The Evolution of Chinese Perspectives on Cyber Deterrence and Attribution

Eric Siyi Zhang
Rogier Creemers

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

March, 2023

The LeidenAsiaCentre is an independent research centre affiliated with Leiden University and made possible by a grant from the Vaes Elias Fund. The centre focuses on academic research with direct application to society. All research projects are conducted in close cooperation with a wide variety of partners from Dutch society.

More information can be found on our website:

www.leidenasiacentre.nl

For contact or orders: info@leidenasiacentre.nl

M. de Vrieshof 3, 2311 BZ Leiden, The Netherlands

LEIDEN ASIA CENTRE

Partners in Research and Knowledge

Executive Summary

Deterrence, a concept developed primarily in order to deal with the perils presented by the nuclear age, has become central to debates on how to counter cyber-attacks. However, one major challenge of deterrence in cyberspace is the covert nature of cyber opertations: without means to identify the culprit of an attack, accountability becomes a vacuous concept. As such, the question of attribution is becoming increasingly politically sensitive, particularly as part of the growing tensions between the United States and China on cyber affairs.

This report reviews China's evolving strategic thinking of cyber deterrence and attribution. China's early practice of cyber deterrence focused on developing asymmetrical offensive capabilities to create a state of 'mutually assured destruction' in cyberspace. However, China's growing digitalisation prompted a pivot to defensive capabilities such as network resilience and more recently cyber attribution capabilities. On cyber attribution, China had previously maintained that technical attribution is near impossible, and that public attribution is counterproductive and hypocritical. Meanwhile, China has most likely heavily invested in cyber forensic technologies. With the recent CVERC attribution, it is logical to assume that China's official position on attribution has changed. However, it remains to be seen if China will adopt the 'naming and shaming' tactics of public attribution.

The perceptions that Chinese authors have of other actors in cyberspace seem to reflect prevelant Chinese geopolitical views in the physical space: while Chinese authors have consistently referred to the US as the 'cyber hegemon', China has meticulously studied how the US practises cyber deterrence and attribution and adopted it, when in China's interest, as far as China's capabilities allow. In comparision, there is substantially less Chinese literature written on European countries, while their strategies in cyberspace are often described as defensive. Lastly, as most Chinese authors reviewed in this report seem to adopt a state-centric approach, they see organisations such as NATO more as state-actors' policy tool, instead of an actor with agency of its own.

Contents

Introduction

As the potential risks from cyber-attacks on vital information systems continue to gain political prominence, much attention in government and security circles has gone to prevention of cyber-attacks. The concept of deterrence, developed primarily in order to deal with the challenges presented by the nuclear age, has become central to these debates, albeit with a considerable degree of scepticism.[1] One major challenge to deterrence in the digital domain is technical[2] attribution: the process of identifying who is responsible for an attack. Covert in nature, one major advantage of cyber operations is the ambiguity that they provide: no state government has ever claimed responsibility for a cyber-attack. As such, the question of attribution is becoming increasingly politically sensitive, particularly as part of the growing tensions between the United States and China on cyber affairs.[3] Yet it is also an important component of any set of norms on responsible state conduct in cyberspace: without means to identify the culprit of an attack, accountability becomes a vacuous concept.

The debate over attribution has gained increasing currency in recent years, as the United States and several of its like-minded partners have started publicly and officially attributing cyber operations to their main geopolitical adversaries, Russia and China. Both countries have, until recently, steadfastly maintained that attribution is a political act, involving double standards, and technically impossible. Nevertheless, over the last uear, Chinese companies have become increasingly active in the realm of attribution, and in September 2022, China's National Computer Virus Emergency Response Centre attributed a sustained campaign against North-western Polytechnical University in Xi'an to the NSA's Office of Tailored Access operations.[4] This constitutes the first act of public attribution by a Chinese government

[1] Lindsay, J. R. (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, *Journal of Cybersecurity*, 1(1), pp.53-67. https://doi.org/10.1093/cybsec/tyv003

[2] While technical attribution based on cyber forensics is the basis for any follow-up actions, it does not automatically entail responses from the attributor: decision-makers can choose to take no actions, non-public response (e.g. diplomatic messaging, cyber action), or public response.

[3] Levite, A. E.; Lu, C.; Perkovich, G.; Fan, Y. (28 March, 2022). Managing U.S.-China Tensions Over Public Cyber Attribution, Carnegie Endowment for International Peace. Retrieved from: https://carnegieendowment.org/2022/03/28/managing-u.s.-china-tensions-over-public-cyber-attribution-pub-86693

[4] CVERC. (5 September, 2022). Investigation report on the US NSA's cyber-attack on North-western Polytechnical University (One). Retrieved from:

actor, and will likely have consistent ramifications for China's engagement with notions of attributions and deterrence in the cyber realm.

Cyber operations are also becoming increasingly integrated in traditional military environments. The profile of cyber considerations has grown consistently in organisations such as NATO, which recognised cyberspace as a domain of operations in 2016 and issued a Comprehensive Cyber Defence Policy in 2021. This recognizes that under certain circumstances, cumulative malicious cyber activities might be considered an armed attack under the Organization's Charter, and contains greater commitment concerning offensive cyber operations and deterrent practice.[5] More specifically, NATO acknowledged the attribution of a major cyber operation against Microsoft Exchange servers by Organization members against China.[6]

Yet, where NATO has seven decades of history and practice in engaging with complex questions of strategy and security, such considerations are far newer for China, which is only now emerging as a major power. There still is considerable debate in Chinese policy circles on the very definitions of terms such as deterrence and attribution, how they are determined by the specific context of the digital domain, and how they might be applied as part of a geopolitical strategy or security doctrine. Not having had to contend with NATO previously, Beijing now also needs to develop a stance on engaging with a broad-spectrum alliance, as opposed to merely the United States. This report will review the state of these debates in China. Drawing on a thorough review of existing policy documents and literature, its main observations can be summarised as follows:

- Chinese notions of cyber deterrence have largely converged with Western ones over the past decade.
- There is not yet a uniform Chinese translation for the term cyber attribution. On the one hand, both of the terms 归因[guiyin] and 溯源[suyuan] refer to the technical

https://web.archive.org/web/20220905161834/https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm

[5] NATO. (14 June, 2021). Brussels Summit Communiqué. Retrieved from: https://www.nato.int/cps/en/natohq/news_185000.htm

[6] NATO. (19 July, 2021). Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise. Retrieved from: https://www.nato.int/cps/en/natohq/news_185863.htm

process of identifying a source or cause, while on the other, the terms 点名[dianming] and 羞辱[xiuru] refer to the notion of public accusation with political motives; those terms are closely associated with public attribution. Some earlier Chinese literature has also used a broader term 'cyber situational awareness'[网络态势感知],[7] which often also include elements of cyber attribution. The debate fragments along these lines.

- A predominant majority of Chinese literature on cyber deterrence is focused on the United States. In this context, Chinese authors often refer to the US as the 'cyber hegemon'[网络霸权], and perceives the US as China's main adversary in cyberspace. This report argues that such perceptions are a logical consequence of the reflection of the US-China geopolitical relation in cyberspace. On the other hand, there seems to be a pattern of 'mirroring' in Chinese strategic thinking of warfare – China has carefully and meticulously studied and adopted (if China's capabilities allow and if in China's interest) how the US practises cyber deterrence and attribution.
- Chinese authors tend to adopt a state-centric and structural realism approach, meaning that they believe NATO as an organisation, nor its membership outside of the US, have significant agency of their own. Moreover, NATO has not received much attention in China, largely because it was seen as an alliance focused on Europe. This could however change quickly: more recently, NATO has come under fire for being a "Cold War relic", and a vehicle for US warmongering.
- Generally, Chinese observers perceive cyber military strategies of European countries as defensive, although having a deterrence element, and mostly focusing on norm building and regulation. Some authors observe that European cyber positions are relatively close to China's, in the area of countering militarisation of cyberspace and arms control of cyber weapons.[8]

[7] which refers to only the technical aspect of attribution.

[8] Lu, C. (2019). Security Dilemma,Misperceptions and a Roadmap for Big Power Relations in Cyberspace - Taking China-EU Cyber Cooperation as an Example [网络空间大国关系面临的安全困境、错误知觉和路径选择 - 以中欧网络合作为例]. European Studies, 2019(2).

This study relies primarily on Chinese language primary and secondary sources, of which this paragraph provides an overview. First of all, as China has not yet published an official cyber defence strategy that offers operationalized doctrine, this report systematically reviews the discussions on cyber warfare in three editions (2001, 2013, and 2020) of Science of Military Strategy [战略学] (hereinafter SMS). The SMS is the capstone doctrinal publication of the PLA, which is regarded as a theorization of the PLA's military strategy, an important reference for the PLA in conducting training, education and research.[9] The 2001 and 2013 versions are edited by the PLA's Academy of Military Science (AMS)'s Military Strategy Research Department. As the AMS has not published a newer version of SMS, this report also reviewed the 2020 version of SMS edited by another prestigious institution - the National Defence University. Given the institutional affiliation and the influence of the book's editors, this report argues that the SMS is likely the most authoritative available source on China's military thinking on cyber warfare. Second, this report also reviewed Chinese journal publications since 2010 on cyber deterrence and attribution: while the landscape of earlier (approximately before 2017) Chinese secondary literature on those topics was dominated by authors with military affiliations, many Chinese authors with no military affiliations have joined the debate more recently. They effectively diversified the debate with new approaches to or sub-fields of the research, such as cyber norms, global governance, and they have also contributed to the debate in China by presenting nuanced understandings of other actors in cyberspace that are more embedded in their respective national contexts. Third, this report has also consulted official Chinese sources when relevant, among others the Chinese MFA's regular press conference. In particular, they are used to analyse China's evolving position and messaging when there seems to be a substantial Chinese policy change in public cyber attribution in 2022.

It should be pointed out that this report has its limitations, as it relies solely on open-source literature. Consequently, some information, while relevant, is unavailable to this research. As pointed out by one of the literature reviewed by this report, Chinese leader frequently rely on non-public reports from university academics and think tank experts on the issue of cyber warfare, and those reports are rarely declassified.[10] This means some considerations remain

[9] Qiu, M. (2015). China's Science of Military Strategy: Cross-Domain Concepts in the 2013 Edition. CDD Working Paper.

[10] Jiang, T. (2019). From Offence Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar. Chinese Journal of International Review, 2019(1).

unanswerable. There is, for instance, little information on the Chinese perspective on economic espionage. While Western policy-makers, private sector actors, think tank experts, and scholars paid substantial attention to alleged Chinese commercial espionage activities in cyberspace, this study does not find Chinese literature that discusses this issue. This could be because such matters are exclusively discussed internally, or because it is not a matter of much doctrinal or conceptual attention on the whole.

Chinese strategic thinking in cyber warfare and deterrence in cyberspace

Before proceeding with discussing the evolution of Chinese strategic thinking on cyber deterrence, this report underscores that there are meaningful differences between the Western[11] and Chinese terms of 'cyber deterrence'. First, it should be reiterated that many non-Western actors, including China, have a broader understanding of what cybersecurity entails. The mainstream definition in the West of cybersecurity is mostly technical, i.e. the correct functioning of the internet and infrastructure, whereas China's 2016 National Cyberspace Security Strategy suggests that the Chinese definition for cybersecurity also addresses concerns such as economic, cultural and regime security.[12] Although official documents have almost exclusively used the term 'cybersecurity'[13] [网络安全] since 2014, various Chinese authors habitually used 'information security' [信息安全] instead. In particular, literature written by authors with military affiliations are inclined to approach the issue of deterrence through the lens of a broader, more cross-domain concept of 'information security'. Both the 2013 and 2020 versions of SMS suggest that 'information operations' [信息作战] incorporate cyber, electronic and psychological warfare.[14] Also, this is reflected institutionally, as the PLA's cyber force operates under the aegis of the Strategic Support Force,

[11] At the same time, it should be noted that the concept of 'cyber deterrence' is also not totally free of contestation in the west either. Most importantly, it is still debated whether cyber deterrence is achievable? There are also different schools of thought on how cyber deterrence should be practised: whether it should be pursued by enhancing resilience and defence capabilities - 'deterrence-by denial', or by credibly raising the costs for potential attackers - 'deterrence-by-punishment'.

