Andrzej Kozłowski

University of Lodz

The "Cyber Weapons Gap." The Assessment of the China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan

Introduction

During the Cold War the term "missile gap" was created to indicate the United States' delay in the missiles race. Today a similar situation took place in cyberspace, where more and more policymakers and pundits pointed out the growing cyber capabilities of China as a threat to the American national security and the destabilizing factor in region. Indeed, the Chinese have started to develop its tools and methods to paralyze the ICT systems of a potential adversary to comply with the quotation from Mao Zedong "to achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears." Considering the uncertain political relations with the United States, China needs to possess the ability to deter this country from engaging in regional conflicts. However, the robust cyber capabilities have a significant role for long-term development strategy and economic prosperity.

The main aim of this article is to evaluate the cyber warfare capabilities of China and simultaneously answer the question about the potential consequences for Cross Strait Relations and the bilateral relations with the United States. In order to do this the strategic aims of the Chinese activity in cyberspace will be examined as well as the character of operations carried out by Chinese hackers. What is more, an analysis of the strong and weak points of Chinese capabilities in this matter will be depicted.

In addition, the potential scenarios of practical usage of cyber warfare will be presented with particular focus on the deterrence of the reaction of the United States in case of war over Taiwan. The article is divided into two parts: one descriptive, which presents the assets of China in conducting cyber warfare operations and the second one, where the evaluation of it and the consequences for regional security system will be presented.

In this article the cyber warfare capabilities are broadly defined as not only the ability to inflict physical damages but also as advanced methods of gathering information through cyber espionage or using them as a multiplier of force to blind enemy systems or as a part of sophisticated information warfare. Evaluation of the cyber warfare capabilities constitutes a more challenging task than classical military capabilities. In the virtual world we cannot count the number of tanks and jets. In this paper in order to assess the Chinese cyber capabilities the various documents were compared and analyzed, which describe and evaluate the degree of the threat. What is more, the most advanced cyber operations will be presented to create a comprehensive view on the cyber warfare capabilities of China.

Defining the Chinese Strategy

China's military history has been defined by asymmetric warfare. Cyber warfare is just a new tactic (Harris 2008). The Chinese strategy of operating in cyberspace comes from the American experience and observations of the first Gulf War and the Balkan intervention. Especially, the operational concept called cooperative target engagement based on sharing data on potential targets simultaneously by the combat platforms on the sea, air and land worried Chinese strategists (Wortzel 2014, p. 3). To join the effort of all military assets effectively the United States needs the global information and command-control systems based on satellites (Weiguan, Xijan, Ji & Jijin 2005, p. 82). In the book entitled *Unrestricted Warfare* two People's Liberation Army (PLA) Air Force officers concluded that the American military is so highly reliant on information that the side that will dominate the aspect of conflict in cyberspace will gain a strategic advantage. The PLA officers suggested that China needed to look for a method to exploit this weakness (Qiao & Xiangsui 2009). The first strategies and doctrines on information warfare (IW), with particular reference to cyberspace were drafted in the midst of 1990s. According to Dr. Shen Weiguan, who is commonly recognized as a father of IW, the main target of IW is "the enemy cognitive and trust systems and the goal is to exert control over

his actions" (Striennon 2010, p. 16). In 2004 a more detailed vision was described by General Xu Xiaoyan, the former head of the Communications Department of Chinese General Staff, who pointed out that China needs a "Network confrontation technology – intercepting, utilizing, corrupting and damaging the enemy's information and using false information, viruses and other means to sabotage normal information systems functions through computer networks" (Thoma 2007, p. 333).

In practice it means that the Chinese focus on defending PLA networks and simultaneously attack in order to penetrate, exploit and perhaps even damage or sabotage through electronic means crucial entities such as integrated battlefield command-and-control systems and warfare networks, financial hubs to paralyze decision-making centers, slow down operations and ultimately decrease the morale of potential adversaries (Inkster 2012, p. 199). It links with altering the results of reconnaissance, thermal imaging, ballistic missile warning and radar sensing (Wortzel 2014, p. 21). They believed that all of these operations can be conducted whilst staying anonymous or with a low-risk of counterattack (Singer & Friedman 2014, p. 142). Chinese strategists also think that advanced cyber warfare capabilities could be used as deterrent. They assumed that any foreign powers, which could threaten China, will be highly dependent on computer systems. The infiltration and disruption of these computers systems is perceived as a defensive measure (Singer & Friedman 2014, p. 143).

