously existing institutions: The State Informatization Leading Group and the State Network and Information Security Coordination Group. The group was chaired by Xi Jinping, with premier Li Keqiang and propaganda chief Liu Yunshan (later replaced by his successor Wang Huning) as deputy chairs. Its further membership includes senior Party leaders, such as the heads or deputy heads of the Central Propaganda Department, the Central Policy Research Office, the Central Military Commission, the Central Political-Legal Commission, the Central Committee General Office, and the Central Secretariat. It also lists directors of important state bodies: the CAC, the Ministry of Public Security, the Ministry of Industry and Information Technology, the Ministry of Foreign Affairs, the National Development and Reform Commission, the Ministry of Education, the Ministry of Science and Technology, the Ministry of Finance, the Ministry of Culture, the State Administration for Press, Publications, Radio, Film and Television, the PLA General Staff and the People's Bank of China. The latter one was the only new addition to the combined membership of the two previous groups[6]. Together with the integration, the administrative rank of the participants was raised: the previous groups had been chaired by the Prime Minister, with delegates of vice-ministerial rank. Now, full ministers would participate in the new Leading Group, with Xi Jinping himself as chairman. A later name change in 2018, from "Central Leading Group" to "Central Commission" was largely symbolic, signaling that this organization was not an ad hoc or provisional affair, and that digital policy would become one of the central

[5] "Central Leading Group for Internet Security and Informatization Established," *China Copyright and Media*, March 1, 2014, https://chinacopyrightandmedia.wordpress.com/2014/03/01/central-leading-group-for-internet-security-and-informatization-established/

[6] "Cybersecurity and Informatization Leading Group: Names and Documents," *China Copyright and Media*, March 13, 2014, https://chinacopyrightandmedia.wordpress.com/2014/03/13/cybersecurity-and-informatization-leading-group-names-and-documents/

pillars of the Party's overall program[7]. As far as can be ascertained from publicly available sources, its composition and policy remit remained the same.

The CCCI operates largely secretively. There is no public record of its meetings, and little indication of the frequency with which they take place. It only produces a few dozen documents per year, most of which are not made public. The few that are usually relate to relatively mundane matters such as the organization of National Cybersecurity Week or the convention of cybersecurity competitions. It has not, thus far, published any major policy planning documents under its own name. Interestingly, and atypically, it may have some direct regulatory competences. Regulations on cybersecurity review processes for components in critical infrastructure accord the CCCI certain reviewing and approval powers[8]. Most of its work, however, consists of interagency coordination and leadership, facilitating decision-making and settling interdepartmental tensions in the area of cybersecurity and informatization. The majority of administrative support is performed through its Office: this is the Cyberspace Administration of China (CAC) under a "one body, two plaques" (*yige jiguo liangge paizi*) arrangement.

The Cyberspace Administration of China

The Cyberspace Administration of China draws back to 2011. At that point, the State Council Information Office, the government's official spokesbody, established a new subordinate department to manage online communications. Then dubbed the State Internet Information Office (SIIO – *Guojia hulianwang xinxi bangongshi*), its main task was, unsurprisingly, advancing the official line in the digital sphere. It had no independent staffing or leadership. This situation changed soon after the accession of Xi Jinping in late 2012. Both the run-up and aftermath of the 18th Party Congress had been marred by online rumors, official scandals and tense political debates about China's future, and the new leadership rapidly demonstrated that regaining control over the raucous online social media sphere became a priority.

[7] Creemers, Rogier et al., "China's Cyberspace Authorities Set to Gain Clout in Reorganization", *New America*, March 26, 2018 https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/

[8] Sacks, Samm et al., "China's Cybersecurity Reviews for 'Critical' Systems Add Focus on Supply Chian, Foreign Control (Translation)", *New America*, May 24, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control-translation/

By the summer of 2013, Beijing propaganda director Lu Wei had become the SIIO's first independent director and had started on an energetic campaign targeting online celebrities and well-known political voices, rapidly curtailing online debate[9]. On that basis, SIIO has since instituted ever-greater limits on online activities, including stricter rules on content, a real-name registration system and limitations to publicly available social media. In 2014, SIIO gained authority over all online content, effectively usurping the powers of the vast majority of the traditional propaganda apparat from the online sphere[10]. Still, all CAC directors have concurrently held a vice-directorship in the Central Propaganda Department.

