Military Cyber Affairs
The Journal of the Military Cyber Professionals Association
ISSN: 2378-0789

Volume 2 | Issue 1 Article 5

2016

People's War in Cyberspace: Using China's Civilian Economy in the Information Domain

Kieran Richard Green
Tufts University, kieran.green@gc.ndu.edu

People's War in Cyberspace: Using China's Civilian Economy in the Information Domain

Cover Page Footnote
The author would like to thank Dr. Alex Crowther for his guidance in producing this manuscript.

People's War in Cyberspace:
Using China's Civilian Economy in the Information Domain

KIERAN RICHARD GREEN, Tufts University

China is identified as posing a key challenge to US national security interests in cyberspace. These threats are incurred across the spectrum of conflict, ranging from low-level crime, to network penetration, to cyberattacks that have the potential to cause major physical destruction. Thus far, the majority of strategic assessments of China's cyber capabilities have focused on the role of the People's Liberation Army (PLA), which is officially tasked with undertaking offensive operations in cyberspace.[1] However, China does not employ its cyber capabilities in isolation. Rather, it considers cyber to be part of the "Information Domain." In Chinese doctrine, controlling the information environment entails the combined use of network, electromagnetic, intelligence, and propaganda assets in both the civilian and military spheres in conjunction with the other elements of national power to achieve strategic objectives. Consequently, over the past two decades, China has adopted a policy of augmenting its information warfare (IW) capabilities by leveraging the civilian sector (notably private institutions, academia, and civilian government institutions). This paper provides a broad survey of China's cyber auxiliary capabilities and assesses how China uses its civilian economy as a "strategic reserve" in all four areas of the Information Domain.

[1] US Naval War College, "China and Cybersecurity: Political, Economic, and Strategic Dimensions," USNWC Study of Innovation and Technology in China [2012] pg. 4-8

1. Strategic Background: the Information Domain as part of "Warfare by Other Means"

In order to understand China's approach to the Information Domain, it is important to examine the evolution of China's geopolitical strategy. Since the 1980's, China has adopted a policy of avoiding direct confrontation with the West. This approach is neatly encapsulated by Deng Xiaoping's injunction that China should "hide its strength and bide its time" when dealing with potential adversaries.[1] The Central Military Commission amended this strategy in 2003 when it concluded that its kinetic assets were of limited utility, and instead opted for a strategy of achieving its objectives via "warfare by other means."[2] Dubbed the "Three Warfares" approach, this strategy seeks to jointly exercise all elements of national power (diplomatic, informational, military, and economic) in order to shape behavior of other nations.[3][4] Specifically, the term "Three Warfares" refers to the use of legal, propaganda, and media operations to degrade the political will of China's opponents without resorting to kinetic force.[5] As part of this effort, China has identified the Information Domain as being the strategic "center of gravity" in any eventual conflict with the United States.[6] Viewed in this context, China's military, propaganda, and intelligence apparati are not separate instruments. Rather, they are components of an information structure designed to support the strategy of undermining the United States' ability

[1] Global Security, "Deng Xiaoping's 24-Character Strategy" globalsecurity.org [2010] accessed 6/29/16
[2] Halper, Stefan, "China: The Three Warfares" Office of Net Assessment, Office of the Secretary of Defense [2013] pg 11
[3] Ibid. pp 12-13
[4] Bajwa, JS, "Defining Elements of Comprehensive National Power" *Center for Land Warfare Studies* Journal [2008] pp. 151-153
[5] Cheng, Dean, "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response" Heritage Foundation Backgrounder #2745 on Asia and the Pacific [2012]
[6] Costello, John, "Chinese Views on the Information 'Center of Gravity:' Space, Cyber, and Electronic Warfare," *China Brief* Volume 15 Issue 8

to safeguard the global commons.[7] The maintenance of sophisticated standoff capabilities ensures that any interference with Chinese interests becomes a high-risk, low-reward affair. Taken one step further, it can be argued that China's practices of conducting industrial espionage, its policy of exercising control of the electronic domain within China's geographical borders, and its attempts to shape the cognition of its citizenry are all part of a concerted attempt to bolster China's leverage in conducting information operations. Additionally, Chinese control of its domestic Information Domain denies the use of IW to its opponents.

