Chinese Cyber Warfare and its Implications on Selected Southeast Asian States

Francis Rico C. Domingo
International Studies Department, De La Salle University
2401 Taft Avenue, Manila 1004
francis.domingo@dlsu.edu.ph

Cyber warfare is a powerful weapon in political conflicts, espionage, and propaganda. Difficult to detect an attack, it is often recognized only after significant damage has been done. Developing offensive warfare capabilities in cyber domain is a key priority indicated in the national strategies of many countries and is explicitly stated in the doctrines of several, including the People's Republic of China (PRC), the Russian Federation, and the United States of America. Considering these strategies, it is projected that states developing offensive cyber warfare capabilities are laying the groundwork for potential cyber conflicts by hacking the networks of adversaries and allies alike.[1] The most active of these states is the PRC which has initiated the production of a new generation of offensive cyber weapons and has continued to train a professional corps of cyber warriors that promise reshape how war is fought in the twenty-first century.

An early example of PRC's engagement in cyber warfare was in 1999 when several U.S. government websites were attacked by suspected Chinese hackers in the aftermath of the unintended, as officially reported, U.S. bombing of the Chinese Embassy in Belgrade on 7 May 1999.[2] Cyber warfare has generally manifested as nuisance attacks (such as website defacement and denial-of-service or DoS attacks), with only sporadic incidents of espionage and infrastructure probes. In rare cases, these attacks have caused extensive failure of the public Internet but have not resulted in large scale injury, loss of life, or destruction of property. However, in recent years, PRC's offensive cyber warfare capabilities have become more disturbing, as it has launched an undefined number of cyber reconnaissance and offensive operations with unknown intent against a variety of countries.[3]

With this background, this paper argues that the cyber warfare capabilities of the PRC is a significant threat to member states of the Association of Southeast Asian Nations (ASEAN), leaving it defenceless in the event of a major cyber attack. The paper examines the cyber warfare capabilities of the PRC in the context of the following questions: *What is cyber warfare? How extensive are the cyber warfare capabilities of the PRC? What is the PRC's intention in building up its cyber warfare capabilities? Given the territorial dispute in the South China Sea, what are the implications of the PRC's cyber warfare capabilities on Vietnam and the Philippines?* The paper concludes that the PRC has the capability and intention to engage in cyber warfare with selected ASEAN member states given the existing territorial dispute in the South China Sea.

---

[1] Goel, Sanjay. 'Cyberwarfare: Connecting the Dots in Cyber Intelligence' *Communications of the AGM* (August 2011) Vol. 54 No. 5

[2] CNN, "Hackers Attack U.S. government Web sites in protest of Chinese embassy bombing," May 10, 1999 http://articles.cnn.com/1999-05-10/tech/9905_10_hack.attack_1_hackers-white-house-site-web-sites?_s=PM:TECH

[3] Magnus Hjortdal, 'China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence' *Journal of Strategic Security* (2011) Volume 4 Issue 2, pp. 1-24.

Cyber War as a contested concept

The concept of cyber war was first introduced by John Arquilla and David Ronfelt in their seminal article "Cyberwar is coming!" published in 1993. In the article Arquilla and Ronfelt described cyber war as a form of warfare that disrupts if not destroys information and communications systems. They also argued that due to the shift in technology or "information revolution", cyber war would become a dominant of mode of conflict and warfare.[4] Since then, the emerging academic literature that focuses on cyber war has generally been influenced by two dominant arguments perpetuated by cyber experts from academia and government institutions.

The first argument which was proposed by Arquilla and Ronfelt, maintains that cyber warfare is an emerging mode of conflict that persists and continues develop.[5] They argue that the cyber attacks against Estonia in 2007 and the cyber attacks against Georgia's command, control and communication systems during the Russo-Georgian conflict in 2008 illuminates the potential of cyber war.[6] Other experts such as Dorothy Denning, supports this perspective by arguing that while future war cannot be predicted, "information warfare, in all its manifestations - espionage, intelligence operations to electronic warfare to psychological operations and perception management" will play an important role throughout history.[7] Richard Clarke maintains that cyber war is the most significant threat facing the United States and proposes measures such as the creation of a "Defensive Triad" and the implementation of a "Cyber War Limitation Treaty" to address the threat.[8] George Rattray points out that "the use of non-violent digital attacks to achieve political objectives must be understood as part of a new form of warfare."[9] Finally, prominent strategic studies scholar Colin Gray contributes to the debate by contending that cyberwarfare is all about information, it "refers to warfare in cyberspace; bloodless electronic warfare in the struggle or deny or gain information."[10]

