The International Institute for Strategic Studies, Arundel House, 13-15 Arundel Street, Temple Place, London WC2R 3DX, United Kingdom. www.iiss.org. Incorporated in England with limited liability under number 615259. UK registered charity 206504.

Little Grey Men: China and the Ukraine Crisis

Lora Saalman

Russia's annexation of Crimea and the crisis in Ukraine have affected Chinese views of territorial sovereignty and peripheral stability. Chinese analysts are applying lessons learned from Ukraine to their own regional and international environment. An examination of 434 Chinese-language documents on the Ukraine crisis provides insights into how Chinese academics, economists, engineers, officials and military personnel view Russian tactics and strategy, as well as Western intentions, and suggests that China is moving towards a more holistic and 'Russian' view of hybrid and proxy warfare – particularly in cyberspace.

Identification with Russia

Chinese coverage of the Ukraine crisis, although it is geographically distant, extends beyond simply recounting its impact on Russia, Ukraine and the United States, and frequently addresses the implications of the crisis for China.[1] Using the oft-touted accusation of 'Cold War thinking' (*lengzhan siwei*) on the part of Western powers, Chinese analysts frame the Ukraine crisis as a 'great-power game' (*daguo boyi*) between Washington and Moscow.[2] In a number of cases, Chinese writers are conflicted on how to evaluate the costs and benefits of the Ukraine crisis for Beijing.

In terms of advantageous fallout, a range of Chinese studies note that the Ukraine crisis distracted Washington from its rebalance to the Asia-

Lora Saalman is the Director of, and Senior Researcher at, the China and Global Security Programme at the Stockholm International Peace Research Institute (SIPRI).

Survival | vol. 58 no. 6 | December 2016–January 2017 | pp. 135–156 DOI 10.1080/00396338.2016.1257201

Pacific, created questions over US commitments to its regional partners and carved out space for Beijing to shape its own regional interests.[3] However, a number of negative trends are also identified in these writings. Academics from the China Foreign Affairs University and the University of International Business and Economics in Beijing note that the Ukraine crisis has threatened Asia-Pacific stability by accelerating Washington's efforts to bolster China's neighbours to forestall a Crimea scenario emerging via Beijing's territorial and maritime disputes in the Asia-Pacific region. A counsellor in China's Ministry of Foreign Affairs has suggested that Beijing remains concerned about Ukraine setting a negative precedent for its own regional claims, threatening long-held precepts of territorial sovereignty and non-intervention,[4] and potentially inspiring Taiwan, Xinjiang, Tibet and Hong Kong to engage in independence votes like that held in Crimea.[5]

Chinese analysts applaud Russian defiance

Pulled between Washington and Moscow, the Chinese government has opted for neutrality at the official level, in part by abstaining from the March 2014 vote on Crimean annexation at the United Nations Security Council.[6] Yet, digging deeper, this official stance is muddied by a broader discourse in China that indicates support for Russia's decision-making process and actions in Ukraine.[7] In stark contrast to coverage on the Ukraine crisis in the West, Chinese experts across a wide spectrum of official and non-official backgrounds express appreciation for Moscow's culture of heroism and patriotism; social cohesion and political support; unity and decisiveness of the central government and leadership; strong military and nuclear deterrence; cyber and information security; clarity of national and international stance; maintenance of sovereignty and stability; protection of national interests and territorial claims; resistance to external interference; and grand national strategy and global strategic vision.

Rather than seeing a nation hobbled by sanctions, Chinese analysts applaud Russia for its defiance. In fact, Chinese experts repeatedly emphasise that Russia and China maintain common interests and pursuits when it comes to 'national security, anti-hegemony, and promotion of democra-

tization and multilateralization of international relations'.[8] Analysts from the China Institutes of Contemporary International Relations (CICIR) note Moscow's efforts in the past few years to restore some of the strategic balance between Russia and the United States, particularly when it comes to missile defence, cyber and space warfare.[9] In their view, the Ukraine crisis is part of this recalibration.

As a result, countless Chinese experts view Russia's actions in Ukraine as a decisive and largely justifiable reaction to instability and unrest at its borders, foreign stationing of military systems closer to its territory and loss of access to resources in the face of unrest, as well as the wrongs of history and territorial losses.[10] In making this assessment, these experts highlight China's own concerns over US military deployments to the Asia-Pacific region, citing Washington's threat to Beijing's own territorial claims and freedom of action in the South China Sea and East China Sea.[11]

Chinese historical accounts of the Ukraine crisis further promote identification with Russia's dilemma. Terms like 'invasion' (*ruqin*) and 'encirclement' (*baowei*) are used to express concerns faced by both Beijing and Moscow. Similar to their own territorial claims, Chinese experts detail centuries of Russian history to provide explanations for Moscow's linkages to Crimea.[12] Nearly a quarter of the writings surveyed use the term 'return' (*huigui*) to describe Russia's annexation of Crimea.[13] This term indicates the reappropriation of territories that have been unlawfully or forcibly seized and broken away. It is generally reserved for Hong Kong or Macao finding their rightful place back within China's fold. Its use reflects an overall acceptance of the fact that Moscow had historical, political and strategic impetus and cause to reclaim Crimea.[14]

Furthermore, Chinese writers detail the manner in which Ukraine's 'extreme nationalism' (*jiduan minzuzhuyi*) and inclination towards the West threaten Russia's emergence.[15] They draw ties to the ethno-nationalism in the strategic buffer zones of Xinjiang, Tibet and Taiwan that they believe makes China susceptible to external interference and propaganda.[16] Research conducted in conjunction with an event held by the China Institute of International Studies' Department for European Studies also indicates that Western co-opting of Kiev makes details on Moscow's nuclear programme

vulnerable, by offering both proximity and access to formerly active nuclear facilities and researchers, while at the same time erasing Russia's strategic buffer zone.[17] Given China's own testing of nuclear and advanced conventional weaponry in its own integral buffer zone and border region of Xinjiang, Beijing is seen as facing similar intelligence threats at its restive and porous borders.

