CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Mikk Raud

CHINA AND CYBER: ATTITUDES, STRATEGIES, ORGANISATION

Tallinn 2016

www.ccdcoe.org
publications@ccdcoe.org

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is a NATO-accredited knowledge hub, research institution, and training and exercise facility. The Tallinn-based international military organisation focuses on interdisciplinary applied research, as well as consultations, trainings and exercises in the field of cyber security.

The heart of the Centre is a diverse group of international experts, including legal scholars, policy and strategy specialists who join forces with technology researchers, all from military, government and industry backgrounds.

Membership of the Centre is open to all Allies. As of September 2016, the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States have signed on as Sponsoring Nations (SNs) of the Centre. Austria and Finland have become Contributing Participants (CPs) – the status available for non-NATO nations.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

About this study

The NATO CCD COE series on national organisational models for ensuring cyber security summarise national cyber security strategy objectives and outline the division of cyber security tasks and responsibilities between agencies. In particular, the reports give an overview of the mandate, tasks and competences of the relevant organisations and of coordination between them. The scope of the reports encompasses the mandates of political and strategic cyber security governance; national cyber incident management coordination; military cyber defence; and cyber aspects of crisis prevention and crisis management.

Reports in this series

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in Spain

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the USA

Series editor: Kadri Kaska (Researcher, NATO CCD COE)

Information in this study was checked for accuracy as of August 2016.

China and Cyber:
Attitudes, Strategies, Organisation

By Mikk Raud
Visiting Researcher at the NATO CCD COE

Table of Contents

Introduction

Talking about the unprecedented success story of the People's Republic of China (hereafter simply 'China') has almost become a cliché. However, it is undeniable that China has developed into a key actor in world politics, and other states cannot overlook or ignore its opinion or intentions on whichever considered terrain. With its immense and growing influence over the whole planet, cyberspace is no exception.

According to Internet Live Stats, the number of internet users has already surpassed 3.4 billion, with 721 million coming from China.[1] Naturally, China is increasingly dependent on various cyber assets and the Chinese authorities have reacted accordingly. We have witnessed a growing emphasis on cyber security measures, as well as an increase in the country's readiness to take advantage of the opportunities that the internet provides, and to respond to the threats it poses to national security. With the largest population in the world, China holds a sizeable pool of experts with potential value for the government and its cyber operations.

Understanding China's cyber structure, strategies and organisation is not an easy task. The Chinese have not established an exhaustive approach to cyber issues in the form of a strategy clearly outlining the country's cyber objectives and their execution. This has created much uncertainty for both China's domestic environment and, understandably, outsiders for whom the complex hierarchies, command structures and various defence papers are very confusing. Even though the Chinese do not seem to mind a certain degree of mystery, a step suggesting their increasing desire to manage their cyber operations more efficiently can be seen in the recent creation of the Central Internet Security and Information Leading Group, for which President Xi Jinping has taken personal responsibility to define China's cyber strategy. This also stands as a good example of how the Chinese understand cyber as something strongly integrated with society, and do not separate it from the general flow of governance. Admittedly, the challenges that originate from such a distinctive approach to cyber have great potential to affect the Western world's activities in cyberspace for a number of reasons.

Firstly, the way in which the world's biggest internet community is governed influences the overall development of the internet worldwide. Granting netizens the opportunity to become a part of the online world free from physical constraints, or restricting their access to information and using the internet as a tool against dissent are the two fundamentally different choices facing the Chinese government. As it has so far stuck to the second option, China's participation in the global internet community has been greatly hindered, and thus countless opportunities for cooperation have been missed.

Secondly, there is significant evidence that the Chinese government, together with the Chinese military, private corporations, and unaffiliated citizens, conduct intrusions against major Western powers as well as in the neighbouring region every day, targeting academia, industry and government facilities for the purpose of amassing technological secrets.[2] For example, the Chinese have, among other high-tech weapon system designs, obtained those of the F-35 stealth fighter – America's most expensive military investment ever.[3] The underlying purpose of these activities is to gain advantage in the economic, political and military fields, and often simply show the extensive harm they are capable of causing should the need arise.

---

[1] Internet Live Stats compiles data from six major reliable agencies, including the International Telecommunications Unit and the World Bank. See more at 'China Internet Users.' Internet Live Stats, 2016. Accessed 18 Aug. 2016. <http://www.internetlivestats.com/internet-users/china/>. Internet Live Stats compiles data from six major reliable agencies, including the International Telecommunications Unit and the World Bank.

[2] Richard Clarke, a former special advisor on cyber security to President George W. Bush, illustrates the situation rather comprehensively, believing the Chinese hacking to be unprecedented in the history of espionage: '*Exabytes of data have been copied from universities, industrial labs, and government facilities. The secrets behind everything from pharmaceutical formulas to bioengineering designs, to nanotechnology, to weapons systems, to everyday industrial products have been taken by the People's Liberation Army and by private hacking groups and given to China.'* Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* Ecco, 2010, p. 59.

[3] For an overview of all publicly reported intrusions attributed to China from 2005 to 2013, see Lindsay, Jon R. and Tai Ming Cheung. 'Chapter 3: From Exploitation to Innovation,' pp. 58-61 in Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron (eds) *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain.* Oxford University Press, 2015.

While some experts suggest that China's cyber units have so far 'outmanned and outclassed'[4] their adversaries, the West has actually demonstrated firm responses. For instance, several Chinese telecommunication companies such as Huawei have been banned from contracting and acquiring any broadband network providers in the US and Australia.[5] It seems that whichever direction the Chinese offensive cyber capabilities develop, the West is unwilling to accept any growing danger to its private information, cyber infrastructure or security in general.[6]

In order to establish a comprehensive understanding of China's cyber attitude, it is of paramount importance to know its strengths and weaknesses. For that purpose, this paper aims to give readers a detailed overview of China's cyber capabilities, related documents and strategies, and the general command structure of its tactical execution layer. Importantly, the country's distinct approach raises the necessity of introducing the general national strategic thinking and framework into which cyber falls. The paper acts as a comprehensive starting point for anyone aiming to get a foothold on affairs related to China and cyber.

1. China's Cyber Background and Related Challenges

1.1. Free Information and Foreign Technologies Seen as Threats

As with most states, China is heavily dependent on technology, making the government highly concerned about developments regarding the internet and the information flow that it generates. The Chinese see uncontrolled information as a threat to the regime, paying great efforts to obtain the economic gains that the internet provides, but simultaneously maintain political control.[7] It is believed that, for the Chinese, the whole concept of the internet is built around controlling information through real-time censorship, constituting a completely different view from that in the West.[8] Indeed, ever since the internet became a publicly available communication platform in China, the question was not whether to control it, but rather how to control it.[9] The most explicit example of such regulatory measures is of course the Great Firewall of China, which by monitoring all traffic in Chinese cyberspace enables the authorities to deny access to a variety of selected websites and disconnect all Chinese networks from the global internet network.

Other than being afraid of the growth of internal opposition through information, the government is also very sensitive about foreign information systems. Despite local technology and telecom companies' efforts to supply high quality products for domestic use, a large part of technology connected to Chinese networks still originates from the West. Chinese officials are convinced that these systems are equipped with Trojan horses and loopholes to steal China's national secrets and prevent its further economic upsurge.[10] To counter these fears, the

---

[4] Hannas, William C., James C. Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*. Routledge, 2013.

[5] Stark, Jill. 'US Follows Australia in Naming Huawei as a Possible Security Threat.' *The Sydney Morning Herald*. 9 Oct. 2012. Accessed 18 Aug. 2016. <http://www.smh.com.au/it-pro/security-it/us-follows-australia-in-naming-huawei-as-a-possible-security-threat-20121007-277ad.html>.

[6] The US National Security Agency (NSA) has itself hacked into computers belonging to Huawei and China Telecom, a fact that became public with the Snowden leaked documents evidencing the American worldwide online spying. See more at Sanger, David E., and Nicole Perlroth. 'N.S.A. Breached Chinese Servers Seen as Security Threat.' *The New York Times*. 22 Mar. 2014. Accessed 18 Aug. 2016. <http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0>.

[7] Grauman, Brigid. *Cyber-security: The Vexed Question of Global Rules*. Report by Security & Defence Agenda, 2012, p. 55.

[8] David Bandurski, cited in Lococo, Edmond, and Keith Zhai. 'China Seeks Global Internet Influence at CEO Forum on Canal Bank.' *Bloomberg Technology*. 18 Nov. 2014. Accessed 18 Aug. 2016. <http://www.bloomberg.com/news/articles/2014-11-18/china-seeks-global-internet-influence-at-ceo-forum-on-canal-bank>.

[9] Creemers, Rogier. 'Cyber-Leninism: History, Political Culture and the Internet in China.' (2015): p.10. Draft available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2589884>.

[10] Ernst, Dieter. *Indigenous Innovation and Globalization – the Challenge for China's Standardization Strategy*. Report by the East-West Center, 2010, p. 33. <http://www.eastwestcenter.org/fileadmin/stored/pics/Ernst%20EWC%20NBR%20Report%20%2011%2015%2010.pdf>.

government has imposed heavy controls over the information security industry, deterring foreign investors, especially the Americans, from seeking business opportunities in China. Yet, demonstrating how far the Chinese still are from the desired technological independence, Beijing was not particularly pleased when in early 2014, Microsoft decided to stop customer support for Windows XP, the operating system used extensively in Chinese government computers.

1.2. Chinese Views on Controlling Cyberspace

Public discussion about the nature and future of cyberspace was brought to the international level only very recently.[11] In 2013, the United Nations Group of Governmental Experts, including the representative from China, concluded that the UN Charter and international law are fully applicable to state behaviour in cyberspace, a position which has also been taken by NATO countries.[12] However, this position impliedly assumes the use of already existing institutional framework, which, facilitated by ICANN, is more multi-stakeholder than intergovernmental. The latter would better allow each government to regulate the internet itself, the main premise of China's strong belief in so-called 'cyber sovereignty'.

China has introduced its alternative position through the Shanghai Cooperation Organisation (SCO) in the UN General Assembly, together with Russia and several Central Asian countries, first in 2011, with a revised version in January 2015.[13] A common line between the SCO countries is a belief in the primacy of the nation state, which should be carried over into cyberspace.[14] According to a report by the US-China Security Review Commission, this allows the Chinese to dwell on two corollaries. Firstly, the users of cyberspace, both domestic and foreign citizens within a state's territory, should be controlled by the host state, a clear contradiction of the Western position which supports a liberal cyberspace respecting human rights.[15] In China's political culture, maintaining social order is unquestionably more important than individual privacy.[16] Secondly, China is particularly sensitive in exercising its right to sovereignty in cyberspace and does not want it to be interfered with by any other state or international organisation.[17] Therefore, somewhat contradictory to its position regarding the UN report, China does not see international law as the main regulator of cyberspace, but prefers each state setting its own rules.[18] China has also criticised the Tallinn Manual as an effort to manipulate cyberspace through law.[19]

Another concern characterising China's attitude towards general governance of cyberspace is its antipathy to the US. As many official statements by the Chinese press, the People's Liberation Army (PLA) and academics have shown, China is concerned about the US using its status and influence as the world's leading technology power to establish international rules and norms favourable to the US. Thus, China often justifies its actions in cyberspace as

---

[11] When talking about rules in the internet, it is necessary to distinguish between two separate concepts. First, 'internet governance' is a term for norms, rules and procedures that shape the use of the internet in general, and is facilitated by the Internet Corporation for Assigned Names and Numbers (ICANN). Different from 'internet governance' is the framework of how a sovereign state behaves in cyberspace.

[12] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Report of the United Nations General Assembly, 2013. <http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98>, and North Atlantic Treaty Organization. *Cyber Defence Pledge*. 8 July 2016. Accessed 18 Aug. 2016. <http://www.nato.int/cps/en/natohq/official_texts_133177.htm>.

[13] *International Code of Conduct for Information Security*. Report of the United Nations General Assembly, 2015. <https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf>.

[14] Grauman, 2012, p. 56.

[15] Hsu, Kimberly, and Craig Murray. *China and International Law in Cyberspace*. Report by the U.S.-China Economic and Security Review Commission, 2014, p. 2.

[16] Grauman, 2012, p. 56.

[17] Hsu and Murray, 2014, p. 2. For an example of the Chinese position on these issues, see 'China's Perspective on Building a Peaceful, Secure, Open and Cooperative Cyberspace.' UNIDIR Conference. 10 Feb. 2014. Accessed 24 Aug. 2016. <http://www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf>.

[18] Segal, Adam. 'The Deepening Divide in U.S.-China Cyber Relations.' *The National Interest*. 29 Oct. 2014. Accessed 18 Aug. 2016. <http://nationalinterest.org/blog/the-buzz/the-deepening-divide-us-china-cyber-relations-11568>.

[19] The Tallinn Manual disagrees with any call for new regulations to govern cyberspace.

a response to hostile developments by the US military.[20] A point further strengthening this understanding is the fact that ICANN is located in Los Angeles and is under US jurisdiction, even though it is independent of the US government. Moreover, as the US is a founding member of the majority of the world's international institutions, China believes it to have exceptional control over cyberspace and its governing principles. For example, during the Budapest Conference on Cyberspace in 2012, the official statement of the Chinese representative included points that criticised the US for militarising cyberspace and unfairly allocating cyber resources among only developed states to maintain its control.[21] This is why several Chinese experts believe China has a key role in promoting a new, 'common and inclusive global internet governance'[22] model that redistributes digital resources and governance rights more equitably. Admittedly, such a model would probably lack legitimacy in the eyes of a large part of the international community.[23]

1.3. China vs. the West and the United States

The different understandings of internet governance can be seen as part of the general existential competition between China and the West, which often asks whether China will continue growing as the peaceful lion as it claims, or whether conflict with the liberal democratic ideologies is bound to occur. As the US undeniably has the greatest economic and military capabilities among the West, it has taken the lead in containing China's growth. Whereas physical confrontation has so far been avoided, the situation is certainly fiercer in cyberspace, which both the US Department of Defense (DoD) and the PLA have begun to view as a new domain of conflict, leading to cyber espionage and malicious activities from both parties, who refuse to admit their state-level involvement and rather blame their opponent.[24] China considers itself equal with the US when it comes to comparing the two countries' size, power and influence in the online field, which creates tensions over who should dominate the digital world.[25] Understandably, such tensions frustrate cooperative interaction not only in the cyber domain, but also in the economic and political fields.