The second argument which criticizes cyber warfare describes the concept as doubtful and misleading. Martin Libicki, one of the main proponents of this argument, cautions that the possibilities of 'hostile conquest' in cyber space "may be less consequential than meets the eye."[11] Furthermore, Libicki suggests that the concept that cyberspace as a war fighting domain is misleading because the concept is "not helpful when it comes to understanding what can and should be done to defend and attack networked systems."[12] David Betz argues that the concept of cyberwar as a "single focus" option for states is unrealistic because of the expanse and range of their interests and capabilities."[13] As an alternative, Betz proposes "cyber-skirmish" as the correct frame to describe current low-level cyber attacks against

[4] John Arquilla and David Ronfeldt, 'Cyberwar is Coming!' *Comparative Strategy*, Vol 12, No. 2 (Spring 1993): 31-32
[5] Ibid
[6] John Arquilla, 'Cyberwarfare Is Already Upon Us' *Foreign Policy* March/April 2012, http://www.foreignpolicy.com/ articles/2012/02/27/cyberwar_is_already_upon_us
[7] Dorothy Denning, *Information Security and Warfare*
[8] Richard Clarke and R. Knake, *Cyberwar: The Next Threat to National Security and What to Do About it,* HarperCollins: New York, 2010.
[9] Gregory J. Rattaray, *Strategic Warfare in Cyberspace* Massachusetts: MIT Press, 2001, pp. 17-19.
[10] Colin Gray, *Another Blood Century Future Warfare,* (London: Orion Book Ltd., 2005): 315
[11] Martin Libicki, *Conquest in Cyberspace National Security and Information Warfare*, Cambridge: Cambridge University Press.
[12] Martin Libicki, 'Cyberspace Is Not a Warfighting Domain' *I/S: A Journal of Law and Policy for the Information Society* Vol. 8:2 (2012): 321-336.
[13] David Betz and Tim Stevens, *Cyberspace and the State*, London: The International Institute of Strategic Studies, 2011, pp. 95-97

different states."[14] Thomas Rid contends that previous reports of cyber attacks were not really acts of war because these attacks do not fall within the definition of war as describe by Clausewitz which has to be "violent, instrumental in character, and politically attributed".[15] Therefore according Rid, a cyber war has never happened in the past and it is unlikely that it will occur in the future. Bruce Schneiner, on the other hand argues that the threat of a cyber war has been "exaggerated" due to a power struggle between US government agencies that are trying to control the state's cyber security strategy.[16] Due to the persistence of the U.S. Department of Defense and the National Security Agency, cyberspace has largely been "militarized" through discussions of a cyber war allowing military to control the current US cyber security strategy.

Debates regarding the nature and validity of cyber warfare have transformed the concept into a strategic agenda which has influenced powerful states to develop offensive and defensive capabilities in cyberspace. For example, Timothy Thomas maintains that Chinese and Russian cyber capabilities have increasingly been more visible and disturbing in the past decade. The PRC has launched an unknown number of cyber reconnaissance and offensive activities including espionage conducted in 2005 against computer networks of the U.S. Department of Defense and attacks against a U.S. satellite using high-powered laser attacks in 2006.[17] Russia for its part has recognized the importance of enhancing its cyber capabilities. A report by the reputable think tank Chatham House indicates that Russia utilized cyber technology as part of a 'coordinated and synchronized kinetic and non-kinetic campaign through distributed denial of service (DDoS) attacks which appeared to be orchestrated with military and political operations in both Estonia in 2007 and Georgia in 2008.[18]

With this operating environment, the U.S. government has started exploiting the cyber domain in support of U.S. national interests, to the extent of conducting defensive and offensive operations in cyberspace. Since the U.S considers cyberspace as 'a warfighting domain'[19], it established in June 2009, a dedicated command for military cyber issues or Cyber Command (Cybercom). The creation of Cybercom is a strong statement of intent that confirms how serious the political and military leadership of the U.S. perceives cyber threats to be.