Overall, when detailing these threats to territorial integrity, sovereignty and overall security, the majority of Chinese authors posit that the primary concern remains Washington, not Moscow. A number of analyses allege hypocrisy in US policies on Ukraine versus Kosovo: Washington argued for elections in Kosovo under the guise of human rights, while denouncing elections in Crimea under the argument of sovereignty. These analyses laud how Russia has managed to turn the tables on Washington's 'double standards' (*shuangzhong biaozhun*) in using humanitarian intervention as an excuse to incite regional instability and government overthrow.[18] Chinese assessments use such linguistic parallels to connect the challenges faced by both Moscow and Beijing. And in both cases, the primary threat comes from Washington.

Criticism of US proxies

In contrast to their conflicted, but ultimately sympathetic, coverage on Moscow's role in Ukraine,[19] Chinese analysts are much less oblique about how Washington has violated principles of sovereignty and non-intervention. They compare the way in which the United States has exploited tensions between Russia and Europe with how it has divided ethnic and religious groups such as Sunnis and Shi'ites, and countries such as China and Japan.[20] Chinese authors describe the United States' attempts to use the Ukraine crisis to expand its transatlantic influence and to mitigate its 'hegemonic system crisis' (*baquan de jiegouxing weiji*) of decreasing control and relevance.[21]

NATO members are seen as proxies through which Washington is able to provide military and cyber assistance to Kiev,[22] while pursuing political and economic objectives via sanctions on Moscow.[23] NATO Secretary-General Jens Stoltenberg's statement on 16 June 2016 that 'a severe cyber

attack may be classified as a case for the alliance' to respond suggests that Chinese criticisms of American use of allies in Europe and Asia as tools for interference and escalation will only grow.[24] By contrast, Chinese references to Moscow's use of 'proxies' (*dailiren*) often place the term in quotation marks to question its veracity.[25] They make relatively few references to the downing of Malaysian Airlines Flight MH17 by pro-Russian rebels. In fact, some of these writings refer to key details of the crash as conjecture,[26] choosing instead to focus on how propaganda has reframed global opinion.[27] In their view, the true 'little green men' are not deployed by Russia, but rather by the United States.

Chinese discussions stress that the Ukraine crisis is rooted in Washington's aim to provoke Moscow into a war with its European neighbours by eliminating its buffer zone and fomenting instability and opposition in its periphery. These articles create a link between Washington and myriad colour revolutions in the guise of proxy warfare, whether through US partner nations and allies, non-governmental organisations, online propaganda or other means.[28] In highlighting these claims, Chinese writings note that Russia made an initial pledge not to intervene in Ukraine, until forced to react to provocation from Western powers.[29]

When it comes to the Asia-Pacific, this assertion echoes how Chinese authors emphasise Beijing's 'reactive' (*beidong*) or 'forced' (*beipo*) approach when confronting Washington and its proxies in the Asia-Pacific region. Analyses contend that the Ukraine crisis allows Washington to expand its access to alliances and resources.[30] Similarly, they suggest that tensions in the South China Sea are used by the United States to enlist such countries as the Philippines and Vietnam in threatening Beijing's 'Maritime Silk Road' initiative.[31] As in the case of European nations, Washington is seen as aiding smaller Asia-Pacific countries to enhance their military interoperability, weakening Beijing's territorial stance via the Permanent Court of Arbitration at The Hague and isolating China economically with the Trans-Pacific Partnership.[32]

Overall, these Chinese analyses highlight political, legal, military and economic challenges that are similar to those faced by Russia. They posit US strategy in both Europe and Asia as spreading instability to maintain

relevance and to avoid marginalisation; driving a wedge between regional players to strengthen America's grasp on the global system; and containing, weakening and destabilising the rise and re-emergence of countries such as China and Russia.[33] A number of Chinese experts argue that the United States' greatest failure has been to push Beijing away from Washington and towards Moscow.[34] US policy documents, such as the 2010 Nuclear Posture Review and 2013 Air–Sea Battle Concept, exacerbate these trends by making explicit connections between China, the former Soviet Union and Russia.[35]

Widening this gulf even further, Chinese academics and officials increasingly argue for distancing their own capital from Washington and the democratic precepts of 'so-called' (*suowei*) freedom, democracy and human rights,[36] as well as external 'interventionism' (*ganshe zhuyi*), which are seen as divisive and bringing instability to Ukraine.[37] They argue that democratic principles and trends are out of sync not only with Ukraine's development needs, but also with China's own culture and emergence.

In looking toward a different model, Chinese writings note that Russia has been able to domestically capitalise on its hard power of military modernisation to enhance its sense of national pride. In terms of soft power, they point to Russia's heroic traditions as integral to strengthening domestic cohesion and popular opinion to combat Western influences.[38] Moscow has worked to reinvigorate its own national power and to shape the international system by standing up to the West. Chinese analysts entreat Beijing to position itself as a pole in the global structure to counterbalance US influence in the Asia-Pacific region, and to make China a great power. In this effort, hybrid warfare plays a central role.

Future of hybrid warfare

Hybrid and proxy warfare are hardly new concepts in China. Decades ago, Beijing followed Moscow in supporting 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 notes 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 U.S. soft war of economic penetration and political subversion of China, combined with instigation of proxy warfare against China by neighboring countries with which it has historical disputes'.[39]

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' (*wangluo zhan*) conducted by the West in Ukraine through its use of cyberspace to control and manipulate public opinion and to attack the government; conduct network monitoring and information attacks on government and military systems; and provide substantial funding and information to support opposition groups.[40] His use of the term 'warfare' when describing these activities suggests Chinese application of a broader Russian definition to characterise conflict in cyberspace.