After the US indicted five PLA officers for stealing data from American corporations in May 2014,[26] many saw the cyber-agreement between President Xi and President Obama in September 2015 as a positive development. Both Presidents pledged not to knowingly conduct or support cyber theft, including that of intellectual property, trade secrets, or confidential business information in general.[27] Some cyber security firms have indeed noted a reduced number of attacks against American businesses, but this might be due to improved tactics making the attackers harder to detect, or simply a turn to new, uninformed targets in other countries, and not because of any deep

[20] Hsu and Murray, 2014, p. 1.
[21] Hurwitz, Roger. 'A Scene from the Road to Cyber Governance: The Budapest Cyberspace Conference.' *MUNK School of Global Affairs*. 26 Feb. 2013. Accessed 19 Aug. 2016. <http://www.cyberdialogue.ca/2013/02/a-scene-from-the-road-to-cyber-governance-the-budapest-cyberspace-conference/>.
[22] Jiang, Li, Zhang Xiaolan, and Yu Feibao. 'Deadlock in International Cooperation Regarding Cyber Security and Its Solutions.' *Xiandai Guoji Guanxi - Contemporary International Relations* 9 (2013), cited in Liffran, Camille. 'Chinese Perspectives on Cyber Security and International Relations.' *China's Expanding Cyberspace* (2014): pp. 5-7. <http://www.ecfr.eu/page/-/ChinaAnalysisEng_June2014.pdf>.
[23] The subject of a broader-based internet governance model was brought up at the World Conference on International Telecommunications in 2012. The outcome was a clear split between nations favouring the introduction of a multilateral governance model (most of the so-called BRICS countries, with the exception of India, and developing countries) and those opposed to it, including the USA, EU member states, Australia and Japan.
[24] Lindsay, Jon. *China and Cybersecurity: Political, Economic, and Strategic Dimensions*. Report by the University of California Institute on Global Conflict and Cooperation, 2012, p. 1. <https://www.usnwc.edu/Academics/Faculty/Derek-Reveron/Documents/China-and-Cybersecurity-Workshop-Report-final.aspx>.
[25] Cyrus Mewawalla, cited in Lococo and Zhai, 2014.
[26] This was an act of seemingly no great significance, but at the time conveyed a highly symbolic meaning about the countries' bilateral relations in the cyber field in general. See more at Tiezzi, Shannon. 'US Indicts 5 PLA Officers For Hacking, Economic Espionage.' *The Diplomat*. 20 May 2014. Accessed 19 Aug. 2016. <http://thediplomat.com/2014/05/us-indicts-5-pla-officers-for-hacking-economic-espionage/>.
[27] 'The Obama-Xi Cyber Mirage.' *The Wall Street Journal*. 27 Sept. 2015. Accessed 19 Aug. 2016. <http://www.wsj.com/articles/the-obama-xi-cyber-mirage-1443387248>.

respect for the agreement.[28] FireEye's recent report states that the China-based units' operations against US companies saw a decline in frequency a year before the Xi-Obama agreement and have since become more focused and calculated and have maintained their level of success. The report attributes such changes to military and political changes within China, the frequent exposure of Chinese hackers, as well as the pressure and threat of sanctions from the US.[29] Nevertheless, the overall situation has remained fairly static and therefore the Xi-Obama agreement should not be seen as a turning point.

It is essential to note that the foundation of such behaviour, as well as Chinese thinking on asymmetric warfare in general and particularly on cyber-war, was laid down in *Unrestricted Warfare* – a book written by two PLA colonels Qiao Liang and Wang Xiangsui in 1999 to provide a strategy of how China as a weaker country could defeat a technologically superior foe outside the scope of using hard military power. Part of the American media irresponsibly depicted the book a grand strategy to destroy the US due to its precise scrutiny of the American military. Indeed, the colonels identified the US military's main weakness as its dependence on ICT-networked systems through which the Chinese could obtain an asymmetric advantage.[30] According to SIPRI's database, at the time of the book's publication, the difference in the two countries' military expenditure was about 15-fold. Even though the gap has closed significantly, the US defence budget is still around three times that of China.[31] Therefore, if the front door remains closed, the smart player will try to sneak in through the back door or a window. That is exactly what the Chinese strategy is about – knowing that even with wholesale modernisation, it will not be the equal of the US military for decades, and so China is ready to win any confrontation without physical battles by using efficient and overwhelming cyber-attacks.[32]

However, even though the book has predominantly been characterised as a plan to defeat the US, it really should be perceived as an opportunity to understand China's different operational thinking on the power struggle in general. This is something that needs to be noticed and learned not only by the US, but also by other Western powers if they want to be on par with China in the cyber race. Colonels Qiao and Wang noted that it is vital to recognise that the battlefields in future wars will be traditionally non-war spheres like cyberspace, which strongly affect national security.[33]

1.4. Understanding the Chinese Cyber Definitions

In looking into Chinese cyber developments, one should also be aware of their dissimilar terminology for cyber as compared to the North-Atlantic area.[34] Efforts have been made to reconcile the mismatches, but these continue to be met by a remarkable lack of enthusiasm. What can be done for the purpose of this research is to explain the most significant differences.

---

[28] Harold, Scott Warren. 'The U.S.-China Cyber Agreement: A Good First Step.' *RAND Corporation*. July 2016. Accessed 19 Aug. 2016. <http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>.

[29] *Red Line Drawn: China Recalculates Its Use of Cyber Espionage*. Report by FireEye, 2016, pp. 12, 15. <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf>.

[30] Qiao, Liang, and Wang Xiangsui. *Unrestricted Warfare*. PLA Literature and Arts House, 1999. Unofficial translation of the book is available at Cryptome's website at: <http://www.cryptome.org/cuw.htm>.

[31] 'SIPRI Military Expenditure Database.' *SIPRI*. 2016. Accessed 19 Aug. 2016. <http://www.sipri.org/research/armaments/milex/milex_database>.

[32] Clarke and Knake , 2010, p. 53.

[33] Qiao and Wang , 1999, pp. 144-145, cited in Thomas, Timothy L. *The Dragon's Quantum Leap*. Foreign Military Studies Office, 2009, p. 27.

[34] As Keir Giles and William Hagestad point out in their comprehensive paper on English, Chinese and Russian mismatching cyber definitions, the common disparities need to be removed to achieve a mutual understanding on governing cyberspace. It is easier to accept the current situation, but a better solution may exist in composing an international cyber lexicon that addresses all the relevant terms. This, however, will be a tremendous challenge due to the opposition of China and other alternative players like Russia, who find it more appealing to seek cooperation among themselves and other like-minded countries instead of engaging into a constructive dialogue with the US-led English-speaking countries. See more at Giles, Keir, and William Hagestad II. *Divided by a Common Language: Cyber Definitions in Chinese, Russian and English*. Proceedings of 5th International Conference on Cyber Conflict, Tallinn. 2013. *NATO CCDCOE Publications*. <https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf>.

To begin with, the Chinese do not use the word *cyber* as extensively as the West. They perceive everything related to cyber developments as part of a broader transformation from an industrial society to an information society, referring to the process as ***informationisation*** or ***informatisation*** (the latter is normally used in translations and has wider use).[35] Similarly, while the West classifies *cyberspace* as the global domain covering the use of electronics, interdependent networks of information technology infrastructure including the internet, and other telecommunication networks and data,[36] the Chinese term closest to what would translate as *cyberspace* merely entails the necessary components of a connected device and actions related to using it.[37] For the Chinese, *cyberspace* is thus only a subset of ***information space*** – the landscape for the largest scale communication to the world's population, which includes human information processing and cognitive space.[38]

It is also important to distinguish between *cyber security* and *information security*. The West, including the NATO allies, sees *cyber security* as the security of computer and information systems as physical and logical entities, and *information assurance* or *information security* as referring to security of the content. The Chinese, however, view both the information systems and the content of information as integral and connected parts of ***information security***.[39] This holistic understanding thus extends the use of the term from purely ICT-related issues to mental aspects and explains why the Chinese government's approach to *information security* has been control-seeking and restrictive. Likewise, the Chinese have adopted ***information warfare*** as a distinct, yet integrated and discrete discipline, which is incompatible with the Western view, which has recently been dividing the concept into smaller and separate disciplines, such as psychological operations and strategic communications. The Chinese use c*yber warfare* only when describing Western countries and their cyber operations.[40]

It would be a major challenge to have each player adopt a single lexicon, but as long as one understands what is behind the varying definitions, it will become easier to evaluate cyber relationships between China and the West. In this paper, unless specifically referring to a Chinese initiative or particular concept, *cyber* and its derivations should be read in the conventional Western understanding. However, dissimilar terminology is certainly not the hardest of the obstacles on the way to elaborating sophisticated cyber cooperation between China and the West. China's notion of sovereignty and independence has restrained it from considering Western points of view and international law's efficiency in cyberspace. Reluctant to adopt the US-led positions, the Chinese prefer to control cyberspace through the government and military, as opposed to the West which prefers a liberal environment, giving space to individuals and private corporations. Having analysed China's previous behaviour and firmly held attitudes, it seems unlikely that its stance will see a significant change any time soon. Therefore, instead of fighting the red dragon in the dark and without much success, it might be more useful to get to know her first. However, it is a large and complicated task due to continuing uncertainties that are not only a problem for the outsiders, but also for the Chinese themselves.

2. Assembling China's Cyber Strategy and Its Main Goals

In 1999, colonels Qiao and Wang presented dependence on ICT-networks as the main weakness of the US military. Today, the PLA has reached a point where its reliance on information technology is no less than that of the Americans. At the same time, cyber security is also concerned with industrial and civilian developments where public and private sector actors' interests often mismatch, making it difficult to implement a streamlined

[35] Zhao, Xiaofan. 'Practice and Strategy of Informatization in China.' State Council Informatization Office Department of IT Application Promotion. Shanghai. 18 Oct. 2006. <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025040.pdf>.
[36] 'Cyberspace.' *Defense Technical Information Center of the US Department of Defense.* Accessed 19 Aug. 2016. <http://www.dtic.mil/doctrine/dod_dictionary/data/c/10160.html>.
[37] Giles and Hagestad , 2013, p. 7.
[38] Ibid.
[39] Thomas, Timothy L. 'Information Security Thinking: A Comparison of U.S., Russian, And Chinese Concepts.' *Foreign Military Studies Office Publications*. July 2001. Accessed 19 Aug. 2016. <http://fmso.leavenworth.army.mil/documents/infosecu.htm>.
[40] Giles and Hagestad, 2013, p. 9.

approach. Logically enough, cyber security has become one of the priorities for both the PLA and the Chinese government, which has taken various steps to address the challenges of legal loopholes, incomplete institutions, and unsatisfactory education among the public.[41] As a bystander, it is not easy to understand what exactly China's cyber policies are built on, as rather than a single official document systematically listing out its cyber strategy, the policies derive from several key founding documents that have been adopted over time and have been most influential in policy-making in the cyber sphere. However, analysing these together allows gaining a rather sharp picture of China's overall position in cyberspace. Even though many of the adopted initiatives have seen only limited success, this chapter will shed light on the most important documents together with their main content and goals. It will conclude by analysing China's new strategic direction taken after establishing the Central Leading Small Group for Internet Security and Informatisation in February 2014.

2.1. China's Civilian Documents on Information Security

Prior to establishing China's national civilian cyber security plan, referred to as Document 27, several working groups had touched upon related issues. However, lack of coordination and constant restructuring have continuously caused much uncertainty for all the players. A national-level focus on information technology began in 1986 with the establishment of the State Economic Information Management Leading Small Group, and continued in 1999 and 2001 with the establishment and re-establishment of the State Informatisation Leading Group (SILG). In 2003, the State Network and Information Security Coordination Small Group (SNISCSG) was created as a sub-group under SILG, chaired by the current Premier Li Keqiang. The objectives for these three groups were to develop indigenous information technologies and place them into a national security context.[42] China's tenth Five-Year Plan of 2001 prioritised developing domestic information security infrastructure and initiating large-scale investments to both state-sponsored and private IT-firms, which were to focus on anti-malware protection and general internet security.[43] In the early 2000s, ICT development received attention from both President Jiang Zemin and President Hu Jintao who started to talk about national security and economic security as an indivisible pair, hence promoting the need to 'leapfrog' over the competitors in order to turn China's historical disadvantages into strengths through innovative development.[44]

2.1.1. *Document 27*: Opinions for Strengthening Information Security Assurance Work (2003)

In 2003, SNISCSG issued Document 27, which implemented major cyber security related policies and national strategies, including disaster recovery, incident management and e-government security plans.[45] The initially classified Document 27's persisting idea was the concept of 'active defence',[46] drawing various policies for protecting critical infrastructure, enhancing encryptions and dynamic monitoring, improving indigenous innovation, and also touching upon cyber security's leadership, better coordination and funding. Document 27 was helpful in formulating necessary policies, but the dismissal of SNISCSG in 2008 left China's civilian cyber security disorganised, leading to various separate, unaligned policy initiatives from different bodies. Even though SNISCSG was reconstituted in 2009, no open records of its meetings are available and various ministries have been assigned

[41] Li, Yuxiao. 'Cyberspace Security and International Cooperation in China,' p.4 in Lindsay, 2012.
[42] Wang, Yukai, 'Zhongyang wangluo anquan yu xinxihua lingdao xiaozu de youlai ji qi yinxiang (The Origins and Influence of the Central Network Security and Informatisation Leading Small Group),' *Zhongguo Gongchandang Xinwen Wang (Communist Party of China News Network)*, 3 Mar. 2014. <http://theory. people.com.cn/n/2014/0303/c40531-24510897.html>, cited in Chang, Amy. *Warring State: China's Cybersecurity Strategy*. Report by the Center for a New American Security, 2014, p. 16. <http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf>.
[43] 'China: Summary of the Tenth Five-Year Plan (2001-2005) – Information Industry'. Available at <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan022769.pdf>.
[44] Jiang, Zemin. 'Lun zhongguo xinxi jishu chanye fazhan (On China's Information Technology Industry Development),' *Xinhua*, 22 Apr. 2009. <http://news.xinhuanet.com/newscenter/2009-04/22/content_11232665_1.htm.>, cited in Chang, 2014, p. 16.
[45] Li, 2012, p. 5.
[46] 'Active defence' in Chinese understanding is based on Mao Zedong's idea of attacking only after receiving an attack. Explained in Blasko, Dennis J. 'Chapter 3: The Evolution of Core Concepts: People's War, Active Defense, and Offshore Defense,' in Kamphausen, Roy, David Lai, and Travis Tanner (eds). *Assessing the People's Liberation Army in the Hu Jintao Era,* Strategic Studies Institute, 2014, p. 81, cited in Chang, 2014, p. 20.

the responsibilities to implement Document 27's strategies.[47] Materials in English about Document 27 are limited, and therefore the exact directions on how and through which means the strategies were to be executed also remain unclear.