The leadership's intent to integrate the previously fragmented cyber governance landscape, coincided with the ambitions of Lu Wei, who actively sought to secure ever greater resources and powers for the SIIO. It not only gained the Office of the CCCI in February 2014, but it also took over two departments from MIIT, covering cybersecurity coordination and informatization promotion[11]. Later that year, it gained authority over CNNIC, which runs the Chinese Domain Name System (DNS). It would also take control over online emergency responder CNCERT/CC in 2018. Reflecting this broadening of responsibilities, its English-language name changed to Cyberspace Administration of China in 2014, although its Chinese-language name remains the same. CAC also attempted to play a role internationally: it sent delegations alongside the Ministry of Foreign Affair's ones to international cyber events, Lu Wei himself addressed the 57th ICANN meeting in London[12], and the Wuzhen World Internet Conference was established as a showcase event for China's global digital vision. However, Lu's ambitions came to an abrupt end in 2016, when he was removed from office. He would later be convicted for

[9] Creemers, Rogier, "Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century," *Journal of Contemporary China* 26, no. 103 (2017): 85-100.

[10] "Notice concerning Empowering the Cyberspace Administration of China to be Responsible for Internet Information Content Management Work", *China Copyright and Media*, August 26, 2014, https://chinacopyrightandmedia.wordpress.com/2014/08/26/notice-concerning-empowering-the-cyberspace-administration-of-china-to-be-responsible-for-internet-information-content-management-work/

[11] Zhang, Mengjie, "工信部机构职能调整：设网络安全管理局", *21st Century Business Gerald*, July 10, 2015, https://m.21jingji.com/article/20150710/herald/6eb60db043161658cad615b9825fafcb.html

[12] "ICANN50 in London: Lu Wei, Minister of Cyberspace Affairs Administration of China", ICANN, June 23, 2014, https://www.icann.org/news/multimedia/301

corruption[13]. Rumors circulated that Lu had made powerful enemies in the security services, attempting to take over the MPS' cybersecurity responsibilities. The truth of these rumors is a matter of conjecture, but what is clear is that CAC has been put in its place after Lu's removal. It was, for instance, publicly castigated for not satisfactorily contributing to the implementation of the Cybersecurity Law (CSL)[14], and its presence in international conversations has been dialed down. This does, however, not mean that it became unimportant. On the one hand, as the main working body of the CCCI, it plays a major coordinating role in the organization of digital policy. On the other hand, it has considerable regulatory responsibilities of its own. Apart from being in charge of online content control and related licensing formalities for online operators, the CSL appoints CAC as the competent department for cybersecurity review and critical information infrastructure management[15]. It is also the lead department for online personal data protection[16], co-manages data security together with MPS[17], and has drafted the National Cyberspace Security Strategy[18].

Outside of these direct responsibilities, CAC also oversees the work of a number of subordinate organizations, which in and of themselves have a major impact on Chinese digital policy making and the operation of its network infrastructure.

---

[13] Gao, Charlotte, "Double-Faced Lu Wei Jailed for 14 Years for Bribery", *The Diplomat,* March 27, 2019. https://thediplomat.com/2019/03/double-faced-lu-wei-jailed-for-14-years-for-bribery/

[14] Wang, Shengjun, "全国人民代表大会常务委员会执法检查组关于检查《中华人民共和国网络安全法》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》实施情况的报告", *NPC People*, December 25, 2017, http://npc.people.com.cn/n1/2017/1225/c14576-29726949.html

[15] Cybersecurity Law of the People's Republic of China, November 11, 2016. http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

[16] Creemers, Rogier et al., "China's Draft 'Personal Information Protection Law; (Full Translation)", *New America*, October 21, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/

[17] Creemers, Rogier et al., "Translation : China's 'Data Security Law (Draft)'", *New America*, July 2, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/

[18] "National Cyberspace Security Strategy", *China Copyright and Media*, December 27, 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

National Committee for the Standardization of Information Security (Technical Committee 260)

TC260 was established in 2002, in order to centralize the drafting of technical information security standards, which was previously fragmented across several government departments. For the first part of its existence, it worked under the leadership of MIIT, but was moved to CAC oversight together with the MIIT's cybersecurity departments. Since then, it has rapidly accelerated its work. There are nearly 300 standards currently in force, of which over 200 were introduced after this move. Dozens more are at various stages of the drafting process. While TC260 is nominally an independent organization, its close link with CAC is underscored by the fact that its head is CAC deputy director Zhao Zeliang. The list of deputy commissioners equally indicates how intertwined the Committee's work is with the rest of the cyber-architecture, including representatives from MIIT, MPS, CNITSEC, the State Cryptography Administration, the National Administration of State Secrets Protection, and the State Administration of Market Regulation. Its secretariat is run by the China Electronics Standardization Institute, which also hosts the Committee's offices[19].