The PLA treats cyberspace differently than, for example, Israel does and perceives it as an additional domain, which can influence shaping the battle space but rather not as a replacement for conventional war.[1] From the Chinese point of view, cyber warfare takes place in the electromagnetic spectrum and due to this fact it overlaps with traditional electronic warfare (Sheldon 2011, pp. 36–51). The Chinese perceived cyber capabilities as "bloodless" (Xinhua Publishing House 2000, pp. 213–215).

There is also another important aim of China in cyberspace – gathering strategic data to speed up the modernization process. The roots of these behaviors date back to the 1980s and the 863 program that involved a large-scale operation of gathering information about Western technologies. Initially this process was chaotic, however, later it started to be supervised by the military and industry complex and has become more effective. The widespread use of the Internet has given a new tool for conducting this process and has allowed to decrease using human intelligence

[1] Israel strategists believe that cyber warfare can constitute an equivalent of classical military activity (Kozłowski 2014e).

(HUMINT) operations, which were highly risky and could finish with an embarrassing diplomatic scandal in the case of catching spies (U.S.-China Economic And Security Review Commission 2009).

The significance of Chinese cyberspace was underscored in the latest National Defense Doctrine by statements about the necessity of possessing the developed abilities to conduct information operations, building an integrated system of electronic warfare and the satellites reconnaissance. It should consist of cosmic stations, computers and integrated computer networks, information networks and a broad range of different software both with a defensive and offensive character in order to protect the national interests in the military, economic and geopolitical dimensions far away from Chinese borders (Buczyński 2014, p. 256).

Chinese Cyber Warfare Capabilities Assets

Chinese units responsible for conducting different cyber warfare activities are divided into two groups: professional hackers within the PLA and the "patriotic hackers" who, from time to time, work for the government and support different operations in cyberspace. The Chinese structure of supervision over cyber operations is not so clearly presented as in the case of the United States. Nonetheless, most experts believed that the majority of cyber operations were conducted under the auspices of the PLA General Staff Department's Third Department. This structure seems similar to the American National Security Agency (NSA) and concentrates its efforts on signals intelligence, code breaking and communications security of the PLA. 130,000 people worked there (Singer & Friedman 2014, p. 141). The most important element of this department is the Beijing North Computer Center (PLA 61539 Unit). It supervised ten subdivisions, which work on "the design and development of computer network defense, attack and exploitation systems" (Singer & Friedman 2014, p. 141). China also focuses a lot on training and therefore there are twelve special training facilities located all around the country. A special role is played by a unit in Zhurihe that simulates the behavior of the United States and its allies in cyberspace and is used to train Chinese units and improve their abilities (Singer & Friedman 2014, p. 141).

The widely recognized cyber unit of China is the Second Bureau of the Third Amy, Unit 61398.[2] This unit consisted of the most experienced and

[2] This entity has become popular and widely recognized after the American IT security company Mediant published in 2011 a report indicating the authorship of the majority

skillful IT specialists, electronic engineers, mathematicians and linguists – mostly English speaking – with the main headquarters in Shanghai. Unit 61398 plays a role not only as the typical conventional unit but rather it constitutes an operational center, which realized the decision undertaken in Beijing about activity in cyberspace (Buczyński 2014, p. 258). What is more, it acts as the research center responsible for acquiring and developing new IT technologies and implementation to their own computer networks in order to secure them and conduct effective invigilation of potential adversaries (Buczyński 2014, p. 258). The main aim of this unit is to steal the most vulnerable information about developmental trends, economy, technology and research especially in the area of military industry or data about the strategies and doctrines of potential adversaries. These activities are aimed at gaining advantage over other countries in the region and in the world, developing the operational advantage in case of a potential armed conflict (Buczyński 2014, p. 258).