2.1.2. National Medium and Long Term Science and Technology Development Plan – A 15-Year Strategy

Since February 2006, all information security developments and related policies can in one way or another be linked to China's 15-year grand strategy for future innovation. Issued by the State Council, it is more precisely entitled the 'The National Programme for the Development of Science and Technology in the Medium and Long Term 2006-2020'. Dieter Ernst from the East-West Centre considers this document a cornerstone to China's overall standardisation strategy, which consists of various legal documents and policy initiatives. He also believes that the strategy should be analysed in a broader context with China's goal to level up with the Western life quality and income level, not only when talking about technology or cyberspace. In order to achieve that goal, instead of merely accepting the current standards, the government wants to become a lead shaper, or at least a co-shaper, of international standards through innovation.[48] Accordingly, the document lists China's goals for technological indigenous innovation and recognises the need for increased investment in research and development.

Other research[49] suggests that the plan reflects China's resolve to overcome domestic, social and environmental issues through technological innovation, while continuing with the firm understanding that only the government can drive such innovation, guiding enterprises and the business sector which will execute the strategies. Perhaps the most important aspect for the international community is Beijing's strong determination to loosen ties with foreign innovation firms and set the foundation for a truly independent base of knowledge. Concerns over the possibly of an emergent 'techno-nationalism' seem therefore justified. The plan calls for China not to obtain any 'core technologies in key fields that affect the lifeblood of the national economy and national security' from abroad, including next-generation internet technologies, digitally controlled machine tools, and high-resolution earth observation systems.[50]

In order to deliver this, the government has increased R&D expenditure which will rise to 2.5% of GDP by 2020. While it is believed that China will have overtaken the US by 2020,[51] estimated figures for China in 2016 remain around 2%, or $396.3 billion, while those of the US are 2.77% and $514 billion, still maintaining a significant gap between the two.[52] Even though China's figures show an almost two-fold increase from $213.4 in 2010[53], they need to be taken with a degree of scepticism, as large part of the budget is spent on developing infrastructure, rather than on scientific research. Nevertheless, Chinese researchers and enterprises do have increasingly more incentives and support to develop intellectual property, fulfilling the government's wish to reduce dependence on foreign technologies. Despite good intentions, such policies may actually amplify industrial espionage, as many local businesses lack the required skills and thus acquire the needed technology from abroad and simply modify it as necessary, often illegally.[54] Here, one can find another controversy: a part of the Chinese understanding of 'indigenous' highlights producing original innovations such as new products and services.[55] This seemingly

[47] Li, 2012, p. 6.
[48] Ernst, 2010, p. 96.
[49] Swedish Institute for Growth Policy Studies has conducted one of the most comprehensive studies on the 15-year plan and its implications. See more at Serger, Sylvia Schwaag, and Magnus Breidne. 'China's Fifteen-Year Plan for Science and Technology: An Assessment.' *Asia Policy* 4 (2007): 135-64. <http://docplayer.net/191328-China-s-fifteen-year-plan-for-science-and-technology-an-assessment.html>.
[50] Ernst, 2010, p. 24.
[51] 'China Headed to Overtake EU, US in Science & Technology Spending, OECD Says.' *OECD*. 12 Nov. 2014. Accessed 22 Aug. 2016. <http://www.oecd.org/newsroom/china-headed-to-overtake-eu-us-in-science-technology-spending.htm>.
[52] *2016 Global R&D Funding Forecast*. Report by Industrial Research Institute, 2016. <https://www.iriweb.org/sites/default/files/2016GlobalR%26DFundingForecast_2.pdf>.
[53] 'Gross Domestic Spending on R&D.' *OECD Data*. 2016. Accessed 22 Aug. 2016. <https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm>.
[54] Suttmeier, Richard P., 'Information Security and the Dynamics of Innovation,' p. 12 in Lindsay, 2012.
[55] Ernst, 2010, p. 25.

contradicts the purpose of Chinese cyber espionage, which allows the perpetrators to remain far from originality and rely instead on already established models.

The 15-year strategy does not address any particularly military related goals or concerns. Its further aim is to prioritise energy, water supply and environmental technologies together, and to recognise that a better position on intellectual property rights would also strengthen China's general competitiveness in the world markets.[56] However, Timothy Thomas has brought out the plan's aspects that could in some ways be associated with enhancing China's capabilities in the offensive side, considering the strategy a counterpart to the American National Military Strategy for Cyberspace Operations.[57] One interpretation of the strategy's goal would therefore be the desire to secure the home front before assaulting other countries. Indeed, given the intertwined nature of digital world, civilian cyberspace is certainly the most vulnerable target and would suffer the most harm if successfully attacked. By contrast, Dieter Ernst believes that the crux of this plan remains how to execute the key objective of indigenous innovation while becoming more and more integrated into global corporate production networks, often led by Western ideals.[58]

While the 15-year strategy has initiated the improvement of China's innovation system, its success depends on reinforcing open markets and international linkages between China's technology and global standards, while executing its domestic innovation and thus creating a 'two-track' approach.[59] Indeed, China's technology giants such as Huawei and Xiaomi are gradually entering the world markets, but the opposite direction allowing foreign technology firms to trade in China is still restricted. For example, the extensive 'Multi-Level Protection Scheme' introduced in 2007 intended to protect national security through prohibiting foreign companies from selling any core products to the government, banking, transportation, and other critical infrastructure companies, and the 2010 'Compulsory Certification for Information Security Scheme' required that foreign companies wishing to sell to the Chinese government must give their products' intellectual property rights to the government. A continuation to that trend in February 2015 saw the beginning of a 'cyber security new regime' which assumes that all foreign technology firms supplying Chinese banks might be required to share their source code and even include back doors into hardware and software.[60] The attention that everything related to cyberspace and information technology is continuously receiving shows that the Chinese have not given up their ambitions.

2.1.3. State Council's Information Office's New Policy Opinion

In July 2012, the State Council's Information Office (SCIO) issued a New Policy Opinion (NPO), translated as *'The State Council vigorously promotes informatisation development and offers several opinions on conscientiously protecting information security'*.[61] Even though released nearly a decade after Document 27 and more than half a decade after the 15-year strategy, its overall concerns remain the same, showing that not all goals have been met. It persistently notes China's exposure to urgent challenges in international competition over the control, use and acquisition of information. More precisely, the disparity between the West and China in digital infrastructure, inefficient exchange of information between government and industry, poor cyber security planning, inadequate defence capabilities, and a continuously large share of control over core technologies by foreigners attract the most attention.[62] Unlike previous documents, the NPO connects developments in information security to people's

[56] Serger and Breidne, 2007, p. 145.
[57] Thomas, Timothy L. 'Chapter 20: Nation-State Cyber Strategies: Examples from China and Russia,' in Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz (eds) *Cyberpower and National Security*, National Defense University Press and Potomac Books Inc., 2009. Accessed via <http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-20.pdf>.
[58] Ernst, 2010, p. 1.
[59] Ibid., p. 26.
[60] Segal, Adam. 'What to Do About China's New Cybersecurity Regulations?' *Council on Foreign Relations*. 2 Feb. 2015. Accessed 22 Aug. 2016. <http://blogs.cfr.org/cyber/2015/02/02/what-to-do-about-chinas-new-cybersecurity-regulations/>.
[61] The full text of the NPO in Chinese is available at <http://politics.gmw.cn/2012-07/17/content_4571519.htm>.
[62] Segal, Adam. 'China Moves Forward on Cybersecurity Policy.' *Council on Foreign Relations*. 24 July 2012. Accessed 22 Aug. 2016. <http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-on-cybersecurity-policy/>.

economic and social improvement. This shows an expansion from 'safeguarding national security information' to 'promoting stable and rapid economic development and social harmony and stability'.[63]

Giles and Hagestad have distilled the NPO's four policy mandates, which like the previously analysed documents focus on civil cyber defence:

- Firstly, the NPO places strong emphasis on the security of all critical information systems and infrastructure, especially focusing on information networks. This can be interpreted as an order, rather than guidance, on what the policymakers must protect – the internet, radio networks and private telecommunications systems, as well as information networks related to finance, energy and transportation. Its clear goal is to secure those industries where a cyber attack would cause tremendous harm to China's economy.[64]
- Secondly, the NPO seeks to strengthen the governmental and classified information security systems, which are often attractive targets for hacktivists like Anonymous. For execution, the State Council expects the government agencies to reduce their internet connectedness and enhance information security and confidentiality protection monitoring by establishing a hierarchical system to protect classified information systems.[65]
- Thirdly, the NPO seeks to increase protection of industrial control systems of facilities such as oil and gas pipelines, nuclear and power infrastructures, as well as transportation and urban facilities, all invoking the memory of Stuxnet. This should be achieved through strengthening regulations and conducting more frequent security checks and risk assessments.[66]
- Finally, the NPO turns to safeguarding Chinese citizens' personal information, noting its significance in achieving the general welfare of the country and thus promising protection of demographic, geographical or similarly sensitive data.[67] This step can be considered a countermove to an attack in 2012 which compromised millions of users' data on an opinion forum, Tianya, and a retail site, 360buy.com.[68]

The NPO is certainly a very comprehensive document, which covers the majority of essential areas of cyber security. The State Council's recommendations indicate the main weaknesses of China's information security model, and point out the increased vulnerabilities from growing dependence on the internet. Continuing hostility towards foreign technologies also suggests that related trade barriers will not be abolished in the near future. However, as an intriguing point in light of President Xi's anti-corruption campaign, the NPO does not seem to address corruption, which is widespread within the technology industry. As the crackdown has not proven fully successful, the government could think of rewarding legitimate officials and entrepreneurs to prevent dishonest players from compromising the industry's development. Overall, the NPO indicates that information security had, by 2012, already become one of the government's priorities.

2.2. Formulating a New National Information Security Strategy

The analysis of these documents indicates that China's main information security concerns have remained rather similar throughout the years. Guided by these principles, 2014 was finally considered a year of breakthrough towards a better regulated cyberspace. The establishment of the Central Leading Small Group for Internet Security

[63] Xue Ruihan, 'Jianli jianqian guojia wangluo he xinxi anquan chang xiao jizhi (Establish and improve the national network and information security long-term mechanisms),' *Renmin Wang (People's Daily Online)*, 17 Apr. 2014, <http://leaders.people.com.cn/n/2014/0417/c347621- 24909496.html>, cited in Chang, 2014, p. 17.
[64] Gu, Fa, 'State Council vigorously promotes the development of information technology and to effectively protect the information security.' 2012, cited in Giles and Hagestad, 2013, p. 12.
[65] Ibid, p. 13.
[66] Ibid.
[67] Ibid.
[68] Zhu, Yishi. 'Hackers Find Holes Behind the Great Firewall.' *Hackers Find Holes Behind the Great Firewall*. 21 Jan. 2012. Accessed 22 Aug. 2016. <http://english.caixin.com/2012-01-21/100350690.html>.

and Informatisation on 27 February 2014 shows President Xi's personal commitment, as he is the first party head to chair a leading small group related to information management.[69] When explaining the necessity of the new body, Xi has pointed out China's need to catch up with the West in innovation, and further developed his argument that 'no internet safety means no national security and no informatisation means no modernization'.[70] The leading group gives unprecedented priority to both internet security and information management as a single concept, trying to fight the lack of a coordinated approach that has caused problems in the past. President Xi has referred to internet security and information management as 'two wings of one bird, two wheels on one car'.[71] With Xi as its head, the new group should be able to make firm demands and solve internal discrepancies where necessary.