TC260 has seven regular working groups, of which the first three are not open to foreign membership. These respectively are in charge of overall coordination, classified information security and encryption. The other four groups, which do have foreign members, cover authentication and authorization, security assessment, telecommunications security, and security management. A special working group, also open to foreign participation, addresses big data security. TC260 operates in a relatively open and transparent manner. However, where there is an overriding domestic interest, the voices of foreign members tend to be ignored, or a standard project is moved to a non-open working group[20].

The standards TC260 produces are, for the most part, not legally mandatory but "recommended" (*tuijian*). Even so, they have a major impact for cybersecurity regulation. In some cases, this is simply because they are held to espouse best industry practice, and in cases of inspection or enforcement, the party in question will need to explain why they deviated. They can also be used as requirements in government procurement processes. In other cases, standards are explicitly incorporated

[19] "全国信息安全标准化技术委员会", Accessed November 2020: https://www.tc260.org.cn/front/tiaozhuan.html?page=/front/gywm/ldsz_Detail

[20] Sacks, Samm; Li, Manyi Kathy, "How Chinese Cybersecurity Standards Impact Doing Business in China", CSIS Center for Strategic & International Studies, August 2, 2020, https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china

into new regulations by government departments. This can be a very useful way of bypassing interagency frictions on new regulations, as well as way of attracting less international attention to potentially impactful rules.

The Chinese Academy of Cyberspace Studies

CACS was founded in 2015, to serve as an affiliate think tank to CAC. It has, however, maintained a low profile. It publishes annual reports on the development of the Internet within China and globally[21], which provide a useful insight in the priorities and outlook of the cyberspace bureaucracy. It may also provide internal reporting to CAC and affiliated entities. It is, however, not active in the international environment, it does not play a prominent role in Track 1.5 or 2 discussions, nor does it seem to have solid relations with overseas counterparts.

CNCERT/CC

Sources disagree on when CNCERT was founded, somewhere between 1999 and 2001[22]. By 2003, it had established branches in 31 provincial level regions, and become member of the Forum of Incident Response and Security Teams (FIRST), an international industrial association to enhance cyber incident response. It is also on the Steering Committee of the Asia-Pacific Computer Emergency Response Team. Established under the then-Ministry of Information Industry, it remained subordinate to its successor organization MIIT until 2018, when it was reassigned to the CAC[23].

Its main task is, like CERTs worldwide, to respond to cyber-attacks. It aims to prevent, detect and counter vulnerabilities and incidents, monitor malware activity, coordinate the relevant industry actors, and engage internationally. It releases brief weekly, monthly and annual reports on its activities[24], and maintains the China National Vulnerability Database. However, although CNCERT's website claims it is a non-governmental technical center, it is also closely associated with the National Computer Network and Information Security Management Centre, amongst others sharing its address. This Centre

---

21 《世界互联网发展报告 2019》和《中国互联网发展报告 2019》蓝皮书发布, Cyberspace Administration of China, October 20, 2019, http://www.cac.gov.cn/2019-10/20/c_1573104612829741.htm

22 National Computer Network Emergency Response Technical Team/Coordination Center of China, CNCERT/CC, Accessed November 2020, https://www.cert.org.cn/publish/english/index.html

23 中共中央印发《深化党和国家机构改革方案》, Xinhuanet, March 21, 2018, http://www.xinhuanet.com/zgjx/2018-03/21/c_137054755.htm

24 National Computre Network Emergency Response Technical Team/ Coordination Center of China, CNCERT/CC https://www.cert.org.cn/publish/main/17/index.html

has played an important role in the development of the Great Firewall of China. GFW architect Fang Binxing was its director between 2002 and 2006. It was also implicated in the Great Cannon attack on software sharing platform Github in 2015[25].

China Internet Network Information Centre

CNNIC was established in 1997, under the aegis of the Chinese Academy of Sciences (CAS). It was transferred to CAC authority in 2014. Its most important role is that it oversees the technical operations of the DNS for the .cn top-level domains, as well as for Mandarin-language domain names. As such, it is an active member of the Asia-Pacific Network Information Centre. It is equally prominently present in the orbit of ICANN, whose outreach office in Beijing is located on CNNIC premises. Furthermore, it actively cooperates with computer science and computer engineering institutes in research, including departments of CAS, on whose campus CNNIC is still located. Lastly, CNNIC published statistical reports on the development of China's Internet every six months, which provide an authoritative view and analysis on the state of China's IT infrastructure and use[26].