An important role is also played by the Fourth Department (Electronic Warfare and Electronic Countermeasure Department) of the General Staff of the PLA (4/PLA), which conducts offensive electronic warfare, electronic countermeasures (jamming and counter-jamming). The last initiative of this unit covers the establishment of the new Information Safeguards Base in order to address cyber threats and strengthen the information security and infrastructure (Pu 2010). The Third and Fourth Department closely cooperate with each other. The former one analyzes and exploits the cyber information gathered by the latter one (Wortzel 2014, p. 23).

Moreover, the Third Department assigned to every military region headquarters department at least one technical reconnaissance bureau in order to monitor foreign communications and cyber activity (Melvin 2005, p. 1–2). Under the auspices of the Third Department also function three research institutes, four operational centers and twelve operational bureaus, which monitor phone, radio, satellite and computer communications (Stokes, Lin & Hsiao 2011).

A significant community of so-called patriotic hackers exists in China, who conduct simple operations in cyberspace like DDoS attacks, web defacement and email bombing. To these groups belong the members of university IT departments, employees in the IT departments of state-owned enterprises, online gamers and even criminals. Sometimes they

of sophisticated cyber attacks against the United States to PLA 61398 (Mandiant_APT1_Report 2012).

act alone without orders from authorities but it is important to stress that their activity is all the time monitored by the Chinese government. There are also certain situations, when they follow the orders of official authorities attacking a particular target (Inkster 2012, p. 202).

Operations of Chinese Hackers

The first kind of operation conducted by Chinese hackers reflects the information warfare in the virtual domain. The tremendous pace of Internet development gave a variety of novel options to achieve information domination. The first primitive actions taken by the Chinese hackers can be traced back to the turn of 1999 and 2000, to the next scene of Chinese-Taiwanese conflict, when then President of Taiwan Lee Teng-Hui announced that Taiwan is an independent country and does not constitute a part of China. This declaration led to simple hacker web defacement attacks, where the governmental website of Taiwan was covered with the inscriptions that only one China exists and one China is needed and also they put a red flag (Gawrycki 2003, pp. 166–167).

The second important event was the confrontation of Chinese and American hackers who clashed with each other over the air collision between the Chinese jet and American reconnaissance plane, which was forced to land in China. Americans started web defacement attacks posting on Chinese administrative websites insulting pictures, passwords and carried out attacks against the China Nuclear Information Center and China Telekom. In response Chinese hackers created the Killus.com website to facilitate conducting operations in the virtual world against websites of American governmental institutions (Węderska 2014, p. 77). These kinds of information and parts of information warfare always appeared to reflect tensions in bilateral relations. It happened many times in the case of the United States or the regional rival.

In 2012 new tensions aroused between China and Philippines regarding the Scarborough Shoal and Spratly Islands and quickly this situation transformed into conflict in cyberspace, where the Philippines official administration websites and other institutions were defaced (Passeri 2012). A similar situation happened in disputes with Japan over an island (The Globe and Mail), South Korea (Al Jazeera 2013) and Vietnam (TuoiTre News). The Chinese also attack newspapers, which published unfavorable articles about the domestic situation or the leaders of China (Perlroth

2013). The majority of these simple and unsophisticated attacks are conducted by volunteer hackers, who sometimes do not possess adequate skills and can be traced by foreign countries. However, the lack of international law regulating such cases caused that cyberspace allows China to demonstrate their dissatisfaction about certain behavior of different countries.

The second kind of operation can be described as a Chinese specialty. It is a cyber espionage operation addressed against other countries, as well as against private enterprises. The first well-known operation was Titan Rain. This operation, which started in 2003 and ended in 2005 was aimed at stealing secrets from United States research labs, military branches and agencies and defense contractors, with the most valuable data systematically stolen. Data such as the plans of American defense systems, the F-35 fighter jet or data about the American probe sent to Mars (Stiennon 2010, pp. 1–11). Titan Rain was not the only large scale cyber espionage operation against the United States. It was followed by the Shady Rat operation, which started in 2006 and lasted till 2011. The investigators of this case informed that more than 72 institutions not only in the United States but in the whole world suffered the breach. Among them were American military enterprises, international corporations, the networks of the United Nations organizations and even the International Olympic Committee (McAfee 2014). In 2011 a Chinese hacker penetrated the resources of RSA Security, a company responsible for producing the sophisticated coding mechanism for the government. These actions can allow for easier penetration of the Department of Defense (DoD) and other governmental institutions (Blogs.RSA). In 2013 the most serious leak of military data was revealed and the Chinese hackers stood behind it (Kozłowski 2014a). The Chinese hackers attacked not only the United States. They also breached the cyber defense of Israel and stole secrets about the latest antimissile system called "Iron Dome" (Kozłowski 2014b). In addition, the European Union members and institutions were also among the victims of Chinese cyber espionage (Gayathri 2013). The hackers are not limited to actions against the governmental institutions or military branch representatives but also hacked Google accounts in order to trace the data of human rights activists (Kozłowski 2014c, p. 230).