As part of the new initiative, November 2014 saw the first World Internet Conference, hosted in Wuzhen, China. With the presence of representatives from various big names like Apple and Microsoft, President Xi affirmed that under the terms of mutual respect and trust, China was willing to cooperate with other states to achieve a peaceful cyberspace and a multilaterally governed, transparent internet, while sticking to the notion that state sovereignty must be fully respected in cyberspace.[72] At the second Conference a year later, President Xi delivered a keynote speech in which he called for 'building a cyber community of common destiny and put forward the principles of respecting cyber sovereignty, safeguarding cyber security, encouraging cyber opening up, and building cyber order'.[73] As part of his ideas, Xi proposed building an internet governance system based on a multilateral approach, and denounced unilateralism in which only a few parties discuss the future of the internet.[74] His other proposals concerned the digital gap, cultural diversity in cyberspace, the digital economy, and cyber security in general, indicating the core elements of China's cyber strategy. While this call might be a chance for deeper cooperation with China, it also impliedly depicts China's dissatisfaction with the current system and the desire to guide the existing structure and governance of cyberspace and technological development closer to their way of thinking.[75] Indeed, in the National Meeting on Cyber Security and Information Technology held in April 2016, President Xi once again reaffirmed the importance of cyber sovereignty, implying a rejection of the applicability of international law and existing regulations in cyberspace.[76]

Overall, despite the lack of one single strategy clearly listing China's future plans and ambitions, the different pieces of information allow a number of conclusions. The existing and newly created mechanisms must improve the security of the domestic internet infrastructure, reinforce the move towards indigenous innovation detailed in the 15-year plan, and, most importantly, help China become the leading actor on the global stage by promoting an alternative attitude to internet governance. The Chinese government understands the value and power of technology, innovation, and the internet, but remains extremely careful in operating the 'double-edged sword', being aware that free information, once released, is impossible to stop and has great potential to shake the foundation of the communist party and the political order of China. Last year, for example, the government set up a doctrine of Seven Baselines for using the internet, requiring that whatever is expressed online, must respect

[69] Rountree, Florence. 'Information management and internet regulation in China.' *China's Expanding Cyberspace* (2014): pp. 11-13. <http://www.ecfr.eu/page/-/ChinaAnalysisEng_June2014.pdf>.
[70] Zhu, Ningzhu. 'Xi Jinping Leads Internet Security Group.' *Xinhuanet*. 27 Feb. 2014. Accessed 22 Aug. 2016. <http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm>.
[71] 'Xi Jinping: Ba wo guo cong wangluo daguo jianshe chengwei wangluo qiangguo (Xi Jinping: From a big internet country to a powerful internet country).' *Xinhuanet*. 28 Feb. 2014. Accessed 23 Aug. 2016. <http://news.xinhuanet.com/info/2014-02/28/c_133148804.htm>.
[72] 'Chinese President Xi Jinping Calls for International Cooperation on Cyberspace Security.' *The Economic Times*. 19 Nov. 2014. Accessed 23 Aug. 2016. <http://economictimes.indiatimes.com/news/international/world-news/chinese-president-xi-jinping-calls-for-international-cooperation-on-cyberspace-security/articleshow/45205445.cms>.
[73] 'Infographic: Achievements of the 2nd WIC.' *China Daily*. 21 Dec. 2015. Accessed 23 Aug. 2016. <http://www.chinadaily.com.cn/business/tech/2015-12/21/content_22761073.htm>.
[74] Zhang, Rui. 'China Headlines: Xi Slams 'double Standards,' Advocates Shared Future in Cyberspace.' *CCTV.COM*. 17 Dec. 2015. Accessed 23 Aug. 2016. <http://english.cntv.cn/2015/12/17/ARTI1450334752126739.shtml>.
[75] Lu, Chuanying. 'China's Emerging Cyberspace Strategy.' *The Diplomat*. 24 May 2016. Accessed 23 Aug. 2016. <http://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/>.
[76] Ibid.

seven elements: laws and regulations, the socialist system, the country's national interest, citizens' lawful rights and interests, public order, morality, and accuracy.[77] Given this, it is likely that the government will continue with a similar supervisory mind-set.

3. China's Strategic Cyber Governance

Institutional fragmentation has been a constant feature in China's cyber organisation. A mixture of government institutions and military departments, together with uncoordinated action between central and local authorities, has created a strong incentive for establishing a more streamlined and synchronised approach. To give a clear overview of the exact institutions in play, this chapter will introduce the past and recently launched initiatives that shape China's cyber governance, including Xi Jinping's Central Leading Small Group for Internet Security and Informatisation. The chapter will examine both civilian and military organs, and will first cover how the general responsibility of cyber security is organised and coordinated by looking at the bodies responsible for the decisions and execution.

The military part of the chapter first introduces the military's strategic thought and then focuses on the role of the People's Liberation Army and its cyber espionage and intelligence units, which have previously acted mainly under the 3rd and 4th Departments of the General Staff Department, but are expected to see a restructuring under the newly created Strategic Support Force. This section also includes an analysis of the patriotic hacktivist groups which, despite their usefulness to the government, may seriously hamper China's overall development and foreign relations.

3.1. Civilian Government Agencies

As Amy Chang has noted, the key driver for formulating China's cyber security strategy remains maintaining the communist party's ruling power.[78] Therefore, as with any other subject, the party ultimately commands all the mechanisms regulating China's cyberspace. So far, it has not been able to effectively reduce the large number of stakeholders with competing interests. However, like the noticeable trend in several other countries like Israel and the US, China's recent steps have allowed it to move towards a more streamlined unified command line for cyber.

The highest-level decision-makers in China are the **Politburo Standing Committee**, the **State Council**, and the **Central Military Commission**. For policy-making, it is the State Council that usually adopts new initiatives, including those in cyberspace, such as the 15-Year Plan in 2006 and the New Policy Opinion in 2012, but there are several government agencies charged with the execution of policy. In 1982, when China was not even connected to the internet, the State Council set up a government body for digital affairs, seeking to centralise control over the developing 'computers and large-scale integrated circuits'.[79] Groups with similar structures and roles remain the key organisations today, but before turning to explaining their current functions, ministerial-level agencies which mostly perform general policy implementation will be introduced:

- The **Ministry of Industry and Information Technology (MIIT)** was established in 2008 as an attempt to centralise information technology development. It undertakes all State Council work on information management and carries similar domestic responsibilities to the Department of Homeland Security in the US. It also sets standards, holds exercises, inspects network security, and coordinates information and telecoms security through a special department.[80] Whereas the primary duty to respond to cyber-attacks rests with the **National Computer Network Emergency Response Technical Team/Coordination Centre**

[77] Creemers, 2015, p. 10.
[78] Chang, 2014, p. 32.
[79] Wang, 2014, cited in Rountree, 2014, p.11.
[80] *The Cyber Index: International Security Trends and Realities*. Report by the United Nations Institute for Disarmament Research, 2013, p. 15. <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>.

of China (**CNCERT**) – a non-governmental technical centre established in 2002, MIIT has been influential in supporting its work through helping it build virus and vulnerability databases, finding malicious IP and domain name providers, and guiding CNCERT to engage in international cooperation.[81] MIIT also contains the **State Administration for Science, Technology and Industry for National Defence (SASTIND)**, which drafts guidelines, policies, laws and regulations involved with science, technology and industry for national defence.[82] Prior to MIIT a separate ministry, the **Commission for Science, Technology and Industry for National Defence (COSTIND)**, carried out similar tasks.

- The **Ministry of Public Security (MPS)** investigates cybercrime and takes care of critical infrastructure protection together with development work through a wide network of research labs.[83] It is also responsible for overseeing the commercial products used by the government and controlling all commercial information security companies. Importantly, MPS operates the Great Firewall of China and is also involved with conducting domestic intelligence.[84]
- The **Ministry of State Security (MSS)** functions as an organ to conduct counterespionage, counterintelligence, foreign intelligence, and domestic intelligence. Its efforts originally focused on countering separatism, terrorism and religious extremism, which are often described as the three existential challenges to the Communist Party. However, despite having attracted little public attention, MSS's estimated cyber capabilities have grown significantly in order to collect further political and economic data on foreign governments, NGOs and domestic dissidents.[85]

Other than these institutions, various sources have also highlighted the importance of the **State Encryption Bureau**, which conducts party, civilian and military encryption management, including restricting the import and export of any encrypted devices; and the **State Secrets Bureau**, which manages all classified networks and has been increasingly engaged in keeping up with the technological changes China is witnessing.[86] As all of the three ministries and the two bureaus operate under the State Council, they are seemingly equal in hierarchy. However, looking at past actions and attention, the Ministry of Industry and Information Technology seems to be the main force behind executing the tangible progress of China's cyberspace.

On the research and development side, further attention has been paid to a number of government affiliated research institutions, such as the **Chinese Institute of Contemporary International Relations**, which acts directly under MSS, the **Chinese Academy of Engineering**, and the **Chinese Academy of Sciences**. Not surprisingly, **Tsinghua University** and **Peking University**, the top two academic institutions in China, are closely related to the government's information technology related research work. Deeper strategic development is run by the PLA through institutions such as the **Academy of Military Science** and the **PLA Information Engineering University**. March 2016 saw the launch of the **Cyber Security Association of China**, consisting of academic institutes, individuals and internet companies such as Tencent, to speed up the development of industry standards and better coordinate research on cyber security.[87]

---

[81] Fu, Jingguang. 'Policies and Practices on Network Security of MIIT.' Workshop on Cybersecurity Policy Development in the APEC Region. Hangzhou. 27 Mar. 2011. Accessed 23 Aug. 2016. <http://mddb.apec.org/Documents/2011/TEL/TEL43-SPSG-WKSP/11_tel43_spsg_wksp_004.pdf>. To learn more about China's national CERT, see their website <http://www.cert.org.cn/publish/english/index.html>.

[82] 'State Administration for Science, Technology and Industry for National Defense (SASTIND).' *Nuclear Threat Initiative*. 1 Oct. 2011. Accessed 23 Aug. 2016. <http://www.nti.org/learn/facilities/781/>.

[83] Goodrich, Jimmy, 'Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy,' p. 6 in Lindsay, 2012.

[84] Feakin, Tobias. *Enter the Cyber Dragon*. Report by the Australian Strategic Policy Institute, 2013, p. 3. <https://www.aspi.org.au/publications/special-report-enter-the-cyber-dragon-understanding-chinese-intelligence-agencies-cyber-capabilities/10_42_31_AM_SR50_chinese_cyber.pdf>.

[85] Inkster, Nigel. *China's Cyber Power*. Routledge, 2016, p. 54.

[86] Goodrich, 2012, p. 6.

[87] 'China Launches First Cybersecurity Organisation.' *Cyber Security Review*. 26 Mar. 2016. Accessed 23 Aug. 2016. <http://www.cybersecurity-review.com/china-launches-first-cybersecurity-organisation-report>.

3.2. Streamlining of Cyber Administration

Central leading groups and Leading small groups have become a common feature in China's political culture to tackle issues that the existing bureaucratic machine is incapable of solving. Complying directly with the orders of the party's highest leaders, these are perhaps the most efficient mechanisms to the adoption of successful reforms. Whereas the **State Informatisation Leading Group (SILG)** and the **State Network and Information Security Coordination Small Group (SNISCSG)** – the first efforts to develop China's indigenous information technologies and formulate a secure Chinese cyberspace – were guided by the State Council, the recently established **Central Leading Small Group for Internet Security and Informatisation (CLSGISI)** acts directly under the direction of President Xi, and has thereby assumed unprecedented authority. The leading group reportedly consists of 22 members: next to Xi Jinping, the Premier Li Keqiang and a Standing Committee member Liu Yunshan act as vice-chairs, to lead eight other Politburo members and eleven ministerial-level officials. As it is common in China for a new body to take over the duties of a previously existing organ, this group has subsumed the roles of the SILG and SNISCSG, by merging most of the members from the previous two bodies.[88] Next to the obvious significance of the group deriving from its high leadership which shows cyber security's weight in Chinese policy-making, the group is hoped to act as a middleman resolving internal misunderstandings between the ministerial-level institutions described above.

More than two years after its establishment, the CLSGISI itself has not been much discussed in the English-speaking media, but the executive body implementing President Xi's reforms – the **Cyberspace Administration of China (CAC)** – has caught its attention rather often. The CAC is basically a refreshment of the **State Internet Information Office (SIIO)** as its Chinese name and chairman Lu Wei remained the same, although Lu unexpectedly stepped down in June 2016 to be replaced by Xu Lin. SIIO was founded in 2011 to better coordinate the 'rectification' of the internet, working in close cooperation with MIIT and MPS to patrol social media, where user-created content generates a serious nuisance to the government. Establishing SIIO was a specific step by the **State Council Information Office (SCIO)**, which manages the general domestic information flow.[89] Seemingly tied with Xi's power consolidation and countering domestic disobedience, CAC's predominant function remains the same as that of SIIO – to monitor information movement and further strengthen the grip on websites allegedly undermining domestic stability.

The creation of CAC also represents an attempt to combine propaganda with technological innovation and development.[90] For example, CAC has published a choral anthem, which includes verses such as 'with loyalty and devotion, we watch over our domain day and night.'[91] Affirming the significance of the future of China's cyberspace, *Time Magazine* included Lu Wei among the 100 most influential people in 2015, emphasising his (former) power to pilot more than 700 million Chinese netizens.[92] CAC has so far executed its power by blocking foreign VPNs, closing and monitoring WeChat (the most popular messaging application in China) accounts of individuals perceived as threatening, and possibly coordinating cyber-attacks against anti-censorship groups such as GreatFire.org, an organisation seeking to bring transparency to the Great Firewall by providing information on any blocked websites and keywords.[93] The beginning of 2016 saw a proposal for a new cyber security law that

[88] Creemers, Rogier. 'Cybersecurity and Informatization Leading Group: Names and Documents.' *China Copyright and Media*. 13 Mar. 2014. Accessed 23 Aug. 2016. <https://chinacopyrightandmedia.wordpress.com/2014/03/13/cybersecurity-and-informatization-leading-group-names-and-documents/>.

[89] Rountree, 2014, p. 12.

[90] Creemers, 2015.

[91] Sisi, Wei, and Qiu Wei. 'China's Internet Censors Have a Choral Anthem and It's Everything You Want It to Be.' *Quartz*. 16 Feb. 2015. Accessed 23 Aug. 2016. <http://qz.com/345377/chinas-internet-censors-have-a-choral-anthem-and-its-everything-you-want-it-to-be/>.

[92] Huntsman, Jon. 'The 100 Most Influential People: Lu Wei.' *Time*. 16 Apr. 2015. Accessed 23 Aug. 2016. <http://time.com/3823285/lu-wei-2015-time-100/>.

[93] The team at GreatFire.org wrote an open letter to Lu Wei in January 2015, drawing on evidence from a variety of sources and showing CAC's involvement in man-in-the-middle attacks against foreign technology giants such as Apple, Yahoo, Microsoft and Google, and calling for it to enhance Chinese cyberspace, rather than patrol and intimidate internet users. See more at: 'An

would include provisions theoretically banning local service providers from enabling connections to sites with domain names registered abroad. MIIT has, however, said that the core of the new regulations has been misunderstood, and they would not affect foreign companies launching services in China or users accessing such websites.[94] Despite the fact that the second reading of the draft regulations in June 2016 saw certain amendments, the existing draft further reaffirms the state's strict approach to controlling cyberspace and is soon expected to become adopted as law.[95]

Each of these mentioned bodies has been trusted with specific tasks. While academia and specific institutions conduct research and strategic development work, it is the ministerial-level organisations which come up with policy initiatives and direct the required changes. Establishing the Central Leading Small Group for Internet Security and Informatisation and the CAC as its executive body represents an additional step from the previously existing bureaucracy, as their authoritative leadership guarantees a better coordinated action between the ministries and bureaus. In terms of policy-making efficiency, it is a positive step towards a less fragmented system, but it also constitutes a part of President Xi's campaign to restrict anti-party and liberal movements through the opportunities the internet creates, which is demonstrated by the CAC's predominantly restricting activities.

