8. New Domains of Crossover and Concern in Cyberspace

This chapter maps out the crossover between China and Russia in cyberspace. Amirudin Bin Abdul Wahab offers an overview of their growing complementarity of positions on cyber governance and norms. He notes with concern the overall direction of cyberwarfare operations, the lack of common definitions and agreement, and the implications for Malaysia. Lora Saalman explores the appropriation of cyberspace as the newest domain for hybrid warfare, citing cases of alleged cyber intrusion and attack from Ukraine to the South China Sea. Acknowledging the difficulties of attribution, she argues that such cases illustrate a potential growing Chinese–Russian convergence on responding to external threats and shaping their security environment through cyberspace.

8.1. Amirudin Bin Abdul Wahab[1]

Introduction

Chinese and Russian interactions in cyberspace are marked by considerable crossover. The first Russia–China Information and Communication Technologies Development and Security Forum, held in Moscow in April 2016, demonstrated their expanding cooperation on cyber governance. It emphasized the 'separate sovereignty of each nation in cyberspace'. This notion of cyber sovereignty, which advocates that each state control information flows, has gained increasing acceptance among a number of states in regions such as South East Asia. This guiding concept has also been criticized for potentially heralding the fragmentation of the Internet. As the debate over approaches continues, China and Russia's common vision aims to support their respective cyber-related social and economic interests, focusing on the security and governance of Internet communication structures, general data security and social development.

Dynamics in cyberspace

China's interest in cyberspace is far-reaching and ambitious. Among its various aspects, China's Belt and Road initiatives (BRI) underline China's intention to focus on global connectivity and economic cooperation, in part through what has come to be known as the Digital Silk Road. To support these efforts, China has launched its new satellite navigation services and expanded its e-commerce, industrial networks and Internet banking abroad. These initiatives indicate China's intention to achieve superiority in cyberspace, with cybersecurity as one of its top priorities. China is likely to leverage all necessary means to protect its information security, including use of its military. China is not alone in this approach.

[1] Amirudin Bin Abdul Wahab is the Chief Executive Officer of CyberSecurity Malaysia.

When it comes to protecting and penetrating networks, both China and Russia will seek to enhance their global cyber surveillance to mitigate threats.

Within this growing connectivity, experts already acknowledge the existence of cyber aggression conducted by states and state-sponsored actors. It should come as no surprise that such acts of aggression, including cyber espionage, system intrusion and high-scale cyberattacks, are being performed with ever-growing technical sophistication. Cyberspace has become a new battlefield for various hostile activities and acts of exploitation often involving China, Russia and the United States. The USA regularly claims that its critical systems have come under attack, allegedly from Chinese and Russian hackers. In response, the US Government has declared its critical infrastructure a strategic national asset, making any attack on these computer networks an act of war.

At the same time, leaks of classified information from the US National Security Agency (NSA) by the former contractor for the US government, Edward Snowden, have captured global attention as they expose expansive US activities in cyberspace. Current Chinese, Russian and US tensions demonstrate the alarming threat of cyberwarfare. While this concept remains poorly defined, a war in cyberspace is no longer simply an issue of intangible data theft or undetected attacks. Instead, the cyber intrusions and attacks of the future could have disastrous effects on industrial critical processes, jeopardizing the operation of generators and machinery and causing physical destruction.

From Malaysia's perspective, the global community has yet to derive a suitable approach to dealing with the pressing issues of cyber aggression involving the superpowers of China, Russia and the USA. Cyberwarfare is not currently being openly or adequately addressed. The fact that cyberwarfare has long been part of traditional national and military doctrines presents obstacles to future cooperation. China, Russia and the USA are reluctant to talk about their cyberwarfare programmes and this makes the world far less transparent. Despite this lack of clarity, there are current global collaborative efforts on cybersecurity and these should be used as opportunities to begin to build a greater understanding of the divergence of viewpoints on what constitutes cyberwarfare.

