China's Cyber Warfare Strategy and Approaches toward Taiwan

Ming-shih Shen

Associate Professor & Director,
Graduate Institute of Strategic Studies,
National Defense University

Abstract

Chinese cyber warfare is known to the international society as a means of information penetration, account hijacking and secret sabotage. Given its aim to eventually unify Taiwan, China's efforts to penetrate, disrupt, and spy on Taiwan in the name of United Front will be never-ending, which in turn justifies Taiwan as a testing site for its cyber warfare. Although there are still technical gaps between China's network defense know-hows and those of advanced western countries, China's unrestrained online hacking behavior in the name of unlimited warfare and without regard for international norms are indeed disturbing in the eyes of western societies. Given these strategies used by Chinese Cyber Army, two policy recommendations are put forward that can be further divided into offensive and defensive measures.

Keywords: Cyber Warfare, China Cyber Army, Cyber Strategy, Cyber Attack, Cyber Defense

I. Forewords

Looking into the warfare in the 21st century, there are various weapon systems to be integrated, and when the C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) are put to work, humans can maximize the efficiency of weapon system to full strength to the extent that a digitalized hi-tech battlefield that is engaged by digital weapon systems will become commonplace. That said, one important combat requirement is to boost combat efficiency and to prevent damage caused by an information attack with the purpose of dominating cyberspace, given the fact that supremacy over the electro-magnetic environment (the

so-called wartime electro-magnetic dominance 制電磁權) and its related security are the backbone of today's hi-tech warfare. The point to be cautious here is that, with the advancement of information technologies, information tools and networking nodes are no longer limited to a supportive role. They are instead taken as platforms to launch attacks. These platforms can even be transformed into professional units engaged in network clashes and information warfare. Today, service units such as the Cyber warfare Wing under the Information-Communications-Electronics Corps in Taiwan, Cyberspace Combat Elements under Strategic Support Units (zhan zhi san bu 戰支三部) in China, and US Cyber Command are cases that have started to take cyber troops as an arm, in line with ground, marine, air, and space, as a domain worthy of further development so that in order to gain an upper hand against an adversary.

Take Chinese information tools and networking kits for instance. The Chinese actions in performing cyber warfare are known to the international society as a means of information penetration, account hijacking and sabotage. Given Beijing's objective to attempt to eventually unify Taiwan, the Chinese effort to penetrate, disrupt, and spy on Taiwan in the name of the United Front will be never-ending, which in turn justifies Taiwan as a testing site for its cyber warfare.

"Cyber Army," in this paper, refers to (a) PLA's formally organized combat units, (b) research units and technological universities that take part in the smuggle of technological data, (c) information units under local governments, the department of national security, and the department of people's public security and (d) all network operators recruited by these government units. These units and actors will be examined in-depth in this paper.

II. Resources in the Hand of the PLA against Taiwan

Since China developed its Cyber Army as a dedicated service, it has launched the so-called "863 project on human resources," and focused recruiting and training those skillful talents to work out hi-tech capabilities. This indicates that China's Cyber Army does not necessarily have a military background. Civil sectors and academic fields are also involved in the penetration efforts of cyber warfare against external governments and they receive grants from the second department under the Headquarters of the General Staff. The recent network bombardments from China's Cyber Army

on the US and Japan have to been seen in this perspective.

1. Cyber Warfare Department: A Strategic Support Force

The previous Department of Reconnaissance Technology that used to manage cyber warfare and exploitations changed its nomination, designation, insignia, and now is called "PLA Cyberspace Operation Unit of the Strategic Support Corps." This unit upgraded itself from a subordinate one under Headquarters of the General Staff to as battle troop, the third department of the Strategic Support Force. It consists of three elements: (a) Cyber Army, which is in charge of offensive and defensive cyber warfare; (b) aerospace force, which refers to military space units that are in charge of reconnaissance satellites and navigation satellites; and (c) electronics units, which are to interfere and misdirect the enemy's radar and communications. It will take some time to see the final settlement of the re-organization in place, because, firstly, if the Strategic Support Force is a service by nature, in parallel with army, navy and air force, the so-called Cyber Army, aerospace force, and electronics units will be taken as military branches or arms, and their cooperation will in fact be more complicated. Secondly, the transfer of command of the cyber warfare units is too sensitive an issue that it takes time to see if it is settled.