3.3. Military's Cyber Activities

The following sections will look more closely at China's cyber security from the military's strategic and organisational perspective, which is intertwined with the goals and activities of the civilian agencies thus far discussed. While the militaries of the US and Russia have each published official documents on activities in cyberspace, the PLA has not issued any specific doctrine. However, the concept of information has always been extremely important in China's military strategies, and the contemporary emphasis on gathering information and intelligence is entirely in line with ancient Chinese strategists such as Sun Zi. Therefore, it is essential to be aware of the guiding principles of the PLA's conducts before engaging in analysing the specific activities of its cyber units.

3.3.1. The Chinese Military's Strategic Thinking on Cyber

The concept of information plays a central role in Chinese military thinking. As cyberspace is strongly related to information, one can find relevant content within general military documents which explain the PLA's ambitions in cyberspace. For example, the *Military Strategic Guidelines*, normally renewed every 10-15-years, lead defence and military policies strongly towards modernisation, while recognising the importance of the ability to fight in 'technical conditions' and implying the significance of information technology in overall strategies.[96] Furthermore, the recently updated *Science of Military Strategy*, a book issued by the Academy of Military Sciences, the most important research institution of the PLA, puts even stronger emphasis on conflict in the network domain and elaborates on developments of high-tech local war, giving guidelines on how to behave in such circumstances.[97] In fact, its chapter on information warfare openly declares that China does have specialised network warfare units, operating within both the military and the civilian spheres, and carrying out both offensive and defensive cyber operations.[98]

Open Letter to Lu Wei and the Cyberspace Administration of China.'*Greatfire.org*. 26 Jan. 2015. Accessed 23 Aug. 2016. <https://en.greatfire.org/blog/2015/jan/open-letter-lu-wei-and-cyberspace-administration-china>.

[94] Chin, Josh. 'China Says New Internet Regulations Won't Increase Blocking of Foreign Websites.' *The Wall Street Journal*. 30 Mar. 2016. Accessed 23 Aug. 2016. <http://www.wsj.com/articles/china-says-new-internet-regulations-wont-increase-blocking-of-foreign-websites-1459351655>.

[95] For a full draft of the proposed law on cybersecurity, see Creemers, Rogier. 'People's Republic of China Cybersecurity Law (Second Reading Draft).' *China Copyright and Media*. 6 July 2016. Accessed 18 Aug. 2016. <https://chinacopyrightandmedia.wordpress.com/2016/07/06/peoples-republic-of-china-cybersecurity-law-second-reading-draft/>.

[96] Jiang, Zemin. 'Guoji xingshi he junshi zhanlüe fangzhe (The Global Situation and Military Strategic Outline)' in *Jiang Zemin Wenxuan (Jiang Zemin Anthology).* Beijing, 2006, cited in Chang, 2014, p. 19.

[97] Chang, 2014, p. 25.

[98] Tiezzi, Shannon. 'China (Finally) Admits to Hacking.' *The Diplomat*. 18 Mar. 2015. Accessed 23 Aug. 2016. <http://thediplomat.com/2015/03/china-finally-admits-to-hacking/>.

Another initiative was launched in October 2014 when President Xi and the Central Military Commission issued a document entitled *Opinion on Further Strengthening Military Information Security Work*, which listed the basic principles and priorities for the PLA, but also provided directives for the military in the information security field.[99] In May 2015, the Chinese Ministry of National Defence issued *China's Military Strategy*, also referred to as the *2015 Defence White Paper*, which places intense focus on the informatisation of warfare, and declares China's intention to further develop cyber force and 'enhance its capabilities of cyberspace situation awareness, cyber defence, support for the country's endeavours in cyberspace and participation in international cyber cooperation'.[100] Importantly, the document also reaffirms China's goal to build an informationised military to be able to win future informationised wars.[101]

China's ambition to achieve superiority in cyberspace is related to the belief that disabling the enemy's most valuable operation systems in the initial phases of a conflict would bring a quick victory. Looking at the available documents, it seems that China is moving towards a common approach that incorporates cyber war with a kinetic attack.[102] This also corresponds with the Chinese strategists' hypothesis that informatisation creates a new battlefield which the PLA must master.[103] However, there are also pragmatic economic and political objectives behind the military's cyber activities, mainly short and long-term gains from espionage against other governments and the private sector. Next to collecting valuable information from abroad, perhaps even more essential is the surveillance conducted against the Chinese citizens in order to maintain control and political stability within the communist system. The main targets normally include political dissidents and democracy activists, but also Tibetans, Uighurs and Falun Gong followers to examine their networks and communication methods.[104] While these activities are not conducted only through military mechanisms, the paper will later show that the PLA's role is certainly vital in sustaining such operations.

Interestingly, China has always emphasised its defensive nature in every aspect of warfare, including information security. The *2013 Defence White Paper* proclaimed China's right to protect its interests of national security and delivered a promise not to attack unless attacked first, including in cyberspace.[105] Whereas several Western countries have communicated a similar position, the Chinese attitude relies on Mao Zedong's 'active defence' as already emphasised in Document 27 in 2003, assuming to attack only after being attacked.[106] Yet, Mao's 'active defence' can also be interpreted as the alternative use of defensive and offensive. This, together with different strategic cultures, creates a situation where an act considered defensive by the Chinese might seem offensive to the West.[107] As an interesting parallel, 'active cyber defence' is widely discussed in the West, referring to the ability to detect and mitigate key threats before suffering from any damage, including the capacity to launch aggressive and offensive countermeasures.[108] Thus, Western actions taken under the concept of 'active cyber defence' might similarly seem offensive to the Chinese. Connecting the Chinese and the Western understandings of active defence, it seems that each has understood that in cyberspace, mere defensive capabilities are not enough to deter adversaries from attacking one's networks. As the Chinese have recently admitted the existence of purely

[99] 'Jing Xi Jinping zhuxi pizhun zhongyang junwei yinfa 'guanyu jinyibu jiaqiang jundui xinxi anquan gongzuo de yijian (Chairman of the Central Military Commission Xi Jinping approved the issuance of 'Opinion on Further Strengthening Military Information Security Work'),' *Jiefangjun bao (PLA Daily)*, 7 Oct. 2014. <http://news.xinhuanet.com/mil/2014- 10/07/c_1112726181.htm>, cited in Chang, 2014, p. 19.

[100] 'Document: China's Military Strategy.' *US Naval Institute News*. 26 May 2015. Accessed 23 Aug. 2016. <https://news.usni.org/2015/05/26/document-chinas-military-strategy>.

[101] Ibid

[102] Deal, Jacqueline N. 'Chinese Information War: Historical Analogies and Conceptual Debates,' pp. 18-22 in Lindsay, 2012.

[103] Peng Guangqian and Yao Youzhi eds., 'Chapter 20: Rise of the High-Tech Local War and Its Historic Status,' in *The Science of Military Strategy*, Academy of Military Science Strategic Research Department. Beijing, 2005, cited in Chang, 2014, p. 25.

[104] Feakin, 2013, p. 5.

[105] Information Office of the State Council. *The Diversified Employment of China's Armed Forces*. Apr. 2013. Accessed 23 Aug. 2016. <http://www.nti.org/media/pdfs/China_Defense_White_Paper_2013.pdf>.

[106] Blasko, 2014, cited in Chang, 2014, p. 20.

[107] Chang, 2014, p. 25.

[108] Dewar, Robert S. *The 'Triptych of Cyber Security': A Classification of Active Cyber Defence*. Proceedings of 6th International Conference on Cyber Conflict, Tallinn. 2014, p. 10. <https://ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf>.

offensive cyber units in the PLA, it is increasingly clear that conflict in cyberspace has achieved fundamental importance in the Chinese understandings of policy making, both in peacetime, and in any future war.[109]

3.3.2. Impact of Reforms on People's Liberation Army's Approach to Cyber

In 1986, China launched Programme 863 to catch up with the West in key strategic industries through foreign intelligence collection, and to reduce its dependence on foreign technologies. The plan was intensified after the Gulf War in 1991, when the PLA was stunned by the sophistication of US weaponry.[110] Relying on this imperative, the Chinese military has implemented numerous reforms and modernisation plans, the latest and most comprehensive of them approved in December 2015 to adjust to the 21st century's cyber era and exploit its opportunities. Parts of the Chinese military have become useful tools for the government to conduct political and economic cyber espionage, and also to help reduce the PLA's own technological and strategic disadvantages relative to its competitors.

Prior to the largest restructuring within the PLA's modernisation drive, the General Staff Department's Communications Department was restructured into the **Informatisation Department**, together with establishing several smaller information-related departments in the PLA regions and academia to raise the level of informatisation in the PLA.[111] However, it seems that these developments should not receive too much attention in light of the reforms President Xi announced on the last day of 2015. Three new organs were introduced: the PLA Rocket Force, the PLA Strategic Support Force, and the Army Leadership Organ. Importantly, the Rocket Force assumed the responsibilities of the PLA Second Artillery Force and earned promotion to a status equal to the PLA Army, Navy and Air Force. By today, it appears that the **Strategic Support Force (SSF)** has also been given a status equal to these professional service branches, and will likely formulate the core of China's information warfare effort by comprising forces in the space, cyber and electromagnetic domains, thus finally bringing China's military-related informatisation activities under one umbrella.[112]

However, the reforms are currently being implemented and the date of actual completion remains unknown.[113] So far, two (former) executive bodies of the PLA's General Staff Department (GSD): the 3rd and the 4th Departments, had been trusted with cyber intelligence and cyber-warfare respectively. Even though both departments will most likely become integrated under the SSF, their successors' corresponding goals and practices are expected to remain similar, and therefore, it is appropriate to introduce these institutions in more detail.

3.3.3. General Staff Department's 3rd Department

Before giving full attention to the **3rd Department (3/PLA)**, sometimes also referred to as the Technical Department, it is necessary to recall that the MSS carries similar intelligence responsibilities in the civilian side. Also, the General Staff Department's 2nd Department (2/PLA) is considered the conventional intelligence gathering agency and is involved with collecting and analysing mainly open-source information through its global network of defence attachés. Whereas it is not regularly engaged with covert operations, its non-official cover officers are believed to have had significant success in collecting valuable data about US and other Western weapon systems.[114] Nevertheless, neither MSS nor 2/PLA have played as significant role in cyber intelligence as 3/PLA.

---

[109] For a detailed account on Chinese thinking on cyber conflict, see Pollpeter, Kevin. 'Chapter 6: Chinese Writings on Cyberwarfare and Coercion,' in Lindsay et al., 2015.

[110] Inkster, Nigel. 'Chinese Intelligence in the Cyber Age.' *Survival: Global Politics and Strategy* Vol 55(1) (2013): 45-66, p. 50. <https://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-february-march-2013-3db7/55-1-05-inkster-936c>.

[111] Thomas, Timothy L. *Three Faces of the Cyber Dragon*. Foreign Military Studies Office, 2012, pp. 69-72.

[112] Costello, John. 'The Strategic Support Force: China's Information Warfare Service.' *The Jamestown Foundation*. 8 Feb. 2016. Accessed 23 Aug. 2016. <http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=45075&cHash=9758054639ab2cb6bc7868e96736b6cb#.V6RA_Lt95aQ>.

[113] It might be assumed that the PLA targets to complete the reforms by around 2020.

[114] Inkster, 2013, p. 49.

According to Nigel Inkster, 3/PLA has so far been the main operational force of the PLA's cyber activities, as almost all operations that have been tracked originate from its official premises.[115] Appearing to be a counterpart to the National Security Agency in the US, 3/PLA's main focus has been on collecting signals intelligence (SIGINT). Before the internet's surge, it operated as a conventional SIGINT agency, but did not possess known overseas collection capabilities matching those of the Americans or the British.[116] More recently, its role has been narrowed to cyber network exploitation (CNE) or espionage, and despite its presence in scandalous news stories quite often, 3/PLA has proven to be a highly beneficial component of China's military. At the same time, it has managed to remain rather mysterious about its interactions with other domestic intelligence units, including the MSS, leaving open the question of how efficient the coordination and information sharing among the domestic bodies is. Nevertheless, looking at 3/PLA's wide-ranging structure, traditional competence in SIGINT, its high performance in computing and cryptology, and its status as China's largest employer of professional linguists, one may assume its respective importance, or even a central role among other institutions.[117] However, with the announced creation of the SSF, it is likely that China's strategic intelligence and informatisation units will be merged into one central intelligence structure, leaving open the question of in what form 3/PLA will continue, if at all.