Cybersecurity Association of China

CSAC was founded in 2016. It operates in close conjunction with CAC and other subordinate organizations: its director is CAC vice-director Wang Xiujun, and its legal representative CACS vice-director Li Yuxiao[27]. It is an intermediary organization, which broadly serves to assist government departments with the effective implementation of laws, regulations and policies. As such, it is tasked with matters such as facilitating interaction between government and its members, organizing policy research and publishing a sectoral journal, providing expertise for the drafting of legislation and standards, engaging in international multi-stakeholder discussions on cybersecurity, organizing talent and award schemes, organizing specific training and awareness-building, and supporting self-regulation among its members[28]. It has close to 300 member organizations (mostly businesses) and a similar number of individual members. It has four subordinate work committees, respectively dedicated to talent and education, cyber governance and

[25] Marczak, Bill et al., "An Analysis of China's "Great Cannon"", USENIX, Accessed November 2020 https://www.usenix.org/system/files/conference/foci15/foci15-paper-marczak.pdf

[26] "第 46 次《中国互联网络发展状况统计报告》", The Central People's Government of the People's Republic of China, September 29, 2020, http://www.gov.cn/xinwen/2020-09/29/content_5548176.htm

[27] "中国网络空间安全协会负责人", December 5, 2019, https://www.cybersac.cn/News/index/type/75

[28] "中国网络空间安全协会简介", Last Accessed November 2020, https://www.cybersac.cn/News/getNewsDetail/id/86/type/2

international cooperation, cybersecurity competitions and exercises, and law and public policy. Internationally, it is most visible through its repeated participation in the UN Internet Governance Forum (IGF), where it has organized sessions in successive years.

Ministry of Public Security

Prior to the establishment of the CCCI and the CAC, the MPS was one of the dominant actors in cybersecurity issue, a position that it has sought to maintain and consolidate. It fulfils a number of roles: it is one of the institutions giving direct instructions to news outlets, Internet businesses and the GFW on how to report on or censor particular kinds of information. As it commands Chinese police forces, it is also a necessary player in general enforcement of laws and regulations, as well as targeted campaigns concerning high-priority issues that are launched from time to time. However, its most important tasks in the cybersecurity area are those fulfilled by its 11th Bureau: The Cybersecurity Protection Bureau. This is one of the oldest institutions in the cyber landscape, having been established in 1983 as the Computer Management and Supervision Bureau[29]. First and foremost, this Bureau oversees the operation of the multi-level protection system (MLPS) for information security. This system divides all information systems within China into five tiers, with security protection requirements as well as governmental inspection and oversight increasing for higher-tiered networks. The system was established in 2007 and overhauled in 2018 on the basis of new requirements in the CSL[30]. The MLPS has also fueled administrative turf battles with the CAC: the MPS successfully resisted CAC attempts to take over the system. The CSL created a mandate for a separate system for the protection of critical information infrastructure, to be run by CAC. However, recent policy documents suggest that the MPS has managed to integrate these two systems under its own authority[31]. The MLPS also covers significant aspects of data protection, and it is noteworthy that although the CAC issued several draft regulations on data protection, none of these has ever entered

[29] "新中国成立 70 年来网络安全保卫工作成就回眸", Xiamen Julong Information, Sohu.com, September 24, 2020, https://www.sohu.com/a/343020166_120104342

[30] Sacks, Samm; Li, Manyi Kathy, "How Chinese Security Standards Impact Doing Business in China", *Center for Strategic & International Studies, August* 2, 2018, https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china

[31] Creemers, Rogier et al. "Chinese Government Clarifies Cybersecurity Authorities (Translation)", *New America*, September 25, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-government-clarifies-cybersecurity-authorities-translation/

into force. Instead, data security protection has now become subject to dedicated draft legislation, in which MPS plays the leading role – albeit with CAC assistance[32]. This solution bypasses interagency wrangling at the legislative stage, but does not resolve the overlap on the ground, which will continue to affect implementation and enforcement.