Some background to the third department, the Headquarters of the General Staff, may be helpful to see the whole picture. There were 10,000 Cyber Army, linguists, analysts and related technical officers in this department, divided into 16 bureaus, each of which was in charge of communication missions around the globe. The central command of this department was located in Haidian District, Beijing, with branch offices in Shanghai, Qingdao, Sonya, Chengdu, and Guangzhou. 61398 Unit that was discovered by the US in 2013 belonged to the Second Bureau under the Third Department that was in charge of hacking into areas that communicate in English, such as the United States, Europe, Australia, New Zealand and India. Other Cyber Army branches that were listed under other bureaus have language expertise ranging from Japanese and Korean to Russian and Spanish. Aside from these cyber warfare professionals, the PLA's Computer Science & Information Engineering University, in Zhengzhou, Henan Province, is the cradle of hackers for the military, and the majority of its graduates are recruited into the Strategic Support Force. The other sources for the Cyber Army are research students in computer science and mathematics

in civil universities at home.

At least 115 US enterprises have suffered from information leakage of trade secrets since 2006 and the PLA's Unit 61398, a cyber warfare unit was identified as being responsible. Since 2007, cyber-attacks on western defense contractors' information systems again were found to be the result of another cyber warfare unit, Unit 61486. What makes the picture more threatening is that these units share information and cooperate closely. The School of Information Security Engineering, Shanghai Jiao Tong University, has been found providing technological support to Unit 61486 and even some scholars on the campus work closely with the unit. Cyber warfare Unit 61419 with its headquarters in Qingdao, Shandong province was also found specifically in charge of a cyber-attack on Japan.

Figure 1. China Admits It Has Cyber Army

Source: Mohit Kumar, "China Finally Admits It Has Army of Hackers," *The Hacker News*, March 20, 2015, <https://thehackernews.com/2015/03/china-cyber-army.html>.

2. Defense Research Units and Intelligence Agencies

Aside from the cyber warfare units with specific roles, intelligence units and defense research units that specialize in information technology also have their own cyber warfare machines in charge of hijacking technologies and intelligence gathering

via networks. As to intelligence-based warfare, there are the joint-staff and liaison department under the Political Affairs Department, the National Security Department under the PRC's State Council and public security units under the judicial body. The National Security Department is mainly in charge of counter-intelligence and opposition, the latter of which refers to Tibetan independence, Xinjiang independence and Falun Gong. Public Security is basically in charge of public order, which is also supported by counter-intelligence measures. In terms of network operations, the National Security Department affiliates control domestic information by blocking network nodes and attacking overseas opposition by cyber-attacks. Cyber-attacks include hijacking information and neutralizing distant hosts by techniques such as DDoS (Distributed Denial of Service). The Cyber Army is commanded by the PLA and is mainly in charge of hijacking information requests.

Beijing has also designed three engineering systems to strengthen governmental control of the internet at home. These include the *Golden Shield Project* under the command of propaganda system, the Great Firewall under the command of public security departments, and the *Green Dam* under the command of the Ministry of Industry and Information Technology. These engineering and controlling mechanisms not only keep in close contact with the National Security Department and the PLA's counter-intelligence units, but also cooperate with public security departments on intelligence sharing.

3. Hackers in the Private Sectors

In addition to the above organizational units such as the PLA, Beijing is keen to cooperate with the private sector actors ranging from the earlier *Honker Union of China* to the more recent *Woo Yun* Net. Insiders with these private web sites are the targets Beijing seeks for their non-governmental identities, so they suit missions in grey areas. According to reports in July 2018, cyber warfare Unit 61398 had just completed its augmentation at the end of June, the largest in size in history. It was reported that the augmentation is supported by Zhongnanhai, the central decision-making body of the Chinese Communist Party. The overall project lasted for half a year and involved military academies and branch schools, research institutes, and experts selected by operation zones. Strengthening surveillance and control of various networks and online communities and using DDoS attacks on specific targets around

the world continue to be their routine training.