[12] Cyber Administration of China. (27 December, 2016). National Cyberspace Security Strategy, Full Text[国家网络空间安全战略全文].Retrieved from: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

[13] English versions of Chinese official documents use the term 'cybersecurity', while the precise translation of the original Chinese term '网络安全' should be 'network security.'

[14] AMS Military Strategy Research Department (ed.) (2013), The Science of Military Strategy [战略学].

AMS Military Strategy Research Department (ed.) (2020), The Science of Military Strategy [战略学], Beijing: Military Science Press. p. 130.

which incorporates cyber, electronic, and space warfare.[15] This should inform European policy makers that China's strategy and conduct of cyber deterrence and cyber warfare likely has cross-domain features, and cybersecurity is not only about internet networks and systems, but also about the tactical use of information. However, this report mostly confines its discussion to the network aspect of China's strategic thinking on deterrence.

As for the concept of deterrence, there are also notable differences between Chinese and Western understandings. Jiang (2019) points out that the Chinese conceptualisation originates from its own (mis)understanding of Western deterrence strategies: Chinese strategists argue that Western deterrence strategies are inherently aggressive, to intimidate perceived adversaries into submission.[16] Lexically, the Chinese translation of deterrence consists of two characters: weishe[威慑], where wei[威] stands for the display of power, and she[慑] stands for to terrorise and to compel. Chinese understanding of the nature of Western 'deterrence' does not only include dissuading potential adversaries from attacking, but also compelling adversaries into taking certain actions.[17] To a certain extent, the Chinese understanding of deterrence as aggressive may be influenced by its experience of nuclear "blackmail" by the US and the Soviet Union during the 1950s and 1960s. Regardless of whether this understanding is factually correct or logically consistent, the initial Chinese strategic thinking on cyber warfare originated from this assumption, and early Chinese literature suggests that the primary strategic objective of China's strategic deterrence is 'anti-coercion'[反威压].[18] Implicitly, the strategic thinking of 'anti-coercion' draws direct parallels from China's thinking on nuclear deterrence: in order to prevent adversaries from coercing China, China must have its own nuclear weapons.[19] AMS's 2001 edition of SMS argues that 'information deterrence'[信息威慑] is similar to nuclear deterrence, as it can lead to large-scale damage to

[15] State Council of China. (2019) China's National Defence in the New Era. Retrieved from: http://www.gov.cn/zhengce/2019-07/24/content_5414325.htm.

[16] Jiang, T. (2019). From Offence Dominance to Deterrence.

[17] Cheng, D. (2020). An overview of Chinese thinking about deterrence, in Osinga, F., Sweijs, T. (ed.). Netherlands Annual Review of Military Studies 2020 – Deterrence in the 21st Century – Insights from Theory and Practice. The Hague: Asser Press.

[18] Li, B. (2006). Debating and Analyzing China's Nuclear Strategy [中国核战略辨析]. World Economics and Politics, 2006(6).

[19] Jiang. (2019). p.9.

both the deterrent and the deterred.[20] Similarly, AMS's 2013 edition of SMS argues that cyber deterrence shares certain characteristics with nuclear deterrence, and 'cyber great powers may be able to achieve a status quo where all possess cyber offensive capabilities but no one resorts to the use of cyber weapons'.[21] Some other Chinese authors explicitly point out that the concept of 'mutually assured destruction' should be applied in cyberspace. This line of thought has persisted across Chinese strategic thinking on cyber deterrence, and not only in writings advocating 'offensive dominance', but also those calling for a more defensive approach to cyber deterrence.[22]

Appreciating the foundations of Chinese thinking on cyber deterrence enables understanding why recent Chinese policy documents describe other states' pursuit of cyber deterrence as a destabilising factor. Chinese strategic thinking generally assumes that compellence is an inherent part of Western deterrence strategies. An important question in this context is whether Chinese authors believe China's own deterrence posture should have a compellence element when a potential adversarial state or non-state actor is perceived to have inferior cyber warfare capabilities to China. There are a few sporadic references to the issue in early Chinese literature, whereas the discussion of the relation between compellence and China's cyber deterrence is absent in more recent Chinese literature reviewed by this report. 2001 SMS argues that cyber deterrence can be used to 'shock and awe'[不战而屈人之兵] perceived adversaries and 'achieve a bloodless victory'. The 2007 edition of the PLA Encyclopaedia defined the purpose of information deterrence is to allow the deterring side to 'achieve certain political goal'[达到一定的政治目标].[23] This suggests earlier Chinese strategic thinking might have pondered the possibility to use cyber deterrence to secure at least tactical objectives

[20] AMS Military Strategy Research Department (ed.) (2001), The Science of Military Strategy [战略学], Beijing: Military Science Press. p. 237.

[21] AMS Military Strategy Research Department (ed.) (2013), The Science of Military Strategy [战略学], p. 196.

[22] E.g. Jiang, Y. (2015). Strengthening the construction of cyber deterrence power is the tactic to strengthen a state in the information era[加强网络威慑力量建设是信息时代的强国之策]. Cyberspace Strategy Forum, 2015(11).

Cheng, Q., He. Q. (2015). Building China's cyber deterrence strategy[构建中国网络威慑战略]. Cyberspace Strategy Forum, 2015(11).

[23] Chen, D. (2020). An overview of Chinese thinking about deterrence.

during both peacetime and wartime, while it is unclear whether this school of thought has remained among Chinese experts in the 2010s.

The initial strategic thinking in China on cyber and electronic warfare originated almost exclusively from commentators with military affiliations, and it was largely prompted by the demonstrated cyber capabilities of the US.[24] In particular, during the First Gulf war, the US and its allies' using cyber, electronic and information warfare to defeat the Iraqi army inspired the PLA to develop its own information warfare capabilities. The early stages of China's strategic thinking on cyber warfare from the 1990s to the 2000s are characterised by a belief in the doctrine of 'offensive dominance'. This holds that deterrence in cyberspace is achieved by possessing and demonstrating the ability to conduct cyber-attacks. In this context, it is worth noting the similarities and differences between 'deterrence by punishment' (as widely used among literature published in Western countries) and 'offensive dominance'. Arguably, both concepts aim to deter perceived adversaries from attacking by the credible threat of unacceptable counteraction, while their differences lie in how the threat of counteraction is signalled. Offensive dominance espouses the ontological view that warfare [实战] and deterrence is integrated in cyberspace,[25] and prescribes that states should actualise deterrence through engaging in (pre-emptive) cyber-attacks. For example, Yuan Yi, an author affiliated to the AMS, argues that cyber deterrence is characterised by the integration of deterrence and warfare [慑战结合], and deterrence is achieved by demonstrating capability and willingness with 'small-scale and precise (cyber) warfare'.[26] The more authoritative 2001 SMS, argues that

[24] Jiang, T. (2019).

[25] Kania, E.B. (2016). Cyber Deterrence in Times of Cyber Anarchy – Evaluating the Divergences in U.S. and Chinese Strategic Thinking. 2016 International Conference on Cyber Conflict. Retrieved from: https://ieeexplore.ieee.org/document/7836619.

[26] 'The general requirement of the application of deterrence in cyberspace is: combining deterrence and warfare, and to demonstrate ability and willingness [to deploy cyber weapons] by real power and real warfare, and striving for demonstrating deterrence with small battles, and to ensure deterrence though precise strikes, in order to achieve the purpose of deterrence with relatively low costs. [网络空间威慑总的运用要求是：慑战结合，以实力、实战展示能力和决心，力求以小战体现威慑、以精打确保威慑，以较小的代价实现威慑目的' in

Yuan, Y. (2015). A short analysis of the characteristics, types, and important points of applications of cyberspace deterrence[浅析网络空间威慑的特征、类型和运用要点]. Cyberspace Strategy Forum, 2015(11)

deterrence and warfare in cyberspace is inseparable, and cyber deterrence is usually concurrent with cyber-attacks.[27]

For China in the 2000s, 'offensive dominance' as a strategy resulted from a cost-benefit analysis based on two factors: (1) the assessment that technical conditions disproportionately favoured offence and complicated defence, and the cost for the defence outweighed that of the attacker during a cyber war,[28] and (2) that China in the 2000s was a 'digital have-not' country with little digital and internet assets to defend. Chinese literature enumerated a number of reasons why engaging in cyber-attacks is favourable: cyberattack was perceived as a low cost, covert, but destructive, while the resources required to conduct effective defence in cyberwarfare are asymmetrically large, particularly because early detection and attribution of cyberattacks and attribution is difficult.[29] Offensive dominance is an attractive course for 'digital have-nots', as they have relatively less incentive and stake in dissuading adversaries from attacking their own digital assets. In any case, the damage caused to the adversaries would likely disproportionately outweigh the damage sustained by themselves. China was a digital late-comer, and the gap between the digital vulnerability surface of China and its prime adversaries (mainly the US) was vast. Consequently, early Chinese literature generally argues that cyber deterrence is more effective towards states with more developed ICT infrastructure, and cyber-attacks can offset China's disadvantage in other capabilities in order to achieve the strategic objective of 'anti-coercion'.[30] Yuan Yi from the PLA's AMS metaphorically described cyber weapons as 'the atomic bomb of poor states' [穷国的原子弹].[31] Early Chinese literature also pointed to the 'first-mover-advantage' in cyber warfare: the 2001 edition SMS suggested that offensive dominance-oriented cyber deterrence is an effective cross-domain deterrence

[27] It is often the case [in cyberspace] that informational deterrence and informational attack occur simultaneously, and the border between deterrence and warfare is unclear[往往是信息威慑与信息进攻并举，威慑与实战界限不甚分明] in

AMS Military Strategy Research Department (ed.) (2001), The Science of Military Strategy [战略学], p. 237.

[28] AMS Military Strategy Research Department (ed.) (2001), The Science of Military Strategy [战略学]

[29] Yuan, Y. (2015). A short analysis of the characteristics, types, and important points of applications of cyberspace deterrence.

[30] AMS Military Strategy Research Department (ed.) (2001). p.238.

[31] Yuan, Y. (2015). A short analysis of the characteristics, types, and important points of applications of cyberspace deterrence.

tool, as it can potentially deter adversaries from launching conventional offensives. Specifically, it points out that China could launch a 'digital Pearl-Harbour-styled' large-scale cyber-attack to disable the adversary's ability to start a war.[32]

Overtime, while more recent Chinese and Western analysts still assess that the offence possesses disproportionate advantage in cyber warfare (albeit several developments such as better forensic technologies favouring the defence),[33] the development of China's ICT industry and the digitalisation of China's armed forces has shifted the cost-benefit analysis. In cyberspace, those developments have prompted Chinese strategic thinking on cyber deterrence to take a more precautionary and defensive turn since the early 2010s. As 2013 SMS puts it, China has become a 'major power'[大国] in cyber affairs,[34] and the strategic objectives in cyberspace of states is defined by the nature of the regime, national strategic goals, more importantly the level of development of informatisation and states' IT industry[35]. Specifically, the growing number of Chinese digital assets which can come under attack or retaliation from other actors in cyberspace made offensive dominance less attractive. Meanwhile, China's prime adversary, the US, still possesses superior cyber capabilities and an effective dominance in internet resources, and a conflict in cyberspace between nation-states would not be in China's interest. 2013 SMS refers to the US hegemony in global cyberspace as "China's disadvantage in cyber confrontation".[36] Moreover, it argues that hegemonic state(s), a term often used to ambiguously refer to the US, pursue absolute security, and often establish controlling the internet as a strategic goal.[37] Consequently, to China, the US's actions in cyberspace are destructive, antagonistic, and exclusive. Besides, cyber incidents such as Stuxnet, the Snowden revelations and, to a lesser extent, Russian cyberattacks against Estonia

[32] AMS Military Strategy Research Department (ed.) (2001). p.237.