On Cyberpower and Cyber Warfare

To defend their national interests and to gain power over their rivals, states develop military capabilities which are developed in each of the natural domains: sea power, land power, air power and space power. The purpose of these powers is for states to establish control and exert influence within and through the domains, control and influence being steps toward the

[14] Ibid
[15] Thomas Rid. 'Cyber War Will Not Take Place' *Journal of Strategic Studies*, (2012) Volume 35 Number 1, pp. 5-32.
[16]Bruce Schneiner, 'Threat of "Cyberwar" Has Been Hugely Hyped' *CNN Opinion*, July 7, 2010. http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/ [Accessed on 7 March 2012].
[17] Timothy Thomas, "Nation-state Cyber Strategies" in *Cyberpower and National Security*, eds. Frankin D. and others (Virginia: National University Press, 2009): p. 466
[18] Paul Cornish, David Livingstone and others, *On Cyberwarfare: A Chatham House Report,* London: Royal Institute of International Affairs (Chatham House), 2010
[19] Keith Alexander, 'Warfighting in Cyberspace', *Joint Forces Quarterly* Issue 46 (3rd Quarter 2007), p. 60

state achieving its national interests.[20] States create armies to control, defend, and extend their borders; navies to protect their coasts, control sea lanes, and attack others' by sea; air and outer space forces to attack through the sky, defend against like attacks, and monitor adversaries. Each of these powers is intended to secure a domain to the advantage of the state. These powers can also support and strengthen the powers dominant in the other domains. Land power protects ports and airfields from which sea and air power originates. Air and space power provides overhead protection for land and sea power. Air and sea power allows land power projection. While designed to operate primarily in its own domain, each of the powers can exert influence into the other domains.[21]

Cyberpower is the ability of states to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.[22] Obtaining cyberpower is dependent on the state's ability to develop appropriate resources to operate in cyberspace. Cyberpower as part of the capability of a state is equal to land, sea, air, or space power. Instead of tanks, warships, and aircrafts, the state needs networked computers, telecommunication infrastructure, programs and software, and "cyber warriors" or people with the necessary skills to understand how to fight a cyber war.[23] As with the land, sea, air, and space domains, the state can generate outcomes within cyberspace or into another domain through cyberspace. A cyber attack could corrupt an adversary's logistics database, degrading the adversary's rapid deployment capabilities or block the signals of a global positioning satellite, interfering with a warship's ability to navigate or target its weapons systems.[24]

The U.S. Department of Defense refers to applications of cyberpower as Computer Network Operations (CNO) and divides them into three categories: Computer Network Defense (CND), Computer Network Attack (CNA), and Computer Network Exploitation (CNE).[25]These categories are similar to the PLA's perception of cyber warfare. The offensive capabilities of cyberpower are CNA and CNE. CNA are destructive, "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves."[26] The direct objective of CNA is to deny the enemy the ability to use their computer systems, stored information, and networks as designed or intended. The secondary objective is to disrupt all those people, systems, or organizations that rely on that information technology, interfering with or denying them the ability to function, much like the effects of a distributed denial of service attack.[27]

CNEs on the other hand are intrusive, involving unauthorized entry into a network, but do not necessarily cause damage. CNEs are "enabling operations and intelligence collection to gather data from automated information systems or networks." As an enabler, a CNE not only gathers information, but can map networks for future attacks and can leave behind backdoors or malware designed to execute or facilitate an attack. Finally, CND involves defensive

[20] Daniel Kuehl, 'From Cyberspace to Cyberpower' in *Cyberpower and National Security*, eds. Frankin D. and others (Virginia: National University Press, 2009): 38
[21] Jayson Spade, *Information as Power: China's Cyber Power and America's National Security*, (Carlisle, Pennsylvania:U.S. Army War College, 2012): 6-7
[22] Daniel Kuehl, *From Cyberspace to Cyberpower* p. 38
[23] Richard Clarke *Cyberwar: The Next Threat*, p. 34
[24] Jayson Spade, *Information as Power*, p. 6-7
[25] Dorothy Denning, 'Computer Network Operations' in *Information Strategy and Warfare*, eds. John Arquilla and Douglas Borer, p. 189
[26] Timothy Thomas, *Nation-state Cyber Strategies*, pp. 466-467
[27] Jayson Spade, *Information as Power* pp. 6-7

measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.[28] For instance, preventing a hostile cyber power from retrieving the procurement system and introducing hardware or software equipped with malicious code: "back doors for future access, logic bombs to create on demand malfunctions, viruses to infect a network, or kill switches to bring down parts of the network."[29]