Using this broadened definition of warfare, a number of Chinese experts denounce the negative impact of Western influence via ethnic and religious nationalism and democratic principles that are spread via exchange students, non-governmental organisations and economic interactions within a globalised market economy.[41] All of these trends are facilitated by information flows that occur through cyberspace. Many Chinese analyses discuss the role of external propaganda and elections in Ukraine. Some pinpoint how Washington has used its own proxies in the form of non-government agencies and online propaganda to infiltrate and influence local opinion.[42] Others provide detailed accounts of how platforms such as Facebook, Twitter, Vkontakte, YouTube and others have been put to the use of the Euromaidan movement.[43] On this basis, Beijing and Moscow have increasingly aligned on such issues as internet sovereignty, under which cyberspace is regarded as a territorial domain that can be controlled and regulated in terms of its information flows.[44]

In fact, experts from China's Second Artillery Corps and the National Security Policy Committee, among others, have directly linked instability in Ukraine to US and European cyber operations to control and manipulate online content, opposition parties and domestic public opinion.[45] In the face

of the revelations of former US government contractor Edward Snowden on US cyber-espionage programmes, the prevailing sense in China is that it remains especially vulnerable and needs to make advances in not just detection, but also defence, retaliation and offence.[46] These analysts argue that Washington sees Beijing as a 'new rival' (*xin duishou*) on a par with, or even exceeding, Moscow, citing Western references to a 'new Cyberspace Cold War' (*wangluo kongjian xin lengzhan*).[47] In doing so, they mimic Russian sources by referring to threats from 'external cyber terrorism' (*waibu wangluo kongbuzhuyi*) and 'Western hacker attacks' (*xifang wangluo heike de gongji*).[48]

At the national level, Chinese experts decry how the West has used cyberspace to control civilian networks and infrastructure, to demonise national leaders and their policies, and to spread rumours that result in ethnic conflicts and social disorder.[49] Zhu Zhihua, deputy director of the Association of Contemporary International Studies, points to how external powers have used incidents such as the 5 July 2009 unrest in Xinjiang, the 3 July 2011 train collision in Wenzhou and the 8 March 2014 Malaysia Airlines flight disappearance to wage online campaigns to undermine Beijing.[50] In doing so, Zhu notes that the stronger cyber capabilities of the Five Eyes countries – Australia, Canada, New Zealand, the United Kingdom and the United States – 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.[51]

At the regional level, Chinese analysts see cyberspace as a key mechanism used by Washington to reinforce its hegemonic role, exacerbating a spectrum of concerns in Taiwan, Xinjiang and Tibet, as well as the East and South China seas. As a result, they argue that Beijing must learn from how the US and European powers infiltrated and controlled the Ukrainian government and military networks. In confronting these threats, Chinese experts emphasise development of civil–military integration and interoperability in cyber-command countermeasures and mitigation techniques, as well as in cyber-reconnaissance and -attack capabilities.[52] They advocate China strengthening its public and private networks, exerting greater control over content and hardening broadband networks to close techni-

cal loopholes used by other countries to undermine China's 'sovereignty security' (*zhuquan anquan*), 'political security' (*zhengzhi anquan*) and 'social stability' (*shehui wending*).[53]

Overall, Chinese analysts note that, in the face of Western encirclement on land and sea, and now in cyberspace, Beijing must follow Russia's example by placing a greater emphasis on both the reputation and modernisation of its own military to ensure its security and national interests. In the words of Ministry of Foreign Affairs Counsellor Chu Maoming, China must learn from Russia's actions in Ukraine to be confident in its theory, path and system to unswervingly forge ahead in its 'emergence' (*fuxing*).[54] To this end, Moscow's own prioritisation and modernisation of its military could be equated with what Beijing's official and non-official discourse labels its 'Strong Military Dream' (*qiang jun meng*), an extension of the 'China Dream' (*zhongguo meng*).[55]

Little grey men

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 their own variant of 'little green men' (nomads and paramilitaries at land borders) and 'little blue men' (fishermen and coastguard vessels at maritime borders),[56] Chinese and Russian views are increasingly aligned in cyberspace, which cuts across both of these 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.

Indeed, in cyberspace the line between combatants and non-combatants is blurred, making it the perfect environment for carrying out hybrid warfare. Nonetheless, despite the centrality of this sphere for future proxy activities,[57] it remains the least understood. This is, in part, due to the difficulty of attribution and the number of patriotic hackers and proxy entrants into this field. Determining the actions of a proxy individual or group versus 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, whether pertaining to alleged cyber intrusions and attacks in Ukraine or in other networks.[58]

With advancements in forensics, such dilemmas may diminish in the future. In the meantime, however, civilian and military analysts in China have pushed for and made improvements to cyber security, military and civilian integration and legal structure, as well as better regulation of and jointness within cyber-attack and defence mechanisms.[59] They have also advocated for comprehensive cyber-warfare practices that place an emphasis on counter-attack capabilities and interference, as well as protection and monitoring of networks improved via defensive and offensive exercises.[60]

Cyber-intrusion campaigns are likely to become more common

China's integration of proxies into information operations is apparently already under way, with the alleged involvement of domestic universities, foundations and industries – thought to often have support from the People's Liberation Army or Ministry of State Security – in broader campaigns that intrude on the networks of multiple countries in Southeast Asia and South Asia, as with Advanced Persistent Threat 30 (APT30).[61] The latter series of incidents, alleged to have come from within China given its scope, duration and focus on the South China Sea, lasted more than ten years and compromised government, media and industry in 17 countries.[62]

Much like Russian hybrid warfare, which prioritises 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. In essence, they take the contemporary US model in command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) and look to shape it to Chinese requirements both on and off the battlefield. Since, once again, cyberspace does not discriminate in the same way between combatants and non-combatants, this new realm of engagement allows for a permanent campaign.

The connections between persistent Chinese and Russian multilayered tactics, cyber-command countermeasures and cyber-attack capabilities

also appear to be growing. Similar malware campaigns are alleged to have emerged from within both China and Russia with an emphasis on using spear-phishing, man-on-the-side, man-in-the-middle and watering-hole attacks to exploit browser, VPN and social-engineering vulnerabilities.[63]

Among these, a 2015 distributed denial-of-service (DDoS) attack, allegedly using an Adobe Flash exploit, was conducted against the website of the Permanent Court of Arbitration at The Hague, while it was adjudicating the Philippines' case against China on the South China Sea.[64] While often considered a nuisance attack to take down systems, this kind of DDoS attack could also have been used to weaken the perimeter of the system to access and to potentially exfiltrate information on the proceedings. While employing different tactics, this incident is similar in nature to a 2015 intrusion and exfiltration 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.[65]

By 2016, the mass theft of data from the Democratic National Committee, reminiscent of the exfiltration of the clearance data of an estimated 25 million US employees from the US Office of Personnel Management discovered in 2015, pointed again to a basic form of cyber intrusion – spear-phishing and remote-access Trojans – as a means of creating domestic crises of confidence, damaged political systems and potential future blackmail.[66] From The Hague to Washington, these cases show organisations and individuals with political and legal significance to Beijing and Moscow finding themselves subject to cyber intrusion and attack.