4. Internet and IOT

After Xi Jinping came to power, the "Central Leading Group for Cyber Security and Informatization" and the PRC's "Internet of the Things (IoT) Office" were set up. These state-own units are in charge of network integration, development and control, and are directly led by Xi Jinping, whose efforts is geared toward becoming a cyber power by encouraging innovative breakthroughs. In several speeches, Xi has said that network security is the key to national security and he has listed network security as the first priority of national security. More significantly, President Xi takes the development of networks as the main technological thrust for industry information. China looks to the future with projects such as "Made in China in 2025" and "IoT+" so that they can maximize the economic utilities. However, with the development of network technologies, Beijing's control of internet users and manipulation of public opinion will be increasingly firmer. This can be evidenced in Huawei, SMIC, Xiaomi, and 360 Security Guard.

III. Operational Strategy of the Chinese Cyber Army

Based upon the varying demands of peace time and war, the Chinese strategy to apply cyber warfare to Taiwan consists of hijacking information, network neutralization, network guard systems, network psychological warfare, network command and control and the other strategic measures.[1]

1. Online Information Hijacking

This refers to implantation of Trojan horses, phishing and viruses into hardware systems with a view to taking away all the information of the targeted users. The warfare network units will categorize the great amount of collected information and then dispatch it to related units for further analysis and application. In other words, information hijacking is a means of information collection. With computer viruses, Trojan horses,

1. Chen Ye & Pao-hsen Chao, "The People's Liberation Army Officer Wrote An Article About Cyber Warfare, Summary of Five Combat Styles," *China Youth Daily*, June 3, 2011, <http://news.ifeng.com/mainland/detail_2011_06/03/6802050_0.shtml>.

and hacking software, cyber warfare units are capable of hunting valuable information.

Cyber-attacks mainly target two kinds of information. First is the ordinary data in life such as data to do with household registration and health care. Anyone having them in hand will have access to the personal data of the others. The information system of the Sanitary Bureau, Taipei City Government, was attacked and 2.98 million pieces of personal data were stolen. The theft was not known to the City Government until the data were diverted to a conference. Further investigation verified that the attacker's IP was from abroad.[2]

The important targets for the Cyber Army also include government confidential documents and key process technologies held by the hi-tech enterprises. For instance, 2013 witnessed the Chinese Cyber Army's attempt to steal data about the US's F-35 fighters, which was circulated among the mass media.[3]

According to investigation by *iDefense*, an information collection institute under a network counselling company called Accenture Security, one of the Chinese Cyber Army units, APT40, sent malware to several universities in the US, Canada, and other Southeast Asian countries. It did this under the guise of greeting letters for academic exchanges. This ill-intended move proves that a new wave of cyber-attacks from the Chinese side have emerged. Statistics show that since at least April 2017, the Chinese Cyber Army' network operation has targeted at 27 universities, aiming to steal the end-products of US maritime R&D. The victims so far have included some elite institutes, such as MIT, Penn State, Duke University and Washington University.[4]

---

2. "More than 2.98 Million Personal Data from Taipei City Health Bureau Hacked by China Hackers," *ETtodaynews*, January 2, 2019, <https://www.ettoday.net/news/20190102/1346169.htm#ixzz5mr56BoVb>.
3. Ryan O'Hare, "China Proudly Debuts Its New Stealth Jet It Built 'By Hacking Into US Computers and Stealing Plans,'" *Mail Online*, November 1, 2016, <https://www.dailymail.co.uk/sciencetech/article-3893126/Chinese-J-20-stealth-jet-based-military-plans-stolen-hackers-makes-public-debut.html>.
4. Fred Plan, Nalani Fraser, Jacqueline O'Leary, Vincent Cannon, & Ben Read, "APT40: Examining a China-Nexus Espionage Actor," *Fire Eyes*, March 4, 2019, <https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html>.