The PRC will utilize these tools to pursue its national interests. Studies completed by the U.S. government and independent think tanks indicate that China has three primary national security objectives[30]: sustaining regime survival (rule of the Chinese Communist Party), defending national sovereignty and territorial integrity, and establishing China as both a regional and world power. Vital to these objectives are sustaining stable economic and social development, modernizing the military, and preventing Taiwan's independence. The CCP must maintain a position of national and international strength to sustain China's security and their legitimacy as the PRC's ruling body. [31]

From the perspective of the PRC, they are a rising global power and the U.S., as the only superpower, is the standard for military technological achievement and its principal adversary for regional dominance.[32]The PRC views the U.S. as trying to encircle and contain it with military bases and alliances with in surrounding states. It sees U.S. concerns over human rights, particularly concerning groups the CCP sees as subversive or separatist elements, as a means of destabilizing the regime. Moreover, the U.S. relationship with and military support for Taiwan is a significant issues because it threatens the PRC's national sovereignty and regime legitimacy.[33]

Framework and Methodology

In analysing Chinese cyber warfare capabilities this paper adopts a framework developed by Professor Dorothy Denning of Georgetown University. Denning argues that cyber threats from nation-states are a function of three factors: intention, capability and opportunity.[34] To simplify the framework, the paper equates "opportunity" with existing contentious issues between the PRC and selected ASEAN member states. Regarding "intention", the paper considered any credible official document or published statements by Chinese government officials or its military leaders concerning adoption of an offensive cyber warfare program as sufficient to imply motivation to at least develop a cyber attack capability.[35]

This paper will utilize content analysis to establish that Chinese cyber warfare is a significant threat to selected ASEAN states. More specifically it will examine primary sources such as

[28] Dorothy Denning, *Computer Network Operations*, p. 189
[29] Jayson Spade, *Information as Power*, p. 9
[30] See for example Billo, Charles and Chang,Welton. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States*, (New Hampshire: Institute for Security Technology Studies, Dartmouth College, 2004), James Mulvenon et al., *Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense* (Arlington, Virginia: Rand Corporation, 2006): 7-8; Office of the Secretary of Defense, *Annual Report on Military and Security Developments Involving the People's Republic of China 2010* (Washington DC: U.S. Department of Defense, 2010).
[31] Jayson Spade, *Information as Power*, p. 11
[32] Jason Fritz, 'How China will use Cyber Warfare to Leapfrog in Military Competitiveness' *Culture Mandala*, Vol. 8, No. 1, (October 2008): 40.
[33] *China's National Defense in 2010*, p. 4; *US National Security Strategy 2010*, p. 43
[34] Dorothy Denning, *Information Security and Warfare*, p. 12
[35] Charles Billo and Welton Chang, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* (New Hampshire: Institute for Security Technology Studies, Dartmouth College, 2004).

government documents, official government statements and government websites. Since states only disclose general information about their cyber warfare programs, the paper will also rely on secondary sources including journal articles, books, independent policy studies, and newspaper articles to supplement the data collected from primary sources.

Assessing Chinese capabilities

During the early 1990s, the PRC's military recognized that a revolution of military affairs (RMA) was emerging which resulted from new possibilities made available by information technologies. PRC's military started looking into cyber attacks as method of countering a technologically superior adversary within and outside of the battlefield. With the support of an integrated national plan, the People's Liberation Army (PLA) developed a cyber warfare doctrine which focuses on applying information technologies to command, intelligence, training, and weapon systems.[36] This emerging doctrine is based on what the PLA calls "informationization" or adapting to the changes of the international security environment and the increasing challenges presented by the RMA worldwide.[37]

Several intrusions including the "Titan Rain" cyber espionage ring in 2004 and the attacks against Pentagon computer network in September 2007 indicates that the Chinese government condones and may even sponsor computer hacking.[38] The PRC's intelligence services continue their systematic collection of highly sensitive information pertaining to newly developed military hardware and software and commercial information technology assets. While military cooperation with Russia, a country that may have developed a substantial cyber warfare program, continues, the PRC may be developing its own models for military information collection and for the use of cyber attack technologies.[39]