The 11th Department is also responsible for fighting cybercrime. While the majority of its efforts are focused domestically, it has also taken part in international operations. It worked together with the FBI on cases of identity theft and child pornography[33], while official media boast about cooperation with countries ranging from the UK, Canada and Australia to Fiji, Indonesia, Malaysia and Cambodia[34]. However, international cooperation remains hampered for a number of reasons. Both Chinese and foreign police forces may be wary of sharing technical information, a phenomenon that is likely to worsen as global technology tensions increase. Language barriers and limited Chinese operational capabilities equally play a role. At the same time, the legal underpinnings for such cooperation are far from mature. From the European perspective, for instance, China does not have mutual legal assistance treaties with many European countries. It also has not joined the Budapest Convention on Cybercrime, preferring a dedicated treaty to be concluded within the UN framework[35]. Lastly, cybercrime cooperation with China is likely to cause opposition in cases where Beijing might seek the arrest of dissidents or members of sensitive ethnic communities for politically related crimes.

Ministry of Industry and Information Technology

As indicated earlier in this report, MIIT was one of the lead ministries in the Chinese cyber landscape until it ceded several departments, and their concomitant responsibilities to the CAC. Nonetheless, MIIT retains an important role

[32] Rafaelof, Emma et al, "Translation: China's 'Data Security Law (Draft)'", *New America*, July 2, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/

[33] Cheng, Ron, "Prospects for U.S.-China Cybercrime Cooperation: The Road Thus Far", *The Lawfare Blog*, March 9, 2017, https://www.lawfareblog.com/prospects-us-china-cybercrime-cooperation-road-thus-far

[34] Cao, Siqi; Zhang, Ye, "China Active in Fighting Global Cybercrimes", *Global Times*, September 5, 2018, https://www.globaltimes.cn/content/1118356.shtml

[35] Peters, Allison, "Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime", *Foreign Policy*, September 16, 2019, https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/

concerning Internet and telecommunications infrastructure. According to a 2015 document arranging responsibilities between MIIT and CAC[36], it remains in charge of the construction and management of network infrastructure, including the roll-out of 5G technology, and related security protection tasks. To the latter end, its Telecommunications Protection Bureau was – somewhat confusingly – renamed into Cybersecurity Management Bureau and given a wide range of tasks. Illustrating the continued need for interagency coordination, these sometimes overlap with CAC and MPS responsibilities, for instance concerning harmful information, data security[37] or cybercrime. MIIT also retains regulatory authority over the DNS, even though CNNIC was transferred to CAC authority[38].

China Academy for Information and Communication Technologies

In the same way that CACS is the think tank doing research and policy development work for CAC, CAICT carries out this work for MIIT. In contrast with CACS, however, CAICT has a highly visible and years long track record in issuing authoritative publications reflecting the state of the field in research. Originally called Chinese Academy for Telecommunications Research, its name was updated to reflect the broadening remit of MIIT's operations.

Its rules and capacities are diverse. It is not merely concerned with policy-oriented research, it also hosts considerable technological capabilities, including on the industrial Internet, cloud computing and the Internet of Things[39]. It regularly issues White Papers on emerging technologies, such as blockchain, AI and big data, outlining MIIT's vision on their social and economic impact. It provides input to industry and government on standards and technical trials, acting for instance as a technical certifier in ongoing 5G trials. It is deeply embedded in China's digital ecosystem, hosting, supporting or participating in dozens of industry bodies and associations, as well as technical

[36] "Notice Concerning Adjustment of the Ministry of Industry and Information Technology's Relevant Duties and Bodies", *China Copyright and Media,* April 20, 2015, https://chinacopyrightandmedia.wordpress.com/2015/04/20/notice-concerning-adjustment-of-the-ministry-of-industry-and-information-technologys-relevant-duties-and-bodies/

[37] "Guidelines for the Construction of the Online Data Security Standards System", *China Copyright and Media",* April 13, 2020, https://chinacopyrightandmedia.wordpress.com/2020/04/10/guidelines-for-the-construction-of-the-online-data-security-standards-system/

[38] "Internet Domain Name Management Rules", *China Copyright and Media,* October 16, 2020, https://chinacopyrightandmedia.wordpress.com/2017/08/24/internet-domain-name-management-rules/

[39] "中国信息通信研究院的组织机构", *CAICT,* Accessed November 2020 http://www.caict.ac.cn/wygk/zzjg/

working groups[40]. Lastly, CAICT is one of the major "third-party technical organizations" holding certifications to conduct cybersecurity review procedures of network services and products, one of the sub-regimes of the Cybersecurity Law. As such, CAICT plays an often outsized role in the on-the-ground build-up of China's digital economy[41].