3/PLA's headquarters is in Beijing, where it runs political and logistics departments together with the Science and Technology Intelligence Bureau and the Science and Technology Equipment Bureau, which commands three research institutes responsible for computing, sensor technology and cryptography, respectively named the 56th, 57th and 58th Research Institutes. In addition, 3/PLA manages or is affiliated with several Computer Network Defence-related institutions such as the National Research Centre for Information Security Technology, the Information Security Research Institute, and the PLA Communications Security Bureau.[118] Next to these bodies, it is the 12 operational bureaus that play the most important role in 3/PLA's structure. Each of the bureaus usually carries out a specific task, for example intercepting radio or satellite communications, conducting cryptology, translation, or intelligence analysis on diplomatic communications, foreign militaries, economic entities, educational institutions, and individuals considered worthy of surveillance.[119]

The 2nd and 12th Bureaus deserve further attention.[120] First, the Shanghai headquartered **2nd Bureau**, also known as Unit 61398 by its Military Unit Cover Designator, seems to specifically target the US and Canada to obtain political, economic, and military intelligence. It was exposed in February 2013, when Mandiant published an unprecedentedly thorough report on a unit they named APT-1, which has achieved public attention through its very similar missions, capabilities, resources and location to the 2nd Bureau. After having observed APT-1's long-term and extensive cyber espionage operations for several years, Mandiant concluded that APT-1 is most likely government-funded and one of the most prolific and dangerous of China's cyber actors.[121] According to the size of its physical infrastructure, APT-1 is staffed by at least hundreds, if not thousands of people, all required to be competent in computer network operations and English.[122] Indeed, as Mandiant notes, 87% of APT-1's victims are in English-speaking countries and belong to industries that China has said to carry strategic importance to national growth. With the apparent help of recruited linguists, malware authors and industry experts, APT-1 had by the

[115] Inkster, Nigel. 'Chinese Intelligence Operations and Transnational Consequences,' p. 24 in Lindsay, 2012.
[116] Inkster, 2013, p. 49.
[117] Stokes, Mark A., Jenny Lin, and Russell Hsiao. *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*. Report by Project 2049 Institute, 2011, p. 3. <https://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf>.
[118] Stokes et al., 2011, pp. 4-5.
[119] Stokes et al., 2011, p. 7.
[120] For an overview of all 12 bureaus, see Stokes, Mark A. 'Chapter 7: The Chinese People's Liberation Army Computer Network Operations Infrastructure,' p. 169 in Lindsay et al., 2015.
[121] *APT1: Exposing One of China's Cyber Espionage Units*. Report by Mandiant, 2013, p. 2. <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.
[122] The five PLA officers that the US indicted in 2014 summer were also working for Unit 61398. For a detailed overview of the 2nd Bureau, see Stokes, Mark A. *The PLA General Staff Department Third Department Second Bureau*. Report by Project 2049 Institute, 2015. <http://www.project2049.net/documents/Stokes_PLA_General_Staff_Department_Unit_61398.pdf>.

time of the report's publication obtained hundreds of terabytes of data from at least 141 organisations over 20 industries.[123]

A year after the Mandiant's report, a threat intelligence firm CrowdStrike disclosed another unit of 3/PLA. Namely, the **12th Bureau**, or Unit 61486, also headquartered in Shanghai is believed to support China's space surveillance network and tasked to intercept satellite communications and collect space-based SIGINT.[124] According to the CrowdStrike report, the group, also called Putter Panda, has been active since 2007, allegedly targeting the aerospace industries in both Europe and the US through attacks on the government, defence, research and technology sectors. The group's methodology relies on deploying malware through targeted emails in the form of spear phishing.[125] The uncovering of the 12th Bureau shows that China can use cyber espionage on two strategic levels: illegally obtained intellectual property allows it to speed up its own space-related developments, but also enables exploitation of an opponent's satellite weaknesses during a real conflict.[126]

Evidently, collecting foreign intelligence through cyber espionage has been fully institutionalised and prioritised for 3/PLA. However, 3/PLA's operations are often in parallel with those of the Military Region Technical Reconnaissance Bureaus (TRB), which operate under seven military regions and are independent of 3/PLA. Like 3/PLA, the TRBs' responsibilities include computer network exploitation, but also cryptology and communications intelligence.[127] Next to the military region TRBs, the PLA runs Service TRBs which intercept communications in areas related to their interests, such as the air force or the navy.[128] It is likely that TRBs will also be integrated with the SSF.

3.3.4. General Staff Department's 4th Department

Even though the **4th Department (4/PLA)** has received less attention than 3/PLA, it (or its respective future successor under the SSF) is expected to fall under greater scrutiny due to the revelation of the existing network attack forces in the 2013 edition of *The Science of Military Strategy*.[129] Also known as the Electronic Countermeasures Department, 4/PLA is the institution one should become familiar with when seeking to prepare for the increasingly hyped danger of cyber war. Hierarchically the equal of 3/PLA, 4/PLA was traditionally responsible for electronic warfare, but has recently also assumed the task of carrying out computer network attacks (CNA)[130] as a result of the PLA's adoption of an offensive information warfare doctrine, the Integrated Network Electronic Warfare (INEW), which is an 'organic combination of electronic warfare and computer network warfare', as explained by General Dai Qingmin, former Commander of 4/PLA.[131] Therefore, unlike 3/PLA, this

[123] APT-1 has demonstrated the ability to establish its presence on the victim's network and revisit it over several years (the longest recognised period exceeding four years) to access the victim's intellectual property, business plans, technology blueprints, etc. See more at APT-1, 2013, pp. 3-5. The Chinese side has called the Mandiant's report 'amateurish' and argued it is technologically highly unlikely to track the origin of specified attacks. See more at 'Chinese Media Slam Cyber-Hacking Report.' *VOA*. 21 Feb. 2013. Accessed 24 Aug. 2016. <http://www.voanews.com/content/china-media-slam-cyber-hacking-report/1607835.html>.

[124] Stokes et al., 2011, p. 11.

[125] See more at *CrowdStrike Intelligence Report: Putter Panda*. Report by CrowdStrike, 2014. <https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf>.

[126] Cheng, Joey. 'Cyber Conflict Escalates: Second Chinese PLA Hacking Group Accused.' *Defense Systems*. 10 June 2014. Accessed 24 Aug. 2016. <http://defensesystems.com/articles/2014/06/10/chinese-military-hacker-unit-crowdstrike.aspx>.

[127] Stokes et al., 2011, p. 12.

[128] Stokes, Mark. 'People's Liberation Army Infrastructure for Cyber Reconnaissance,' p. 23 in Lindsay, 2012.

[129] Indeed, even though analysts consider the newly confirmed fact rather a self-promotion and sensationalism without conveying anything substantially new, it does make other countries even more cautious when it comes to cooperating with China in any cyber-related developments. See more at Tiezzi, 2015.

[130] Krekel, Bryan, Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Report by Northrop Grumman, 2012, p. 44. <http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf>.

[131] Lu Daohai, *Information Operations.* PLA Arts and Literature Press, 1999, p. 324, cited in Mulvenon, James. 'Chapter 8: PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability,' in Kamphausen, Roy, David Lai, and Andrew Scobell (eds.) *Beyond the Strait: PLA Missions other than Taiwan*, Strategic Studies Institute, 2009, p. 260.

department's mission is offensive, rather than defensive electronic warfare or pure intelligence collection and analysis.[132] The simplest offensive activities could be denial-of-service attacks to disrupt services or the use of worms or Trojan Horses to obtain sensitive data. 4/PLA can also engage in collecting electronic intelligence and providing tactical electronic support measures.[133] Furthermore, it manages electronic countermeasures (ECM) units, which have obtained increasing coverage in the PLA media due to the increasing interconnection between information and electronic-based missions and conventional army elements during military exercises.[134]

Importantly, 4/PLA is also responsible for managing a number of research institutions related to developing new ECM. Apparently, the most notable of these is the **54th Research Institute**, which provides engineering support and facilitates the department's connection with other entities under the China Electronic Technology Corporation. For training junior officers, 4/PLA runs the PLA Electronic Engineering Academy located in Hefei as the primary academic electronic warfare centre in China.[135] Interestingly, and again deriving from the Chinese historic understanding of information as the key to victory, several of the research institutes under 4/PLA have focused on how to counter key American C4ISR systems. Some of the methods include, for example GPS jamming, Joint Tactical Information Distribution System countermeasures, and synthetic radar jamming. Such electronic warfare capabilities would be coordinated with CNA tools to conduct a complete attack against the enemy's key command and networks.[136]

Regarding the interaction between 3/PLA and 4/PLA, it is likely that some of their duties, such as R&D, intelligence collection, or managing a joint network warfare training system overlap.[137] However, the offensive nature of 4/PLA's operations distinguishes it from 3/PLA and has thereby made it a centre of discussion on cyber warfare. Yet, 3/PLA has undeniably been more attractive to foreign researchers due to its enduring cyber espionage activities, which are currently more tangible than actual cyber war. What might indicate the next possible targets of the PLA cyber units is China's thirteenth five-year plan introduced in October 2015, which outlines the industries in which China aims to achieve the most growth. Therefore, other than the defence sector, developers of clean energy, electric cars, computer chips as well as healthcare should implement greater security in their online operations.[138]

However, it is important to bear in mind that the overall 'Chinese cyber threat' is often exaggerated and not placed into proper context, especially by the Americans. While not justifying China's actions, Greg Austin, a well-regarded China expert, draws attention to factors such as commercial lobbying and attention seeking by American cyber security firms, a media environment too receptive to cyberspace intrigues and anti-China rhetoric, and the general lack of knowledge even among the highest decision-makers on the details and conduct of the US's own cyber espionage and operations against China.[139]

3.3.5. The Newcomer: PLA Strategic Support Force

The establishment of the **Strategic Support Force (SSF)** was somewhat unexpected for foreign observers, but it is actually a logical step within the general modernisation of the PLA. For example, the launch of the **PLA's Cyberspace Strategic Intelligence Research Centre** in June 2014 to 'provide strong support in obtaining high-quality intelligence research findings and help China gain advantage in national information security' already led

[132] Krekel et al., 2012, p. 47.
[133] Inkster, 2013, p. 49.
[134] Easton, Ian, and Mark A. Stokes. *China's Electronic Intelligence Satellite Developments*. Report by Project 2049 Institute, 2011, p .5. <https://project2049.net/documents/china_electronic_intelligence_elint_satellite_developments_easton_stokes.pdf>.
[135] Krekel et al., 2012, p. 47.
[136] Ibid, p. 48.
[137] Stokes et al., 2011, p. 15.
[138] CrowdStrike has mapped the groups potentially targeting particular industries according to their previously observed activities. See more at *China Global Threat Report*. Report by CrowdStrike, 2015. <https://www.crowdstrike.com/wp-content/uploads/Global_Threat_Report-2015/China-2015/Infographic_China-2015.html>.
[139] Austin, Greg. 'Cyber Security: All China's Fault?' *The Globalist*. 30 Aug. 2015. Accessed 24 Aug. 2016. <http://www.theglobalist.com/cyber-diplomacy-us-china-problem/>.

observers to conclude that the PLA's focus was increasingly falling on cyberspace.[140] Indeed, as it seems that information warfare has become central to China's 'active defence' strategic concept, the SSF will likely become the main force behind its execution, acting as a culmination of years of technological advancement and institutional change.[141] Moreover, as the SSF will assume control over the PLA's space and cyber operations, it will cover two aspects of China's new strategic 'triad' of nuclear, space, and cyber forces, which were noted as the three 'critical domains' in the *2015 Defence White Paper*.[142]

While detailed information about the SSF's structure remains limited, several Chinese military experts have commented on the new initiative. For example, a former officer Song Zhongping stated that the SFF will be composed of three separate forces: space troops (recognition and navigation satellites), cyber troops (offensive and defensive hacking), and electronic warfare forces (jamming and disrupting radars and communications).[143] Additionally, Rear Admiral Yin Zhuo of the PLA Navy and who is believed to have direct links to the SSF's creation said in January 2016 that its main task will be ensuring the military's local advantages in aerospace, space, cyber, and electromagnetic battlefields through operations such as target tracking and reconnaissance, satellite navigation, and attack and defence in cyber and electromagnetic spaces – the underlying goal of which should be attaining victory in future wars. Yin also believes the SSF will assume responsibilities in defending the civilian infrastructure to increase the security of China's financial institutions as well as people's daily lives in general.[144] Indeed, greater assimilation with the civilian sector seems essential in executing China's cyber ambitions given the rapidly growing dependence on information technology as well as the potentially dangerous aspect of informatisation to the current regime.

It thus appears that the SSF will be responsible for every aspect of information warfare, including intelligence, technical reconnaissance, cyber warfare, and electronic warfare, which are central to China's strategic thinking on asymmetric warfare and pre-emptive attack. In a larger picture, this and other ongoing military reforms aim to streamline the military activities into a 'combined wartime and peacetime military footing', which should give the country an advantageous position should a war break out against a technologically advanced opponent, such as the US.[145] Overall, this desired dominance in the information space forms an essential part of China's strategic thinking, which sees paralysing and sabotaging the enemy's operational and command systems as a key to achieving dominance in all other domains: air, sea, and land.[146]

Inevitably, the creation of the SSF and other radical changes in the structure of the PLA have brought about a reshuffling difficult to follow. Announced in February 2016, the previous seven military area commands were regrouped into five geographical theatre commands. This also meant a reorganisation of the General Staff Department, under which 3/PLA and 4/PLA have so far operated, into the Joint General Staff Department, which will not have operational control of the army unlike its predecessor.[147] Regarding the SSF, it will most likely draw forces from both 3/PLA and 4/PLA, as well as 1/PLA (operations), 2/PLA (intelligence), and the Informatisation Department, which is expected to move under the SSF entirely. This means a significant increase in efficiency when it comes to China's cyber-related operations, as computer network attack and defence, technical reconnaissance,

[140] Yao, Jianing. 'PLA Cyberspace Strategic Intelligence Research Center Founded.' *China's Military*. 30 June 2014. Accessed 24 Aug. 2016. <http://eng.chinamil.com.cn/news-channels/china-military-news/2014-06/30/content_6025789.htm>.
[141] Costello, 2016, *The Jamestown Foundation.*
[142] Costello, John. 'China Finally Centralizes Its Space, Cyber, Information Forces.' *The Diplomat*. 20 Jan. 2016. Accessed 24 Aug. 2016. <http://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/>.
[143] Costello, 2016, *The Jamestown Foundation*. Original comments in Chinese are available at <http://mil.huanqiu.com/observation/2016-01/8392698.html>.
[144] Costello, 2016, *The Jamestown Foundation.* Original comments in Chinese are available at <http://military.people.com.cn/n1/2016/0105/c1011-28011251.html>.
[145] Costello, 2016, *The Jamestown Foundation.*
[146] Costello, 2016, *The Diplomat.*
[147] Ying, Yu Lin. 'The Implications of China's Military Reforms.' *The Diplomat*. 7 Mar. 2016. Accessed 24 Aug. 2016. <http://thediplomat.com/2016/03/the-implications-of-chinas-military-reforms/>.