[33] Kania, E. B. (2016);

Academy of Military Science Military Strategy Research Department (ed.) (2013).

[34] AMS Military Strategy Research Department (ed.) (2013). p.195.

[35] AMS Military Strategy Research Department (ed.) (2013). p.194.

[36] '但计算机、网络的相关核心技术，以及因特网的控制权等，基本上还掌握在他国手中，中国在网络对抗中整体上处于劣势[While the core technologies of computers, internet, and other related core technologies, as well as the power of controlling internet, is yet essentially in the hands of other states, China is holistically in a disadvantaged position in cyber confrontation]'. in AMS Military Strategy Research Department (ed.) (2001). p.195.

[37] AMS Military Strategy Research Department (ed.) (2001). p.185.

and Georgia also prompted the need for China to develop cyber defence capabilities.[38] Moreover, the US began to express concern over cyber-attacks from China - 'naming and shaming' strategy of publicly accusing Chinese actors has caused negative effects on China's reputation.[39] This too, could be a factor for Chinese analysts in the 2010s to more critically reflect on offensive dominance. For instance, Jiang (2015) characterised the 2013 Mandiant report, which exposed Unit 61398 of the PLA as an incident that 'familiarised the Chinese people with the nature and effects of cyber deterrence' and 'prompted China's research on its own cyber deterrence technologies and theories'.[40]

Still, some Chinese observers, especially those with PLA affiliations, continue to advocate for 'offensive dominance',[41] and there is no consensus among Chinese experts on the 'theory and practice' of cyber deterrence.[42] Judging from the affiliation and positions held by those authors, their influence is likely more than marginal. For example, Li Minghai, the (then) vice-director of the Cybersecurity Research Centre of the People's Liberation Army National Defence University (PLANDU), inspired by the impact of Russian meddling in the 2016 US presidential election, claimed that the incident dealt a major blow to the US hegemony in cyberspace, and argued China should resort to cyber offensives to deter and contain adversaries.[43] Another prominent and more controversial example is Yuan Yi, an AMS-affiliated scholar, who argues that it is impossible to separate deterrence and warfare in cyberspace [慑战结合], and cyber-attacks from adversaries should be dissuaded by pre-emptive combat operations.[44] Yuan's article has been perceived by a number of Western

[38] Jiang, T. (2019)

[39] Jiang, Y. (2015).

Ventre, D. (ed.). (2014). Chinese Cybersecurity and Defence. New Jersey: ISTE Ltd. and John Wiley & Sons Inc., pp. 278–282.

[40] Jiang, Y. (2015). p.55.

[41] E.g. Yuan, Y. (2015).

Li, M. (2017). The inspirations from the "Hackergate" Incident in the US Presidential Election[美总统选举"黑客门"事件的启示]. Wangluo Chuanbo, 2017(1).

[42] Academy of Military Science Military Strategy Research Department (ed.) (2013). p.194.

[43] Li, M. (2017). The inspirations from the "Hackergate" Incident in the US Presidential Election.

[44] Yuan, Y. (2015).

observers as troublingly escalatory.[45] However, a more nuanced perspective might be the key difference between Yuan's approach and the PLA's early offensive dominance is that Yuan suggests a cyber deterrence ladder, where cyber operation is considered to be a last resort if previous attempts to deter an adversary are unsuccessful. Yuan's proposal of cyber deterrence confines the use of cyber operations to fairly limited and specific situations, and resembles the concept of 'active defence' which is gaining momentum more recently in both Chinese and Western strategic thinking. Specifically, the first three steps of the cyber deterrence ladder consist of signalling capabilities and willingness to conduct offensive cyber operations. First, 'deterrence through cyberspace technology experimentation' [网络空间技术试验威慑] entails periodically developing, testing, and displaying network technologies that can be used in cyber warfare. Then, 'deterrence through displaying cyberspace weapons' [网络空间装备展示威慑] entails revealing the development and deployment of cyber weapons of China to perceived adversaries. After that, 'deterrence through cyber wargames' [网络空间作战演习威慑] aims to use simulated environments to display cyber capabilities. Yuan mentions the space and cyber wargames conducted by the US and its allies in this context. The last step in Yuan's cyber deterrence ladder is 'deterrence through actual network operations' [网络空间作战行动威慑], which can be triggered for two reasons: (1) when China's cyber reconnaissance detects an imminent cyber-attack, or (2) when an adversary has launched a tentative cyber-attack in order to deter the incoming cyber-conflict from escalating[46].

Yet, these voices likely represent a minority, or at least do not represent the authoritative or official views in China on cyber deterrence. At this point, the majority of Chinese literature seems to have shifted towards convergence with Western notions of deterrence-by-punishment and deterrence-by-denial, which is also evidenced by official documents such as China's 2015 and 2019 military strategies,[47] and the 2013 SMS. 2013 SMS shows significant

[45] Kania, E. A. (2016).

[46] Yuan, Y. (2015).

[47] 'Accelerate the building of cyberspace forces and improve the ability of cyberspace situational awareness, cyber defense, support for the ability to participate in inter-state struggles in international cooperation in cyberspace 加快网络空间力量建设,提高网络空间态势感知、网络防御、支援国家网络空间斗争和参与国际合作的能力' in State Council of China. (2015). China's Military Strategy;

changes in the understanding of cyber warfare, interpreting the relation between deterrence and warfare in cyberspace more cautiously. It defines cyber deterrence as 'displaying the capability of cyber offence and defence, and the willingness to retaliate, in order to dissuade adversaries from conducting large scale cyber-attacks.' It no longer asserts the inseparability of deterrence and warfare in cyberspace as the 2001 edition did. Conversely, it argues that China should aim to achieve an equilibrium akin to 'mutually assured destruction' in cyberspace where potential cyber conflicts between major powers would never break out.[48] At least theoretically, this brings the Chinese approach of cyber deterrence closer to Western ones.

In operational terms, the 2013 edition of SMS defined the PLA's main objective in cyberspace as "defending the state's vital information, and information and cybersecurity". Although the assessment that cyber warfare favours offence remained unchanged, it argues that China should focus on developing defensive capabilities in cyberspace. As individual actors[个体用户] in cyberspace usually cannot cause serious damage, China should mainly deter cyber threats from adversarial states and 'very few extremist groups'.[49] Around the same time, several other Chinese authors advocated for a more expansive approach to cyber deterrence. Major General Jiang Yamin of the AMS, for instance, argued that cyber deterrence should also 'detect, trace, prevent, and forbid the illegal and immoral cyber behaviour with the help of the capabilities and technologies of military, legal and moral forces'.[50] Jiang is also one of the first Chinese authors that suggested some sort of 'civil-military integration' in China's cyber deterrence, arguing that cyber deterrence forces consist of not only the armed forces, but also law enforcement and 'people's cyber defence forces' [民众网络安全防护力量], referring to

'The PLA accelerates the construction of cyberspace forces, vigorously develops cybersecurity defense means, builds cyberspace defense forces commensurate with China's international status and is compatible with a cyber major power, strengthens national cyber border defense, detects and defends against cyber intrusions in a timely manner, and safeguards information network security , resolutely defend national cybe-sovereignty, information security and social stability.[中国军队加快网络空间力量建设,大力发展网络安全防御手段,建设与中国国际地位相称、与网络强国相适应的网络空间防护力量,筑牢国家网络边防,及时发现和抵御网络入侵,保障信息网络安全,坚决捍卫国家网络主权、信息安全和社会稳定。]' in State Council of China. (2019). China's National Defence in the New Era.

[48] Academy of Military Science Military Strategy Research Department (ed.) (2013). p.194.

[49] Ibid.

[50] Jiang, Y. (2015). p.55.

non-state actors such as Chinese cybersecurity companies.[51] Elaborating on the idea of 'civil-military integration' in China's cyber deterrence, Li (2017) proposed a division of labour in cyber deterrence where 'the military leads the offence, and the nation (referring to civilian entities) conducts the overall planning of defence'.[52]

Echoing official narratives on the 'peaceful use of cyberspace' and 'community of common destiny', some Chinese literature after 2017, mostly written by authors with no military affiliations, ostensibly denounce the idea of 'cyber deterrence' as a whole, and argue that it is necessary for major cyber-powers to enhance communication, build mutual trust, and prevent confrontation and the militarisation of cyberspace.[53] However, their ostensible rejection of cyber deterrence should in principle be understood as criticism towards cyber deterrence practised by the US, instead of the rejection of the concept of cyber deterrence as a whole. To illustrate, many of those analysts, while proposing alternatives to cyber deterrence in their policy recommendations, also advocate for China to develop cyber deterrence capabilities matching those of the US, in order to achieve a 'two-way deterrence'[双向威慑].[54]

Criticism by this group of Chinese literature towards cyber deterrence takes shape in both theoretical and practical terms: Gui (2017) argues that the concept of deterrence has very limited applicability in cyberspace: while theories of deterrence mainly derive from experiences of nuclear deterrence during the Cold-War, the realities of deterrence in cyberspace significantly differs from nuclear deterrence. While deterrence theory presumes that actors are rational and unitary state actors, and interstate interactions are between dyads

[51] Ibid. p.57.

[52] Ibid.

[53] . Beyond 'the theory of cyber deterrence and build a 'community of common destiny'.

Hao, Y. (2017). Facing the threat of cybersecurity, the path of deterrence is not acceptable [面对网络安全威胁，威慑之路不可取]. Information Security and Communications Privacy, 2017(10).

Zhao, Z. , Zhang, J. The Dilemma of U.S. Cyber Deterrence and Its Impact on Global Governance in Cyberspace[美国网络威慑面临困境及对网络空间全球治理的影响]. Information Security and Communications Privacy,2021(3):24-30.

Zhou, H. (2017). Jointly building a cyber community of common destiny. [共同构建网络空间命运共同体]. Information Security and Communications Privacy,2017(7):p.9.

[54] Zhao, Z. , Zhang, J. The Dilemma of U.S. Cyber Deterrence and Its Impact on Global Governance in Cyberspace.

and triads of states,[55] the presence of relevant non-state actors in cyberspace and technical difficulties in timely and accurate attribution entails that states' access to information is often untimely and incomplete, thus undermining rationality.[56] Some Chinese authors also argue that the US's practice of cyber deterrence has been unsuccessful, in that it has not led to a cessation or decrease in cyber-attacks,[57] and counterproductive, in that it has prompted more states[58] to develop offensive cyber capabilities and confrontation between the US and China and between the US and Russia - a phenomenon many Chinese authors refer to as the 'militarisation of cyberspace'[网络空间军事化].[59]

Prescriptively, this group of Chinese literature call for de-escalation in cyberspace and argue that 'major powers' in cyberspace should abandon the paradigm of cyber deterrence and propose various mechanisms as what they see as alternatives to cyber deterrence. Those proposals include institutionalised communication channels between 'major powers' in cyberspace to share information and intelligence about cyber threats and cyber incidents, in order to prevent interstate conflicts in cyberspace.[60] Some Chinese authors with military affiliations have also explored the possibilities for states to engage in negotiations for different forms of cyber weapons arm control. For example, a PLANDU-affiliated analyst, Xu Weidi,

[55] Huth, P., Russett, B. (1984). What Makes Deterrence Work? Cases from 1900 to 1980. World Politics. 36 (4): 496–526.