In practice, China's IW strategy dictates a constant state of enhanced cyber readiness. The PLA routinely conducts reconnaissance and penetration of American networks.[8] These "Intelligence, Surveillance and Reconnaissance" (ISR) and "Operational Preparation of the Environment" (OPE) operations do not imply that the Chinese leadership views conflict as being inevitable or even likely. Rather, China's stance draws comparison to the United States' and the Soviet Union's strategies during the Cold War, when both sides' intelligence and military apparatus constantly maneuvered to ensure a favorable position if conflict broke out.[9] As a result, the PLA has worked to develop an integrated approach to warfare in order to achieve its political objectives in a world largely dominated by the US and its allies. In this framework, China uses non-kinetic capabilities to support its conventional forces, employing diplomacy and the threat of force to isolate and divide its opponents.[10]

2. Civil-Military Integration in the Information Domain: a Combined Effort

Though Western attention has been focused primarily on China's military cyber capabilities (especially those that target critical infrastructure), those capabilities comprise only a part of China's information warfare strategy. Indeed, one of the hallmarks of China's cyber strategy is the degree to which it integrates their civilian economy into its approach to the Information Domain. In all four components of the Information Domain, the PLA routinely coordinates with parts of the civilian economy to use it as a "force multiplier." These informal capabilities do not have an official place within the PLA's order of battle.[11] From an outsider's perspective, it seems that China's informal cyber capabilities are little more than a loose association of government workers, criminal organizations, and patriotic hackers that can be grouped together under the umbrella term of "cyber auxiliaries." Upon further examination, however, these cyber auxiliaries comprise a critical component of China's cyber forces.

From a civil military perspective, Chinese Communist Party (CCP) cooperation with the civilian economy can be split up into to broad categories: absorption and integration. Of the two concepts, absorption is the more straightforward. It entails the direct recruitment of talented civilians to work directly for the PLA, Ministry of State Security (MSS), Office of Propaganda, etc.[12] Integrated groups can be broadly defined as personnel working in the civilian sector whom the government can call upon to perform IW tasks when necessary. Using integrated civilian units provides several advantages for the PRC. First, it enables the government to tap into

[7] US Naval War College, "China and Cybersecurity: Political, Economic, and Strategic Dimensions," pp 20-33
[8] Ibid. pp. 3-8
[9] Costello, John, "China's Irregular Warfare in the Cyber Domain," Real Clear Defense [2015] Accessed 6/29/2016
[10] Chase, Michael S., Chan, Arthur, "China's Evolving Approach to 'Integrated Strategic Deterrence'" RAND Corporation, [2016] pp. 9-19
[11] Sheldon, Robert, & McReynolds, Joe, "Civil-Military Integration and Cybersecurity," *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain."* Oxford University Press 2015 pp 190-193
[12] Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" pp. 40-45

DOI: http://doi.org/10.5038/2378-0789.2.1.1022

civilian expertise that it may otherwise have been unable to access due to an inability to compete with private sector wages. Second, it allows the government to dramatically expand its manpower resources when necessary, without having to put the economy on a wartime footing. Third, it facilitates technology transfers to government agencies (most notably the PLA and state-owned enterprises) and helps its modernization process.

China's cyber auxiliary force can be further divided into two groups: personnel that are subordinated to the PLA (so-called "cyber militias") and personnel that are subordinated to other agencies (most notably the Ministry of State Security, the Publicity Department of the CCP, and the State Security Bureau). These subordinate elements share a common organizational structure and common goal. China's IW strategy incorporates both military and non-military personnel, just as China's grand strategy calls for use of all elements of national power via both civilian and military organizations. In all cases, these elements of the civilian economy represent a "strategic reserve" that the Chinese government can call upon to support both the CCP and PLA in the Information Domain. Hence, for the purpose of this paper, a "cyber auxiliary" is defined as having four basic characteristics. To define an organization as cyber auxiliary, it must:

- Be part of the civilian peacetime economy
- Have the capacity to be mobilized in times of crisis
- Be highly responsive to orders
- Have a mission that can be described as fulfilling one or more of the four components of information warfare (the network, electromagnetic, psychological, and intelligence domains).