Takeaways

Cyberspace is both a national asset and a global common. There is, therefore, a need to protect both national and global interests. Any cyber conflict should be resolved diplomatically through the various international platforms, such as the United Nations and the Association of South East Asian Nations (ASEAN) Regional Forum. For such collaboration to begin, cultivating a better understanding of national and regional definitions of cyberwarfare will serve as a crucial first step. Currently, the Tallinn Manual contains one of the few multilaterally developed definitions of cyberwarfare. However, given its origins under the auspices of the North Atlantic Treaty Organization, this definition lacks the perspective of powers in Asia, particularly South East Asia. It is essential that countries respect each other's stance, recognizing that acts of cyber aggression can threaten trust in cyberspace. In this regard, Malaysia supports any global efforts to ensure cybersecurity. If cyberwarfare escalates and takes on kinetic dimensions, this will be damaging to the world as a whole.

8.2. Lora Saalman[2]

Introduction

In the wake of the crisis in Ukraine and Russia's annexation of Crimea, Western analyses have paid relatively sparse attention to the impact of these geopolitical shifts on Chinese views on territorial and peripheral stability. This essay uses 434 Chinese-language documents as a baseline to analyse how experts in China have internalized the lessons learned from the crisis in Ukraine.[3] Understanding how Chinese academics, economists, engineers, officials and military personnel view Russian tactics and strategy in Ukraine offers insights into how the concept of hybrid warfare and the use of proxies might factor into China's future calculations. This analysis suggests that beyond allegations of employing its own 'little green men' on land and 'little blue men' at sea to enforce its territorial claims, China may be trending towards a more holistic and Russian view of hybrid and proxy warfare in a new territory—cyberspace.

Hybrid warfare and cyberspace

Hybrid and proxy warfare are hardly new concepts in China. Decades ago, China followed Russia in supporting a revolution that spanned the breadth of society. More recently, in 2003, China's Central Military Commission and Communist Party codified the 'three warfares' as psychological, media and legal operations. Beyond the similarity with Russian views on holistic campaigns that penetrate multiple levels of society, the Deputy Secretary General of the China National Security Forum has noted that, similar to Ukraine, in the Asia-Pacific, '…small to medium scale military conflict or tensions are difficult to completely rule out, particularly given the US soft war of economic penetration and political subversion of China, combined with instigation of proxy warfare against China by neighbouring countries with which it has historical disputes…'.[4]

While hybrid warfare may be a well-worn concept, a new key element in this 'soft war' and the future of hybrid warfare is cyberspace. An expert in the Unit of Engineers in China's National Security Policy Committee points to 'network warfare' (网络战) conducted by the West in Ukraine through its use of cyberspace to: (*a*) control and manipulate public opinion and attack the government; (*b*) con-

[2] Lora Saalman is the Director of and a Senior Researcher in the China and Global Security Programme at SIPRI.

[3] For more information see Saalman, L., 'Little grey men: China and the Ukraine crisis', *Survival*, vol. 58, no. 6, (2016), <http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1257201?needAccess=true&journalCode=tsur20>.

[4] 彭光谦 [Peng, G.], '冷战后欧亚大陆首次出现地缘战略逆袭' [The first appearance of geostrategic counterattack in Eurasia following the end of the cold war], 经济导刊 [*Economic Herald*] (July 2014), pp. 85–86.

duct network monitoring and information attacks on government and military systems; and (c) provide substantial funding and information to support opposition groups.[5] His use of the term 'warfare' when describing these activities suggests China's application of a broader Russian definition to characterize conflict in cyberspace.

Using this broadened definition of warfare, Chinese experts denounce the negative impact of Western influence through ethnic and religious nationalism and democratic principles that are spread through exchange students, non-governmental organizations and economic interactions in a globalized market economy.[6] These trends are all facilitated by information flows through cyberspace. Over a quarter of the Chinese analyses surveyed cover the role of external propaganda and elections in Ukraine. Some pinpoint how the USA has utilized its own proxies in the form of non-governmental agencies and online propaganda to infiltrate and influence local opinion.[7] Others provide detailed analyses on how Facebook, Twitter, Vkontakte and YouTube, among others, were leveraged for the Euromaidan movement.[8] Given this basis, China and Russia have become increasingly aligned on such issues as Internet sovereignty and the control of information flows.[9]