[56] Gui, C. (2017).

Shen, Y., Jiang, T. (2018). Offense-Defense Balance in Cyberspace and a Proposed Model of Cyber Deterrence[网络空间的攻防平衡与网络威慑的构建]. World Economics and Politics, 2018(2).

[57] Gui, C. (2017). p.40.

[58] Gui (2017) observes that there is a growing trend in the discussion of cyber retaliation and cyber deterrence within Western think tanks. Apart from the US, a number of US allies (UK, France, Germany, Japan, South Korea, the Netherlands are named in the publication) are also developing cyber weapons.

[59] Xu, W. (2020). A fool's errand: seeking military/strategic stability in cyberspace by cyber deterrence [缘木求鱼：以网络威慑求网络军事/战略稳定]. Information Security and Communications Privacy, 2020(9).

Zhao, Z. , Zhang, J. The Dilemma of U.S. Cyber Deterrence and Its Impact on Global Governance in Cyberspace[美国网络威慑面临困境及对网络空间全球治理的影响]. Information Security and Communications Privacy,2021(3):24-30.

[60] Gui, C. (2017).

Lu, C. (2019). 中美关系中的网络安全困境及其影响[China - US Cybersecurity Dilemma and Its Impacts]. Contemporary International Relations, 2019(12).

has called for states to conclude agreements committing not to attack certain targets, such as critical infrastructure, and the supply chain of ICT products.[61] Another two PLANDU analysts, Zhao Ziping and Zhang Jing called for states to negotiate arms control agreements on cyber weapons, particularly those that can be easily duplicated and thus proliferated, such as ransomware.[62] Interestingly, citing the theories of deterrence and balance of power by Brodie and Kissenger, they seem to envision that (stronger) states would only be interested in negotiations of arms control in cyberspace, when an interstate balance of power is reached.[63] In other words, China still needs to develop cyber deterrence capabilities to a level similar to the US in order to entice the US to engage in such dialogues, while it is currently not yet in the interest of the US to do so as it enjoys effective hegemony in cyberspace, at least according to Chinese experts. While cyber norms are beyond the scope of this report, it should not be ignored that, albeit incidentally, some Chinese literature also points to the concept of deterrence-by-norms a set of commonly agreed rules of acceptable state behaviour in cyberspace, reiterating official Chinese positions of cyber sovereignty and the central role of the UN in global governance of cyberspace.

Implications of the Russian invasion of Ukraine on Chinese thinking of warfare in cyberspace

The Russian invasion of Ukraine has become the bloodiest armed conflict in Europe since WWII. While China has so far refrained from substantial military support for Russia,[64] many Chinese officials and experts have engaged in narratives sympathetic to Russia in several aspects, including the root cause of the war and the objection of sanctions imposed on Russia.

[61] Xu, W. (2020). A fool's errand: seeking military/strategic stability in cyberspace by cyber deterrence.

[62] Zhao, Z. , Zhang, J. (2021). The Dilemma of the U.S. Cyber Deterrence and Its Impact on Global Governance in Cyberspace.

[63] 一旦网络空间的双向威慑新范式被广泛认可，各国以更加积极主动的姿态参与网络空间治理，对网络武器的军控将同步得到加强 in

Zhao, Z. , Zhang, J. (2021).

[64] It should be emphasised that this viewpoint is debated among scholars in Europe.

This is a position that is often referred to as 'pro-Russian neutrality'.[65] While discussing the overall Chinese position on Russia's invasion of Ukraine is beyond the scope of this report, the following paragraphs aim to unpack Chinese perspectives on the cyber and information aspect of the war and the possible implications for China's strategic thinking in cyberspace. As Yan Ming, an expert affiliated to China Computer Federation, puts it, a prominent school of thought among Chinese analysts is the following: 'while the US-led West has waged public opinion warfare, cyber warfare, and information warfare on Russia, China needs to think whether it can in the future withstand the crisis that Russia is facing now.'[66] For many Chinese analysts, the Russian invasion of Ukraine is a reminder that cybersecurity is all the more relevant in future armed conflicts. As a prelude to Russia's full-scale invasion of Ukraine, Russia's cyber forces conducted large-scale DDoS attacks on Ukraine's critical infrastructure and governmental websites, which brought down Ukraine's digital government service portal Diya[67] and the websites of several ministries.[68] Ukraine has also launched cyber-attacks on Russian governmental and state-media websites, as well as the Belarussian railway infrastructure in order to disrupt Russian military logistics.[69] In general, there seems to be a consensus among Chinese authors that Ukraine, with the involvement of Western states, enjoys a technological superiority in cyberspace. At a tactical level, Li (2022) argues that the provision of Starlinks system to Ukraine essentially nullified Russia's effort to disrupt the communication of Ukrainian command and control (C2).[70] Yan (2022) also points to the US's intelligence gathering and sharing with Ukraine's armed forces, which led to successes on the battlefield such as the sinking of the flagship of the Russian Black Sea Fleet - Moskva cruise

[65] see e.g. Poita, Y. (8 September, 2022). Russian Invasion Casts Shadow over Ukraine-China Ties. China Observers in Central and Eastern Europe. Retrieved from: https://chinaobservers.eu/russian-invasion-casts-shadow-over-ukraine-china-ties/.

[66] Yan, M. (2022). Reflections on the Cyberspace Confrontation in the Russian-Ukrainian Conflict [对俄乌冲突中网络空间对抗的思考]. China Information Security, 2022(6).

[67] The Ukrainian system of digital portal of governmental services for citizens, a Dutch equivalent would be DigID.

[68] Ukrayinska Pravda. (23 February 2022). Government websites do not open. The Ministry of Statistics reports a massive DDoS attack [Урядові сайти не відкриваються. Мінцифри повідомляють про масову DDoS-атаку]. Retrieved from: https://www.epravda.com.ua/news/2022/02/23/682651/.

[69] Li, H. (2022). Russia-Ukraine Conflict Cyber Confrontation and Its Impact on Cyberspace Security[俄乌冲突网络对抗及其对网络空间安全的影响]. China Information Security, 2022(6).

[70] Ibid.

ship.[71] At a more strategic level, the fact that many of the tech-giants are Western companies has enabled the West to carry out an effective embargo against Russia of products and services that are crucial for the correct functioning of critical infrastructure and the arms industry, such as semiconductors and cybersecurity software.[72] It is noteworthy that several Chinese authors discussed the relevance of Russia's 'sovereign RuNet' project: it is a project aiming to increase the centralisation of the management of the internet traffic between Russian users and contents accessed on Russian territory. A 2018 corresponding Russian legislation requires Russian telecom operators to (1) install equipment on their networks enabling Roskomnadzor[73] to manage internet traffic routes through it.[74] In addition, (2) a 'national domain name system (DNS)' is to be created, which would be independent of the global DNS system managed by ICANN.[75] Jie & Wang (2022) argues that the 'sovereign RuNet' has enhanced the independence of Russia's internet and weakened the cyber deterrence of the US and European countries against Russia. Paradoxically, while many Western experts and some Russian officials[76] argue that the main purpose of the project is to increase the effectiveness of online censorship in Russia (this the first aspect of the project), Chinese experts exclusively focus on the second aspect which supposedly should ensure the functioning of the Russian internet in case it is cut off from foreign servers.[77] This at least suggests that some Chinese experts remain wary of ICANN's role in managing the global DNS system, even after it was

[71] Yan, M. (2022). Reflections on the Cyberspace Confrontation in the Russian-Ukrainian Conflict.

[72] Ibid.

[73] Russian cyber administration.

[74] RBK. (09 April 2022). Experts evaluate the level of 'sovereignty' of Runet[Эксперты оценили уровень «суверенности» Рунета]. Retrieved from: https://www.rbc.ru/technology_and_media/09/04/2019/5cac78529a79474612133263.

[75] Domańska, M. (2019). Gagging Runet, silencing society. 'Sovereign' Internet in the Kremlin's political strategy. Centre for Eastern Studies (OSW). Retrieved from: https://www.osw.waw.pl/en/publikacje/osw-commentary/2019-12-04/gagging-runet-silencing-society-sovereign-internet-kremlins#_ftn26.

[76] E.g. Aleksandr Zharov, former head of Roskomnadzor, said the project would enable Russian authorities to block telegram in Russia, in

Domańska, M. (2019). Gagging Runet, silencing society. 'Sovereign' Internet in the Kremlin's political strategy.

[77] Jie, J., Wang, B. (2022). The significance of Russia's "disconnection" exercise from the perspective of the Russian-Ukrainian conflict[从俄乌冲突看俄罗斯"断网"演习的意义]. China Information Security, 2022(6). This article also offers interesting insights into the degree to which Chinese authors are factually accurate. Multiple Russian sources indicate that the exercises to run RuNet as an autonomous network cut off from the rest of the world resulted in many technical side-effects and defects, yet the Chinese literature presents it as a success.

freed in 2016 from US governmental oversight. For example, Li (2022) seems to suggest that ICANN and the multi-stakeholder model of global governance of internet is susceptible to politicisation in armed conflicts, citing the fact that Ukrainian minister of digital transformation Mykhailo Fedorov has asked ICANN on 28 February 2022 to revoke Russia's top-level domains.[78] It should be pointed out, however, that ICANN rejected this request, as the ICANN President argued that the organisation maintains neutrality and its mission does not extend to taking punitive actions.[79] Besides, a number of western countries have been vocal against this request.

Perhaps, the most important observation about recent Chinese literature on Russia's invasion of Ukraine in cyberspace is that the majority of those Chinese publications have also focused substantively on the tactical use of information, apart from network infrastructure. This corroborates with the argument mentioned in previous chapters of this report, that the Chinese (and Russian, incidentally) conceptualisation of cybersecurity is wider than the mainstream Western one, because it also comprises informational and psychological elements. In the foreword of one of the 2022 issues of an authoritative journal in the field of cybersecurity in China - China Information Security, the editor of the journal Zhong Xin'an has enumerated three aspects of what he sees in the Russian invasion of Ukraine as the 'historical transformation of the form of warfare in the digital age': the omnipresence of public opinion warfare, the ubiquity of cyber warfare, and the limitlessness of information warfare.[80] While

[78] Marby, G. (2 March 2022). Letter to Mykhailo Fedorov - Deputy Prime Minister, Minister of Digital Transformation of Ukraine. ICANN Correspondence. Retrieved from: https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf.

[79] Ibid.