espionage, electronic countermeasures, intelligence, as well as majority of communications and information management will all be operating under one command.[148]

Overall, the creation of the SSF is a landmark development, giving a clear indication of the PLA's focus on informationised warfare, which raises questions of whether these actions should be seen as provocative preparations for an overt conflict, or merely to provide China with more credible deterrence in the face of technologically advanced Western powers. The developments must also be placed into political context, as they shift control over China's most powerful and strategically important weapons from the army to the Central Military Commission, headed by President Xi.[149]

3.4. Hacktivist Units and Cyber Militia

Other than the PLA cyber units, various other groups operate from the Chinese cyberspace. Research by Jeffrey Kwong in 2012 suggested that most of the openly confirmed attacks actually originated from such independent hacktivist units. Even though the assertion was made more than four years ago, it should not be disregarded as it relies on data from 1990 to 2012 and thus enables the assertion of an interesting theory: whenever the Chinese lack influence over foreign threats, attacks by independent units increase China's credibility in the opponent's eyes. Kwong brings out clear evidence that the government's threats against another country are directly followed by widespread cyber-attacks to increase domestic and international credibility. Since the groups are uncontrolled and more nationalistic than the state, they create a risk of domestic unrest if the government should decide to retreat from its demands. Therefore, the Chinese government faces a double threat from cyber-attacks: adopting too mild approach against the opponent could invite the attacker groups to turn against China to express displeasure; while letting the groups go completely untamed creates a risk of falling into a bilateral conflict with another state.[150]

An example of such a group is the Red Hacker Alliance. The group has not been widely covered in the media, but it is believed to have a membership of several hundred thousand. It has been noted that the government tolerates and most likely even supports the group because of the large quantity of stolen data available from its members. At the same time, while the Red Hacker Alliance is afraid of a crackdown on its activities, the government fears an online rebellion by the hacktivists if it decides to oppose them.[151] Overall, it is an intriguing paradox that the Chinese government needs to address. However, despite the risk of becoming malicious against the motherland itself, or the chance of cyber incidents spiralling out of control, the groups have efficiently proven their value and are thus unlikely to fall under more serious control by the government.

Slightly different from the above described organs are the so-called 'cyber militias', which consist of hackers, IT companies, scientists, network engineers, foreign language speakers, and others with useful skills. Their main mission is to take part in military exercises as part of the National Emergency Drill Structure. However, they are not directly managed by the PLA in order to avoid the possible ambiguity over their combatant status and activities.[152] The cyber militias are seen as part of the effort to enhance civil-military cooperation within the country and were even impliedly provided with a strategic impetus in the civilian 15-year strategy issued in 2006.[153] Contrary to popular belief, the groups tend to have a rather defensive nature, and conduct training missions for the PLA

[148] Costello, 2016, *The Jamestown Foundation.*

[149] For a detailed overview of the nature and the impact of the ongoing military reforms, see Allen, Kenneth, Dennis J. Blasko, and John F. Corbett. 'The PLA's New Organizational Structure: What Is Known, Unknown and Speculation (Part 1).' *The Jamestown Foundation*. 4 Feb. 2016. Accessed 25 Aug. 2016. <http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=45069&no_cache=1#.V8gxG7t95aQ>.

[150] Kwong, Jeffrey. 'State Use of nationalist Cyber Attacks as Credible Signals in Crisis Bargaining,' pp. 30-32 in Lindsay, 2012.

[151] Feakin, 2013, pp. 4-5 and Henderson, Scott. 'Beijing's Rising Hacker Stars: How Does Mother China React?' *IO Sphere* (2008): pp. 25-30. <http://fmso.leavenworth.army.mil/documents/Beijings-rising-hackers.pdf>.

[152] Stevens, Tim. 'Breaching Protocol: The Threat of Cyberespionage.'*Academia.edu*. Accessed 24 Aug. 2016. <http://www.academia.edu/1158361/Breaching_Protocol_The_Threat_of_Cyberespionage>.

[153] Sheldon, Robert and Joe McReynolds. 'Chapter 8: Civil-Military Integration and Cybersecurity,' p. 196 in Lindsay et al., 2015.

operators and research on cyber warfare.[154] Consisting of over eight million citizens, all related to Chinese developmental programmes, it is a powerful force. While open source information on who controls such a large number of people remains unavailable, it is believed that the cyber militia are commanded through hierarchical layers of administration similar to a regular militia. However, the extent of the cyber militias' connections and accountability to the government and the PLA remains unclear and deserves further examination.[155]

As a concluding remark on the military's role regarding China's overall use of cyberspace, it has undoubtedly achieved much in coming closer to its ultimate goal of mastering information – both foreign and domestic – to ensure the state's stability and exploit the opportunities arising from cyber espionage. Having worked hand in hand with the government, 3/PLA and 4/PLA had so far played a critical role in executing China's overall ambition to catch up with Western technological development, and also obtain economic and political advantage in order to increase China's international bargaining power. As the responsibilities of these two departments have likely been integrated into the Strategic Support Force, the efficiency of China's state-led cyber operations is further expected to increase and the intense focus on information warfare indicates China's ability to adapt its military force to the changing nature of international conflict. Simultaneously, the patriotic hacking units are in a way trying to help the government, but also risk harming China's reputation and other countries' willingness to cooperate, which is already hampered by the PLA's cyber units' activities. Yet, the Chinese government is unlikely to put a stop to further development of cyber espionage and cyber warfare capabilities, and perhaps rightfully so, looking at similar surveillance activities of its main competitors and potential adversaries on the international arena.

[154] Sheldon, Robert and Steve Gilnert. 'Civil-Military Integration and China's Cyberspace Operations: Investigating PLA Cyber Militias,' p. 24 in Lindsay, 2012. However, as later research suggests, the cyber militia do sometimes conduct cyber attacks and cyber espionage if necessary. See more at Sheldon and McReynolds, 2015, p. 200.
[155] For a detailed overview on cyber militia, see Sheldon and McReynolds, 2015.

Bibliography

Books

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* Ecco, 2010.

Hannas, William C., James C. Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*. Routledge, 2013.

Inkster, Nigel. *China's Cyber Power*. Routledge, 2016.

Jiang Zemin Wenxuan (Jiang Zemin Anthology). Beijing, 2006, cited in Chang, 2014, p. 19.

Kamphausen, Roy, David Lai, and Travis Tanner (eds). *Assessing the People's Liberation Army in the Hu Jintao Era*, Strategic Studies Institute, 2014, cited in Chang, 2014, p. 20.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron (eds) *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*. Oxford University Press, 2015.

Lu Daohai, *Information Operations.* PLA Arts and Literature Press, 1999, p. 324. Cited in Mulvenon, James. 'Chapter 8: PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability,' in Kamphausen, Roy, David Lai, and Andrew Scobell (eds) *Beyond the Strait: PLA Missions other than Taiwan*. Strategic Studies Institute, 2009, p. 260.

Peng Guangqian and Yao Youzhi, 'Chapter 20: Rise of the High-Tech Local War and Its Historic Status,' in *The Science of Military Strategy*, Academy of Military Science Strategic Research Department. Beijing, 2005, cited in Chang, 2014, p. 25.

Qiao, Liang, and Wang Xiangsui. *Unrestricted Warfare*. PLA Literature and Arts House, 1999.

Thomas, Timothy L. 'Chapter 20: Nation-State Cyber Strategies: Examples from China and Russia,' in Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz (eds) *Cyberpower and National Security*, National Defense University Press and Potomac Books Inc., 2009. Accessed via <http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-20.pdf>.

Thomas, Timothy L. *The Dragon's Quantum Leap*. Foreign Military Studies Office, 2009.

Thomas, Timothy L. *Three Faces of the Cyber Dragon*. Foreign Military Studies Office, 2012.

Academic Articles

Creemers, Rogier. 'Cyber-Leninism: History, Political Culture and the Internet in China.' (2015). Draft available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2589884>.

Dewar, Robert S. *The 'Triptych of Cyber Security': A Classification of Active Cyber Defence*. Proceedings of 6th International Conference on Cyber Conflict, Tallinn. 2014, pp. 7-21. <https://ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf>.

Giles, Keir, and William Hagestad II. *Divided by a Common Language: Cyber Definitions in Chinese, Russian and English*. Proceedings of 5th International Conference on Cyber Conflict, Tallinn. 2013. *NATO CCDCOE Publications*. <https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf>.

Henderson, Scott. 'Beijing's Rising Hacker Stars: How Does Mother China React?' *IO Sphere* (2008): pp. 25-30. <http://fmso.leavenworth.army.mil/documents/Beijings-rising-hackers.pdf>.

Inkster, Nigel. 'Chinese Intelligence in the Cyber Age.' *Survival: Global Politics and Strategy* 55(1) (2013): pp. 45-66, <https://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-february-march-2013-3db7/55-1-05-inkster-936c>.

Jiang, Li, Zhang Xiaolan, and Yu Feibao. 'Deadlock in International Cooperation Regarding Cyber Security and Its Solutions.' *Xiandai Guoji Guanxi (Contemporary International Relations)* 9 (2013), cited in Liffran, Camille. 'Chinese Perspectives on Cyber Security and International Relations.' *China's Expanding Cyberspace* (2014): pp. 5-7. <http://www.ecfr.eu/page/-/ChinaAnalysisEng_June2014.pdf>.

Serger, Sylvia Schwaag, and Magnus Breidne. 'China's Fifteen-Year Plan for Science and Technology: An Assessment.' *Asia Policy* 4 (2007): 135-64. <http://docplayer.net/191328-China-s-fifteen-year-plan-for-science-and-technology-an-assessment.html>.

Reports

2016 Global R&D Funding Forecast. Report by Industrial Research Institute, (2016). <https://www.iriweb.org/sites/default/files/2016GlobalR%26DFundingForecast_2.pdf>.

APT1: Exposing One of China's Cyber Espionage Units. Report by Mandiant, (2013). <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.

Chang, Amy. *Warring State: China's Cybersecurity Strategy*. Report by the Center for a New American Security, 2014. <http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf>.

China Global Threat Report. Report by CrowdStrike, (2015). <https://www.crowdstrike.com/wp-content/uploads/Global_Threat_Report-2015/China-2015/Infographic_China-2015.html>.

CrowdStrike Intelligence Report: Putter Panda. Report by CrowdStrike, (2014). <https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf>.

Easton, Ian, and Mark A. Stokes. *China's Electronic Intelligence Satellite Developments*. Report by Project 2049 Institute, (2011). <https://project2049.net/documents/china_electronic_intelligence_elint_satellite_developments_easton_stokes.pdf>.

Ernst, Dieter. *Indigenous Innovation and Globalization – the Challenge for China's Standardization Strategy*. Report by the East-West Center, (2010). <http://www.eastwestcenter.org/fileadmin/stored/pics/Ernst%20EWC%20NBR%20Report%20%2011%2015%2010.pdf>.

Feakin, Tobias. *Enter the Cyber Dragon*. Report by the Australian Strategic Policy Institute, (2013). <https://www.aspi.org.au/publications/special-report-enter-the-cyber-dragon-understanding-chinese-intelligence-agencies-cyber-capabilities/10_42_31_AM_SR50_chinese_cyber.pdf>.

Grauman, Brigid. *Cyber-security: The Vexed Question of Global Rules*. Report by Security & Defence Agenda, (2012).

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the United Nations General Assembly, (2013). <http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98>.

Hsu, Kimberly, and Craig Murray. *China and International Law in Cyberspace*. Report by the U.S.-China Economic and Security Review Commission, (2014). <http://origin.www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf>.

International Code of Conduct for Information Security. Report of the United Nations General Assembly, (2015). <https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf>.

Lindsay, Jon. *China and Cybersecurity: Political, Economic, and Strategic Dimensions*. Report by the University of California Institute on Global Conflict and Cooperation, (2012). <https://www.usnwc.edu/Academics/Faculty/Derek-Reveron/Documents/China-and-Cybersecurity-Workshop-Report-final.aspx>.

Red Line Drawn: China Recalculates Its Use of Cyber Espionage. Report by FireEye, (2016). <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf>.

Stokes, Mark A. *The PLA General Staff Department Third Department Second Bureau*. Report by Project 2049 Institute, (2015). <http://www.project2049.net/documents/Stokes_PLA_General_Staff_Department_Unit_61398.pdf>.

Stokes, Mark A., Jenny Lin, and Russell Hsiao. *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*. Report by Project 2049 Institute, (2011). <https://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf>.

The Cyber Index: International Security Trends and Realities. Report by the United Nations Institute for Disarmament Research, (2013). <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>.

Official documents and press releases

Information Office of the State Council. *The Diversified Employment of China's Armed Forces*. Apr. 2013. Accessed 23 Aug. 2016. <http://www.nti.org/media/pdfs/China_Defense_White_Paper_2013.pdf>.

North Atlantic Treaty Organisation. *Cyber Defence Pledge*. 8 July 2016. Accessed 18 Aug. 2016. <http://www.nato.int/cps/en/natohq/official_texts_133177.htm>.

Presentations and speeches

'China's Perspective on Building a Peaceful, Secure, Open and Cooperative Cyberspace.' UNIDIR Conference. 10 Feb. 2014. Accessed 24 Aug. 2016. <http://www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf>.

Fu, Jingguang. 'Policies and Practices on Network Security of MIIT.' Workshop on Cybersecurity Policy Development in the APEC Region. Hangzhou. 27 Mar. 2011. Accessed 23 Aug. 2016. <http://mddb.apec.org/Documents/2011/TEL/TEL43-SPSG-WKSP/11_tel43_spsg_wksp_004.pdf>.

Zhao, Xiaofan. 'Practice and Strategy of Informatisation in China.' State Council Informatisation Office Department of IT Application Promotion. Shanghai. 18 Oct. 2006. Accessed 19 Aug. 2016. <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025040.pdf>.

Online resources

'An Open Letter to Lu Wei and the Cyberspace Administration of China.'*Greatfire.org*. 26 Jan. 2015. Accessed 23 Aug. 2016. <https://en.greatfire.org/blog/2015/jan/open-letter-lu-wei-and-cyberspace-administration-china>.