In fact, experts from China's Second Artillery and the National Security Policy Committee, among others, have directly linked instability in Ukraine to US and European cyberattacks to control and manipulate online content, opposition parties and domestic public opinion.[10] In the face of the revelations of Edward

[5] Yu Zhonghai is a Senior Fellow in the Unit of Engineers in China's National Security Policy Committee. 于中海 [Yu, Z.] ed., 'Ukraine first disintegrated online' [乌克兰首先在网络被瓦解], *Theory Herald* [理论导报], p. 63.

[6] 葛汉文 [Ge, H.] and 丁艳凤 [Ding, Y.], '乌克兰民族主义: 历史演进、政治诉求与极端发展' [Ukrainian nationalism: historical evolution, political demands and extreme development], 俄罗斯研究 [*Russia Studies*], no. 3, June 2014, pp. 62–76; Zhang Yanbing is Deputy Director of the International Institute for Strategic and Development at the School of Public Management. Zeng Zhimin is a graduate student at Tsinghua University. 张严冰 [Zhang, Y.] and 曾志敏 [Zeng, Z.], 乌克兰危机及其对中国发展的启示 [The Ukraine crisis and its impact on China's development], 和平与发展 [*Peace and Development*], no. 1 (Jan. 2015), pp. 72–83.

[7] Zhu Zhihua is Deputy Director of the Association of Contemporary International Studies. 朱志华 [Zhu, Z.], '乌克兰危机背后折射的大国博弈及教训启迪' [Reflections on the great power game and lessons behind the Ukraine crisis], 战略决策研究 [*Strategic Decision Making Studies*], no. 6 (June 2014), pp. 20–29.

[8] Internet Lab consists of Fang Xingdong, Pan Feifei, Liu Kaiguo and Zhang Qing. 方兴东 [Fang, X.], 潘斐斐 [Pan, F.], 刘开国 [Liu, K.] and 张静 [Zhang, Q.], '互联网在乌克兰冲突中的作用' [The use of the Internet in the Ukraine conflict], '警惕社交网络安全风险暗流涌动' [Simmering societal alerts and network security risks], 网事纵横 [*Network Latitude*], 焦点 [*Focus*] (July 2014), pp. 67–71; and Hu Yong and Li Na are affiliated with Peking University's School of Journalism and Communication. 胡泳 [Hu, Y.] and 李娜 [Li, N.], '社交网络与乌克兰抗议运动' [Social networking and the Ukraine protests], 社交媒体与公共事件 [*Social Media and Public Events*], no. 6 (June 2014), pp. 17–24.

[9] '尊重国家网络主权 [Respect National Network Sovereignty], 中华人民共和国 [The People's Republic of China], 17 Feb. 2016, <http://www.gov.cn/zhengce/2016-02/17/content_5042042.htm>; Bazylev, S. I. et al., *The State and Prospects of Russian Military Cooperation on International Information Security*, (Ministry of Defence of the Russian Federation: Moscow:, 2014).; 俞晓秋 [Yu, X.], '新冷战"条件下网络空间的应对之策' [Cyberspace countermeasures under 'new cold war' conditions], 观点 [*Viewpoint*], July 2014, p. 117.

[10] Yang Chengjun holds a doctorate and is a professor and researcher in the Army Research Department of the Second Artillery Command. He has also held affiliations with the Ministry of Foreign Affairs and the National Security Policy Committee, as a PLA reviewer of military discipline, army equipment theorist, missile technology expert, nuclear strategy and arms control expert, military theorist and historian. 杨承军 [Yang, C.], '从乌克兰剧变看网络战对国家安全的影响' [Ukraine's upheaval: viewing the impact of cyberwarfare on national security], 世界观 [World View], 祖国 [*Motherland*], Mar. 2014, pp. 14–15; 于中海 [Yu, Z.] ed., 'Ukraine first disintegrated online' [乌克兰首先在网络被瓦解], *Theory Herald* [理论导报], p. 63.