Historically, China has extensively employed civilian auxiliary forces as a means of internal defense and policing. During the Cold War, local militias were a key component of Mao's concept of "People's War" (人民战争).[13] After 1978, these militias decreased in importance as the PLA modernized and professionalized.[14] Nevertheless, the government still routinely called upon militias to provide both air and maritime defense.[15] Following the conclusion of the Gulf War, the PLA conducted an extensive internal review and modernization process as part of the "Revolution of Military Affairs."[16] As part of this process, the PLA significantly strengthened China's IW capabilities. During the late 90's and early 2000's, Chinese IW capabilities were still in their nascent stage, so Chinese nationals routinely conducted operations with comparatively little oversight or guidance from the CCP. For example, following the Belgrade embassy bombings in 1999, numerous US government websites incurred large-scale distributed denial of service (DDOS) attacks from Chinese patriotic hacking groups.[17] This episode was mirrored in 2001 after a collision between a US Navy aircraft and a Chinese interceptor aircraft. For several weeks after the incident, Chinese and American hackers exchanged numerous attacks, defacing websites and shutting down web infrastructure before a

[13] Zedong, Mao, "On Protracted War" From the Selected Works of Mao Tse-tung," Foreign Language Press, pp 113-174

[14] Bo, Zhiyue, "The PLA and the Provinces: Military District and Local Issues," Civil-Military Relations in Today's China: Swimming in a New Sea," Edited by David M. Finkelstein and Kristen Gunness, CNA Corporation [2007] pp. 96-130

[15] Sheldon, Robert, & McReynolds, Joe, "Civil-Military Integration and Cybersecurity," pp. 193-195

[16] Stokes, Mark, "China's Strategic Modernization: Implications for the United States" United States Army War College Strategic Studies Institute pp. 12-13

[17] Krekel, Bryan, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" *US-China Economic and Security Review Commission*, Prepared by Northup Grumman [2009] pp 67-69

truce was eventually called.[18] The Chinese government initially encouraged these adventures, but by 2002 the CCP began to rein in these freelancers while simultaneously replacing them with auxiliaries dedicated to information warfare.[19] Patriotic hackers were either "absorbed" into the PLA through recruitment, or integrated through the militia system.[20]

Today, China's cyber auxiliaries comprise part of the PLA's 8-million man militia system, as well as part of the forces of other PRC agencies.[21] Though open source information on the exact functions of IW auxiliaries is rare, it appears that units are recruited from and organized as "cells" within government, telecommunications and academic institutions.[22] These units are interfaced to operate cooperatively with China's government to achieve their national security objectives. The lack of open-source information on the organizational structure of China's cyber auxiliaries ensures that any understanding of their function will remain incomplete and ever-evolving. Hence, the following provides a snapshot of how the West understands China's cyber auxiliaries.

3. Shaping Cognition: Propaganda and Information Operations

One of the bedrock components of China's cyber strategy is its approach to information operations and information warfare. According to China's 2015 defense white paper, the PLA is devoting considerable resources to "informationizing" its forces.[23] Operationally this is not limited to ensuring access to intelligence and military deception operations. Instead, the PRC views controlling information inflows and outflows as critical component of ensuring China's national security. Suppression of potentially damaging information has allowed the Chinese Communist Party to eliminate dissent, while the use of information operations abroad has enabled it to limit the political options of external adversaries. Thus, the PRC undertakes "information operations" to give it the greatest degree of flexibility in achieving its strategic objectives. From a political warfare perspective, control of public discourse allows the PRC to protect its informational "strategic rear area." This attitude is summarized in a report from the Center for the Study of Intelligence:

> "What Beijing really appears to be aiming for is creation of the capacity to create a panoptic state, a capacity that goes beyond what normally is thought of as domestic intelligence. In the CCP's leading journal, China's senior leader responsible for security and stability, Zhou Yongkang, laid out the desired "social management system" (shehui guanli tixi), which he said would include integrating MPS (the Ministry of Public Security) intelligence with public opinion monitoring and propaganda to shape people's decision making about appropriate actions in the public sphere"[24]

The PRC routinely uses cyber auxiliaries in disseminating propaganda to shape the cognition of its populace as well as the public opinion of foreign nations. These posters have