[80] 'Since the outbreak of the Russia-Ukraine conflict, the US has openly called for cyber attacks on other countries. From big data intelligence gathering to remote combat command, from Starlink signal transmission to algorithmic manipulation of public opinion on social media platforms, from critical infrastructure vulnerability scanning to the application of deep-fakes, all of these demonstrate a major historic change in the form of warfare in the digital age - the omnipresence of public opinion warfare, the ubiquity of cyber warfare, and the limitlessness of information warfare. [俄乌冲突爆发以来, 美国公然号召对别国进行网络攻击。从大数据情报收集到远程作战指挥，从星链信号传输到算法操控社交平台舆论，从关键基础设施漏洞扫描到信息深度伪造应用，这些无不彰显数字时代战争形态的重大历史性转变—舆论战无时不在、网络战无处不有、信息战无所不为。]'

In Zhong, X. (2022). Russia-Ukraine conflict sounds alarm to ensure cybersecurity[俄乌冲突敲响保障网络安全警钟]. China Information Security, 2022(6).

it is unclear whether the author truly believes so or they were merely echoing China's official position, some Chinese literature seem to be arguing that the US calling out Russia for preparing for an invasion and Russia's denial before 24 February 2022 should be considered elements of information warfare.[81] During the active phase of the war, information has been used extensively in a tactful manner to affect morale of the warring parties, and legitimacy in the eyes of the global public.[82] Western companies also enjoy a dominant share of the global social media market, which enables the West to significantly undermine Russia's information warfare, by taking down Russian state-affiliated channels.[83] Rather than the appeal of the message, Lang (2022) suggests that the Western dominance in the global social media market is the reason why Russia lost the battle for public opinion in the Western world.[84] New technological developments can also change the dynamic of information warfare. For example, Miao (2022) discusses the application of deep-fake[85] by both belligerents, mainly at the early stages of war, to cause disruptions and affect enemy morale. In the area of information warfare too, Chinese analysts draw a few lessons. Strategically, Russia has made efforts in terms of propaganda to no avail, which some Chinese authors attribute to the fact that Russia's political discourses are not as attractive as Western ones,[86] and others to the market dominance of Western social media platforms.[87] In light of this, China should expedite the development of China's international rhetorical power [话语权] and a set of globally attractive Chinese discourse. Institutionally, China should build an integrated information warfare system and be able to mobilise civilian potentials in war time, as the current 'international propaganda' [外宣] would not suffice under the framework of an 'total information war'. Tactically, China

[81] Fan, Y., Han, Q. (2022). Characteristics and Enlightenment of Network and Information Warfare in the Russia-Ukraine Conflict. [俄乌冲突网络信息战的特征与启示]. China Information Security, 2022(6).

[82] Ibid.

[83] Yan, M. (2022).

[84] Lang, P. (2022). Discussing the Tendency of Cyberspace Weaponization and Its Influence from the Russia-Ukraine Conflict[从俄乌冲突看网络空间武器化倾向及其影响]. China Information Security, 2022(6).

[85] See e.g. Euronews. (16 March, 2022). Deepfake Zelenskyy surrender video is the 'first intentionally used' in Ukraine war. Retrieved from: https://www.euronews.com/my-europe/2022/03/16/deepfake-zelenskyy-surrender-video-is-the-first-intentionally-used-in-ukraine-war.

[86] Lang, P. (2022). Discussing the Tendency of Cyberspace Weaponization and Its Influence from the Russia-Ukraine Conflict.

[87] Ibid.

should, in potential future armed conflicts, prevent the outflow of information from the zones of active armed conflict through unspecified ways of physical control of information,[88] which could include, among others, internet shutdowns or electronic warfare to interfere with cellular signals. This entails using network and electronic means to achieve informational goals at the battlefield.

[88] Fan, Y., Han, Q. (2022). Characteristics and Enlightenment of Network and Information Warfare in the Russia-Ukraine Conflict.

Chinese perspectives on attribution in cyberspace

Technical attribution is when an entity is identified as being responsible or accountable for an act.[89] Typically through technical forensics and intelligence information, the attribution of a cyber-attack aims to arrive at a definitive answer to three questions: (1) whether the incident is malicious, (2) what is the identity of the perpetrators and what are their motives, and (3) what is the gravity of the incident.[90] In this context, this report emphasises the difference between the concept of 'attribution' and 'public attribution': while attribution entails acquiring information about the incident, public attribution is when all or a part of that information is revealed publicly. It should be pointed out that public attribution is not the only possible kind of communication to a cyber-attack when the attribution is considered to be complete; an apparent alternative is private attribution - communicating with the party believed to be or behind the perpetrator through diplomatic messaging or other communication channels. As briefly mentioned in previous chapters of this report, cyber attribution is a crucial component of states' cyber deterrence capabilities, as the covertness of operations in cyberspace would otherwise make timely and accurate response unfeasible, thus undermining the credibility of deterrence.

Public attribution has been a part of the US's 2015 Department of Defence (DoD) cyber strategy and the 2018 National Cyber Strategy.[91] In the 2015 DoD cyber strategy, the official reasoning why the US pursues public attribution is that the reputation costs incurred on the attributed parties can act as a deterrent, and 'public and private attribution can play a significant role in dissuading cyber actors from conducting attacks in the first place'.[92] Beyond calculations for deterrence, there are several other reasons why the US engages in public

[89] Levite, A., Lee, J. (2022). Attribution and Characterization of Cyber Attacks. Carnegie Endowment. Retrieved from: https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698.

[90] Ibid.

[91] Department of Defence. (2015). The Department of Defence Cyber Strategy;

The White House. (2018). National Cyber Strategy.

[92] Department of Defence. (2015). The Department of Defence Cyber Strategy. p.12.

attribution, for example to increase public awareness and to shape international norms.[93] In the last decade, most of the public attributions are made by the US against other nation-state actors, among others China, Russia, Iran, and North Korea. Some other Western states have also engaged in collective attribution - an act of attribution by more than one state. On 10 May 2022, The EU accused the Russian authorities of carrying out a cyberattack against a satellite network an hour before the invasion of Ukraine.[94] While NATO has not made its own cyber attribution, it acknowledged the attribution against China for the Microsoft Exchange Server compromise in 2021,[95] and against Iran for cyber attack on Albania's national information infrastructure in 2022.[96] The difference between collective attribution and acknowledge of other actors' attribution is indeed a fine line, whereas most Chinese experts do not distinguish the two and refer to NATO acknowledgement of cyber attribution as NATO's cyber attribution: from the Chinese perspective, the distinction has little practical relevance, as the reputational costs incurred would be the same.

Until recently,[97] the Chinese official position was that attribution of cyber-attacks is technically almost impossible, and public attribution is counterproductive and is a manifestation of the hypocrisy and double standards of the US-led West, in order to damage China's image with ulterior political motives. Politics aside, it is also only logical that it is more scrutinous and critical towards the issues, especially the burden of proof, given that China is usually on the receiving end of public cyber attribution. During the 2020 World Internet Conference in Wuzhen, Chinese Ministry of Foreign Affairs (MFA) coordinator in cyber affairs has made a thinly-veiled accusation against the US that it has disregarded the

[93] Bateman, J. (2022). The Purposes of the U.S. Government Public Cyber Attribution. Carnegie Endowment. Retrieved from: https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698.

[94] Euractiv. (16 May, 2022). EU blames Russia for satellite hack ahead of Ukraine invasion. Retrieved from: https://www.euractiv.com/section/cybersecurity/news/eu-blames-russia-for-satellite-hack-ahead-of-ukraine-invasion/.

[95] NATO. (19 July, 2022). Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise. Retrieved from: https://www.nato.int/cps/en/natohq/news_185863.htm.

[96] NATO. (8 September, 2022). Statement by the North Atlantic Council concerning the malicious cyber activities against Albania. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_207156.htm.

[97] Until China started to engage in their own public attribution: in September 2022, China's National Computer Virus Emergency Response Centre attributed the cyber-attack on North-western Polytechnical University to the US's NSA, which signifies a major policy change.

complexity and sensitivity of cyber attribution, and has extensively engaged in the 'political attribution' of cyber-attacks, in order to defame other countries and to use cyber attribution as a pretext to sanction and launch cyber-attack against other countries, which has undermined the effort to build a set of international rules and norms in the global governance of cyberspace.[98] In addition, China has also cited the technical difficulties of attribution as a reason why China is against the application of international law of war (in particular jus ad bellum) in cyberspace.[99] The head of the Chinese delegation to the UN, Wang Lei, has argued that the application would, due to the technical difficulties in attribution and the existence of non-state actors, provide 'certain major cyber power' with excuses to abuse the right to self-defence in order to contain other states.[100] In practice, the position that attribution is technically difficult and the burden of proof can usually not be satisfied, has also been consistently cited by the Chinese MFA in response to China's alleged involvement in cyberattacks. For example, in March 2021, MFA spokesperson Hua Chunying argued that there is no evidence to support Facebook's claim that a hacker-group located on Chinese territory has launched a cyber-attack on overseas rights groups, as 'the issue of cyber-attack attribution is very complicated'.[101] In June 2021, MFA spokesperson Wang Wenbin made a

[98] Chinese MFA. (24 November, 2020). Global Data Security Initiative injects new impetus into global governance [《全球数据安全倡议》为全球治理注入新动力]. Retrieved from: https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/fywj_674643/202011/t20201124_7668989.shtml.

[99] Chinese MFA. (18 October, 2019). Speech by Wang Lei, head of the Chinese delegation, on the use of international law at the first meeting of the United Nations Open-ended Working Group on security of and in the use of information and communications technologies[中国代表团团长王磊参赞在联合国信息安全开放式工作组首次会上关于国际法使用问题的发言]. Retrieved from: https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/fywj_674643/201910/t20191018_7668929.shtml.

[100] Ibid.

[101] 'Then Where is Facebook's evidence? As we have said many times, the issue of cyber attack source tracing is very complicated, and sufficient evidence should be used for attribution'[那脸书的证据在哪里？我们多次说过，网络攻击溯源问题非常复杂，定性时需基于充分证据。] in

Hua, C. (25 March, 2021). On March 25, 2021, Foreign Ministry Spokesperson Hua Chunying hosted a regular press conference. [2021 年 3 月 25 日外交部发言人华春莹主持例行记者会]. Retrieved from: https://www.mfa.gov.cn/fyrbt_673021/jzhsl_673025/202103/t20210325_9171234.shtml.

similar comment in regard to alleged cyber infiltration by PRC-linked hacker groups in New York City Transit Authority.[102]

However, various Chinese cybersecurity companies and governmental agencies have made their own public cyber attribution since 2022 about US cyberespionage. In February, PanGu published a report which alleged that the US National Security Agency (NSA) used a backdoor, dubbed Bvp47, to monitor 287 targets in 45 countries.[103] In March, another Chinese cybersecurity company Qihoo 360 claimed in a report that a hacking group known as APT-C-40 is affiliated with the US government and has been secretly attacking China's leading companies, governments, research institutes, and infrastructures over the past decade. Another March report said that the personal information of millions of Chinese internet users had already been stolen by the same US hacking group.[104] It should be emphasised that those attribution reports issued by Chinese cybersecurity companies are echoed and amplified through official channels: MFA spokesperson Hua Chunying has expressed 'grave concern on the malicious cyber activities exposed by PanGu's report' and demanded clarification from the US during the regular press conference on 24 February.[105] The MFA also made two similar statements regarding 360's reports in March. In the context of Russia's invasion of Ukraine, it should not be ignored that the Chinese MFA has also accused 'actors originated from the US' of conducting cyber-attacks against Russia, Ukraine and Belarus (87% of the targets are allegedly in Russia) by hijacking computer networks in China.[106] Prior to the attribution

[102] Wang, W. (3 June, 2021). On June 3, 2021, Foreign Ministry Spokesperson Wang Wenbin hosted a regular press conference [2021 年 6 月 3 日外交部发言人汪文斌主持例行记者会]. Retrieved from: https://www.mfa.gov.cn/fyrbt_673021/jzhsl_673025/202106/t20210603_9171279.shtml.

[103] PanGu Lab. (23 February, 2022). Bvp47-The top backdoor of the American NSA's Equation Group [Bvp47-美国 NSA 方程式组织的顶级后门]. Retrieved from: https://www.pangulab.cn/post/the_bvp47_a_top-tier_backdoor_of_us_nsa_equation_group/.

[104] Li, J. (23 March, 2022). China cybersecurity firm alleges US National Security Agency is behind hacking group that has stolen a mass of critical data. SCMP. Retrieved from: https://www.scmp.com/tech/tech-war/article/3171587/china-cybersecurity-firm-alleges-us-national-security-agency-behind.

[105] Hua, C. (25 February, 2022). Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on February 24, 2022 [2022 年 2 月 24 日外交部发言人华春莹主持例行记者会]. Retrieved from: https://www.fmprc.gov.cn/web/wjdt_674879/fyrbt_674889/202202/t20220224_10645295.shtml.