Internet Society of China

The ISC was the original intermediary organization for the Internet sector and remains one of the most prominent. It was established in 2001, and its membership comprises leaders in China's private digital sector, as well as research institutes. It has 16 working groups, addressing issues ranging from online copyright protection and rural informatization to spam messaging and Internet finance[42]. It operates under the guidance of MIIT, and its current director is Shang Bing, a previous vice-Minister at MIIT and currently the CEO of telecommunications provider China Mobile. While the ISC presents itself as a non-governmental organization, it nevertheless plays a regulatory role. On the one hand, it has produced numerous self-disciplinary pledges and conventions, to which their members commit[43]. On the other hand, some policy documents reserve a specific role for the ISC in mobilizing industry and social support for digital policy[44] or even directly address it in line with government departments[45]. Internationally,

[40] "中国信息通信研究院的行业组织", *CAICT,* Accessed November 2020 http://www.caict.ac.cn/wygk/hyzz/

[41] Triolo, Paul; Webster, Graham, "Profile: China Academy for Information and Communications Technology (CAICT)", *New America,* October 16, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/profile-china-academy-information-and-communications-technology-caict/

[42] "Internet Society of China Organization", *ISC,* January 5, 2014, https://www.isc.org.cn/english/About_Us/Organization/listinfo-15318.html

[43] "Self-Discipline Norms for Internet Search Engine Service Companies on Resisting Obscenity, Sex and Other Such Unlawful and Harmful Information", *China Copyright and Media,* December 22, 2004, https://chinacopyrightandmedia.wordpress.com/2004/12/22/self-discipline-norms-for-internet-search-engine-service-companies-on-resisting-obscenity-sex-and-other-such-unlawful-and-harmful-information/

[44] "Opinions concerning Stimulating the Healthy and Orderly Development of the Mobile Internet", *China Copyright and Media,* January 15, 2017, https://chinacopyrightandmedia.wordpress.com/2017/01/15/opinions-concerning-stimulating-the-healthy-and-orderly-development-of-the-mobile-internet/

[45] "Guiding Opinions concerning Strengthening Cybersecurity Work in the Telecommunications and Internet Sectors", *China Copyright and Media,* August 28, 2014, https://chinacopy-

the ISC has been fairly active in venues such as the IGF over the years, presenting itself as a multi-stakeholder organization for the Chinese digital environment. Conversely, the ISC established the "China IGF" in May 2020[46]. It is also an accredited entity with the ITU[47].

Ministry of State Security

The MSS is China's intelligence and security agency, and as such is also responsible for foreign intelligence gathering. Unsurprisingly, there is little public information about its role in setting cyber policy – it does not even have an official website. It is, however, very active in cyber-enabled espionage and intelligence gathering. According to attribution reports, it is associated with the APT3 or "Gothic Panda" hacking group[48], as well as with APT10 or "Stone Panda"[49]. In 2020, the FBI indicted two individuals associated with the MSS, who had targeted research related to COVID-19 diagnosis tools and vaccines[50].

Furthermore, the MSS is of particular importance for China's cyber-diplomacy and the implementation of its cybersecurity agenda because of two institutions it oversees: CICIR and CNITSEC

China Institutes of Contemporary International Relations

CICIR is a think tank and research institution focusing on international affairs. It is closely associated with the MSS and much of its senior leadership has a background in intelligence. It is tasked with a range of activities, including publicly available academic research and teaching, as well as with providing analysis and reports to the senior leadership. It is also the primary institution responsible for Track 1.5 and

rightandmedia.wordpress.com/2014/08/28/guiding-opinions-concerning-strengthening-cybersecurity-work-in-the-telecommunications-and-internet-sectors/

[46] "China IGF Established in Beijing", *Internet Society of China,* July 10, 2020, https://www.isc.org.cn/english/Events&News/ISC_Events/listinfo-37877.html

[47] "Council Working Group of the Resolution 141", *International Telecommunication Union,* June 10, 2008, https://www.itu.int/council/groups/stakeholders/consultation2008/ms/replies/Entity-ISC.pdf

[48] "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3", *Recorded Future,* May 17, 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3/

[49] Kozy, Adam, "Two Birds, One STONE PANDA", *Crowdstrike,* August 30, 2018, https://www.crowdstrike.com/blog/two-birds-one-stone-panda/

[50] Warner, Gary, "Chinese "Covid-19" Hackers indicted after 11 year hacking spree", *Security Boulevard,* July 23, 2020, https://securityboulevard.com/2020/07/chinese-covid-19-hackers-indicted-after-11-year-hacking-spree/

Track 2 relationships with the outside world. With Europe, CIRIC currently maintains two such initiatives: the Sino-Europe Cyber Dialogue and the Sino-European Expert Working Group on the Application of International Law in Cyberspace. With the US, CICIR has collaborated on similar projects with the Center for Strategic and International Studies.