[18] Anderson, Kevin, "'Truce' in US-China Hacking War" British Broadcasting Corporation Asia-Pacific, [2001] accessed 6/26/16
[19] Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" pp 33-37
[20] Ibied. Pg. 38
[21] Information Office of China's State Council, "China's National Defense in 2004," *Information Office of the State Council of the People's Republic of China"* [2004]
[22] Sheldon, Robert, & McReynolds, Joe, "Civil-Military Integration and Cybersecurity," pp. 212-215
[23] State Council Information Office of the People's Republic of China, "China's Military Strategy" Chinese Ministry of National Defense, [2015]
[24] Mattis, Peter, "The Analytic Challenge of Understanding Chinese Intelligence Services" CIA Library Center for the Study of Intelligence pp. 50-51

DOI: http://doi.org/10.5038/2378-0789.2.1.1022

become known colloquially as the "50 Cent party" " (五毛党), who are tasked with engaging citizens online and spreading pro-government messaging, collectively producing over 448 million posts per year.[25] 50c posters are technically subordinated to the State Council Information Office (国务院新闻办公室). Unlike the US and other Western entities, the PRC does not consider cyber capabilities to be a distinct domain (along with land, sea, and air power).[26] Instead, cyber operations are nested within the broader concept of the "Information Domain".[27] Hence China's "civilian" propaganda apparatus is central to the PLA's IW strategy. Initially, it seemed that paid freelance commentators conducted this "internal messaging".[28] However, more recent analysis of leaked documents from the Zhagong Information Ministry has concluded that government workers conduct most 50c posting as part of their jobs.[29] 50c posters are generally employed as a "strategic distraction" by the Chinese government.[30] They generally do not engage directly with anti-government posters, but instead seek to spread pro-government messaging. These efforts are coordinated by the CCP to "surge" in volume to highlight pro-CCP events (such as the Martyr's Day festival) or to distract from politically damaging incidents (such as the Urumqi rail explosion).[31]

Taken in a broad strategic sense, 50c posting serves two main purposes. First, it reinforces the credibility of the regime by propagating ersatz favorable grassroots coverage (otherwise known as "astroturfing"). Second, they seek to deny and pre-empt collective action that could threaten the stability of the regime. Though it would be easy to dismiss this as serving an internal policing function, China has routinely employed 50c posting in conjunction with its censorship regime to maintain strict control over China's informational "center of gravity" which is of vital importance when encouraging or discouraging calls for Chinese engagement abroad. This approach was displayed prominently during the 2012 Senkaku/Diaoyu island dispute. During this period, the CCP engaged in "selective censoring" to "dial up" or "dial down" anti-US and anti-Japanese sentiment, depending on the political needs and objectives of the government.[32] Unofficial (e.g. 50c) channels can further augment this "official" messaging approach. The unofficial channels are used to "flood the zone" of social commentary, effectively shaping the content of public debate.[33] [34] [35] If we extrapolate this model further, it is likely that

[25] King, Gary, Pan, Jennifer, & Roberts, Margaret, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument," Institute for Quantitative Social Science, Harvard University Press [2016]
[26] Costello, John, "The Strategic Support Force: China's Information Warfare Service," The Jamestown Foundation, [2016]
[27] Sheldon, Robert, & McReynolds, Joe, "Civil-Military Integration and Cybersecurity," pg. 197
[28] Bristow, Michael, "China's Internet 'Spin Doctors" British Broadcasting Company (BBC) [2008] accessed 6/26/2016
[29] King, Pan, & Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument," pp 19-22
[30] Ibid. pp 26-27
[31] Ibid. pg. 11
[32] Cairns, Christopher, Carlson, Allen, "Real-world Islands in a Social Media Sea: Nationalism and Censorship on Weibo during the 2012 Diaoyu/Senkaku Crisis," *The China Quarterly*, [2016] pp. 29-40
[33] Report to Congress, "US-China Economic and Security Review Commission, "One Hundred Eleventh Congress First Question," [2009] pg 282
[34] Feng, Miao, & Yuan, Elaine J. "Public Opinion on Weibo: The Case of the Diaoyu Islands Dispute," University of Illinois, Chicago [2013]
[35] King, Pan, & Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument," pp 29-32

China, in any future geo-political conflict, will have the option of leveraging this cyber auxiliary force in conjunction with its state censorship to prevent subversive activity.