Snowden on US cyber espionage programmes, the prevailing sense in China is that it remains particularly vulnerable and needs to make advances in not just detection, but also defence, retaliation and offence.[11] These analysts argue that the USA sees China as a 'new rival' (新对手) on a par with or even exceeding Russia, citing Western references to a 'new cyberspace cold war' (网络空间新冷战).[12] In so doing, they mimic Russian sources by referring to threats from 'external cyber-terrorism' (外部网络恐怖主义) and 'Western hacker attacks' (西方网络黑客的攻击).[13]

At the national level, Chinese experts decry how the West has used cyberspace to control civilian networks and infrastructure, to demonize national leaders and their policies and to spread rumours that result in ethnic conflicts and social disorder.[14] Zhu Zhihua, Deputy Director of the Association of Contemporary International Studies, highlights how external powers have used such incidents as the 5 July 2009 unrest in Xinjiang, the 3 July 2011 railway incident in Wenzhou and the 8 March 2014 Malaysian Airlines flight disappearance to wage online campaigns to undermine China.[15] Zhu notes that the stronger cyber capabilities of the Five Eyes countries—Australia, Canada, New Zealand, the United Kingdom and the USA—allow them to work in concert with the US Rebalance to the Asia-Pacific to attack the Chinese Communist Party and the Central People's Government from within by fabricating rumours, inciting extreme emotions, intensifying ethnic conflicts and encouraging social chaos.[16]

At the regional level, Chinese analysts see cyberspace as a key mechanism used by the USA to reinforce its hegemonic role, exacerbating a spectrum of concerns over Taiwan, Xinjiang and Tibet, as well as the East China Sea and South China Sea. They argue that China must learn from how the USA and European powers infiltrated and controlled Ukraine's government and military networks. In confronting these threats, Chinese experts emphasize the development of civil-military integration and interoperability in cyber command countermeasures and mitigation techniques, as well as in cyber reconnaissance and cyberattack capabilities.[17] They advocate China strengthen its public and private networks, exert greater control over content and harden its broadband networks to close the technical loopholes used by other countries to undermine China's 'sovereignty security' (主权安全), 'political security' (政治安全) and 'social stability' (社会稳定).

Overall, Chinese analysts note that in the face of Western encirclement on land, sea and now in cyberspace, China must follow Russia's example by placing a greater emphasis on the reputation and modernization of its own military to

[11] 江凌飞 [Jiang, L.], '面对世界乱局,中国要沉着应付' [Facing chaos in the world: China should calmly confront it], 当代世界 [*Contemporary World*] (May 2014), pp. 19–21.

[12] 俞晓秋[Yu, X.], '新冷战"条件下网络空间的应对之策' [Cyberspace countermeasures under 'new cold war' conditions], 观点 [*Viewpoint*] (July 2014), p. 117.

[13] 方兴东 [Fang, X.], 潘斐斐 [Pan, F.], 刘开国 [Liu, K.] and 张静 [Zhang, Q.], '互联网在乌克兰冲突中的作用' [The use of the Internet in the Ukraine conflict], '警惕社交网络安全风险暗流涌动' [Simmering societal alerts and network security risks], 网事纵横 [*Network Latitude*], 焦点 [*Focus*] (July 2014), p. 69.

[14] 于中海 [Yu, Z.] ed. (note 5).

[15] 朱志华 [Zhu, Z.] (note 7).

[16] 朱志华 [Zhu, Z.] (note 7).

[17] 于中海 [Yu, Z.] ed., 'Ukraine first disintegrated online' [乌克兰首先在网络被瓦解], *Theory Herald* [理论导报], p. 63.

ensure its security and national interests. In the words of Chu Maoming, a Counsellor in China's Ministry of Foreign Affairs, China must learn from Russia's actions in Ukraine to be confident in its theory, its path and its system in order to unswervingly forge ahead with its 'emergence' (复兴).[18] To this end, Russia's own prioritization and modernization of its military could be equated with that which Chinese official and non-official discourses label its 'Strong Military Dream' (强军梦), an extension of the 'China Dream' (中国梦).[19]

Cyber convergence

As the China Dream and Strong Military Dream play out in cyberspace, China's and Russia's tactics and strategies are showing signs of convergence. Beyond China's alleged use of what could be deemed their own variant of 'little green men' with nomads and paramilitaries at land borders, or 'little blue men' with fishermen and coastguard vessels at maritime borders,[20] Chinese and Russian views are becoming increasingly aligned on cyberspace, which cuts across both spheres. The holistic nature of cyberspace lends itself to more pervasive and ultimately punishing political, economic and military campaigns against broader populations and non-combatants.