[106] Zhao, L. (14 March, 2022). On March 14, 2022, Foreign Ministry Spokesperson Zhao Lijian hosted a regular press conference [2022 年 3 月 14 日外交部发言人赵立坚主持例行记者会]. Retrieved from: https://www.fmprc.gov.cn/web/wjdt_674879/fyrbt_674889/202203/t20220314_10651532.shtml.

reports on the North-Western Polytechnical University cyber incident published in September, China's National Computer Virus Emergency Response Centre (CVERC) has also called out US cyberespionage: Three reports on cyberweapons used by the US cyber forces, FoxAcid, NOPEN, and Hive, were issued in early 2022.[107]

However, a key difference between those public attribution acts and typical cyber attribution acts by the US is that they were about identifying cyber weapons or a hacking group, instead of about specific cyber incidents. However, the CVERC attributed the cyber incident of North-Western Polytechnical University in June to the NSA,[108] signifying the most significant change in the Chinese practice of cyber attribution so far. It is noteworthy that the CVERC claimed that the NSA has used NOPEN and FoxAcid cyberweapons, which the CVERC had claimed the NSA possessed prior to the North-western Polytechnical University formally reporting the incident in June. This indicates that the CVERC attribution to NSA could be more of a coordinated signalling of China's cyber attribution capabilities, potentially aiming to coerce other parties to dialogues and negotiations, than a real policy shift towards public cyber attribution. As mentioned in previous chapters of this report, two PLA affiliated authors have argued that states would only be interested in negotiations of arms control in cyberspace, when a sort of balance of power is reached.[109]

---

[107] CVERC. (14 March, 2022). "NOPEN" Remote Trojan Analysis Report ["NOPEN"远控木马分析报告]. Retrieved from: https://www.cverc.org.cn/head/zhaiyao/news20220314-nopen.htm.;

CVERC. (19 April, 2022). Analysis Report on the CIA's "Hive" Malicious Malwarel Weapon Platform—An Early Warning on the CIA's Main Battle Network Weapons [美国中央情报局（CIA）"蜂巢"恶意代码攻击控制武器平台分析报告—关于美国中情局主战网络武器的预警]. Retrieved from: https://www.cverc.org.cn/head/zhaiyao/news20220419-hive.htm.;

CVERC. (29 June, 2022). Technical Analysis Report on the U.S. National Security Agency (NSA) 'FoxAcid' Loophole Attack Weapon Platform [美国国家安全局（NSA）"酸狐狸"漏洞攻击武器平台技术分析报告]. Retrieved from: https://www.cverc.org.cn/head/zhaiyao/news20220629-FoxAcid.htm.

[108] CVERC. (5 September, 2022). Investigation Report on Northwestern Polytechnical University Cyber Attack by NSA (Part 1) [西北工业大学遭美国 NSA 网络攻击事件调查报告（之一）]. Retrieved from: https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm.;

CVERC. (27 September, 2022). Investigation Report on Northwestern Polytechnical University Cyber Attack by NSA (Part 2) [西北工业大学遭美国 NSA 网络攻击事件调查报告（之二）]. Retrieved from: https://www.cverc.org.cn/head/zhaiyao/news20220927-NPU2.htm.

[109] 一旦网络空间的双向威慑新范式被广泛认可，各国以更加积极主动的姿态参与网络空间治理，对网

Compared with the abundant Chinese literature on deterrence, literature on cyber attribution itself is rare and has only appeared in the last two years. As mentioned in previous chapters of this report, some literature advocating for the 'peaceful use of cyberspace' refer to the difficulties in cyber attribution as a part of their argument why classical deterrence theory cannot be applied to cyberspace. Apart from elaborating on the aforementioned Chinese official position on public cyber attribution, they have also proposed alternatives to unilateral public attribution. Given the institutional affiliations of those authors and the fact that there is a high degree of convergence in their arguments, it is plausible that their viewpoint reflects the preferences of the Chinese government. They seem to advocate for an independent 'international attribution mechanism'[国际溯源机制], which can include the following elements: (1) a multilateral cyber attribution organisation under the framework of the UN,[110] (2) a set of standards for evidence,[111] (3) a norm[规范] that the attributor should hold compulsory and confidential consultation with the accused party before making public attribution,[112] (4) the international mechanism should focus on fighting cybercrime from non-state actors, and (5) the international mechanism should be based on the goal of limiting the use of force in cyberspace, especially on states' critical information infrastructure.[113] It should be immediately pointed out that the fact that China now conducts its own public cyber attribution does not mean that the aforementioned positions of Chinese authors are irrelevant

---

络武器的军控将同步得到加强 in

Zhao, Z. , Zhang, J. (2021).

[110] Lu, C. (2022). Reflection on the Differences of understanding in Public Attribution the Field of International Security[对国际安全领域公开溯源问题认知差异的思考]. China Information Security, 2022(5).;

Xu, M. (2022). Rethinking Cyber Public Attribution from the Perspectives of Technology, Politics and International Governance [以技术、政治和国际治理视角反思网络公开溯源]. China Information Security, 2022(5).;

Tang, L. (2022). Analysis on the Necessity and Feasibility of International Cyber Attribution Mechanism [国际网络攻击溯源机制的必要性和可行性探析]. China Information Security, 2022(5).

[111] Lu, C. (2022). Reflection on the Differences of understanding in Public Attribution the Field of International Security.

[112] Yang, F. (2022). Research on Unsubstantiated Allegations of Cyber Attribution from the Perspective of International Law [国际法视角下的网络公开溯源欠实指控研究]. China Information Security, 2022(5).

[113] Xu, M. (2022). Rethinking Cyber Public Attribution from the Perspectives of Technology, Politics and International Governance.

or invalid: those points could be the baseline of China's starting position in potential future bilateral and multilateral dialogues in managing cyber conflicts and the governance of cyberspace. It is also interesting to note that the vice-secretary general of Peking University's Institute of International and Strategic Studies, Sun Yilin published a commentary on Global Times in October after the CVERC's public attribution report, calling for the US government to cooperate with other countries and to engage in 'effective' cyber attribution, in order to counter cyber-attacks and cyber-crimes.[114] As this study relies solely on open sources, it is unclear whether there has been undisclosed diplomatic messaging between China and the US regarding the issue.

Prior to 2022, although the official position is that the public cyber attribution conducted by the US government and American companies is nothing but hypocritical, some non-state-affiliated Chinese literature suggest that there has been a more nuanced discussion on cyber attribution among Chinese experts and policy makers in the area of cybersecurity, which could have prompted China to start developing its own cyber attribution capabilities no later than 2018. Chen (2022), while echoing the official Chinese position that the US's practice of public cyber attribution is political in nature, argues that those practices have been mostly credible and that the US enjoys technological supremacy in the area of cyber attribution.[115] This report draws attention to a few articles published on Anquan Neican [安全内参], a source affiliated to a private Chinese cybersecurity company - Qi'anxin,[116] which are among the earliest Chinese literature arguing the necessity for China to develop cyber attribution capabilities. An 2018 article on Anquan Neican seems to hold the view that the Mandiant

[114] The U.S. government should abandon political manipulation of cyber attribution, and sincerely cooperate with countries around the world to effectively engage in cyber attribution and combat cyber attacks and cyber crimes [美国政府应放弃政治操弄网络攻击溯源行动，真诚与世界各国合作，有效开展网络攻击溯源，打击网络攻击和网络犯罪] in

Sun, Y. (6 October, 2022). Carry out effective cyber attribution to maintain global cyberspace security [开展有效网络攻击溯源 维护全球网络空间安全]. Huanqiu. Retrieved from: https://opinion.huanqiu.com/article/49rslnWVhjw.

[115] Chen, B. (18 January, 2022). In-Depth Analysis: Technical Advantages and Strategic Trends of US Government Cyber Attribution [深度分析：美国政府网络归因的技术优势与战略动向]. Retrieved from: https://www.secrss.com/articles/38433.

[116] Tianyancha. (n.d.). Basic Information of the Enterprise - Anquan Neican [企业基本信息 - 安全内参]. Retrieved from: https://www.tianyancha.com/product/c5df83a95b0240fd88d4a4f5d3decb50.

report[117] established 'solid and reliable chains of evidence' and is a textbook case of cyber attribution, and it reflects that the US (both US governmental agencies and cybersecurity companies such as Mandiant and FireEye) has achieved technological, market, and political success in the area of cyber attribution.[118] Besides, the author argues that, contrary to the common misconception among Chinese experts and policy makers, cyber attribution is technically feasible, as the attacker may (1) expose their intent, (2) reveal their modus operandi, and (3) commit human errors.[119] Anquan Neican also lamented China's 'disadvantaged position in cyber attribution, which the author argued to be caused by the misconception of relevant Chinese authorities on the issue of cyber attribution and therefore the lack of investments in this area.[120] Citing Xi Jinping's speech during the 2016 cybersecurity and informatisation work seminar [网络安全和信息化工作座谈会], Anquan Neican indicates that China's strategy in cyber warfare (at the time) was to develop asymmetrical offensive capabilities with 'silver bullet'[杀手锏] characteristics, which dismissed the necessity to develop cyber attribution technologies - an integral part of cyber defence capabilities.[121] This school of thought was likely to be dominant in China at the time, as it is corroborated by many Chinese literature reviewed in previous chapters of this report,[122] with similar or corresponding ideas such as offensive cyber weapons as 'poor countries' nuclear bomb' or mutually assured destruction in cyberspace. From a strategic point of view, Anquan Neican emphasised that not only offensive capabilities can disrupt balance of power, defensive capabilities can also do so. An analogy in nuclear deterrence would be the anti-missile system enabling its possessors to acquire unilateral deterrence against its adversaries. Similarly, cyber attribution can at least in theory be regarded as a disruptive technology as it enables states

[117] Mandiant. (2013). APT1: Exposing One of China's Cyber Espionage Units. Retrieved from: https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units.

[118] Anquan Neican. (25 September, 2018). Discussion on Misunderstandings of Cyber Attribution (1)[网络归因溯源之误区刍议（一）]. Retrieved from: https://www.secrss.com/articles/5319.

[119] Anquan Neican. (26 September, 2018). Discussion on Misunderstandings of Cyber Attribution (2)[网络归因溯源之误区刍议（二）]. Retrieved from: https://www.secrss.com/articles/5351.

[120] Anquan Neican. (25 September, 2018). Discussion on Misunderstandings of Cyber Attribution (1).

[121] Anquan Neican. (28 September, 2018). Discussion on Misunderstandings of Cyber Attribution (3)[网络归因溯源之误区刍议（三）]. Retrieved from: https://www.secrss.com/articles/5408.

[122] such as Yuan (2015) and Cheng & He (2015).

with such capabilities to carry out cyber-attacks on their adversaries without being traced or at least credibly identified, whereas their adversaries would risk retaliation.[123]

Based on open-source information alone, it is impossible to evaluate the true influence of the aforementioned literature on Chinese strategic thinking on and investments in cyber attribution. However, it is very likely that China has indeed invested in cyber attribution capabilities in recent years and has reached significant progress: an indication could be the uptick in 2020 of journal articles on China National Knowledge Infrastructure (CNKI)[124] under the academic discipline 'computer technology' on cyber attribution: In 2016-2019, there are around fifty published articles every year that contain the keyword 'cyber-attack attribution'[网络攻击溯源], whereas 142 articles that contain the same keyword were published in 2020, 117 in 2021, and another 109 so far in 2022. This report also highlights that the CVERC's attribution reports reflect a certain degree of mirroring of the US's practice of cyber attribution. Similar to the Mandiant report which China has always dismissed as baseless, the CVERC cited modus operandi such hacking activities being in line with the American working schedule and public holidays, and 'American-English' linguistic features to substantiate their claim that the attack originates from the NSA.[125] Besides, although China has previously dismissed public cyber attribution by US cybersecurity companies as unreliable, the CVERC attribution is conducted in cooperation with Qihoo 360 - a Chinese cybersecurity company.