In addition to securing the CCP's domestic base of support, cyber militias also play a role in China's strategy of shaping opinion abroad. Since connectivity between the Chinese web and the West is rather limited, this practice has not been refined to the degree that it has been in Russia, where Information Warfare is routinely employed as part of Russian Political Warfare strategy.[36] [37] Nevertheless, China does employ an extensive propaganda apparatus abroad to positively shape external perceptions of the Chinese government, as well a part of their broader "information warfare" strategy, which generally seeks to portray Chinese involvement abroad as being benevolent and justified. To achieve this, the Chinese use official media such as China Central Television (CCTV) and academic institutions such as Confucius Institutes, the Chinese People's Association for Friendship with Foreign Countries (CPAFFC), and the China Institutes of Contemporary International Relations (CICIR) which are all dedicated towards enhancing China's "soft power abroad."[38] [39] In some cases, such as that of CICIR, these organizations have direct ties to Chinese Intelligence (CICIR reports directly to the Ministry of State Security).[40] All of these organizations are designed to counter what the Chinese government views as an informational "siege" of China.[41] The 2015 military strategy paper specifically cites foreign instigated "color revolutions" as being one of the foremost threats to Chinese national security.[42] Taken at face value, this fits in with existing Chinese doctrine regarding the vital need for control over the Information Domain. Whereas the West conceptualizes the free flow of information as being inherently apolitical, China (along with other non-liberal powers such as Russia and Iran) views the free flow of information as a tool of Western subversion, and posit that the United States in particular enjoys "information dominance" within the global press. Consequently, in official documents released by the CCP, media is regarded as a "weapon" that can be used to conduct "defense, confrontation, and counterattacks" against perceived incursions from the Western media.[43]

Though auxiliaries contribute to a significant part of China's information operations strategy within Chinese networks, their role outside official Chinese networks is less clear. It is relatively rare to find references to 50c posting outside the Chinese-language internet. Though this is merely speculation on the part of the author, it is probable that posters with valuable English and foreign language skills would seek alternative forms of employment, rather than comparatively low-paying government employment. There has also been speculation that China's government has lent its tacit support to "patriotic hacking groups" such as the Honkers Union (红客联盟) which has targeted and defaced numerous media outlets in the United States,

[36] Darczewska, Jolanta, "The Anatomy of Russian Information Warfare" Centre for Eastern Studies (Ośrodek Studiów Wschodnich), [2014]
[37] Sindelar, Daisy, "The Kremlin's Troll Army," The Atlantic, 2014, accessed 6/27/16
[38] Inkster, Nigel, "China's Cyber Power: Policy, Capability, and Exploitation," International Institute for Strategic Studies [2016]
[39] Volodzko, David, "China's Confucius Institutes and the Soft War," The Diplomat (online publishing), 2015 accessed 6/27/16
[40] Open Source Center, "Porfile of MSS-Affiliated PRC Foreign Policy Think Tank CICIR," Open Source Center Report, [2011]
[41] Report to Congress, "US-China Economic and Security Review Commission pp 293-294
[42] State Council Information Office of the People's Republic of China, "China's Military Strategy" Chinese Ministry of National Defense, [2015]
[43] Ibid. pg. 293

DOI: http://doi.org/10.5038/2378-0789.2.1.1022

Vietnam, Taiwan, and the Philippines.[44] [45] [46] The CCP, however, has largely tried to distance itself from these groups, and has attempted to tamp down destabilizing ultra-nationalist sentiment.[47] [48] [49] Hence, for the time being traditional government institutions will take the lead in China's psychological and media operations abroad. This role may change in the future, as China's internet user base continues to grow and become more integrated with the West, creating a larger talent base that the Chinese government could employ to mold Western thinking. In the future Chinese social media operations may develop according to the Russian model, wherein state-run media outlets generate content, which paid commentators and trolls then distribute. Indeed propaganda materials released by the Chinese government have become increasingly well suited to the internet age, using catchy and memetic messaging to appeal to a broader potential audience.[50] [51] [52]