Moreover, non-combatants do not exist in cyberspace, making it the perfect environment to carry out hybrid warfare. Despite the centrality of this sphere for future proxy activities, it remains the least understood.[21] This is, in part, due to the difficulty of attribution and the number of patriotic hackers and proxy entrants in this field. Determining whether actions are those of a proxy individual or group as

[18] 方兴东 [Fang, X.], 潘斐斐 [Pan, F.], 刘开国 [Liu, K.] and 张静 [Zhang, Q.] (note 13), p. 71.

[19] The increase in the use of the term 'emergence' (*fuxing*) in connection with both China and Russia is noteworthy, since it indicates not only greater connectivity between the two but also how 'rise' (*jueqi*) has increasingly fallen out of favour in describing China. Chu Maoming is a Counsellor in China's Ministry of Foreign Affairs. 储茂明 [Chu, M.], '乌克兰危机与中国的选择' [The Ukraine crisis and China's options], 战略决策研究 [*Strategic Decision Making Studies*], no. 3 (Mar. 2014), p. 11.

[20] 储茂明 [Chu, M.] (note 19); Zhang Jinying is affiliated with Unit 69223 as a Deputy Political Teacher and as a PhD candidate at Xian's Political School. Nan Weihua is an instructor at the Academy for Boder Defence and Training. 张金英 [Zhang, J.] and 南卫华 [Nan, W.], '强军兴军是中国军队的唯一选项-乌克兰动荡的反思' [Building a powerful army is the only option for the Chinese military: Reflections on Ukraine's turmoil], 军事政治学研究 [*Military Political Study*], no. 1 (Jan. 2014), pp. 146–49; and '2015中国国防白皮书 "中国的军事战略" (全文)' [China's 2015 National Defence White Paper, 'China's Military Strategy' (Complete Text)], 中国日报 [*China Daily*], 26 May 2015, <http://world.chinadaily.com.cn/2015-05/26/content_20821000.htm>.

[21] *Express Tribune*, 'Chinese pressure sees Pakistan mull constitutional status of Gilgit-Baltistan', 7 Jan. 2016, <http://tribune.com.pk/story/1023523/chinese-pressure-sees-pakistan-mull-constitutional-status-of-gilgit-baltistan>; Lam L., 'The thugs of mainland China', *New Yorker*, 8 Oct. 2014, <http://www.newyorker.com/news/news-desk/thugs-mainland-china-hong-kong-protests>; Porter, T., 'Hong Kong: "hired Triad thugs attacked demonstrators" claims legislator', *International Business Times*, 4 Oct. 2014, <http://www.ibtimes.co.uk/hong-kong-hired-triad-thugs-attacked-demonstrators-claims-legislator-1468529>; Popham, P. and Legge, J., 'Beijing allegedly call hired thugs to incite Hong Kong riots', *Morning Bulletin*, 4 Oct. 2014, <http://www.themorningbulletin.com.au/news/beijing-allegedly-call-hired-thugs-incite-hong-kon/2408957/#/0>; Rajagopalan, M., 'China trains "fishing militia" to sail into disputed waters', *Reuters*, 30 Apr. 2016, <http://www.reuters.com/article/us-southchinasea-china-fishingboats-idUSKCN0XS0RS>; Bussert, J., 'Chinese maritime assets enforce ocean territorial claims', *Signal Magazine*, 1 July 2014, <http://www.afcea.org/content/?q=chinese-maritime-assets-enforce-ocean-territorial-claims>; and Leaf, P., 'Learning from China's oil rig standoff with Vietnam', *The Diplomat*, 30 Aug. 2014, <http://thediplomat.com/2014/08/learning-from-chinas-oil-rig-standoff-with-vietnam>.