'China Headed to Overtake EU, US in Science & Technology Spending, OECD Says.' *OECD*. 12 Nov. 2014. Accessed 22 Aug. 2016. <http://www.oecd.org/newsroom/china-headed-to-overtake-eu-us-in-science-technology-spending.htm>.

'China Internet Users.' Internet Live Stats, 2016. Web. Accessed 18 Aug. 2016. <http://www.internetlivestats.com/internet-users/china/>.

'China Launches First Cybersecurity Organisation.' *Cyber Security Review*. 26 Mar. 2016. Accessed 23 Aug. 2016. <http://www.cybersecurity-review.com/china-launches-first-cybersecurity-organisation-report>.

'Chinese Media Slam Cyber-Hacking Report.' *VOA*. 21 Feb. 2013. Accessed 24 Aug. 2016. <http://www.voanews.com/content/china-media-slam-cyber-hacking-report/1607835.html>.

'Chinese President Xi Jinping Calls for International Cooperation on Cyberspace Security.' *The Economic Times*. 19 Nov. 2014. Accessed 23 Aug. 2016. <http://economictimes.indiatimes.com/news/international/world-news/chinese-president-xi-jinping-calls-for-international-cooperation-on-cyberspace-security/articleshow/45205445.cms>.

'Cyberspace.' *Defense Technical Information Center of the US Department of Defense.* Accessed 19 Aug. 2016. <http://www.dtic.mil/doctrine/dod_dictionary/data/c/10160.html>.

'Gross Domestic Spending on R&D.' *OECD Data*. 2016. Accessed 22 Aug. 2016. <https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm>.

'Infographic: Achievements of the 2nd WIC.' *China Daily*. 21 Dec. 2015. Accessed 23 Aug. 2016. <http://www.chinadaily.com.cn/business/tech/2015-12/21/content_22761073.htm>.

'SIPRI Military Expenditure Database.' *SIPRI*. 2016. Accessed 19 Aug. 2016. <http://www.sipri.org/research/armaments/milex/milex_database>.

'State Administration for Science, Technology and Industry for National Defense (SASTIND).' *Nuclear Threat Initiative*. 1 Oct. 2011. Accessed 23 Aug. 2016. <http://www.nti.org/learn/facilities/781/>.

'The Obama-Xi Cyber Mirage.' *The Wall Street Journal*. 27 Sept. 2015. Accessed 19 Aug. 2016. <http://www.wsj.com/articles/the-obama-xi-cyber-mirage-1443387248>.

'Xi Jinping: Ba wo guo cong wangluo daguo jianshe chengwei wangluo qiangguo (Xi Jinping: From a big internet country to a powerful internet country).' *Xinhuanet*. 28 Feb. 2014. Accessed 23 Aug. 2016. <http://news.xinhuanet.com/info/2014-02/28/c_133148804.htm>.

'China: Summary of the Tenth Five-Year Plan (2001-2005) – Information Industry'. Available at <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan022769.pdf>.

'Jing Xi Jinping zhuxi pizhun zhongyang junwei yinfa 'guanyu jinyibu jiaqiang jundui xinxi anquan gongzuo de yijian (Chairman of the Central Military Commission Xi Jinping approved the issuance of 'Opinion on Further Strengthening Military Information Security Work'),' *Jiefangjun bao (PLA Daily)*, 7 Oct. 2014. <http://news.xinhuanet.com/mil/2014- 10/07/c_1112726181.htm>, cited in Chang, 2014, p. 19.

Allen, Kenneth, Dennis J. Blasko, and John F. Corbett. 'The PLA's New Organizational Structure: What Is Known, Unknown and Speculation (Part 1).' *The Jamestown Foundation*. 4 Feb. 2016. Accessed 25 Aug. 2016. <http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=45069&no_cache=1#.V8gxG7t95aQ>.

Austin, Greg. 'Cyber Security: All China's Fault?' *The Globalist*. 30 Aug. 2015. Accessed 24 Aug. 2016. <http://www.theglobalist.com/cyber-diplomacy-us-china-problem/>.

Cheng, Joey. 'Cyber Conflict Escalates: Second Chinese PLA Hacking Group Accused.' *Defense Systems*. 10 June 2014. Accessed 24 Aug. 2016. <http://defensesystems.com/articles/2014/06/10/chinese-military-hacker-unit-crowdstrike.aspx>.

Chin, Josh. 'China Says New Internet Regulations Won't Increase Blocking of Foreign Websites.' *The Wall Street Journal*. 30 Mar. 2016. Accessed 23 Aug. 2016. <http://www.wsj.com/articles/china-says-new-internet-regulations-wont-increase-blocking-of-foreign-websites-1459351655>.

Costello, John. ‘China Finally Centralizes Its Space, Cyber, Information Forces.’ *The Diplomat*. 20 Jan. 2016. Accessed 24 Aug. 2016. <http://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/>.

Costello, John. ‘The Strategic Support Force: China's Information Warfare Service.’ *The Jamestown Foundation*. 8 Feb. 2016. Accessed 23 Aug. 2016. <http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=45075&cHash=9758054639ab2cb6bc7868e96736b6cb#.V6RA_Lt95aQ>.

Creemers, Rogier. ‘Cybersecurity and Informatisation Leading Group: Names and Documents.’ *China Copyright and Media*. 13 Mar. 2014. Accessed 23 Aug. 2016. <https://chinacopyrightandmedia.wordpress.com/2014/03/13/cybersecurity-and-informatization-leading-group-names-and-documents/>.

Creemers, Rogier. ‘People's Republic of China Cybersecurity Law (Second Reading Draft).’ *China Copyright and Media*. 6 July 2016. Accessed 18 Aug. 2016. <https://chinacopyrightandmedia.wordpress.com/2016/07/06/peoples-republic-of-china-cybersecurity-law-second-reading-draft/>.

Gu, Fa, „State Council vigorously promotes the development of information technology and to effectively protect the information security.’ 2012, cited in Giles and Hagestad, 2013, pp. 12-13.

Harold, Scott Warren. ‘The U.S.-China Cyber Agreement: A Good First Step.’ *RAND Corporation*. July 2016. Accessed 19 Aug. 2016. <http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>.

Huntsman, Jon. ‘The 100 Most Influential People: Lu Wei.’ *Time*. 16 Apr. 2015. Accessed 23 Aug. 2016. <http://time.com/3823285/lu-wei-2015-time-100/>.

Hurwitz, Roger. ‘A Scene from the Road to Cyber Governance: The Budapest Cyberspace Conference.’ *MUNK School of Global Affairs*. 26 Feb. 2013. Accessed 19 Aug. 2016. <http://www.cyberdialogue.ca/2013/02/a-scene-from-the-road-to-cyber-governance-the-budapest-cyberspace-conference/>.

Jiang, Zemin, ‘Lun zhongguo xinxi jishu chanye fazhan (On China’s Information Technology Industry Development),’ *Xinhua*, 22 Apr. 2009. <http://news.xinhuanet.com/newscenter/2009-04/22/content_11232665_1.htm.>, cited in Chang, 2014 p.16.

Lococo, Edmond, and Keith Zhai. ‘China Seeks Global Internet Influence at CEO Forum on Canal Bank.’ *Bloomberg Technology*. 18 Nov. 2014. Accessed 18 Aug. 2016. <http://www.bloomberg.com/news/articles/2014-11-18/china-seeks-global-internet-influence-at-ceo-forum-on-canal-bank>.

Lu, Chuanying. ‘China's Emerging Cyberspace Strategy.’ *The Diplomat*. 24 May 2016. Accessed 23 Aug. 2016. <http://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/>.

Rountree, Florence. ‘Information management and internet regulation in China.’ *China's Expanding Cyberspace* (2014): pp. 11-13. <http://www.ecfr.eu/page/-/ChinaAnalysisEng_June2014.pdf>.

Sanger, David E., and Nicole Perlroth. ‘N.S.A. Breached Chinese Servers Seen as Security Threat.’ *The New York Times*. 22 Mar. 2014. Accessed 18 Aug. 2016. <http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0>.

Segal, Adam. ‘China Moves Forward on Cybersecurity Policy.’ *Council on Foreign Relations*. 24 July 2012. Accessed 22 Aug. 2016. <http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-on-cybersecurity-policy/>.

Segal, Adam. ‘The Deepening Divide in U.S.-China Cyber Relations.’ *The National Interest*. 29 Oct. 2014. Accessed 18 Aug. 2016. <http://nationalinterest.org/blog/the-buzz/the-deepening-divide-us-china-cyber-relations-11568>.

Segal, Adam. 'What to Do About China's New Cybersecurity Regulations?' *Council on Foreign Relations*. 2 Feb. 2015. Accessed 22 Aug. 2016. <http://blogs.cfr.org/cyber/2015/02/02/what-to-do-about-chinas-new-cybersecurity-regulations/>.

Sisi, Wei, and Qiu Wei. 'China's Internet Censors Have a Choral Anthem and It's Everything You Want It to Be.' *Quartz*. 16 Feb. 2015. Accessed 23 Aug. 2016. <http://qz.com/345377/chinas-internet-censors-have-a-choral-anthem-and-its-everything-you-want-it-to-be/>.

Stark, Jill. 'US Follows Australia in Naming Huawei as a Possible Security Threat.' *The Sydney Morning Herald*. 9 Oct. 2012. Accessed 18 Aug. 2016. <http://www.smh.com.au/it-pro/security-it/us-follows-australia-in-naming-huawei-as-a-possible-security-threat-20121007-277ad.html>.

Stevens, Tim. 'Breaching Protocol: The Threat of Cyberespionage.'*Academia.edu*. Accessed 24 Aug. 2016. <http://www.academia.edu/1158361/Breaching_Protocol_The_Threat_of_Cyberespionage>.

Thomas, Timothy L. 'Information Security Thinking: A Comparison of U.S., Russian, And Chinese Concepts.' *Foreign Military Studies Office Publications*. July 2001. Accessed 19 Aug. 2016. <http://fmso.leavenworth.army.mil/documents/infosecu.htm>.

Tiezzi, Shannon. 'China (Finally) Admits to Hacking.' *The Diplomat*. 18 Mar. 2015. Accessed 23 Aug. 2016. <http://thediplomat.com/2015/03/china-finally-admits-to-hacking/>.

Tiezzi, Shannon. 'US Indicts 5 PLA Officers For Hacking, Economic Espionage.' *The Diplomat*. 20 May 2014. Accessed 19 Aug. 2016. <http://thediplomat.com/2014/05/us-indicts-5-pla-officers-for-hacking-economic-espionage/>.

Wang Yukai, 'Zhongyang wangluo anquan yu xinxihua lingdao xiaozu de youlai ji qi yinxiang (The Origins and Influence of the Central Network Security and Informatization Leading Small Group),' *Zhongguo Gongchandang Xinwen Wang (Communist Party of China News Network)*, 3 Mar. 2014. http://theory. people.com.cn/n/2014/0303/c40531-24510897.html>, cited in Chang, 2014, p. 16.

Xue Ruihan, 'Jianli jianqian guojia wangluo he xinxi anquan chang xiao jizhi (Establish and improve the national network and information security long-term mechanisms),' *Renmin Wang (People's Daily Online)*, 17 Apr. 2014, <http://leaders.people.com.cn/n/2014/0417/c347621- 24909496.html>, cited in Chang, 2014, p. 17.

Yao, Jianing. 'PLA Cyberspace Strategic Intelligence Research Center Founded.' *China's Military*. 30 June 2014. Accessed 24 Aug. 2016. <http://eng.chinamil.com.cn/news-channels/china-military-news/2014-06/30/content_6025789.htm>.

Ying, Yu Lin. 'The Implications of China's Military Reforms.' *The Diplomat*. 7 Mar. 2016. Accessed 24 Aug. 2016. <http://thediplomat.com/2016/03/the-implications-of-chinas-military-reforms/>.

Zhang, Rui. 'China Headlines: Xi Slams 'double Standards,' Advocates Shared Future in Cyberspace.' *CCTV.COM*. 17 Dec. 2015. Accessed 23 Aug. 2016. <http://english.cntv.cn/2015/12/17/ARTI1450334752126739.shtml>.

Zhu, Ningzhu. 'Xi Jinping Leads Internet Security Group.' *Xinhuanet*. 27 Feb. 2014. Accessed 22 Aug. 2016. <http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm>.

Zhu, Yishi. 'Hackers Find Holes Behind the Great Firewall.' *Hackers Find Holes Behind the Great Firewall*. 21 Jan. 2012. Accessed 22 Aug. 2016. <http://english.caixin.com/2012-01-21/100350690.html>.

Abbreviations and Acronyms

1/PLA	First (Operations) Department of the General Staff Department
2/PLA	Second (Intelligence) Department of the General Staff Department
3/PLA	Third (Technical) Department of the General Staff Department
4/PLA	Fourth (Electronic Countermeasures and Radar) Department of the General Staff Department
CAC	Cyberspace Administration of China
CLSGISI	Central Leading Small Group for Internet Security and Informatisation
CNA	computer network attack
CNCERT	National Computer Network Emergency Response Technical Team/Coordination Center of China
CND	computer network defence
CNE	computer network exploitation
COSTIND	Commission for Science, Technology and Industry for National Defense
DoD	Department of Defense of the United States
ECM	electronic countermeasures
GSD	People's Liberation Army General Staff Department
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	information and communications technology
MIIT	Ministry of Industry and Information Technology
MPS	Ministry of Public Security
MSS	Ministry of State Security
NPO	New Policy Opinion
NSA	National Security Agency of the United States
PLA	People's Liberation Army
SASTIND	State Administration for Science, Technology and Industry for National Defence
SCIO	State Council's Information Office
SCO	Shanghai Cooperation Organisation
SIGINT	signals intelligence
SIIO	State Internet Information Office
SILG	State Informatisation Leading Group
SIPRI	Stockholm International Peace Research Institute
SNISCSG	State Network and Information Security Coordination Small Group
SSF	People's Liberation Army Strategic Support Force
TRB	Technical Reconnaissance Bureau