The Chinese are highly qualified experts in cyber espionage, achieving a lot of success. They aimed at the military technologies being aware that their own military forces have still lagged behind the West and through cyber espionage they wanted to do a low-cost shortcut. According to different sources the advanced espionage operations in the virtual world helped

make up for 15 or 20 years with the Western countries (Zakaria 2014). Not only are the Chinese interested in solely military technology but also in the business plans of different companies or negotiation stances of Western countries to compete with them effectively. It seems that cyber espionage bore the most valuable fruits for the government in China.

The third option covers the cyber operations, which are able to inflict physical damages. Despite the fact that there were no official statements about such an operation, the existing proofs and journalist investigations claimed that it could be different. The suspicions exist that Chinese hackers stood behind several major blackouts in the United States. In 2003 one of the most serious blackouts in the history of the United States took place. 50 million people in a 9,300 square-mile area lost power and several people died. Commonly, it is assumed that it was caused by the malfunction of certain elements of electric networks. However, according to the information provided by Tim Bennett, the former president of the Cyber Security Industry Alliance, this accident was caused by sophisticated malware probably developed by Chinese hackers linked to the PLA. Bennet believes that the Florida blackout, which affected 3 million people, was also produced by the activities of hostile powers, probably coming from China. What is more, Joel Brenner, the government's senior counterintelligence official, neither confirms nor denies these allegations but he states that it seems plausible for him. This surprising news was denied by officials, however, it is extremely difficult to state unequivocally, which version is right due to the fact that majority of electric lines belong to private sector companies that are not eager to share information about these kinds of accidents (Harris 2008). If this information is really true it means that China possesses very advanced cyber warfare capabilities and can inflict serious damage on United States infrastructure, which may even end with a death toll.

The United States security companies and major political and military figures warned public opinion about the threat flowing from Chinese cyber warriors. The majority of the reports created by these enterprises and the hearings in Congress of main officials indicated that Chinese cyber warfare capabilities are really massive and sophisticated. General James Cartwright, the former head of US Strategic Command, told the US – China Economic and Security Review Commission that the particular threat stemmed from the Chinese ability to manufacture massive amounts of automatically generated message traffic. It has the potential

to cause cataclysmic damages, including paralyzing critical infrastructure or military command (Marquand & Arnoldy 2007). He compared it to the usage of mass destruction (Harris 2008). His statements were repeated by former NSA Director, Admiral Mike McConnel, who compared the current situation to the Cold War, when the United States had to protect itself against nuclear attack. Now they must do the same with cyber attacks against elements of critical infrastructure, which is highly dependent on IT systems (McConnel 2010).

Nevertheless, the majority of these statements are exaggerated, mostly because the security companies want more contracts from the scared administration units or individuals, but it is an indisputable fact that Chinese cyber warriors are among the top countries.

Considering the sophistication of technology, China is among the top countries and is owns one of the fastest computers on the whole planet, which allows it to break the most complicated codes and passwords (Vance 2010).

The next powerful cyber weapon lies in the number of Chinese people (around 1.4 billion) (CIA Factbook) and therefore, simultaneously the biggest number of Internet users. In the near future Chinese hackers will flood other countries not with the latest technology but by the number of hackers and thus the uncountable amount of operations in the virtual domain (Segal 2012, p. 20). Chinese hackers have proved their ability to conduct information warfare in cyberspace at the high level (Car 2012, pp. 90–91). Its strength came from the big number of linguists skilled in different languages and in specialized areas, such as financial abilities, energy or military activity.