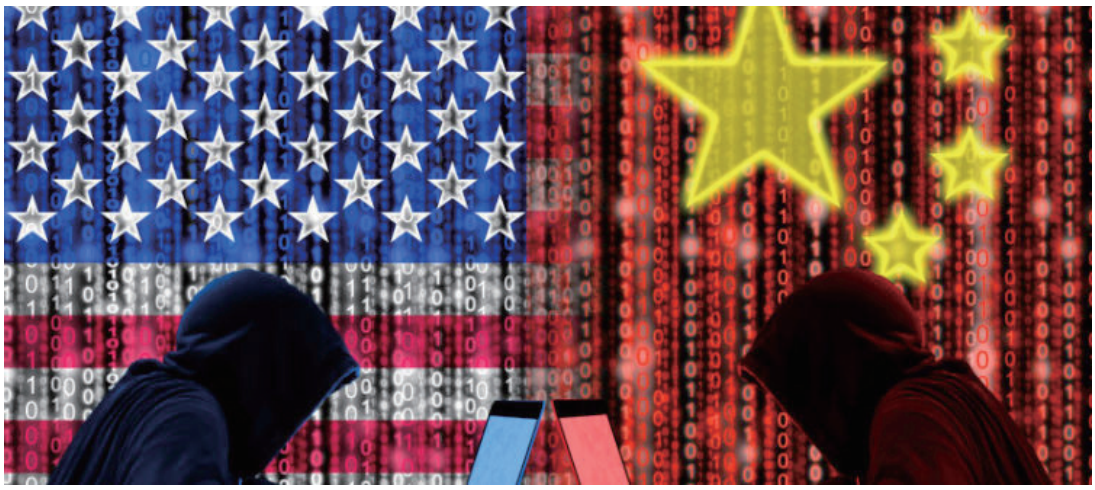

Figure 2. Trade War and Cyber War between the U.S.A. and China

Source: Deveney Roberts, "The U.S.A. and China Trade War – Could This Lead to the Next 'Operation Aurora'?" *EC-Council Blog*, April 17, 2018, <https://blog.eccouncil.org/the-u-s-a-and-china-trade-war-could-this-lead-to-the-next-operation-aurora/>.

2. Network Paralysis

Neutralization or paralysis of a targeted network refers to cyber-attacks stopping the functioning of a targeted network in the form of DDoS via zombie computers. This can also refer to shutting down or interfering with the computer systems of basic infrastructure—energy infrastructure, hospitals, water supplies—causing disruption. They can be applied military network nodes and they will be even more important than daily concerns. "Nodes" from the military perspective refer to those gateway nodes and shared nodes that, with relatively lower cost, will have significant impact in the overall combat situation. For example, in the Russian Cyber Army's cyber-attacks on Estonia and Georgia with the zombie computers in 2007/2008, key websites set up by TV media, financial institutes and communications systems were paralyzed. The governments were forced into chaos. When the airports, logistics and communication technologies malfunctioned as a result of the attacks, military materiel failed to arrive in the right position or at the right time. The potential to fight against Russia, if any, was significantly cut. A direct and visible impact was surely on the social order and the command and logistic structures of the military.[5]

5. Sarah P. White, "Understanding Cyberwarfare: Lessons from the Russia-Georgia War," March

Figure 3. China Cyberattack

Source: Jason Simpkins, "It's Bigger Than Hillary: China's Preparing For War," August 30, 2018, *The Outsider Club*, <https://www.outsiderclub.com/it-s-bigger-than-hillary-china-s-preparing-for-war/83000>.

Note: US firm Mandiant has issued a 74-page report on a global cyber espionage campaign by what it says is a Chinese government-backed organization dubbed APT1(Advanced Persistent Threat 1). APT 1 global attacks since 2006, 141 organizations targeted in 15 countries.