opposed to a military or government remains difficult. This is a point frequently made by Chinese analysts such as Dong Qingling at Beijing's University of International Business and Economics when discounting allegations against Russia and China, pertaining to alleged cyber intrusions and cyberattacks in Ukraine or on other networks.[22]

With the enhancement of forensics, such dilemmas could diminish in the future. In the meantime, civilian and military analysts in China have pushed for and made improvements to cybersecurity, military and civilian integration and legal structures, and enhanced regulation of and joined up working on cyberattack and defence mechanisms.[23] They have also advocated comprehensive cyberwarfare practices that emphasize counterattack capabilities and interference, as well as improved protection and monitoring of networks through defensive and offensive exercises.[24]

There are also indications that China's integration of proxies into information operations is already under way, with the alleged involvement of domestic universities, foundations and industries—thought to often have support from the PLA or Ministry of State Security—in broader campaigns that intrude on networks of multiple countries in South East Asia and South Asia, as with Advanced Persistent Threat 30 (APT30).[25] The latter series of incidents, alleged given its scope duration and focus on the South China Sea to have originated from within China, lasted over 10 years and compromised government, media and industry in 17 countries.[26]

[22] Wang Zhijun is a Professor of International Law in the Department of Military and International Law. Zhang Yaowen is a lecturer in the Department of Military Law and International Relations at the Nanjing Army Command College. 王志军 [Wang, Z.] and 张耀文 [Zhang, Y.], '西方地缘战略理论批判与中国地缘战略理论构建' [Critique of Western geostrategic theory and construction of China's construction geostrategic theory], 学术探索 [*Academic Exploration*], no. 2 (Feb. 2015), p. 32.

[23] Based on a Chinese-language panel moderated by Lora Saalman on '网络安全与军备控制' [Cyber Security and Arms Control] at Tsinghua University's [2016年政治学与国际关系学术共同体会议' [2016 Annual Conference of the Chinese Community of Political Science and International Studies], '三月国际网络和信息安全发展动态' [March International Networks and Information Security Developments], 信息安全与通信保密 [*Information Security and Communications Privacy*], no. 4 (Apr. 2014), pp. 14–17.

[24] Chen Hongchao, Duan Benqin and Li Tao are affiliated with the 1st Military Representatives Office of the Communications Division at PLA General Staff Headquarters in Tianjin. 陈洪超 [Chen, H.], 段本钦 [Duan, B.] and 李涛 [Li, T.], '21世纪战争新概念-网络战' [New concept of wars in the 21st century: network war], 军事通信技术 [*Journal of Military Communications Technology*], no. 4 (Apr. 2001).

[25] 于中海 [Yu, Z.] (note 17); 马良荔 [Ma, L.], 吴清怡 [Wu, Q.], 苏凯 [Su, K.] and 任伟 [Ren, W.], eds, '物联网及其军事应用' [*The Internet of Things and its Military Applications*], (北京: 国防工业出版社 [Beijing: National Defence Industry Press], 2014), p. 187; Zhang Yongjun is affiliated with the Shaanxi Fenghuo Communication Group Co., Ltd. 张勇军 [Zhang, Y.], '物联网及其军事应用' [Internet of Things and its Military Applications], 智能处理与应用 [Intelligent Processing and Application], 物联网技术 [*Internet of Things Technology*], no. 7, 2012, pp. 77–79; 郭若冰 [Guo, R.], 军事信息安全论 [*Military Information Security Theory*], (北京: 国防大学出版社 [Beijing: National Defence University Press, Jan. 2013]), p. 101; 唐跃平 [Tang, Y.], 赵伟峰 [Zhao, W.], 谷麦征 [Yu, M.], 孙建 [Sun, J.], 韩平 [Han, P.], 唐晓婧 [and Tang, S.], 科技信息云服务及军事应用 [*Science and Technology Information of Cloud Services and Military Applications*], (北京: 国防大学出版社 [Beijing: National Defence University Press, Jan. 2015]), p. 258; 宋忠平 [Song, Z.], 大国武器 [*Major Power Weapons*], (北京: 新世界出版社 [Beijing: New World Press, Sep. 2013]); and 宋航 [Song, H.], 物联网技术及军事应用 [*Internet of Things: Technology and its Military Use*], (北京: 国防工业出版社 [Beijing: National Defence Industry Press, 2013]), p. 140.