Taking into account the sophisticated and successful methods of computer network exploitation used by the Chinese in their cyber espionage activities, the same method can be used to attack systems and destroy data. It depends only on the computer user's intent. The skills needed to penetrate networks during peacetime to collect intelligence are the same that are used to penetrate networks during wartime. Chinese hackers conduct many successful cyber espionage operations against private companies and United States government assets (The US-China Economic and Security Review Commission 2009, p. 9).

The Chinese cyber warfare capabilities have also limits and own flaws, which can be easily exploited by their opponents. The Computer Network Defense is the weakest point of Chinese warfare capabilities.

China, according to raw data statistics is the main victim of cyber attacks. The Chinese Ministry of Public Security informed that the number of hostile incidents against the computers in China rose up by more than 80% annually and 10 to 19 million computers belong to botnet networks. The reason behind this situation lies in the widespread use of illegal software that often comes from unreliable sources. Some statistics point out that even 95% of computer software can be pirated, which means that they could not be actualized as the legal license holders do. Therefore China's disregard to intellectual property is a dual-edge sword, bringing both positive and negative effects (Inkster 2012, p. 199).

The second main problem is a centralized structure of Internet governing, which means that it is much easier to paralyze the Chinese Internet through sophisticated attacks than to do the same thing with the United States networks operated by different Internet providers. What is more, the Chinese use American software and hardware, which possess a built in domestic weakness that allows it to conduct attacks (Dziwisz 2013, p. 154).

Implications for Cross-Strait Relations

The development of Chinese cyber warfare capabilities may have a significant impact on the future of Taiwan. It adds one additional dimension to a potential conflict field between the states and maybe even most political tensions will be reflected in cyberspace because the operations in the virtual domain are bloodless. The Chinese cyber capabilities buildup is aimed mainly at deterring and delaying the United States response to an outbreak of conflict over Taiwan.

According to the potential scenarios of war with Taiwan, the Computer Operation Network (CNO) will be carried out in the initial phase of conflict to preemptively strike against information systems and the C4ISR systems of Taiwan and, what is even more important, against the United States (The US-China Economic and Security Review Commission 2009). In reference to Taiwan the PLA strategist believes that the CNO will play a crucial role as the psychological factor that contributes to decreasing the will of Taiwanese people through disrupting and paralyzing the infrastructure and economic vitality. This scenario seems plausible, especially when considering the weakness and fragility of the power grid network characterized by single-point failure nodes and the lack of

subgrids. These kinds of structures make any attack much easier (Mulvenon 2004, pp. 265–258). In a potential war with the United States, China probably will use CNO capabilities to paralyze selected nodes on the military's Non-classified Internet Protocol Router Network (NIPRNET), unclassified DoD and logistics networks of civilian contractors in the continental United States and American allies in the Asia-Pacific region. However, not all of the networks will be attacked but only crucial nodes identified by the PLA planners as those points, which most deeply affect the decision-making process. PLA assessment of US campaigns in Iraq, the Balkans and Afghanistan identified logistics and the force deployment times as the most vulnerable points, the interruption of which will lead to supply delays or shortages. The main reason behind this situation lies in the responsibility of private companies for these kinds of activities on the battlefield, which are much more vulnerable to the attacks due to either a lack of adequate funds to secure networks or the reluctance to do it. PLA CNO activities are aimed to maximally delay US deployment and decrease the effectiveness of American military assets already deployed in the war theatre to allow PLA forces to achieve operational objectives such as landing troops on Taiwan in a cross-strait scenario before the US can effectively intervene (The US-China Economic and Security Review Commission 2009, pp. 12–16). The most optimistic scenario assumes that a cyber attack allows achieving operational success without requiring direct combat with superior US forces (The US-China Economic and Security Review Commission 2009, p. 24). The defeat of the Taiwanese forces and the capitulation of the government on the island would present the United States a *fait accompli* situation upon the arrival of the American main armed forces.