4. Intelligence Domain

Operating concurrently with China's psychological operations apparatus is their intelligence apparatus. This apparatus can be roughly divided in three parts. The first is intelligence gathering that is undertaken by the PLA. In the cyber realm, these actions are undertaken by the PLA's General Staff 2nd Department which handles Human Intelligence Operations (HUMINT) and 3rd Department which handles Signals Intelligence (SIGINT and Computer Network Operations (CNO).[53] Operationally, their activities include going after traditional military and intelligence targets (such as the 2015 Office of Personnel Management hack), as well as cyber reconnaissance or OPE of the cyber environment.[54] [55] The PLA has also been widely accused of facilitating the theft of intellectual property (IP) to provide support for Chinese state-owned enterprises (SOEs).[56] These accusations, coupled with substantial factual evidence eventually led to the Department of Justice indicting five PLA members on charges of cyber espionage in 2014.[57] [58] In part due to this policy of "naming and shaming" as well as a 2015 agreement

[44] Malig, Jojo, "Chinese Hackers Target more PH Websites, " ABS-CBN News, [2012] accessed 6/27/16
[45] East-West Military Affairs, "中国红客反攻战果累累: 越南溃不成军向美国求援' 西沙存方军事 [2011] accessed 6/27/16
[46] Hunt, Katie, and Lu, Shen, "Facebook Trolling, Military Drills: China Responds to Taiwan's New President," CNN Online [2016] Accessed 6/27/16
[47] BBC, "China Denies Spying Allegations," British Broadcasting Company online [2009] Accessed 6/27/16
[48] Cairns, &, Allen, "Real-world Islands in a Social Media Sea: Nationalism and Censorship on Weibo during the 2012 Diaoyu/Senkaku Crisis," pp 26-29
[49] Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" pp. 40-41
[50] Wertime, David, Allen-Ebrahimian, Bethany, "China Takes Teen-Friendly Tack in South China Sea Propaganda Video" Foreign Policy [2016]
[51] Flanagan, Ed, "China's Five-Year Plan Extolled in New Animated Propaganda" NBC News, [2015]
[52] Leng, Shujie, "The Chinese Military's Awkward New Recruitment Video," Foreign Policy Magazine, [2014]
[53] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units" Mandiant, [2013] pp 6-8
[54] Davis, Jlie Hirschfeld, "Hacking of Government Computers Exposed 21.5 Million People," The New York Times, [2015] accessed 6/27/2016
[55] Kania, Elsa, "The Latest Indication of the PLA's Network Warfare Strategy," Jamestown Foundation, China Brief Volume 15 Issue 24 accessed 6/28/16
[56] Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," Report to Congress on Foreign Economic Collection and Industrial Espionage, Security Counterintelligence [2011] pp. 2-11
[57] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units" pp 2-19
[58] Department of Justice, "US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage" DOJ Office of Public Affairs [2014]

between Presidents Xi Jinping and Barack Obama, industrial espionage from the PLA has significantly decreased.[59]

The second component of China's intelligence collection apparatus is comprised of its civilian element. These operations are conducted primarily by China's Ministry of State Security, which focuses on internal state security, counterintelligence, and "safeguarding the country."[60] [61] Functionally, the MSS is charged with countering intelligence operations and collecting information on individuals and firms working within China.[62] Both the Ministry and 2/PLA are also charged with monitoring Chinese nationals living abroad.[63] MSS has also been accused of maintaining a substantial cyber espionage capacity.[64] The MSS, however, has since ramped down this capacity.[65]

The third component of China's intelligence apparatus consists of operators who are not employed directly by the PLA or the MSS, but which still are used to gather information. These include civilian cybersecurity consultants, criminal organizations, PLA/MSS operators "moonlighting" in the private sector, and the aforementioned cyber militias that are drawn from private entities and academia. Neither the PLA nor MSS have publically disclosed the organizational structure or specific functions of their cyber militias. It is possible that their function is simply folded into the responsibilities of other "information warfare" subunits. If that is the case, IW militias could potentially be used to perform network reconnaissance, penetration and other espionage activities to supplement 3/PLA. However, it is unlikely that these groups would be relied upon to conduct sensitive espionage, given that "militia" hackers would have less expertise than their PLA and MSS counterparts, and are thus more likely to be caught. Simultaneously pursuing a strategy of "state-sponsored" and "unofficial" network espionage opens up operations to unnecessary risk. Poorly executed network operations initiated by a militia could undermine more effective PLA professional efforts undertaken to extract information from the same target network.[66] It is possible that cyber militias could conduct network reconnaissance and espionage during times of conflict (when stealth is less imperative and bulk collection is preferred).[67] However, since the PLA has not faced large-scale war in the past couple decades, the exact scope of this militia capability has not yet been demonstrated. Nevertheless, IW militias have been employed to conduct operations that are outside the traditional scope of espionage. This usually takes the form of industrial espionage conducted on behalf of state-owned enterprises. In the recent past, collection on foreign corporations was conducted by state-controlled intelligence units, such as PLA Unit 61398.[68] However, increased