Similar malware campaigns thought to be emanating from within China and Russia include *Clandestine Fox* and *Russian Doll*, which are both thought to use spear-phishing and Adobe Flash exploits to target aerospace and defence, construction and engineering, high-tech industry, telecommunications and transportation infrastructure.[67] Not only are the tactics and intent behind these campaigns convergent, but they are 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.

That this type of warfare is expanding from simple data exfiltration to kinetic attacks on critical infrastructure was demonstrated in a 2015 cyber attack on electric utilities in Ukraine. Forensic reports on the malware, staging and coordination of the attack suggest that the hackers were either based in or supported by Russia.[68] BlackEnergy malware, used in combination with denial-of-service attacks and the wiping tool KillDisk, not only severed the electricity supply of an estimated 225,000 people, it also created confusion and panic among the provider and users alike. Studies suggest that part of the motivation behind the attack was not simply to test out the ability to comprehensively take down critical infrastructure, but also to cause embarrassment.[69]

So while this particular campaign lasted only four hours and was mitigated in part by the utility's ability to use analogue equipment to restore functionality, it shows that cyber attacks can be used in broader campaigns to cut a population's vital services and to raise questions about the competence of first responders and government. Given the level of penetration of campaigns such as APT30 into Southeast Asia and South Asia, the likelihood of similar tactics reappearing in the Asia-Pacific region is significant.

Even with the improvement of bilateral China–Philippines relations under the leadership of Filipino President Rodrigo Duterte, the level of Chinese involvement in the Philippines' critical infrastructure, including power plants and other facilities,[70] means that there remains the potential for their exploitation in the event of future tensions on the South China Sea. Whether from government entities or patriotic-hacker proxies, campaigns that target society as a whole can supplement the conduct of more conventional military campaigns by supporting not only a shutdown in basic services, but also critical infrastructure from electricity plants to nuclear facilities.[71]

* * *

China's current behaviour and rhetoric does not match the violence of Russia's little green men in Ukraine. Still, government-linked Chinese analysts draw enough parallels between the two countries to suggest that China may take that model and craft it into a more penetrating and per-

sistent campaign. Much as in the case of Moscow's dealings with Ukraine, Beijing has repeatedly pointed to Washington's enabling of China's neighbours. Chinese analysts categorise Beijing's actions in the East China Sea, South China Sea and elsewhere as 'reactive' or 'forced' behaviour driven by American actions.

Both Beijing and Moscow find what the Chinese call a 'dark hand' (*hei shou*) in Washington to be manipulating public sentiment and conditions on the ground in their near abroad. Given the two capitals' solidarity and concerns over American 'interference' (*ganshe*), it should not come as a surprise that China's own tactics increasingly resemble Russia's,[72] and that Chinese analysts have learned from Russian experience.[73] As hybrid warfare in cyberspace develops, little green men on land and little blue men at sea may increasingly be joined by China's little grey men online.

Notes

1 See, for example, Zhang Wenmu, 'Wukelan shijian de guoji yiyi' [International Importance of the Events in Ukraine], in 'Wukelan weiji de zhongguo sikao' [Chinese Reflections on the Ukraine Crisis], *Jingji daokan* [*Economic Herald*], April 2014, pp. 57–67. Zhang Wenmu is a professor in the Center for Strategic Studies at Beihang University, formerly known as the Beijing Institute of Aeronautics.

2 Zhang Yi, 'Wukelan weiji: E ou ying shili yu ruan shili de duijue' [The Ukraine Crisis: Contrasting Russia's and Europe's Hard Power and Soft Power], *Shijie taishi* [*World Perspectives*], pp. 52–4. Zhang Yi is an associate researcher in the Institute of Russian, Eastern European and Central Asian Studies at the Chinese Academy of Social Sciences.

3 Li Ling, 'Zhongguo de fuxing xuyao yici xin qimeng yundong' [China's Emergence Needs a New Enlightenment], in 'Chinese Reflections on the Ukraine Crisis', pp. 66–7. Li Ling is professor in the Institute of Economic Research at Peking University. Xu Zhaofeng, 'Jiedu meiguo 2014 nian 'si nian fangwu pinggu baogao' [Interpreting the United States' 2014 "Quadrennial Defense Review"], *Xiandai guoji guanxi* [*Contemporary International Relations*], May 2014, p. 32.

4 Chinese analysts tend to argue that Beijing's abstention from the UN Security Council vote was a reflection of its responsible attitude and pursuit of peace and stability. Gao Fei and Zhang Jian, 'Wukelan weiji beijing xia de daguo boyi ji qi dui guoji anquan geju de yingxiang' [Great-Power Game Behind the Ukraine Crisis and its Impact on the International

Security Structure], *Heping yu fazhan* [*Peace and Development*], June 2014, p. 97; Dai Changzheng and Zhang Zhongning, 'Guonei youyu xia wukelan weiji de genyuan ji qi yingxiang' [Roots of the Ukraine Crisis in the Domestic Domain and their Impact], *Dongbeiya luntan* [*Northeast Asia Forum*], May 2014, p. 96. Gao Fei is director and Zhang Jian is an assistant researcher at the Russia Research Center at the China Foreign Affairs University, which trains many of China's future diplomats. Dai Changzheng is the head and Zhang Zhongning is a graduate student within the China Institute for WTO Studies of the Institute of International Studies at Beijing's University of International Business and Economics.

5 Chu Maoming, 'Wukelan weiji yu zhongguo de xuanze' [The Ukraine Crisis and China's Options], *Zhanlue juece yanjiu* [*Strategic Decision-Making Studies*], no. 3, March 2014, p. 12. Chu Maoming is a counsellor in China's Ministry of Foreign Affairs and a visiting researcher at the Guangdong Research Institute for International Strategies. See also Liao Qiang, 'Wukelan weiji yinian: Huigu, fansi, yu zhanwang' [One Year of the Ukraine Crisis: A Look Back, Reconsideration, and Prospects], *Eluosi yanjiu* [*Russia Studies*], no. 1, February 2015, pp. 28–58; and Dai and Zhang, 'Roots of the Ukraine Crisis in the Domestic Domain and their Impact', p. 97.