Opportunity

The territorial dispute over Spratly and Parcel Islands in the South China Sea is a contentious issue that can potentially instigate cyber conflict between the PRC and five claimant states - Brunei, Malaysia, Vietnam, Taiwan, and the Philippines. Considering that the South China Sea is considered a "core interest" of the PRC, control of this international waterway is critical to its national security. If the PRC chooses to flex its newly developed military muscle, it is likely that it will attempt to seize the disputed islands to reinforce its "indisputable sovereignty over the islands of the South China Sea and adjacent waters."[40] Given this scenario, the PRC will prioritize executing cyber attacks against more assertive claimant states such as Vietnam and the Philippines much like the attacks it carried out against the two states during the past two years.[41] Both states are allies of the U.S., with the Philippines engaged in a treaty alliance and Vietnam identified as prospective 'strategic

[36] Charles Billo and Welton Chang, *Cyber Warfare*, p. 25
[37] Gurmeet, Kanwal, 'China's Emerging Cyber War Doctrine' *Journal of Defence Studies* Vol 3 No. 3 (2009)
[38] Thornburgh, Nathan, 'The Invasion of the Chinese Cyberspies' *Time,* August 29, 2005, http://www.time.com/time/magazine/article/0,9171,1098961,00.html [Accessed on October 27, 2012]
[39] Charles Billo and Welton Chang, *Cyber Warfare*
[40] Embassy of the People's Republic of China in the United States of America, "China Stresses Fishery Vessel on 'Routine Mission' in South China Sea," *Xinhua*, March 17, 2009, at *http://www.china-embassy.org/ eng/zt/xw/t542994.htm* [Accessed on 14 March 2012]
[41] Lee-Brago, Pia, 'DFA slams cyber attacks on Philippines, Chinese websites' *The Philippine Star*, April 24, 2012, http://www.philstar.com/Article.aspx?publicationSubCategoryId=63&articleId=800135 and
Son , Truong, 'Vietnam's websites attacked; Chinese hackers under suspicion' *Thanh Nien News*, July 8, 2011. http://www.thanhniennews.com/2010/pages/20110610135830.aspx

partner' in Southeast Asia,[42] therefore prompting the PRC to adopt a more aggressive posture towards these two states.

Furthermore, expansive claims by the PRC through the use of cyber warfare threaten not only claimant states, but also the ability of the United States, to execute naval operations in open seas and eventually, the security of the sea-lanes through which much of the world's trade passes.[43] More importantly, according to former Defense Secretary Robert Gates the threat of cyber attacks from the PRC may deter force projection, preventing the U.S. from "helping its allies in the Pacific."[44] Although the PRC continues to maintain the largest conventional military force in the world, it knows that its PLA has limited effectiveness due to its incapacity to fight an all-out conventional war with the U.S. as a result, Chinese strategists believe that advanced cyber warfare strategies can play a critical role in an asymmetric victory.[45]

Intention

The PRC's cyber warfare doctrine indicates that the PLA seeks to achieve global "electronic dominance" by 2050, which includes targeting its adversary's financial markets, military and civilian communications capabilities and critical infrastructure before traditional military operations begin. In 1999, the *PLA Daily* stated, "Internet warfare is of equal significance to land, sea and air power and requires its own military branch."[46]

The PRC's intention to employ offensive cyber warfare can be derived from the statements and official documents promoting the use of asymmetric warfare strategies. In July 2004, Jiang Zemin, the Chairman of the Central Military Commission, Communist Party of China emphasized the importance of information technology in advancing Chinese military capability and achieving the "strategic goal of winning information warfare".[47] The impetus for the advancement of Chinese strategy in the area of cyber warfare started during the early 1990s. In the aftermath of the first Gulf War in 1991, the Chinese government and PLA doctrinal thinkers began to analyze the U.S. military victory.[48]

During the first Gulf War, American and Coalition forces utilized coordinated electronic attacks to disable the Iraqi air defense network and to shut down the various power systems around Iraq. In the initial engagement, Tomahawk missiles and precision-guided bombs from F-117 Stealth fighters destroyed most of Iraq's command and control capabilities, as well as its information gathering radar sites. More significantly, Coalition forces further disabled Iraqi military computer systems by employing a computer virus that disabled Windows and mainframe computers. The virus was installed in a dot matrix printer that was assembled in France and shipped to Iraq via Amman, Jordan.[49] The PRC, and other advanced states,