3. Network Guards

The above are all to do with the offensive approaches. Undeniably, however, Beijing is also aware of online threats from the US and other rivals. Beijing is keen to take active and reactive measures to ensure the protection of its own network systems and key infrastructure, which is quite similar to other countries, and who also take preventive measures to guard information infrastructure and information systems and information contents at home from cyber-attacks as prior concern of network security. These preventive measures include the establishment of a defense system that ingrates security evaluation, surveillance and warning systems, and countering

20, 2018, *Modern War Institute*, <https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/>.

intruders and contingency responses. The integration consists of active and reactive forms of defense with a view to preventing information disclosure over the internet, particularly focusing on keeping watch over hackers and attacks from intelligence agencies of hostile countries.[6]

One of the cases in this respect can be inferred from a Tencent-led consortium that invested in Reddit, an American social news aggregator, expresses its pro-Beijing position and seeks to smear at all arguments critical of Beijing. There are therefore some reasons to be skeptical because the user's account of this investor seems to be related to the Chinese Cyber Army. It makes sense for some governments to hold the view that attack is the best defense, and they will not restrain themselves to defensive or counter-attack preparations. Chinese strategic defense force is mainly in charge of defense including, preventive measures that are followed by both military and civil industries. The responsibility for integrating the whole defensive network lies with the Office of Central Cyberspace Affairs Commission (中央網絡安全和信息化委員會辦公室) and Office of Cyberspace Administration of China (國家互聯網信息辦公室) under the State Council. The director of the Cyberspace Administration of China also serves as Vice Minister of the Publicity Department of the CPC Central Committee (as well as Deputy Director, Information Office of State Council).[7] Table 1 lists the branch units that support the Office of Central Cyberspace Affairs Commission (Office of Cyberspace Administration of China).

6. Edward White, Alice Woodhouse, & Xinning Liu, "China Hits Back at US and UK Allegations of Cyber Attacks," *Financial Times*, December 21, 2018, <https://www.ft.com/content/47eb9b12-04da-11e9-99df-6183d3002ee1>.

7. Dan Chin, "China Network and Information Office Control The Free Media," *Up Media*, December 1, 2018, <https://www.upmedia.mg/news_info.php?SerialNo=52559>.

Table 1. Office of Central Cyberspace Affairs Commission (Office of Cyberspace Administration of China)

Affiliate Units	Industries Reporting to the Units
1. Bureau of Cyber Reviews 2. Bureau of Cyber Social Work 3. Bureau of Mobile Network Administration 4. Bureau of Cyber Security Coordination 5. Information Development Bureau 6. International Cooperation Bureau 7. Bureau of Cyber Data and Technology	1. Command Center of Cyber Security Contingency 2. Agency's Service Center 3. Training Center 4. Reporting Center of Illegal and Distorted Information 5. China Internet Development Funds 6. China Cyberspace Research Institute 7. China Network Information Center 8. National Computer Network and Information Security Management Center 9. Internet Public Opinion Center 10. Secretariat, National Informationization Professional Counselling Committee

Source: Compiled by the author.

4. Cyber Psychological Warfare

Beijing used to be without the concept of psychological warfare, for there has long been departments, dictated by the Communist Party, dealing with propaganda. On the other hand, the so-called United Front has been the main effort against enemies by Beijing, who therefore rarely touch upon operations similar to the American version of psychological warfare. The Gulf War in 1991 changed this mindset. In fact, Beijing was enlightened by the US supportive measures including networks, electronic media, and air support to assist in combat operations. Since then, Beijing have begun to have officers to deal with psychological warfare and offer training courses on psychological warfare. It is common for us to see psychological warfare expand its influence via many different platforms. However, seeing the unbounded character of networks and their products being readily altered, Beijing has been keen on the use of networks.