[123] Ibid.

[124] Database of the monopoly Chinese academic journal publishing company.

[125] CVERC. (27 September, 2022). Investigation Report on Northwestern Polytechnical University Cyber Attack by NSA (Part 2).

Chinese perceptions of US and NATO as actors in cyberspace strategy

One of the most seemingly perplexing aspects of the Chinese position in cyber deterrence is that it denounces cyber deterrence as destabilising and escalatory in rhetoric, while nevertheless pursuing its own cyber deterrence strategies. China's 2016 National Cyberspace Security Strategy is a case in point: referring to the US, it claims that 'certain countries' have strengthened cyber deterrence strategy and intensified the arms race in cyberspace, posing new threats to global peace.[126] However, in the section on Strategic Tasks, it stated clearly that China would simultaneously develop 'protection and deterrence', and 'focus on identification, prevention, monitoring, early warning, response handling and other such segments'.[127] More recently, the 2020 edition of SMS explicitly argues that the military strategy of the US in cyberspace is offensive.[128] While the US officially defines its cyber deterrence strategy as a defensive one, aiming to dissuade potential adversaries from attacking US assets in cyberspace, distrust towards declared US policy is prevalent among Chinese analysts. They overwhelmingly argue that the US's cyber deterrence strategy is offensive in nature and is aimed at maintaining the US's global hegemony. Although many Chinese authors recognise that the formulation of cyber strategies of the US and NATO are at least to a certain degree prompted by technical challenges in the cyberspace or cyber-attacks endured by US allies such as the Russian cyber-attack against Estonia in 2008,[129] this does not influence their conclusion of the offensive nature of the US's strategies in cyberspace.

---

[126] Cyber Administration of China. (17 December, 2016). National Cyberspace Security Strategy[国家网络空间安全战略]. Retrieved from: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

[127] Ibid.

[128] Academy of Military Science Military Strategy Research Department (ed.) (2020). Science of Military Strategy. P.154.

[129] e.g. Mao, Y. (2014). NATO's cybersecurity strategy and its implications [北约网络安全战略及其启示]. Journal of International Security Studies, 2014(4).

Gui, C. (2017). Beyond 'the theory of cyber deterrence and build a 'community of common destiny'[超越"网络威慑论"，构建"命运共同体"]. China Information Security, 2017(11).

Du, Y. (2021) The militarisation of cyberspace and its countermeasures [网络空间军事化发展态势及其应对]. Pacific Journal, 2021(12).

This view possibly emerges from a strongly realist ontology on international affairs, encapsulated by Mearsheimer's (2001) statement that great powers fear each other and treat each other with suspicion, and there is thus little room for trust. The origin of such fear is that any state bent on survival must be at least suspicious of other states and reluctant to trust them in a world where great powers have the capability to attack each other and might have the motive to do so.[130] Put simplistically, strategic deterrence is a security dilemma faced by states that identify themselves as superpowers in a perceived anarchic international system. When it comes to the perception of 'others', how the adversary declares their deterrence policy is at best only of secondary relevance. After all, it is 'what they can do' – the adversary's capability that causes concern.

One Chinese scholar's view is representative: the relations between major powers in cyberspace is the reflection of their relations in physical space, while the special characteristics of cyberspace have diminished geographical distance, increasing inter-state frictions.[131] The militarisation of cyberspace and the cyber arms race reflect security dilemmas and the structure of the international system in cyberspace.[132] The mutual perception of US and China in cyber deterrence can be considered a typical case of adversarial great power interaction in a perceived anarchic international system, with low levels of mutual trust and a struggle for states' own security at the expense of others, where the understanding of other states' deterrence posture is filtered through geopolitical perceptions. While both China and the US declare, and seem to genuinely believe that their own deterrence posture is defensive in nature, they do not trust each other's declared defensive postures at the face value and are increasingly wary of the developments of each other's capabilities.

The rest of this chapter aims to unpack those perceptions, and discuss how they influenced China's own cyber deterrence strategies in recent years. There are several contributing factors to China's reading of US offensive intent. First, Chinese authors adopt a more holistic approach in interpreting US's cyber strategies: while declared policies, such as the DoD's 2015 Cyber Strategy and Trump Administration's National Cyber Strategy, are certainly important,

[130] Mearsheimer, J. J. (2001). The Tragedy of Great Power Politics. New York: W. W. Norton & Company. p.32.

[131] Lu, C. (2019). Security Dilemma,Misperceptions and a Roadmap for Big Power Relations in Cyberspace - Taking China-EU Cyber Cooperation as an Example [网络空间大国关系面临的安全困境、错误知觉和路径选择 - 以中欧网络合作为例]. European Studies, 2019(2).

[132] Du, Y. (2021). The militarisation of cyberspace and its countermeasures

they are only understood in the context of the US's state behaviour and demonstrated capabilities in cyberspace. This approach often leads to discrepancies between Chinese and Western experts' assessment on what constitutes deterrence. The Stuxnet incident might not be considered as an example of cyber deterrence under the mainstream Western terminology, as it was not intended to dissuade a cyber-attack. However, Cheng & He (2015) argue that the attack demonstrated the power of US cyber weapons in the field, which increased the credibility of its cyber deterrence.[133] Similarly, Zhao & Zhang (2020) argue that 'persistent engagement' is one of the features of the US's cyber deterrence strategy: the authors interpret offensive cyber operations undertaken by the US cyber force, such as the cyber-attack on Russia's Internet Research Agency during the 2018 midterm election, as a part of its deterrence posture.[134] This also reflects a change in US doctrine, as the line between cyber deterrence and cyber-attacks has become more blurred since the Trump administration, with the introduction of new tactical practices such as 'deterrence by punishment' and 'active defence'.

Second, the US's demonstrated capabilities in cyberspace and declared cyber deterrence posture often influence the evolution of China's strategies in cyberspace. Developing strategic deterrence capabilities that match those of adversaries is rooted in China's 'anti-coercion' strategic thinking. It needs to be emphasised that it is the US's effective cyber, electronic, and information warfare in the First Gulf War that inspired the very foundation of the PLA's own cyber force. China sees the development of the US's cyber-warfare capabilities as potential threats to their own security, and therefore seeks to possess capabilities on par with the US, which several Chinese authors refer to as 'building mutually assured destruction in cyberspace'.[135] This 'inspiration effect' applies to not only capabilities in cyberspace, but also to deterrence postures. Major changes in the US's cyber deterrence posture have led to Chinese experts arguing for aligning China's posture with that of the US, if China's capabilities allow it. Notably, the US declared that it would 'respond to hostile acts in cyberspace, when warranted, through all necessary means' in the 2011 International Strategy

[133] Cheng, Q., He, Q. (2015). Building China's cyber deterrence strategy[构建中国网络威慑战略]. Cyberspace Strategy Forum, 2015(11).

[134] Zhao, Z. , Zhang, J. The Dilemma of U.S. Cyber Deterrence and Its Impact on Global Governance in Cyberspace[美国网络威慑面临困境及对网络空间全球治理的影响]. Information Security and Communications Privacy,2021(3):24-30.

[135] Cheng, Q., He, Q. (2015). Building China's cyber deterrence strategy.

for Cyberspace,[136] which implies a kinetic response when a strategically ambiguous threshold is crossed. Several Chinese authors interpret the aforementioned policy as the US's readiness to retaliate cyber-attacks with nuclear weapons, and prescribe that China's cyber deterrence should be coupled with nuclear deterrence 'based on the calculations of potential worst-case-scenario'.[137] More recently, many Chinese experts observe that the US's cyber deterrence posture has increasingly emphasised 'active defence'[主动防御] since the Trump administration,[138] and they believe that the Biden Administration has inherited the policies of its predecessors and continues to actively deploy offensive and defensive capabilities in cyberspace.[139] While the debate among Chinese analysts on China's cyber deterrence posture is still ongoing, it should be pointed out that the more authoritative and military-affiliated 2020 edition of AMS suggests that the PLA should adopt an active defence posture in the section 'strategic guidance for military conflicts in cyberspace', referring explicitly to its assessment that the US has established an offensive military strategy in cyberspace that must be countered.[140]

In contrast to the attention devoted to the United States, Chinese attention for the role of NATO is relatively scarce. Most Chinese experts hold realist and state-centric worldviews, which ascribe little agency to non-major powers and international organisations.

---

[136] White House. (2011). International Strategy for Cyberspace. Retrieved from: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[137] Cheng, Q., He, Q. (2015).

Tan, H. (2019). Deterrence in cyberspace, and cyberspace in deterrence[网络中的威慑，威慑中的网络]. Anquan Neican. Retrieved from: https://www.secrss.com/articles/11066.

[138] See E.g. Du, Y. (2021).

Guancha. (3 October, 2018). The US will provide its NATO allies with 'cyber war' capabilities, US media outlets compare it to 'nuclear deterrence'[美国将为北约盟友提供"网络战"能力 美媒称堪比"核威慑"]. Retrieved from: https://www.guancha.cn/internation/2018_10_03_474256.shtml?s=zwyxgtjbt.

(Yan & Zhou, 2020) 美国网络威慑能力建设情况分析及借鉴

Wangdiankongjianzhan. (2018). New movements in the US and Europe's development in cyberspace confrontation[2018 年美欧网络空间对抗领域发展新动向]. Retrieved from:https://www.secrss.com/articles/12680

[139] Du, Y. (2021).

[140] National Defence University (ed.). (2020). Science of Military Strategy.

Consequently, they link the origin of NATO's cyber strategies to US policies on international cooperation with partners in the field of cyber defence,[141] and assess that the formation of a NATO cyber-strategy and setting conditions for cyber-attacks triggering Article 4 and Article 5 collective defence are ultimately US attempts to preserve its global hegemony.[142] Illustratively, Mao (2014) argues that collective NATO cyber strategy is an US effort to maintain its leading role in security issues in Europe. NATO is an alliance where members' infrastructure and intelligence are interconnected. However, there are significant discrepancies in NATO members' cyber-capabilities, and several NATO members did not possess any significant cyber forces, which attackers can exploit to jeopardise the alliance's intelligence systems or damage other member's infrastructure.

More recently, the discussion in China of NATO in global cyberspace is often positioned in a broader context of great power confrontation. Some Chinese authors argue that the collective public attribution by US and its allies of China and Russia has impeded trust among major powers and led to the increasing 'bloc-isation'[阵营化] in cyberspace.[143] An article on Guancha, a nationalist media outlet, in 2018, citing the Chinese MFA, has criticised the US providing cyber capabilities to NATO allies as 'a demonstration of the US's cold-war zero-sum mentality', and called for the US to engage in dialogues with countries such as China and Russia to resolve issues in cyber security.[144] Similarly, Du Yanyun, an author affiliated to the PLANDU, has criticised the NATO public attribution (the author used 'defamation' and slandering) towards China and Russia. She argues that the US policy of exclusion and containment of China has extended from the physical space to cyberspace, and that the Biden Administration has inherited the 'containment' policy against China and Russia from the Trump-era. She also suggests that NATO incorporating Ukraine in its Cyberspace Operation

[141] Yan, X., Zhou, Q. (2020). The analysis and implications of the US's development of cyber deterrence capabilities[美国网络威慑能力建设情况分析及借鉴]. Cyberspace Security, 2020(5).

Mao, Y. (2014). NATO's cybersecurity strategy and its implications.