China Information Technology Security Evaluation Centre

CNITSEC was established in 2009, in order to gather information concerning vulnerabilities of software and hardware products, as well as information systems. It manages the China National Vulnerability Database for Information Security (CNNVD). CNITSEC is also certified as a body qualified to perform the security review processes established by the CSL and subordinate regulations. However, it also has a close link with MSS. CNITSEC's former Director, Wu Shizhong, for instance, also held leading positions in the Ministry's 13th Bureau, responsible for science and technology[51]. This has led to concerns that MSS might be using CNITSEC to acquire vulnerabilities to exploit later and seek to leverage the Centre's position as a security reviewer in order to acquire valuable intellectual property and other proprietary information.

Ministry of Foreign Affairs

The Ministry of Foreign Affairs has traditionally been one of the weaker departments in China's central government, and even if foreign policy has become more important and prominent in recent years, it still has a very limited voice in domestic decision- and policy-making. As such, it has little direct authority on any cyber-related policies. Its main role is an interlocutory one: participating in international cyber diplomatic processes to defend the Chinese line and gain insight into other countries' positions. A corollary element of this is that the MFA, together with specific think tanks, acts as an airlock, in order to avoid direct contact between domestic decision-makers and foreign voices. Its leading position in cyber diplomacy has not always been a given: in the first round of the UN GGE, Chinese participants came from the Ministry of Communications[52]. Under Lu Wei's tenure as CAC director, the MFA also had to contend with direct CAC intervention in a number of diplomatic and dialogue processes. With the consolidation of the cyber architecture, CAC has been largely withdrawn from

[51] Kozy, Adam, "Two Birds, One STONE PANDA", *Crowdstrike,* August 30, 2018, https://www.crowdstrike.com/blog/two-birds-one-stone-panda/

[52] Segal, Adam, "Chinese Cyber Diplomacy in a New Era of Uncertainty", *Aegis Paper,* No.1703, June 2, 2017, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf

the cyber diplomacy area, reflected in the MFA being the lead co-authoring department of China's international cyber strategy[53].

Since 2013, the MFA's work on cyber diplomacy has been carried out by a dedicated coordinator, whose position was established in 2013[54] to act as a counterpart to US top cyber diplomat Christopher Painter. In view of the fact that the UN GGE was housed within the UN First Committee, this position was created within the Arms Control Department, and has generally been staffed by career diplomats with arms control expertise. In addition, the Treaty and Law department has built up considerable expertise on global cyber governance, with a particular focus on the areas of cyber conflict and cybercrime[55]. As cyber-related tensioned increased, and as the expertise and experience of China's cyber diplomats have grown, they have become increasingly assertive in international circles, no longer taking a back seat to Russia's traditionally vocal delegations. During the first session of the UN Open-Ended Working Group, China issued its most detailed diplomatic statement thus far[56]. Given the disruption to global diplomatic processes due to the Coronavirus crisis, it is difficult to gauge the current trajectory of the MFA's work. The "Global Data Security Initiative" proposed by foreign minister Wang Yi in September 2020[57] largely echoes earlier Chinese diplomatic statements, and seems to serve as a response to escalating US pressure on Chinese digital businesses, as well as an effort to attract governments from the Global South who equally harbor misgivings about American preponderance in cyberspace.

Other Departments

[53] "International Strategy of Cooperation on Cyberspace", *China Copyright and Media,* March 1, 2017, https://chinacopyrightandmedia.wordpress.com/2017/03/01/international-strategy-of-cooperation-on-cyberspace/

[54] "外交部设立网络事务办公室 负责网络事务外交活动", *Xinhuanet Mobile Net,* June 14, 2013, http://world.people.com.cn/n/2013/0614/c157278-21846234.html

[55] Huang, Huikang, "Statement at Budapest Conference on Cyber Issues", *Chinese Mission Vienna,* October 10, 2012, http://www.chinesemission-vienna.at/eng/zgbd/t977627.htm

[56] "China's Submissions to the Open-ended Working Group", Last Accessed November 2020, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf

[57] Triolo, Paul; Webster, Graham, "Translation: China Proposes 'Global Data Security Initiative'", *New America,* September 7, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-proposes-global-data-security-initiative/

While the abovementioned ministries form the core of the domestic and international cyber affairs *xitong*, several other departments are members of the CCCI, or otherwise involved from time to time. Some of these are specialized technical bodies, including the State Cryptography Administration and the National Administration of State Secrets Protection. These are, amongst others, involved in the Multi-Level Protection System, as well as in the work of TC260. Others are departments supporting the education and research elements of China's digital strategy, such as the Ministry of Science and Technology and the Ministry of Education. The Ministry of Finance is involved both because of its rule in financing many elements of this strategy, as well as because of the importance the leadership attaches to blockchain technology and e-currencies. The latter point also explains the inclusion of the People's Bank of China.