6 See Dai and Zhang, 'Roots of the Ukraine Crisis in the Domestic Domain and their Impact', p. 94; and Jiang Shixue, 'The Ukrainian Quandary', *Beijing Review*, 6 November 2014, pp. 22–3. Jiang Shixue is deputy director of the Institute of European Studies at the Chinese Academy of Social Sciences.

7 Chen Xiaolu, 'Kelimaya shijian dui zhongguo de qishi' [Implications of Crimea Events for China], *Junshi lishi yanjiu* [*Military History Studies*], no. 4, April 2014, pp. 1–12. Chen Xiaolu is head of the South China Sea Research Collaborative Innovation Center and a professor in the Department of History at Nanjing University.

8 Dai and Zhang, 'Roots of the Ukraine Crisis in the Domestic Domain and their Impact', p. 94.

9 CICIR Task Force, '2013 nian eluosi zhanlue xingshi pinggu' [2013 Russia Strategic Situation Assessment], *Eluosi dongou zhongya yanjiu* [*Russia, Eastern Europe, Central Asia Studies*], no. 2, February 2014, pp. 1–9. China Institutes of Contemporary International Relations (CICIR) Task Force members include Feng Yujun, Li Dongfu, Jiang Li, Wang Lijiu, Miao Lijiu, Miao Songfu and Chen Yu. CICIR is among China's largest and most influential civilian research institutes for international studies. It is affiliated with China's Ministry of State Security, which is an intelligence and security agency responsible for counter-intelligence, foreign intelligence and political security.

10 See Wang Xiangsui, 'Cong sange weidu dui weiji zuochu zhengti bawo' [From Three Dimensions of the Crisis Making an Overall Grasp], in 'Chinese Reflections on the Ukraine Crisis', pp. 57–9; and Cao Yongsheng, 'Eluosi dui wukelan qiangying zhanlue muhou

de jige yinsu' [Several Factors Behind Russia's Strong Strategy toward Ukraine], *Zhongguo jun zhuanmin* [*Defense Industry Conversion in China*], 2014, p. 83. Wang Xiangsui is the director of the Center for Strategic Studies at Beihang University. Colonel Cao Yongsheng is a professor in China's National Defense University's Strategic Research Bureau and an expert on Russia.

11 Chen Xulong and Su Shaojun, 'Zhongguo mianlin geng wei fuza de zhoubian he guoji huanjing' [China Faces More Complex Surroundings and International Environment], *Heping yu fazhan* [*Peace and Development*], no. 4, April 2014, pp. 1–10. Chen Xulong is head of the International Strategic Studies Institute at the China Institute of International Studies.

12 'Wukelan de qianshi jinsheng – Zhuanfang zhongguo shehui kexueyuan shijie lishi suo yanjiuyuan wenyi' [Ukraine's Past and Present – Interview with Chinese Academy of Social Sciences World History Researcher Wen Yi], *Lingdao wencui* [*Leadership Digest*], August 2014, pp. 7–22.

13 See, for example, Zhang Wenru, 'Kelimiya: Eluosi de zhengce xuanze' [Crimea's Return: Russia's Political Choice], *Heping yu fazhan* [*Peace and Development*], February 2014, pp. 19–29. Zhang Wenru was a visiting scholar at the Russian Foreign Affairs University at the time of writing this article.

14 *Ibid*., p. 22.

15 Huang Dengxue, 'Xin "lengzhan": Yixiangyi huoshi xianshi – Wukelan weiji beijing xia de emei boyi toushi' [The New 'Cold War': Imagined or Real? – Perspectives on US–Russian Games Under the Ukraine Crisis], *Dongbeiya luntan* [*Northeast Asia Forum*], no. 3, March 2015, pp. 20–30. Huang Dengxue is a professor of Political Science and Public Administration at Shandong University, and a researcher within its Russia and Central Asian Studies Center.

16 Chu, 'The Ukraine Crisis and China's Options', pp. 3–12.

17 The use of the term 'lean' (*yibian dao*) within this writing reflects terminology used to describe countries leaning either towards the United States or the Soviet Union during the Cold War. Bu Shaohua, 'Wukelan weiji, ouzhou xingshi yu zhongou guanxi' yantaohui zongshu' [Summary of a Seminar on 'The Ukraine Crisis, European Trends, and China–Europe Relations'], *Guoji wenti yanjiu* [*International Relations*], January 2015, pp. 132–4; Wang, 'From Three Dimensions of the Crisis Making an Overall Grasp', pp. 57–9; Gao and Zhang, 'Great-Power Game Behind the Ukraine Crisis and its Impact on the International Security Structure', p. 83; Dai and Zhang, 'Roots of the Ukraine Crisis in the Domestic Domain and Their Impact', p. 85. Wang Xiangsui is the director of the Center for Strategic Studies at Beihang University.

18 See Hao Shiyuan, 'Daguo chengchang yu minzu wenti: Zhongguo ji qi guoji bijiao' [Great-Power Growth and Ethnic Issues: China and International Comparison], *Guoji jingji pinglun* [*International Economic Review*], May

2014, p. 14; and Zhang, 'Crimea's Return: Russia's Political Choice', p. 21. Hao Shiyuan is assistant dean of the Chinese Academy of Social Sciences and secretary general of the faculty bureau.

19 See Pan Guoshao, 'Jingguan qibian zhengqu you suo zuowei – Fudan daxue shijie jingji yanjiusuo shen guobing jiaoshou tan wukelan weiji' [Examining Changes and Their Impact on the Ground – Fudan University Institute of World Economics Professor Shen Guobing Discusses the Ukraine Crisis], *Zuguo* [*Motherland*], no. 3, March 2014, pp. 17–8; and Gu Xinyang, 'Diyuan zhengzhi yujingxia de wukelan weiji yu zhongguo jueqi' [Analysis of Ukraine Crisis and China's Rise in Geopolitical Context], *Hefei gonye daxue xuebao (Shehui kexue ban)* [*Journal of Hefei University of Technology (Social Sciences*], no. 4, August 2014, pp. 45–50. Shen Guobing is a professor in Fudan University's Institute of World Economy. Gu Xinyang is affiliated with the College of Humanities and Social Science, Beijing Language and Culture University.