[42] Hillary Clinton, 'America's Asian Century' *Foreign Policy*, November 2011
[43] Renato De Castro and Walter Lohman, *Empowering a New Era in the United States–Philippines Security Alliance* (Washington D.C.: The Heritage Foundation, 2010): 2
[44] Richard Clarke *Cyberwar: The Next Threat*, p. 34
[45] Charles Billo and Welton Chang, *Cyber Warfare*, p. 29
[46] Mike, McConnell, *Cyber Insecurities: The 21st Century Threatscape* in America's Cyber Future: Security and Prosperity in the Information Age Volume 2 eds. Kristin M. Lord and Travis Sharp. (Washington D.C.: Center for New American Security, 2011): 30.
[47] Office of the Secretary of Defense, *Annual Report to Congress*, p. 3
[48] Charles Billo and Welton Chang, *Cyber Warfare*
[49] Dorothy Denning, *Information Security and Warfare*, p. 5

viewed the overwhelming victory combining information technologies and conventional power as a Revolution in Military Affairs.[50]

In the reports and statements released by the Chinese government regarding on cyber warfare, two main ideas can be deduced. First, cyber warfare strategy (as with conventional warfare) in Chinese literature refers to Sun Tzu in practically every written document. While the actual effect of Sun Tzu's strategic principles of warfare on the modern Chinese variety is hard to determine, it is clear that Sun Tzu is a great influence, at the least, on Chinese doctrinal writing. Second, a cyber warfare strategy is in keeping with national goals of the PRC because it is a cost-effective way of conducting asymmetric operations against an enemy.[51]

Capability

PLA leaders have accepted the idea that successful war fighting is predicated on the ability to exert control over an enemy's information and information systems, often proactively. This objective has created a new strategic and tactical high ground, occupying which has become as crucial as controlling the battle space in the physical domain.[52]

The PLA has not overtly disclosed the existence of a computer network operations strategy distinct from other elements of cyber warfare, such as electronic warfare, psychological operations, kinetic strike, and deception, but rather appears to be working toward the integration of cyber warfare with these components in a unified framework broadly known as "information confrontation." This concept, as discussed by the PLA, seeks to incorporate all elements of cyber warfare—electronic and non-electronic—offensive and defensive under a single command authority.[53]

In the past decade, the PLA adopted a multifaceted approach to offensive information warfare that it calls "Integrated Network Electronic Warfare".[54] The INEW Strategy consolidates the offensive mission for both Computer Network Attack (CNA) and Electronic Warfare (EW) under 4th Department of PLA General Staff Department (4PLA). The Computer Network Defence and intelligence gathering responsibilities are likely assigned to the Third Department of the General Staff Department (3PLA). In addition the strategy also integrates different specialized cyber warfare militia units composed of members with skills in essential high technology areas.[55]

Currently, the PLA is progressing towards information confrontation as a broader conceptualization that aims to unite the various components of cyber warfare under a single commander. Coordinating offensive and defensive missions is essential considering that these missions are mutually supporting and driven by the recognition that cyber warfare must be closely integrated with PLA campaign objectives. The establishment of a prospective information assurance command in the General Staff Department suggests that the PLA

[50]Charles Billo and Welton Chang, *Cyber Warfare*

[51] Ibid

[52] Patton Adams, George Bakos, Bryan Krekel. *Occupying the Information High Ground Chinese Capabilities for Computer Network Operations and Cyber Espionage,* (Washington D.C.: U.S.-China Economic and Security Review Commission, 2012): 8

[53] Ibid

[54] Deepak Sharma, 'Integrated Network Electronic Warfare: China's New Concept of Information Warfare' *Journal of Defence Studies* Vol 4 No. 2 (2010).

[55] Deepak Sharma, 'Integrated Network Electronic Warfare', p. 37

might be creating a central command authority for cyber warfare that will likely be responsible for consolidating all efforts that lead to network defense.[56]

Implications on the Philippines

The Philippines does not have the capacity to engage in cyber warfare or even defend itself from sophisticated cyber attacks such as the distributed denial of service attacks in Estonia in 2007. Currently, the Armed Forces of the Philippines (AFP) is shifting its focus from countering internal security threats to addressing territorial defense issues in the South China Sea. Based on the *National Security Policy 2011-2016*, the priorities of the government in terms of territorial defense focus on three main areas: pursuing regional cooperation with various states such as ASEAN member states; to enhancing our cooperative security arrangements with allies and neighbors; and developing a defense capability to protect Philippine sovereignty and strategic maritime interests.[57] Therefore, establishing a program that progresses cyber warfare capabilities of the AFP is not a main priority of the current government.