Conclusion

China's long-standing binding to asymmetric warfare justifies why cyber warfare is so popular among policymakers in this country. Being under the impression of overwhelming American victory over Iraq in the Gulf War and appreciating the role of computer systems in the victory, China, since the middle of the 1990s, has focused on developing cyber capabilities, perceiving them as an important strategic asset in a potential confrontation with the regional actors, particularly Taiwan but mostly against the United States, seeing in the computer network attack an

attractive, asymmetric weapon against a more technologically advanced country. Taking into account many clashes in the past, including the humiliation of China in the 1996 Taiwan Strait Crisis, and still a number of unraveled, potentially troublesome issues, China wants to assure that it possesses a weapon that can inflict damage on the United States and balance the American advantage in conventional weaponry. However, China not only sees operations in cyberspace as a useful tool to deter Americans, but it also as important for the significant cyber espionage campaigns in order to speed up the buildup of conventional armed forces and increase the competitiveness of Chinese entrepreneurship in the world.

The Chinese government builds robust structure, drafts strategists and doctrines of using cyber warfare capabilities and tests it in practice. Three kinds of operations are included in Chinese operations in cyberspace, covering: cyber espionage, information warfare and more sophisticated actions aimed at critical infrastructure. The cyber ability of China is mostly created to dominate the region but first and foremost to deter and slow the United States' reaction to any outbreak of regional conflict, particularly in the case of Taiwan. Despite the fact that China belongs to the absolute top of countries with the most advanced cyber capabilities, the "Cyber Weapons Gap" does not exist as the United States dominates cyberspace and its hegemony there is even more significant than in the real world.

References

Al Jazeera 2014, "South Korea says Chinese IP behind cyber attack," viewed September 19, 2014, http://www.aljazeera.com/news/asia-pacific/2013/03/20133206525580850.html.

Buczyński J 2014, "Chińska Republika Ludowa od wojny ludowo-wyzwoleńczej do cyberprzestrzeni," in Górka M (ed.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku,* Wydawnictwo Difin, Warszawa, pp. 242–262.

Car J 2012, *Inside Cyberwarfare*, O'Reilly Media, Sebastopol.

CIA Factbook, "China," viewed September 19, 2014, https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html.

Dziwisz D 2013, "Rozmowa z dr. Martinem C. Libickim, ekspertem ds. bezpieczeństwa," *Bezpieczeństwo Narodowe*, Vol. 26, No. 2, pp. 147–155.

Gawrycki F M 2003, *Cyberterroryzm,* Fundacja Studiów Międzynarodowych, Warszawa.

Gayathri A 2013, "Chinese Hackers Infiltrated European Ministries' Computers Before G-20 Summit: Report," viewed September 19, 2014, http://www.ibtimes.com/chinese-hackers-infiltrated-european-ministries-computers-g-20-summit-report-1501924.