20 Chen Xulong and Su Shaojun, 'Zhongguo mianlin geng wei fuza de zhoubian he guoji huanjing' [China Faces More Complex Surroundings and International Environment], *Heping yu fazhan* [*Peace and Development*], no. 4, April 2014, p. 6.

21 See Yu Zhengliao, 'Jiangou zhongmei xin xing daguo guanxi de jiegouxing zhangai' [Structural Obstacles to Building a China–US New Type of Great-Power Relations], *Mao zedong deng xiaoping lilun yanjiu* [*Mao Zedong and Deng Xiaoping Theoretical Studies*], June 2014, p. 82; and Gao and Zhang, 'Great-Power Game Behind the Ukraine Crisis and its Impact on the International Security Structure', p. 97. Yu Zhengliao is a professor in the International and Public Policy Institute of the Shanghai Communications University.

22 Zhang Wenzong, Xue Wei and Li Xuegang, 'Shixi wukelan weiji de zhanlue yingxiang' ['Analysis of the Strategic Impact of the Ukraine Crisis], *Xiandai guoji guanxi* [*Contemporary International Relations*], no. 8, August 2014, pp. 20, 26. Zhang Wenzong is a research associate at CICIR. Xue Wei is an associate researcher and Li Xuegang is an assistant researcher at the Harbin Institute of World Economic and Trade Research.

23 Cao, 'Several Factors Behind Russia's Strong Strategy toward Ukraine', p. 83; Gao and Zhang, 'Great-Power Game Behind the Ukraine Crisis and its Impact on the International Security Structure', p. 90.

24 In determining the potential for escalation, this statement may also be combined with indications that the United States will separate Cyber Command and Strategic Command, allowing the former greater speed and flexibility of response. See Francois Lenoir, 'Massive Cyber Attack Could Trigger NATO Response: Stoltenberg', Reuters, 16 June 2016, http://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE?m...d1FFaHZNRldGb3BEdo1LQk1QeFprWWxDWVAycTRNdlNLaVU4WToifQ%3D%3D.

25 'Hei tiane xiaoying' yu wukelan weiji yanhua de keneng qingjing' ['Black

Swan Effect' and Possible Scenarios for the Evolution of Ukraine Crisis], *Shijie zhishi* [*World Affairs*], May 2015, p. 53; Gao and Zhang, 'Great-Power Game Behind the Ukraine Crisis and its Impact on the International Security Structure', p. 80.

26 Jiang, 'The Ukrainian Quandry', pp. 22–3; Cao, 'Several Factors Behind Russia's Strong Strategy toward Ukraine', p. 84.

27 Xu Hua, 'Cong wukelan weiji kan eluosi de guoji chuanbo li – Jianyi guoji zhengzhi boyi zhong de chuanbo zhizheng' [The Ukraine Crisis: Russia's Propaganda War – With a Concurrent Comment on the Communication Rivalry in International Political Games], *Eluosi xuekan* [*Russia Journal*], no. 3, March 2015, pp. 61–8.

28 Han Yuhai, 'Nuli kaituo lushang sichou zhilu' [Work Hard to Open the Terrestrial Silk Road], in 'Chinese Reflections on the Ukraine Crisis', pp. 65–7. Han Yuhai is a professor at Peking University.

29 Gao and Zhang, 'Great-Power Game Behind the Ukraine Crisis and its Impact on the International Security Structure', p. 86.

30 She Shaohua, '"Wukelan weiji, ouzhou xingshi yu zhongou guanxi" yanjiuhui zongshu' ['Ukraine Crisis, European Trends and China-Europe' Research Meeting Summary], *Guoji wenti yanjiu* [*China International Relations*], January 2015, pp. 132–4; Dai, 'Roots of the Ukraine Crisis in the Domestic Domain and their Impact', p. 97.

31 Dai, 'Roots of the Ukraine Crisis in the Domestic Domain and their Impact', p. 97.

32 Yu, 'Structural Obstacles to Building a China–US New Type of Great-Power Relations', p. 84.

33 See 'Chinese Reflections on the Ukraine Crisis'; Zhang, 'Crimea's Return: Russia's Political Choice', p. 23; Yu, 'Structural Obstacles to Building a China–US New Type of Great-Power Relations', p. 82; Gao and Zhang, 'Great-Power Game Behind the Ukraine Crisis and its Impact on the International Security Structure', p. 97; Bu, 'Summary of a Seminar on "The Ukraine Crisis, European Trends, and China–Europe Relations"', p. 133; Wang Zhiyuan, 'Baquan yu zhicai: "Eluosi dongyao" nengfou gandong shijie xin pingheng' [Hegemony and Sanction: Can "Russian Turmoil" Shake the New Balance in the World], *Eluosi xuekan* [*Russia Journal*], no. 4, April 2015, pp. 58–68; Liang Qiang, 'Meiguo zai wukelan weiji zhong de zhanlue mubiao-Jiyu meiwu guanxi de fenxi (1992–2014)' [US Strategic Aims in the Ukraine Crisis – Based on US–Ukraine Relations (1992–2014)], *Eluosi dongou zhongya yanjiu* [*Russia, Eastern Europe, Central Asia Relations*], no. 2, February 2015, pp. 10–19; and Chu, 'The Ukraine Crisis and China's Options', p. 7.

34 Zhang, 'International Importance of the Events in Ukraine', pp. 59–62; Yu, 'Structural Obstacles to Building a China–US New Type of Great-Power Relations', p. 83.

35 See US Department of Defense, 'Nuclear Posture Review Report', April 2010; and Air–Sea Battle Office, 'Air-Sea Battle Concept: Service Collaboration to Address Anti-Access

& Area Denial Challenges', May 2013. Air–sea battle has been renamed 'Joint Concept for Access and Maneuver in the Global Commons' (JAM-GC).

36 Chu, 'The Ukraine Crisis and China's Options', p. 7.

37 Han, 'International Importance of the Events in Ukraine', pp. 65–7; Zhao Minghao, '"Qiao touzi" yu "xin gongshi": Aobama de yazhou zhixing' ['Clever Investment' and 'New Offensive': Obama's Trip to Asia], *Dangdai shijie* [*Contemporary World*], June 2014, p. 29; Cao, 'Several Factors Behind Russia's Strong Strategy toward Ukraine', p. 83.