The only discussion regarding the development of cyber warfare capabilities in the Philippines is outlined in the *National Cybersecurity Coordination Strategy and Implementation Plan* which was crafted by the previous government in 2008. According to this document, developing cyber warfare capabilities is a significant component of a state's cyber security. It delineates that "the AFP shall be responsible for implementing a cyber warfare program which is designed to conduct intelligence operations against potential threats as a way to better know them in terms of organization, modus operandi, plans and linkages."[58] The substance of the plan however, focuses on implementing measures that address cyber crimes like computer fraud, hacking, pornography and spreading malware not cyber attacks from states like China and Russia.

To address constant cyber attacks, the Philippine government responds through its National Cybersecurity Office (NCSO) and the National Computer Emergency Response Team (N-CERT). The N-CERT functions like a command center that monitors cyber incidents and coordinates different response mechanisms with relevant government agencies including the Government Computer Security and Incident Response Team of the Criminal Investigation and Detection Group, the Anti-Fraud and Cyber Crime Division of the National Bureau of Investigation, and professional organizations such as the PH Computer Emergency Response Team (PH-CERT), the Information Systems Security Specialists of the Philippines (ISSSP) and the Philippine Certified Information Systems Security Professionals (PH-CISSP). While the NCSO maintains an extensive database of cyber incidents and operates as the integrating office where various government agencies collaborate efforts and share information.[59]

[56] Patton Adams and others, *Occupying the Information High Ground*, p. 8

[57] Office of the President, *National Security Policy 2011-2016,* (Quezon City: National Security Council, 2011): 39-30

[58] Office of the President, *National Cybersecurity Coordination Strategy and Implementation Plan,* (Quezon City: National Security Council, 2008)

[59] Malou Santelices, *Cyberspace: Threats and Challenges*, (Quezon City: National Cybersecurity Office, 2010), slides.

Bibliography

Adams, Patton, Bakos, George, Krekel, Bryan. *Occupying the Information High Ground Chinese Capabilities for Computer Network Operations and Cyber Espionage,* Washington D.C.: U.S.-China Economic and Security Review Commission, 2012.

Alexander, Keith, 'Warfighting in Cyberspace', *Joint Forces Quarterly* Issue 46 (3rd Quarter 2007)

Arquilla, John 'Cyberwarfare Is Already Upon Us' *Foreign Policy* March/April 2012, http://www.foreignpolicy.com/ articles/2012/02/27/cyberwar_is_already_upon_us

Arquilla, John and Ronfeldt, David, eds. *In Athena's Camp Preparing for Conflict in the Information Age,* Santa Monica, California: RAND Corporation, 1999.

Arquilla, John and Ronfeldt, David, 'Cyberwar is Coming!' *Comparative Strategy*, Vol 12, No. 2 (Spring 1993): 141-165.

Betz, David and Stevens, Tim, *Cyberspace and the State Towards a Strategy for Cyberpower*, London: The International Institute of Strategic Studies, 2011.

Billo, Charles and Chang,Welton. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States*, New Hampshire: Institute for Security Technology Studies, Dartmouth College, 2004.

Clarke, Richard. and Knake R. *Cyberwar: The Next Threat to National Security and What to Do About It,* HarperCollins: New York, 2010.

Clinton, Hillary, 'America's Asian Century' *Foreign Policy,* November 2011.

CNN, "Hackers Attack U.S. government Web sites in protest of Chinese embassy bombing," May 10, 1999, http://articles.cnn.com/1999-05-10/tech/9905_10_hack.attack_1_hackers-white-house-site-web-sites?_s=PM:TECH

Cornish, Paul, Livingstone, David, Clemente, David and Yorke, Claire. *On Cyberwarfare: A Chatham House Report,* London: Royal Institute of International Affairs (Chatham House), 2010.

De Castro, Renato and Lohman, Walter, *Empowering a New Era in the United States–Philippines Security Alliance* Washington D.C.: The Heritage Foundation, 2010.

Denning, Dorothy E., *Information Security and Warfare*, Addison Wesley: New York, 1999.

Embassy of the People's Republic of China in the United States of America, "China Stresses Fishery Vessel on 'Routine Mission' in South China Sea," *Xinhua*, March 17, 2009, at *http://www.china-embassy.org/eng/zt/xw/t542994.htm* [Accessed on March, 14 2012].