[59] Lynch, David J, & Dreyer, Geoff, "Chinese Hacking of US Companies Declines, *Financial Times,* [2016] accessed 6/28/16
[60] Global Security, "Ministry of State Security [MSS] (国家安全部)" Global Security [1997]
[61] Eftimidiades, Nicholas "Chinese Intelligence Operations" Naval Institute Press ch. 6
[62] Mattis, Peter, "The Analytic Challenge of Understanding Chinese Intelligence Services" CIA Library Center for the Study of Intelligence pp 47-53
[63] Ibid. pp. 48-50
[64] Iasiello, Emilio, "Ramping Down Chinese Commercial Cyber Espionage," *Foreign Policy Journal*
[65] Ibid.
[66] Sheldon, Robert, & McReynolds, Joe, "Civil-Military Integration and Cybersecurity," pp. 201
[67] Krekel, Bryan, Adams, Patton, Bakos, George, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage" Security Review Commission Northrup Grumman Corp [2012] pp 50-54
[68] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units" pp 7-11

DOI: http://doi.org/10.5038/2378-0789.2.1.1022

international scrutiny has induced the PLA to scale back its targeting of foreign companies.[69] As external pressure forces the PLA to choose its targets more selectively to avoid detection, more industrial espionage may be "farmed out" to auxiliary cyber units or subcontracted through civilian or criminal entities. "Cyber privateers" may become an increasingly enticing and useful proxy for industrial espionage, offering both a high degree of expertise in addition to plausible deniability for the CCP.[70]

5. Network Domain

The PLA also maintains a sizable militia component dedicated toward network exploitation and maintenance. These are generally civilian specialists who have a high degree of technical expertise who do not function as reservists or members of the PLA, but who nevertheless regularly interface with the PLA through "militias" organized within Internet Service Providers (ISPs), telecommunications companies, city municipalities, etc. From a technical standpoint these organizations fulfill two main functions. First, as a peacetime force, cyber militias act as important civil-military "nodes" for the PLA to facilitate technology transfers from the private sector. They also serve as a talent pool for network expertise.[71] This integration also serves to augment the PLA's stated mission of modernization, insourcing technical expertise from the civilian economy that it may otherwise have been unable to access.[72] Additionally, Chinese media references cyber militias providing technological support to branches of the PLA (such as the PLA Strategic Support Force and the PLA Rocket Force) during military exercises, indicating that the PLA conducts "integration" of PLA units to support peacetime operations in addition to "absorption" of talent from the private sector.[73]

The second main role of cyber militias is to act as a "reserve component force" in the event of a conflict. Under this framework, China's existing "Information Warfare Complex" incorporated Chinese civilian telecom companies."[74] Currently the PLA does not rely upon reserve and militia components to conduct peacetime CNO operations. This is likely because these network operations are highly sensitive and liable to be compromised by inexperienced or unscrupulous militia workers working outside the immediate supervision of the PLA. Nevertheless, given the extensive network expertise available to the PLA it is possible (though unconfirmed) that these militia organizations can undertake mass CNO attacks during a wartime situation, where the volume of attacks would be prioritized over concealment. Additionally, given the emphasis that the PLA places upon operational preparedness and strategic resilience within its cyber networks, it is likely that cyber militia personnel could take on defensive jobs such as updating firewalls, replacing systems and reconfiguring damage or corrupted information systems. This would effectively secure China's cyber "strategic rear area" and would make operations against a potential adversary more durable. Additionally, by taking over these comparatively easy tasks, the PLA could more effectively economize its forces, allowing