38 Xu, 'The Ukraine Crisis: Russia's Propaganda War – With a Concurrent Comment on the Communication Rivalry in International Political Games', pp. 61–8.

39 Peng Guangqian, 'Lengzhan hou ouya dalu shouci chuxian diyuan zhanlue nixi' [The First Appearance of Geostrategic Counter Attack in Eurasia Following the End of the Cold War], *Jingji daokan* [*Economic Herald*], July 2014, pp. 85–6.

40 Yu Zhonghai, 'Wukelan shouxian zai wangluo bei wajie' [Ukraine First Disintegrated Online], *Lilun daobao* [*Theory Herald*], p. 63.

41 Ge Hanwen and Ding Yanfeng, 'Wukelan minzu zhuyi: Lishi yanjin, zhengzhi suqiu yu jiduan fazhan' [Ukrainian Nationalism: Historical Evolution, Political Demands, and Extreme Development], *Eluosi yanjiu* [*Russian Studies*], no. 3, June 2014, pp. 62–76; Zhang Yanbing and Zeng Zhimin, 'Wukelan weiji ji qi dui zhongguo fazhan de qishi' [The Ukraine Crisis and its Impact on China's Development], *Heping yu fazhan* [*Peace and Development*], no. 1, January 2015, pp. 72–83. Zhang Yanbing is deputy director of the Institute of International Strategies and Development of the School of Public Policy and Management, Tsinghua University; Zeng Zhimin is a graduate student at Tsinghua University.

42 Zhu Zhihua, 'Wukelan weiji beihou zheshe de daguo boyi ji jiaoxun qidi' [Reflections on the Great-Power Game and Lessons Behind the Ukraine Crisis], *Zhanlue juece yanjiu* [*Strategic Decision-making Studies*], no. 6, June 2014, pp. 20–9. Zhu Zhihua is Deputy Director of the Association of Contemporary International Studies.

43 See Fang Xingdong, Pan Feifei, Liu Kaiguo and Zhang Qing, 'Hulianwang zai wukelan chongtu zhong de zuoyong' [The Use of the Internet in the Ukraine Conflict], *Wangshi zongheng* [*Network Latitude*], July 2014, pp. 67–71; and Hu Yong and Li Na, 'Shejiao wangluo yu wukelan kangyi yundong' [Social Networking and the Ukraine Protests], *Shejiao meiti yu gonggong shijian* [*Social Media and Public Events*], no. 6, June 2014, pp. 17–24. Hu Yong and Li Na are affiliated with Peking University's School of Journalism and Communication.

44 See People's Republic of China, 'Zunzhong guojia wangluo zhuquan' [Respect National Network Sovereignty], 17 February 2016, http://www.gov.cn/zhengce/2016-02/17/content_5042042.htm; S.I. Bazylev et al., *The State and Prospects of Russian Military Cooperation on International Information Security* (Moscow: Ministry

of Defense of the Russian Federation, 2014); and Yu Xiaoqiu, '"Xin lengzhan" tiaozhan xia wangluo kongjian de yingdui zhice' [Cyberspace Countermeasures Under 'New Cold War' Conditions], *Guandian* [*Viewpoint*], July 2014, p. 117.

45 Yang Chengjun, 'Cong wukelan jubian kan wangluozhan dui guojia anquan de yingxiang' [From Ukraine's Upheaval Viewing the Impact of Cyber Warfare on National Security], *Zuguo* [*Motherland*], March 2014, pp. 14–15. Yang Chengjun is a professor and researcher within the Army Research Department of the Second Artillery Corps. He has also held affiliations with the Ministry of Foreign Affairs National Security Policy Committee. See also Yu, 'Ukraine First Disintegrated Online', p. 63. The author of this article is a senior fellow within the Unit of Engineers in China's National Security Policy Committee.

46 Jiang Lingfei, 'Miandui shijie luanju, zhongguo yao chenzhuo yingdui' [Facing Chaos in the World, China Should Calmly Confront It], *Dangdai shijie* [*Contemporary World*], May 2014, pp. 19–21.

47 Yu, 'Cyberspace Countermeasures Under "New Cold War" Conditions', p. 117.

48 Fang et al., 'The Use of the Internet in the Ukraine Conflict', p. 69.

49 Yu, 'Ukraine First Disintegrated Online', p. 63.

50 Zhu, 'Reflections on the Great-Power Game and Lessons Behind the Ukraine Crisis', p. 28.

51 *Ibid*., p. 28.

52 Yu, 'Ukraine First Disintegrated Online', p. 63.

53 Fang et al., 'The Use of the Internet in the Ukraine Conflict', p. 71.

54 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, 'The Ukraine Crisis and China's Options', p. 11.

55 See Chu, 'The Ukraine Crisis and China's Options', p. 11; Zhang Jinying and Nan Weihua, 'Qiangjun xingjun shi zhongguo jundui de weiyi xuanxiang – Wukelan dongyao de fansi' [Building a Powerful Army Is the Only Option for the Chinese Military – Reflections on Ukraine's Turmoil], *Junshi zhengzhi xue yanjiu* [*Military Political Study*], no. 1, January 2014, pp. 146–9; and '2015 Zhongguo guofang baipishu (Zhongguo de junshi zhanlue) (Quanwen)' [2015 China's National Defence White Paper (China's Military Strategy) (Complete Text)], *Zhongguo ribao* [*China Daily*], 26 May 2015, http://world.chinadaily.com.cn/2015-05/26/content_20821000.htm. Zhang Jinying is affiliated with PLA Unit 69223 as a deputy political teacher and as a PhD candidate at Xi'an's Political School. Nan Weihua is a military training instructor at the Border Defense College.