Fritz, Jason. 'How China will use Cyber Warfare to Leapfrog in Military Competitiveness' *Culture Mandala,* Vol. 8, No. 1, (October 2008): 28-80.

Goel, Sanjay. 'Cyberwarfare: Connecting the Dots in Cyber Intelligence' *Communications of the AGM* Vol. 54 No. 5 (August 2011): 132-140.

Gray, Colin, *Another Blood Century Future Warfare,* London: Orion Book Ltd., 2005.

Hjortdal, Magnus. 'China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence' *Journal of Strategic Security* Vol 4 Issue 2 (2011):1-24.

Kanwal, Gurmeet, 'China's Emerging Cyber War Doctrine' *Journal of Defence Studies* Vol 3 No. 3 (2009)

Kramer, Frankin D. and Stuart, Starr H. and Wentz, Larry K., eds. *Cyberpower and National Security* Virginia: National University Press, 2009.

Lee-Brago, Pia, 'DFA slams cyber attacks on Philippines, Chinese websites' *The Philippine Star*, April 24, 2012, http://www.philstar.com/Article.aspx?publicationSubCategoryId=63&articleId=800135

Libicki, Martin, *Conquest in Cyberspace National Security and Information Warfare*, New York: Cambridge University Press, 2007.

Libicki, Martin. 'Cyberspace Is Not a Warfighting Domain' *I/S: A Journal of Law and Policy for The Information Society* Vol. 8:2 (2012): 321-336.

Lynn, William. 'Defending a New Domain' *Foreign Affairs* Volume 89 Number 5 (2010): 97-108.

McConnell, Mike, *Cyber Insecurities: The 21st Century Threatscape* in America's Cyber Future: Security and Prosperity in the Information Age Volume 2 eds. Kristin M. Lord and Travis Sharp. Washington D.C.: Center for New American Security, 2011.

Mulvenon, James et al., *Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense*, Arlington, Virginia: Rand Corporation, 2006.

Nicoll, Alexander. 'Behind the recent gunboat diplomacy in the South China Sea' *Strategic Comments* Vol 17 Comment 28 London: The International Institute of Strategic Studies, 2011.

Office of the Secretary of Defense, *Annual Report on Military and Security Developments Involving the People's Republic of China 2010,* Washington DC: U.S. Department of Defense, 2010.

Office of the President, *National Cybersecurity Coordination Strategy and Implementation Plan,* Quezon City: National Security Council, 2008.

Office of the President, *National Security Policy 2011-2016,* Quezon City: National Security Council, 2011.

Rattaray, Gregory J, *Strategic Warfare in Cyberspace* Massachusetts: MIT Press, 2001

Rid, Thomas. 'Cyber War Will Not Take Place' *Journal of Strategic Studies*, Volume 35 Number 1, (2012): 5-32.

Schneiner, Bruce. 'Threat of "Cyberwar" Has Been Hugely Hyped' *CNN Opinion,* July 7, 2010. http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/ [Accessed on 7 March 2012].

Son , Truong. 'Vietnam's websites attacked; Chinese hackers under suspicion' *Thanh Nien News,* July 8, 2011. http://www.thanhniennews.com/2010/pages/20110610135830.aspx [Accessed on 7 March 2012].

Spade, Jayson, *Information as Power: China's Cyber Power and America's National Security*, Carlisle, Pennsylvania: U.S. Army War College, 2012.

Rogin Josh. 'The Top 10 Chinese Cyber Attacks' *Foreign Policy* January 22, 2010, *http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we _know _of* [Accessed on March 9, 2012].

Santelices, Malou, *Cyberspace: Threats and Challenges,* (Quezon City: National Cybersecurity Office, 2010), slides.

Sharma, Deepak, 'Integrated Network Electronic Warfare: China's New Concept of Information Warfare' *Journal of Defence Studies* Volume 4 Number 2 (2010): 36- 49.

Thornburgh, Nathan, 'The Invasion of the Chinese Cyberspies' *Time,* August 29, 2005, http://www.time.com/time/magazine/article/0,9171,1098961,00.html [Accessed on October 27, 2012].

Thomas, Timothy, "Nation-state Cyber Strategies" in *Cyberpower and National Security*, eds. Frankin D. and others. Virginia: National University Press, 2009.