Some CCCI members represent the traditional propaganda apparat, from which the CAC emerged. At the top stands the Central Propaganda Department, one of the CCP's most venerable bodies, which has a comparable role to the CAC, in the sense that it is in charge of drafting high-level policies and coordinating the activities of its subordinate government ministries. From Lu Wei onwards, every CAC director has also been a vice-director of the CPD, indicating the close linkage between the two policy fields. Until 2014, the Central Propaganda Department was in charge of all media content in China, including online content. While the prime authority for online content now lies with CAC, the CPD and its subordinate ministries retain a secondary role in terms of setting overall directives and policies for Party propaganda, as well as regulating a number of industries whose content may also be published online, such as the traditional television and press industries, the film and cartoon industries, and video gaming industries.

Implications and Recommendations

The creation of a new governance architecture for cyber affairs, initiated in 2014, seems to now be largely complete. It has entered a stable phase, where relatively little further major institutional adjustments likely are to occur. The primary objective in this process of organizational reform was to integrate and centralize existing government departments dealing with digital affairs, in order to enable more effective policymaking and implementation. To a certain degree, this has been successful, as evidenced by the passing of the CSL, as well as a number of fundamental policies and plans guiding the further development of cyber policy. However, while certain elements of this architecture are new, most notably the CCCI and the CAC, many of its component parts have a longer history, which still leaves its marks on current policy issues. The most notable effect in this regard is the somewhat tense relationship between CAC and MPS, particularly

with regard to the protection of critical information infrastructure and the multi-level protection system, as well as the slowly progressing build-up of the regulatory framework for data protection.

However, departmental interests and turf battles are not the only feature of this architecture that shapes outcomes. While it is clear by now that there is a wide degree of consensus concerning the broad outlines and principles of China's cyber agenda, there are still genuine debates and differences of opinion between the various offices involved on how these should be implemented in practice, and what this means for China's positioning in global cyber affairs. In some cases, these differences stem from the different missions of the departments involved: the MIIT focus on efficiently functioning telecommunications, for instance, will likely lead it to a different risk assessment from the security and stability focus of the MPS. In other cases, they may be the result of differing risk calculations: is it, for instance, better to allow foreign products in critical infrastructure systems after rigorous checking, or is it preferable to mandate domestic technologies, even where they may be less sophisticated or less secure than the foreign equivalents. As such, it should not be assumed that there is a uniform, monolithic "Chinese opinion" on specific policy points.

How, then, can foreign entities, including governments and businesses, engage with this architecture effectively? The first and most important step is to gain awareness of the roles the various Chinese entities play, and the concomitant advantages or disadvantages this generates. Although it may be logical, for instance, for foreign governments to primarily work with the MFA, this may not necessarily be the best versed in the problem, or the institution best placed to solve it. Businesses in specific industry areas would do well to develop a sound relationship with the regulator in charge, but also explore the connected ecosystem of think tanks, industry associations and ancillary bodies, which often provide potentially useful networking opportunities or information sources. Understanding the different positions ministries take might also help in trying to shape Beijing's behavior. The leadership is far more likely to listen to a Chinese voice than a foreign one, which means it might be better to try and amplify those voices rather than push for changes from abroad. What is required in any case, is a broad-spectrum effort to build connections and dialogues with the various parts of this architecture across the board. Interaction between Chinese officials and experts, and their European counterparts, remains highly limited, impeding the development of an epistemic or policy community in which at least some modicum of coexistence can be achieved, and in turn fostering misunderstanding and, at worst, fear. While no-one should be so naïve as to believe greater interaction will remove the often great contrast between Europe's position and that of China on many important points, eliminating distractions will help bring actual is-

sues at hand in greater relief, and mitigate potential destabilizing risk. This will be a difficult and unsatisfactory process for either side, but also an unavoidable one.

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

Universiteit Leiden

This report is published by the LeidenAsiaCentre.

Dr Rogier Creemers is an assistant professor at Leiden University's China Studies department. His main focus of research is the development of Chinese policy in the digital sphere, both domestically and at the global level.

This report forms part of the China in Global Cyberspace project, funded by the Netherlands Ministry of Foreign Affairs