56 See 'Chinese Pressure Sees Pakistan Mull Constitutional Status of Gilgit-Baltistan', *Express Tribune*, 7 January 2016, http://tribune.com.pk/story/1023523/chinese-pressure-sees-pakistan-mull-constitutional-status-of-gilgit-baltistan; Luisa

Lam, 'The Thugs of Mainland China', *New Yorker*, 8 October 2014, http://www.newyorker.com/news/news-desk/thugs-mainland-china-hong-kong-protests; Tom Porter, 'Hong Kong: "Hired Triad Thugs Attacked Demonstrators", Claims Legislator', *International Business Times*, 4 October 2014, http://www.ibtimes.co.uk/hong-kong-hired-triad-thugs-attacked-demonstrators-claims-legislator-1468529; Peter Popham and James Legge, 'Beijing Allegedly Call Hired Thugs to Incite Hong Kong Riots', *Morning Bulletin*, 4 October 2014, http://www.themorningbulletin.com.au/news/beijing-allegedly-call-hired-thugs-incite-hong-kon/2408957/#/0; Megha Rajagopalan, 'China Trains "Fishing Militia" to Sail into Disputed Waters', Reuters, 30 April 2016, http://www.reuters.com/article/us-southchinasea-china-fishingboats-idUSKCN0XS0RS; James C. Bussert, 'Chinese Maritime Assets Enforce Ocean Territorial Claims', *Signal*, 1 July 2014, http://www.afcea.org/content/?q=chinese-maritime-assets-enforce-ocean-territorial-claims; and Paul J. Leaf, 'Learning From China's Oil Rig Standoff With Vietnam', *Diplomat*, 30 August 2014, http://thediplomat.com/2014/08/learning-from-chinas-oil-rig-standoff-with-vietnam.

57 Wang Zhijun and Zhang Yaowen, 'Xifang diyuan zhanlue lilun pipan yu zhongguo diyuan zhanlue lilun goujian' [Critique of Western Geostrategic Theory and Construction of China's Construction Geostrategic Theory], *Xueshu tansuo* [*Academic Exploration*], Issue 2, February 2015, p. 32. Wang Zhijun is a professor, and Zhang Yaowen is a lecturer, at the Nanjing Army Command College.

58 Based on a panel moderated by Dr Lora Saalman on 'Cyber Security and Arms Control' at Tsinghua University's 2016 Annual Conference of the Chinese Community of Political Science and International Studies. See also 'San yue guoji wangluo he xinxi anquan fazhan dongtai' [March International Networks and Information Security Developments], *Xinxi anquan yu tongxin baomi* [*Information Security and Communications Privacy*], no. 4, April 2014, pp. 14–17.

59 Chen Hongchao, Duan Benqin and Li Tao, '21 shiji zhanzheng xin gainian – Wangluo zhan' [New Concept of Wars in the Twenty-First Century – Network War], *Junshi tongxin jishu* [*Journal of Military Communications Technology*], no. 4, April 2001. Chen Hongchao, Duan Benqin and Li Tao are affiliated with the 1st Military Representatives Office of the Communication Division of PLA General Staff Headquarters in Tianjin.

60 Yu Zhonghai, 'Ukraine First Disintegrated in Cyberspace', p. 63; Ma Liangli, Wu Qingzhi, Su Kai and Ren Wei, *Wulianwang ji qi junshi yingyong* [*The Internet of Things and Its Military Applications*] (Beijing: National Defense Industry Press, 2014), p. 187; Zheng Ruobing, *Junshi xinxi anquan lun* [*Military Information Security Theory*] (Beijing: National Defense Industry Press, January 2013), p. 101; Tang Yueping, Zhao Weifeng, Yu Maizheng, Sun Jian, Han Ping and

Tang Shaoqing, *Keji xinxi yun fuwu ji junshi yingyong* [*Science and Technology Information of Cloud Services and Military Application*] (Beijing: National Defense Industry Press, January 2015), p. 258; Song Zhongping, *Daguo wuqi* [*Major Power Weapons*] (Beijing: New World Press, September 2013), p. 140.

61 See 'APT30 and the Mechanics of a Long-Running Cyber Espionage Operation: How a Cyber Threat Group Exploited Governments and Commercial Entities across Southeast Asia and India for over a Decade', FireEye, April 2015, https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf; and Bryan Krekel, Patton Adams and George Bakos, 'Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage', Northrop Grumman Corporation, 7 March 2012, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf.

62 Countries thought to have been compromised by the APT30 campaign include Bhutan, Brunei, Cambodia, India, Indonesia, Japan, Laos, Malaysia, Myanmar, Nepal, Philippines, Saudi Arabia, Singapore, South Korea, Thailand, the United States and Vietnam.

63 Spear-phishing is email fraud that targets an individual or organisation to gain unauthorised 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.

64 'Nation-State Sponsored Cyberwarfare Campaign', TruShield, 2 November 2015, https://trushieldinc.com/wp-content/uploads/2015/11/TS_Advisory_11022015_AD.pdf.

65 Feike Hacquebord, 'Pawn Storm Targets MH17 Investigation Team', TrendMicro, 22 October 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/.

66 See Max Fisher, 'Why Security Experts Think Russia Was Behind the D.N.C. Breach', *New York Times*, 26 July 2016, http://www.nytimes.com/2016/07/27/world/europe/russia-dnc-hack-emails.html; 'Here's What We Know about Russia and the DNC Hack', *Wired*, 27 July 2016, https://www.wired.com/2016/07/heres-know-russia-dnc-hack; and 'OPM Breach Analysis', *Threat Connect*, 2015, https://www.threatconnect.com/blog/opm-breach-analysis-update.

67 'Pinpointing Targets: Exploiting Web Analytics to Ensnare Victims', FireEye, November 2015, https://www2.fireeye.com/rs/848-DID-242/images/rpt-witch-coven.pdf.

68 'Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case', SANS Institute Industrial

Control Systems, Electricity Information Sharing and Analysis Center, 18 March 2016, pp. 1–23, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

69 *Ibid*.

70 Based on not-for-attribution conversations with a Philippines expert at the Daniel K. Inouye Asia-Pacific Center for Security Studies in 2016.

71 The discovery in 2010 of the use of the Stuxnet worm against Iran's nuclear facility at Natanz to cause damage to its centrifuges was among the first harbingers of the kinetic role of a cyber attack against critical infrastructure.

72 For more information, see Lora Saalman, 'Pouring "New" Wine into New Bottles: China–U.S. Deterrence in Cyberspace', *Seton Hall Journal of Diplomacy and International Relations*, Fall/Winter 2015.

73 Hu Hao, 'Eluosi lianbang anquan huiyi de lishi yanjin ji dui zhongguo de qishi' [Evolution of the Russian Federation Security Council and Its Implications for China], *Guoji anquan yanjiu* [*International Security Studies*], no. 5, May 2014, pp. 3–15.