Harris S 2008, "China's Cyber-Militia," *The National Journal*, viewed September 19, 2014, http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531.
http://www.au.af.mil/au/awc/awcgate/china/09_04_30_infl_ops.pdf.
Inkster N 2012, "China in cyberspace," in Reveron S R (ed.) *Cyberspace and national security*, Washington, pp. 191–207.
Kozłowski A 2014e, "Izrael jako cybermocarstwo," *FAE Policy Paper*, No. 21/2014, viewed September 19, 2014, http://fae.pl/faepolicypaperpolitykaizraeljakocybermocarstwo.pdf.
Kozłowski A 2014c, "Nowa zimna wojna? Amerykańsko-chińskie relacje w cyberprzestrzeni," in: Górka M (ed.) *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa, pp. 222–242.
Kozłowski A 2014b, "'Żelazna Kopuła' w rękach czerwonego smoka," viewed September 19, 2014, http://www.defence24.pl/blog_zelazna-kopula-w-rekach-czerwonego-smoka.
Kozłowski A 2014a, "Chińscy hakerzy znowu w akcji," viewed September 19, 2014, http://www.stosunki.pl/?q=content/chi%C5%84scy-hakerzy-znowu-w-akcji.
Kozłowski A 2014d, "LEAM Notes 15: The American Pivot to Asia in Cyberspace," viewed September 19, 2014, http://leamplus.eu/leam-notes-15-the-american-pivot-to-asia-in-cyberspace/.
Mandiant 2013, "APT1. Exposing One of China's Cyber Espionage Unit," viewed September 19, 2014, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
Marquand R & Arnoldy B 2007, "China's Hacking Skills in Spotlight," *The Seattle Times*, pp. 16–20.
McAfee 2014, "Revealed: Operation Shady RAT," viewed September 19, 2014, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.
McConnell M 2010, "Mike McConnell on how to win the cyber-war we're Losing," viewed September 19, 2014, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.
Melvin L E 2005, *Study of the Chinese People's Liberation Army Military Region Headquarters Department Technical*, Taiwan.
Mulvenon J 2004, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," viewed September 19, 2014, http://indianstrategicknowledgeonline.com/web/Ch_8-1.pdf.
Passeri P 2012, "Philippines and China, on The Edge of a New Cyber Conflict?," viewed September 19, 2014, http://hackmageddon.com/2012/05/01/philippines-and-china-on-the-edge-of-a-new-cyber-conflict/.
Perlroth N 2013, "Hackers in China Attacked The Times for Last 4 Months," viewed September 19, 2014, http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0.
Pu P 2010, "PLA unveils nation's first cyber center," viewed September 19, 2014, http://www.globaltimes.cn/content/554647.shtml.
Qiao L & Xiangsui W 2009, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing.
RSA 2011, "Anatomy of an Attack," viewed September 19, 2014, https://blogs.rsa.com/anatomy-of-an-attack/.
Segal A 2012, "Chinese Computers Games," *Foreign Affairs*, Vol. 91, No. 2, pp. 14–22.
Sheldon R 2011, "China's Great Firewall and Situational Awarness," *Strategic Insights*, Vol. 10, No. 2, pp. 36–51.
Singer W P & Friedman A 2014, *Cybersecurity and Cyberwar. What everyone need to know*, Oxford University Press, New York.

Stokes A M, Lin J & Hsiao L C R 2011, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, Project 2049 Institute, Arlington.

Striennon R 2010, *Surviving Cyberwar*, The Scarecrow Press, Toronto.

The Globe and Mail 2014, "Chinese cyber attacks hit Japan over islands dispute," viewed September 19, 2014, http://www.theglobeandmail.com/news/world/chinese-cyber-attacks-hit-japan-over-islands-dispute/article4553048/.

The US-China Economic and Security Review Commission 2009, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," viewed September 19, 2014, http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

Thoma L T 2007, *Decoding the Virtual Dragon*, Foreign Military Studies Office, Fort Leavernworth.

TuoiTrens News, "Chinese hackers attack 745 Vietnam websites in a week: report," viewed September 19, 2014, http://tuoitrenews.vn/business/22202/chinese-hackers-attack-745-vietnam-websites-in-a-week-report.

U.S.-China Economic And Security Review Commission 2009, "China's Propaganda And Influence Operations, Its Intelligence Activities That Target The United States, And The Resulting Impacts On U.S. National Security," viewed September 19, 2014, http://origin.www.uscc.gov/sites/default/files/transcripts/4.30.09HearingTranscript.pdf.

Vance A 2010, "China Wrests Supercomputer Title From U.S.," viewed September 19, 2014, http://www.nytimes.com/2010/10/28/technology/28compute.html?_r=0.

Weiguan S, Xijian J, Ji M & Jijin L 2005, *China's Information Warfare,* China Xinhua Press, Beijing.

Węderska K 2014, "Cybernetyczny Pearl Harbor – mit czy rzeczywistość?," in: Górka M (ed.) *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa, pp. 62–81.

Wortzel M L 2014, *The Chinese People's Liberation Army and Information Warfare*, United States Army War College Press, Carlisle.

Xinhua Publishing House 2000, "The Science of Military Strategy," in: *OSC, CPP20000517000168, Excerpt from "World War, The Third World War – Total Information Warfare".*

Zakaria F 2014, "China's Cyberespionage Presents a 21st Century Challenge," viewed September 19, 2014, http://www.washingtonpost.com/opinions/fareed-zakaria-chinas-cyberespionage-presents-a-21st-century-challenge/2014/05/22/5983aaa4-e1f3-11e3-9743-bb9b59cde7b9_story.html.