The Chinese effort is not difficult to understand. With the expansive character of cyberspace, many media platforms can be integrated and transformed into new social media and community platforms. Cyber psychological warfare, viewed in this light, reveals its purpose, which is to corrupt citizens' support for the government and its morale, shaking the opponents' will to fight. As a tactic, Beijing sends out

many messages through different platforms to not only influence psychology of the opposing side, but also to manipulate the politics and elections of the other side. There are in fact some journalist reports pointing out that China is ready to launch a so-called "cognitive warfare" to win the social space of the Taiwanese people, and this strategic plan is apparently strengthened by networks, social media and fabricated news. Beijing's strategic intent, by nature, is to develop new characteristics of media communication and magnify the effect of public opinions in conveyance, reflection and snowballing. The aim of this strategic intent is to force the popularity and influence of the DPP (Democratic Progressive Party) Government down in two years, disrupt Taiwan's social framework, and tear apart the basic understanding between Taiwanese and President Tsai, and between the Armed Forces and President Tsai, and even the overall social trust shared by the people in Taiwan. Ultimately, Beijing seeks to transform Taiwanese citizens' understanding of western electoral systems, leaving the whole island in a weaker situation, militarily, psychologically and politically.

5. Network Command and Control (C^2) Warfare

Network command and control warfare is termed "Network-Electronic" Warfare by the Chinese and can be defined as a combination of network and electronic warfare with the dual purpose of protecting command, control, communication and intelligence on this side of the battle and, conversely, attack and destroy machines on the enemy side. The goal is to seek military dominance during an armed conflict. On this point, it has to be noted that there are less serious gaps between information technologies for most countries. Also, because there are some overlapping dimensions between military systems and some civil sectors, information tools between the two cultures are less significant, especially compared with the past, which was dominated by the traditional weaponry. Ironically, it is those developed countries which rely heavily on information technologies that are more vulnerable to internet attacks. They are more likely to be exposed to information leakage and put their information security at risk. With this basic understanding, the PLA is firmly convinced that whoever seizes electro-magnetic supremacy at the start of a campaign will win the lottery to ensure victory on the battlefield. To substantiate the idea, the PLA makes use of network command and control warfare as a basic form of "integrated joint warfare" that will consist of electronic warfare, computer cyber warfare and dynamic-killer approaches with a view to interrupting the enemy's theater internet information system that is initially

planned to project more power and to support more resources to the enemy. Table 2 summarizes the Chinese Cyber Army's operational strategies.

Table 2. Operational Strategy of China's Cyber Army

Strategy	Contents	Instances
Online Information Hijacking	Implanting Trojan horse, phishing and viruses into hardware systems to grab the information of the users	F-35 fighter Hi-techs, and maritime R& D in US universities
Network Paralysis	Attacks in the form of DDoS via zombie computers to stop the function of targeted networks and basic infrastructure computer systems	Computer virus incident with TSMC (Taiwan Semiconductor Manufacturing Co.)
Network Guards	Preventive measures to guard information infrastructure, information systems and information contents at home from cyber attacks abroad	Integration of the Office of Central Cyberspace Affairs Commission and Office of Cyberspace Administration of China, State Council to ensure network security
Cyber Psychological Warfare	Corrupting citizens' support of the opposing government and its morale, shaking the opponents' will to fight on	Taiwan's 2018 election that was filled with fake news that tipped the balance of the votes
Network Command and Control (C^2) Warfare	A combination of network and electronic warfare with the dual purpose of protecting command, control, communication, and intelligence on this side of the battle and, conversely, attacking and destroying wrestling machines on the enemy side	PLA making use of network command and control warfare as a basic form of "integrated joint warfare", consisting of electronic warfare, computer cyber warfare and dynamic-killer approaches

Source: Compiled by the author.

6. Penetration or Fabrication Strategies

There are some strategies that are certainly to do with those mentioned above, but are difficult to be grouped into one. A general picture can be drawn, nevertheless. They are mainly to do with fake news or directing the public opinion on social media with a view to manipulating social views and political trends. For instance, *Facebook* accused several industries and individuals in China in 2019 of online misconduct, including fraudulently making, marketing and even selling false accounts, echo counts,

and fans counts on *Facebook* and *Instagram*. Superficially, we may see *Facebook* and *Instagram* as victims of trade mark infringement. A deeper look will show the intention of the PLA, whose real purpose is to buy these fake accounts to shape a false trends and to frame social opinion about certain public issues.