[26] FireEye, 'APT30 and the mechanics of a long-running cyber espionage operation: how a cyber threat group exploited governments and commercial entities across South East Asia and India for over a decade' (Apr. 2015), <https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf>; and Krekel, B., Adams, P. and Bakos, G., 'Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage', Paper prepared for the US-China Economic and Security Review Commission by

Much like hybrid warfare in the Russian context, which prioritizes controlling and shaping the flow of information, such campaigns are likely to become more common in the future. They allow for military operations short of war and for information to be leveraged prior to and during conflict. They take forward the US model studied from the first Iraq war of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and look to shape it to Chinese requirements both on and off the battlefield. Since cyberspace does not discriminate in the same way between combatants and non-combatants, this new realm of engagement allows for a 24/7 campaign.

The connectivity of persistent multi-layered tactics, cyber command countermeasures and cyberattack capabilities between China and Russia also appears to be growing. Similar malware campaigns are alleged to have emerged from within both China and Russia with an emphasis on using spearphising, man-on-the-side, man-in-the-middle and watering-hole attacks to exploit browser, VPN and social engineering vulnerabilities.[27]

Among these, a 2015 distributed denial of service (DDoS) attack allegedly using an Adobe Flash vulnerability was conducted against the website of the Permanent Court of Arbitration at The Hague, while adjudicating the Philippines' case against China on the South China Sea.[28] Although often considered a nuisance attack to take down systems, this type of DDoS attack can also be used to weaken the perimeter of the system to gain access and to potentially exfiltrate information. While differing in tactic, the nature of this incident is comparable with a 2015 intrusion and theft of data allegedly using a fake VPN server against the Dutch Safety Board investigating the MH17 crash, which was thought to have come from the hacker group Pawn Storm in Russia.[29]

By 2016, the mass theft of data from the Democratic National Committee, comparable to the exfiltration of an estimated 25 million US employees' clearance data from the US Office of Personnel Management discovered in 2015, highlighted again a basic form of cyber intrusion—spearphishing and remote access Trojans—as an inroad to domestic crises of confidence, damaged political systems and potential future blackmail.[30] From The Hague to Washington, DC, these cases illustrate

Northrop Grumman Corporation, 7 Mar. 2012, <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf>.

[27] The countries thought to have been compromised by the APT30 campaign are Bhutan, Brunei, Cambodia, India, Indonesia, Japan, Laos, Malaysia, Myanmar, Nepal, the Philippines, Saudi Arabia, Singapore, South Korea, Thailand, the USA and Viet Nam.

[28] Spearphishing constitutes email fraud that targets an individual or organization to gain unauthorized access to confidential data. A man-on-the-side attack and a man-in-the-middle attack are similar. However, in the former case, rather than controlling a network node as in the latter case, the attacker has regular access to the communication channel, allowing him or her to read the traffic and to insert new messages, rather than modifying or deleting messages sent by other participants. A watering-hole exploit compromises a specific group of end users by infecting websites that members of the group are known to visit, so that the attacker can gain access to the network at the target's place of employment.

[29] TruShield, 'Nation-state sponsored cyberwarfare campaign', 2 Nov. 2015, <https://trushieldinc.com/wp-content/uploads/2015/11/TS_Advisory_11022015_AD.pdf>.

[30] Hacquebord, F., 'Pawn storm targets MH17 investigation team', *TrendMicro*, 22 Oct. 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/>.

organizations and individuals with a politically and legally significant impact on China and Russia finding themselves subject to cyber intrusion and cyberattack.