[69] Nakashima, Ellen, "Following U.S. Indictments, China shift Commercial Hacking from Military to Civilian Agency," The Washington Post [2015], accessed 11/27/2016
[70] Costello, John, "China's Irregular Warfare in the Cyber Domain," Real Clear Defense [2015] Accessed 6/29/2016
[71] Sheldon, Robert, & McReynolds, Joe, "Civil-Military Integration and Cybersecurity," pp 195-200
[72] Cooper, Cortez A. III, "Preserving the State: Modernizing and Task-Organizing a 'Hybrid' PLA Ground Force." "*Right Sizing the People's Liberation Army: Exploring the Contours of China's Military*," US Army War College Strategic Studies Institute [2007] pp 245-249
[73] Sheldon, Robert, & McReynolds, Joe, "Civil-Military Integration and Cybersecurity," pg. 201
[74] Hille, Kathrin, "Chinese Military Mobilizes Cybermilitias," Financial Times [2011] Accessed 6/28/16

military professionals to devote more time to skill-intensive tasks such as undertaking sophisticated cyberattacks against an adversary.

6. Electromagnetic Domain

The fourth component of China's Information Warfare Strategy is its use of electromagnetic warfare (EW) capabilities. These capabilities include radar jamming and deception, sensing, and protection of electronic assets to ensure unimpeded access to the Information Domain. Like the United States, China views of control the electromagnetic environment (EME) as critical to mission success. China, however, is unique in the way in which it responds to EW threats. In the United States military, EW operations are stovepiped directly to the operations officer.[75] Consequently, there is little cross-pollination between EW officers and other officers who focus on various information-centric operations (e.g. intelligence, cybersecurity, information operations, etc.). In China, all of these units are integrated from the ground-up, reflecting PLA doctrine which states that they are all components of the same "whole" (i.e. information warfare) which operates across the "full spectrum of conflict."[76]

Much like China's network militias, China currently maintains numerous militia organizations dedicated to supporting PLA EW operations. Though no full open-source survey of Chinese EW militia capabilities exists, open sources state that the PLA is fielding EW militia subunits that are nested within public telecommunications companies, educational institutions and municipal institutions.[77]The inclusion of EW militias within civilian telecoms companies suggests that, in the event of a conflict, the PLA would draw upon a pre-existing infrastructure and C2 system to support its EW operations. The lack of literature and reporting on the subject suggests that EW militias play a fairly limited role in peacetime. However, following the model of other PLA militia organizations (air and maritime defense, etc.) it is likely that these could be rapidly mobilized in the event of conflict.[78] [79] These units would theoretically be capable of providing operational, technical, and logistical support to regular PLA units.[80]

Conclusion

China's civilian economy capability exists as a powerful tool that can be used by Beijing to protect the regime and to advance its foreign policy abroad by augmenting the PRC's IW capabilities. Though the PLA no longer uses the "People's War" doctrine to organize its conventional forces, many of the same principles of mass mobilization can be observed in the way that it conducts operations in the Information Domain. By interfacing with private companies, academia, and civilian institutions, the PLA significantly expands its available resource pool. Both civilian expertise and infrastructure can potentially be called upon to support military and intelligence operations. At the same time, cyber auxiliaries also allow the CCP to shore up its domestic flank by shaping public debate and deflecting criticism. As more open source information on China's cyber auxiliaries becomes available, our understanding of their organizational structure and means of cooperation with the Chinese government will

[75] Joint Staff Joint Publication, "Electronic Warfare," United States Joint Chiefs of Staff, [2007] I-11, II-12
[76] Cheng, Dean, "PLA Views on Informationized Warfare, Information Warfare, and Information Operations," Wiley ISTE, [2014]
[77] Sheldon, Robert, & McReynolds, Joe, "Civil-Military Integration and Cybersecurity," Table 8.A1 pp. 212-217
[78] Global Security, "PLA: The Militia" globalsecurity.org [2010] accessed 6/27/2016
[79] Tisdall, Simon, "Little Blue Men: The Maritime Militias Pushing China's Claims," The Guardian [2016]
[80] Sheldon, Robert, & McReynolds, Joe, "Civil-Military Integration and Cybersecurity," pp 209-211

DOI: http://doi.org/10.5038/2378-0789.2.1.1022

undoubtedly become more nuanced. Regardless, it is clear that any strategy designed to manage China's rise must take into account the powerful role that these civilian auxiliaries play.