In other words, the PLA and the Chinese Cyber Army with Beijing behind is trying to control network news by fabricating fake news, and are using the overseas vocal organs to spread and re-sell news. China is also strengthening its influence by purchasing mass media in Chinese, and bribing western reporters to report in Beijing's favor. Currently, China has begun its contacts with oversea press commentators and grassroots leaders, attempting to shape public opinions to its interests, which in turn means a new wave of interference in foreign media. Having said this, Beijing is now capable of shifting its sub-organizations and propaganda modes. China has proven itself good at switching its base stations off and on. This indicates that the spreading of fake news will become easier than anticipated via cross-Strait mass media, *Facebook*, *Line*, *PTT*, content farms, irresponsible political pundits, and internet celebrities. China seems confident of seeing that the more corresponding echoes are gathering, the easier to lead the public opinions. Caution is certainly needed.

Figure 4. 35% of Cyber Attacks on Official Indian Websites Are from China

Source: "35% Of Cyber Attacks On Indian Sites From China: Official Report," *Defense Aviation Post*, August 23, 2018, <https://defenceaviationpost.com/35-of-cyber-attacks-on-indian-sites-from-china-official-report/>.

IV. Conclusions: Countering Measures

Given the above observation of the strategies used by the Chinese Cyber Army, there are two policy recommendations that can be further divided as offensive and defensive, as follows.

1. From the Offensive Perspective

Although there are still technical gaps between China's network defense know-hows and those of western advanced countries, China's unrestrained online hacking behavior in the name of unlimited warfare and without regard for international norms are indeed disturbing in the eyes of western societies. Strengthening network security and investing in network security technology seem to be a necessary step. By contrast,

if most countries adopt offensive measures, the whole situation will be turned around. Beijing will find that, despite its *Gold Shield Project* or other alternative counter-measures, either its cyber-citizens cannot be effectively barricaded, or that western countries (even Taiwan) may plant viruses into China's information system, seeking revenge. In order to put Beijing into this dilemma, we may consider a cyber-attack on China's key systems as an option. Under the constrained conditions and preconditioned with security, this research is of the view that treating stubborn ones with their stubborn ways may serve as a warning to balance the imbalances.

2. From the Defensive Perspective

For anyone talking about defense, the emphasis is on strengthening self-defense capabilities and flexible responses in accordance with contingency plans. Firstly, for military facilities and key infrastructures, we should strengthen reconnaissance and related countermeasures. Secondly, before any systems are installed, they have to be equipped with capabilities that ensure their survival against electronic-magnetic-pulse attacks. A secure environment for communication and information operations is becoming a basic requirement for surviving cyber-attacks from an adversary. Thirdly, more effort has to be made via R&D on coding techniques to keep online data safer. Fourthly, we need to quicken the integration of information warfare and C^4ISR, looking for the day with effective countermeasures are on hand to survive an information warfare. Fifthly, we should not only build a secure information system but a system with resilience—one that can be immediately responsive and can recover from damage to normal usage sooner.

With the rapid development of information technology, this century has witnessed an increasingly mature military engagement based on information as contents and conveyed via information as a platform. Along with this trend, states' key infrastructure are also run by information technologies, but it is exactly this trend that means the risks of their being attacked and damaged have escalated. We need experts on information technology and network security to be professionally in charge and responsible for their management. As professional teams, they need to meet the requirements to counteract cyber warfare and weather information attacks.

Table 3. Recommendations to Counter the Chinese Cyber Warfare

Measures	Offensive	Defensive
Contents	1. Implanting virus 2. Initiating cyber attacks such DDoS or APT 3. Hacking into systems and stealing intelligence 4. Cyber Psychological Warfare 5. Penetrating into online communities to lay bare Chinese domestic realities	1. Strengthen reconnaissance capabilities and reinforce countermeasures to protect military facilities and key infrastructure, as well as command and control functions 2. Systems installed have to be equipped with capabilities to ensure they survive electronic-magnetic-pulse attacks. Secure environment for communication and information operation is needed. 3. R&D on coding techniques to secure the online data 4. Integration of information warfare capabilities and C^4ISR with effective countermeasures to survive information warfare 5. Building resilient systems so that we can be immediately responsive and recover from damage and be back to normal

Source: Compiled by the author.