[142] Du, Y. (2021).

[143] Lu, C. (2019).

[144] Guancha. (3 October, 2018). The US will provide its NATO allies with 'cyber war' capabilities, US media outlets compare it to 'nuclear deterrence'.

Centre constitutes a threat towards Russia.[145] Until recently, Chinese literature usually refrained from taking a position on security issues in Europe.[146]

[145] Du, Y. (2021).

[146] Ibid.

Chinese perceptions of the EU and its member states as actors in cyberspace

Most EU member states are members of NATO (all excluding Ireland, Austria, Malta and Cyprus after Sweden and Finland's accession), and very little Chinese literature discusses European states as actors in the context of cyber security. The EU is mostly considered in regulatory, not military or security, terms. The review for this report has found no article on? European states by Chinese military-affiliated authors, indicating a clear lack of interest in those circles. However, the AMS's 2020 edition of Science of Military Strategy has briefly indicated that the military strategy of 'Europe' (without defining which individual European states it refers to or the EU) in cyberspace is defensive in nature,[147] which can be considered as the recent authoritative view of China's military experts. For instance, Zhou (2015) claims the EU's development of its cybersecurity strategy is motivated by (1) tackling cyberattacks and cybercrimes technically, and (2) gaining more independent control over the governance of internet[148] both politically and legally. Despite their alliance, there are significant strategic and policy differences between the US and Europe. At the strategic level, while the US pursues cyber hegemony, the EU aims to govern global cyberspace in the spirit of the rule of law and other values that should be universal in the EU's perspective, to protect the rights and interests of its citizens and to promote its ideal of good governance in cyberspace. A few Chinese sources also believe that the Snowden revelations undermined Europe's trust towards the US, and stimulated the EU to pursue a more autonomous cybersecurity strategy.[149] More specific to deterrence, several authors argue that cyber deterrence by European countries mainly entails deterrence-by-denial, with the emphasis on building cyber-defence capabilities and network resilience.[150] Chinese authors have not overlooked that a number of EU (former)

[147] AMS, Science of Military Strategies. (2020).

[148] 争取更具独立性的制网权

In Zhou, Q. (2015). Analysis of the EU cybersecurity strategy[欧盟网络安全战略解析]. European Studies, 2015(3). p.76.

[149] Ibid.

[150] Ran, C., Wang, B. (2019). Study of international strategic models of the security of cyber sovereignty[网络主权安全的国际战略模式研究]. Journal of International Resource Management, 2019(2).

member-states, including Germany, France, the Netherlands,[151] and the UK, have military cyber forces which cooperate and integrate with the US under NATO frameworks,[152] and some authors observe that France and the UK possess credible cyber-offensive capabilities.[153] However, the key difference between European and US cyber forces perceived by Chinese authors is that the cyber-forces of European states are established in order to deter cyber-criminals instead of nation states.[154]

Some more recent Chinese authors point out that China and Europe have similar positions on a number of regulatory and security issues in cyberspace, but lament that geopolitical factors have led to a lack of cooperation. Lu (2019), for instance, argues that it is in the interest of both China and the EU to oppose the militarisation of cyberspace. He also argues that cyber-attacks are more often carried out by non-state-affiliated cyber-criminals and extremist groups, and China's cyber military exercises are more aimed at improving cyber defence capabilities and resilience of infrastructure, which 'does not target other states', similar to Europe.[155] However, as cybersecurity has become an issue in the realm of 'high politics', geopolitics instead of affinity in policy preferences seem to increasingly determine the dynamics of interstate relations in cyberspace. As Lu points out, while China is alarmed by Europe's close relation with the US, Europe in turn is also alarmed by China's growing affinity with Russia.[156] This

---

[151] Ye, L., Li, C. (2016). A Perspective on the Construction Measures of Cyberspace Security in the Netherlands[荷兰网络空间安全建设举措透视] .China Information Security, 2016(5).

[152] Qianqingbaoju. (2020). NATO conducts annual 'Cyber Alliance' exercise virtually for the first time[北约首次通过虚拟方式开展年度"网络联盟"演习]. Retrieved from: https://www.secrss.com/articles/27321.

Ran, C., Wang, B. (2019). Study of international strategic models of the security of cyber sovereignty

[153] Ran, C., Wang, B. (2019).

[154] Zhou, Q. (2015). Analysis of the EU cybersecurity strategy.

Wu, S.; Zhang, L. (2021). Analysis of the new 2020 EU cybersecurity strategy[欧盟 2020 年网络安全新战略解析]. China Trial, 2021(5).

Ran, C., Wang, B. (2019).

[155] Lu, C. (2019).

[156] 'Since China and Russia are friends in cyberspace, they are naturally enemies of the EU; conversely, the alliance between the EU and the US has also led China to be wary of the EU in cyber governance.[由于中国与俄罗斯是网络空间的朋友，自然就是欧盟的敌人；反之，欧盟与美国的盟友关系也导致中国在网络治理中对欧盟存有戒心。]' in

risks overlooking the significant differences between states' positions within each bloc. Ban & Lu (2017), for instance, voice concern that Russia aims to 'overthrow or replace' the current system, which would not be in China's interests.[157] Even so, differences also remain within Chinese literature, particularly in the area of self-perception. For example, while Lu argues that China and Europe's approach to cyber deterrence are similar in the sense that both principally aim to counter crimes in cyberspace, other Chinese writers mentioned earlier indicate that deterring adversarial major powers in cyberspace is the main objective of China's cyber-forces.

Lu, C. (2019).

[157] Ban, J. ; Lu, C. (2017). The Adjustment of Russia's Cyberspace Strategy from the 'Theory of Federal Government Information Security'[从'联邦政府信息安全学说'看俄罗斯网络空间战略的调整],Information Security and Communications Privacy, 2017(2).

Conclusion and discussion

This report has reviewed the evolution of Chinese perspectives on cyber deterrence and attribution, and some key findings are as follows: first and foremost, it needs to be emphasised that China adopts a broader definition of cybersecurity than the mostly technical one known in the West, i.e., the correct functioning of the internet and the infrastructure. Especially for the Chinese military, cyber, informational, electronic, and psychological warfare are fully incorporated under the concept of 'information warfare'. Amid the Russian invasion of Ukraine, Chinese authors paid close attention to the tactical use of all components of information in the war, and they attribute Russia's apparent failure in cyber and information warfare to the West's digital supremacy, in terms of technology, market share, and supply chains. To the authors of this report, it is unexpected yet unsurprising that Chinese experts drew high attention to the role played by Western tech-companies in Russia's botched invasion. As for deterrence in cyberspace, China's strategic thinking originated from the perceived need of countering the implications of US hegemony in cyberspace on China's national security. Its early strategy focused on developing asymmetrical offensive capabilities, which Chinese authors metaphorically described as 'silver bullet'[杀手锏] or 'poor country's nuclear bomb'[穷国的原子弹], in order to create a state of 'mutually assured destruction' in cyberspace and to deter cyber-attacks from the US. However, as China's growing digitalisation (in both military and civilian sectors) unavoidably generates the necessity to also defend its own assets in cyberspace, it prompted China to pivot to defensive capabilities such as network resilience and more recently cyber attribution capabilities. It should also be pointed out that China's deterrence signalling is not declaratory – it is not specified if and what kind of pre-emptive or retaliative attacks China might resort to. This could be related to China's official position that it is categorically against any kind of cyber-attacks, or it could be simply a form of tactical ambiguity. Meanwhile, some Chinese authors did suggest that China should articulate specific kinds of responses in order to make China's cyber deterrence more credible, though there seems to be no policy development in this direction till this day. Lastly, China's position on cyber attribution was previously that it is technically near impossible, and its position on public attribution is that it is counterproductive and hypocritical. On the other hand, China has most likely heavily invested in cyber forensic technologies and possibly in cyber intelligence gathering: with the recent CVERC attribution report and Chinese scholars and officials calling for 'effective attribution', it is logical to assume that China's position on

attribution has changed. However, as explained in greater detail above, this report holds the view that China has not pivoted to the 'naming and shaming' tactics of public attribution. The CVERC attribution is likely a coordinated signalling which may aim to entice the US and potentially other major powers in cyberspace to engage in dialogues on (public) cyber attribution.

This report points to a pattern of 'mirroring' in the evolution of Chinese strategic thinking and in the development of capabilities of cyber deterrence and attribution – China has carefully and meticulously studied the US practices of cyber deterrence and attribution, and adopted them if in China's national interest. Analysts and policy makers should be reminded that initial Chinese literature on cyber warfare always point to the successful conduct of cyber, electronic and information warfare by the US armed forces during the Gulf War; in other words, the US practice of those types of warfare inspired the very foundation of China's military capabilities in cyberspace. More recently, the pattern of 'mirroring' is reflected in that China seeks symmetrical or matching capabilities and deterrence postures with the US in cyberspace. At the tactical level, pointing to the fact that the US has adopted more engaging cyber deterrence policies, such as 'defend forward', 2020 SMS argued that China needs to adopt an active defence posture. At the strategic level, some Chinese literature describe the current dynamic in cyberspace as 'one-way deterrence' – while the US's cyber deterrence is effective on other actors, other actors cannot effectively deter the US. They argue that reaching a 'two-way deterrence' – a balance of power with the US in cyberspace is a precondition of effective dialogues. Mirroring is also reflected in how the CVERC's conducted its recent public attribution: methods such as using the modus operandi and political motives to identify perpetrators has been a part of how US entities conducts public attribution, which China anecdotally has always deemed inadequate and circumstantial as evidence.

More generally about the implication of Russian invasion of Ukraine on Chinese strategic thinking on cyber warfare, Chinese analysts seem to have engaged in some kind of self-projection in the following manner – what the West is doing to Russia now might happen to China in the future. Parenthetically, another development that merits attention is that many Chinese experts in the field of cybersecurity have uncritically taken Russian positions, narratives and sometimes disinformation as facts in their analysis, and some of their conclusions about Russia in cyberspace (e.g., RuNet) also seem to contradict with the consensus of Western and Russian experts. While the self-projection should not be confused with those Chinese analysts' attitude on Russia's war, it does show that they believe that it is

a serious possibility that the 'US-led collective West' will be directly involved in cyber and information warfare during a potential future armed conflict. Along this line of thinking, strategic autonomy in industries which supply goods and services to critical infrastructure and the arms industry would be a strategic priority for China. For China, this would be necessary to prevent disruption in case of a war-time embargo.

This report argues that China's perception of other actors in cyberspace is among others dictated by the dominant geopolitical view in China: as an emerging great power, China sees the perceived current hegemon US as a structural threat and its main adversary in cyberspace. Compared with physical space, it should be pointed out that cyberspace voids the geographical distance between states, increasing the likelihood of frictions and conflicts between major powers. Most Chinese literature reviewed by this report seems to hold a state-centric view, which does not delegate much agency to international organisations such as NATO, and academic attention in China towards NATO's own role as an organisation in cyberspace is low. Chinese authors seem to perceive Europe's position in cyberspace as defensive and more conciliable with China, they also suggest that European countries have a different ideal and strategic goals for governance of cyberspace, while they support the US's positions not because of like-mindedness, but out of deference. Although some parts of such perception might be wishful thinking, it could create more possibilities for European countries to engage with China. Meanwhile, as some Chinese authors quite correctly observe the growing geopolitical determinism in cyberspace, those possibilities may rapidly diminish.

Finally, there are a few propositions which could become what China would push for in the future, should a balance of power in cyberspace, as according to some Chinese authors, ripens the preconditions for negotiations. They may include the following:

- A form of arms control of cyber weapons.
- An international cyber attribution mechanism under the framework of the UN.
- An agreement among major powers in cyberspace that they should not attack each other's critical infrastructure.