Other similar malware campaigns thought to emanate from within China and Russia include the Clandestine Fox and Russian Doll, which are both thought to exploit spearphishing campaigns and Adobe Flash vulnerabilities to target aerospace and defence, construction and engineering, high-tech industry, telecommunications and transport infrastructure.[31] In these cases, the tactics and intent behind the campaigns are not only convergent, but also likely to become increasingly commonplace. The challenges associated with identification of the perpetrators—whether at the technical attribution level or the political diplomatic level—suggest that cyberspace will be the crux of future hybrid warfare.

An example of how this future is expanding from simple data exfiltration to kinetic attacks on critical infrastructure came in a 2015 cyberattack on electricity utilities in Ukraine. Forensic reports on the malware, staging and coordination suggest that the hackers were either based in or supported by Russia.[32] DarkEnergy malware, used in combination with denial of service attacks and the wiping tool KillDisk, not only cut electricity for an estimated 225 000 people, but also created an air of confusion and panic over the restoration of services among providers and users. Studies suggest that the motivation behind the attack was not simply to test out the ability to comprehensively take down critical infrastructure, but also to elicit embarrassment.[33]

Thus, while this campaign lasted only four hours and was mitigated in part by the ability to use the analogue equipment in the facilities to restore functionality, it is telling how cyberattacks can be used in broader campaigns to cut vital services to a populace and to raise questions over the competence of first responders and the respective government. Given the level of penetration of such campaigns as APT30 into South East Asia and South Asia, the likelihood of similar tactics appearing in the Asia-Pacific region is high. Whether from government entities or patriotic hacker proxies, campaigns that target the entirety of society can greatly supplement the conduct of more conventional military campaigns by supporting a shutdown not only of basic services, but also of critical infrastructure from electricity plants to nuclear facilities.[34]

[31] Fisher, M., 'Why security experts think Russia was behind the DNC breach' *The Interpreter* in *New York Times*, 26 July 2016, <http://www.nytimes.com/2016/07/27/world/europe/russia-dnc-hack-emails.html>; *Wired*, 'Here's what we know about Russia and the DNC hack', 27 July 2016, <https://www.wired.com/2016/07/heres-know-russia-dnc-hack>; and *Threat Connect*, 'OPM breach analysis' (2015), <https://www.threatconnect.com/blog/opm-breach-analysis-update>.

[32] FireEye, 'Pinpointing targets: exploiting web analytics to ensnare victims' (Nov. 2015), <https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf>.

[33] SANS Institute Industrial Control Systems and the Electricity Information Sharing and Analysis Centre, 'Analysis of the cyber attack on the Ukrainian power grid: defence use case', 18 Mar. 2016, pp. 1–23, <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf>.

[34] SANS Institute Industrial Control Systems and the Electricity Information Sharing and Analysis Centre (note 33).

Takeaways

Currently, China's rhetoric and activities do not meet the level of violence found in the 'little green men' litmus test of the proxy war that Russia has allegedly waged in Ukraine. Nonetheless, enough parallels have been drawn by China's own academics, engineers, military personnel and officials to suggest that China may transform this model and craft it into a more penetrating and persistent campaign.

Beyond the terrestrial and maritime implications of this methodology, confrontation in cyberspace poses new challenges for how analysts define and confront hybrid warfare. Arguments emanating from China on how it is being targeted with propaganda and destabilizing influences from cyberspace and civil society are often a mirror image of what is being alleged by Russia.

Both find the US 'dark hand' (黑手) to be manipulating public sentiment and conditions on the ground, whether on Ukraine or the South China Sea. Given their solidarity and concerns over this 'interference' (干涉) in their own domestic and regional spheres, it should not come as a surprise if China's own tactics and responses increasingly fall along similar lines to those of Russia.[35] Moving beyond appreciation of Russia's willingness to stand up to the USA, Chinese adaptation to Russia's alleged tactics and strategy on hybrid warfare is likely to increase.

[35] For more information see Saalman, L., 'Pouring "new" wine into new bottles: China–US deterrence in cyberspace', *Seton Hall Journal of Diplomacy and International Relations* (Fall/Winter 2015).