REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 10/27/2017	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE Cyber Engagement with the Philippines: Bolstering a Key Ally's Cyber Defenses	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Borovies, Jason A., LtCol, USMC	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Military Operations Department Naval War College 686 Cushing Road	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited Ref: DODD 5230.24

13. SUPPLEMENTARY NOTES

A paper submitted to the Naval War College in partial satisfaction of the requirements of the JMO Department. The

14. ABSTRACT

15. SUBJECT TERMS

Philippines, China, Cybersecurity, Network Warfare, South China Sea, Cyber Warfare, Cyber Engagement

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Chairman, JMO Department, USNWC
UNCLASS	UNCLASS	UNCLASS		17	**19b. TELEPHONE NUMBER** *(Include area code)* 401-841-3556

Cyber Engagement with the Philippines: Bolstering a Key Ally’s Cyber Defenses

Jason Andrew Borovies

A paper submitted to the Faculty of the United States Naval War College Newport, RI in partial satisfaction of the requirements of the Department of Joint Military Operations.

DISTRIBUTION A. Approved for public release: distribution unlimited. The contents of this paper reflect the author’s personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

October 9, 2017
Word Count 4,846

CONTENTS

ABSTRACT

Cyber Engagement with the Philippines: Bolstering a Key Ally's Cyber Defenses

Tensions between China and the Philippines relating to overlapping maritime claims in the South China Sea are likely to persist. Should these tensions escalate, the first shots of any China-Philippines conflict will likely be fired in cyberspace and see China employ its arsenal of potent network warfare capabilities against an opponent that is uniquely vulnerable to cyber attack. The Philippine economy depends on information communications technology; financial remittances from overseas Filipino workers and the business process outsourcing sector together generate revenues equivalent to approximately 20% of Philippine gross domestic product. Furthermore, endemic software piracy makes penetrating Philippine networks less complicated for an adversary. U.S. Pacific Command should take steps to bolster the cyber defenses of the Philippines, a key U.S. ally, through "cyber engagement." Engagement activities should complement Filipino efforts outlined in the Philippine *National Cybersecurity Plan 2022*. Specifically, USPACOM should support the development of computer emergency response teams by the Philippine Department of Defense and Armed Forces of the Philippines regional unified commands. Cyber events should be incorporated into U.S.-Philippine military exercises synchronized with Philippine national cyber drills. Also, USPACOM should support the development of a regional, cooperative cybersecurity framework in Southeast Asia along with a cybersecurity center of excellence.

Admittedly, the Philippines' state of cybersecurity is still at its infancy stage…

-Philippines *National Cybersecurity Plan 2022* (May 2017)

INTRODUCTION

Tensions between the People's Republic of China (PRC) and the Republic of the Philippines relating to overlapping maritime claims in the South China Sea have already resulted in shots fired and even death. With no agreed-upon code of conduct to regulate relationships between claimant nations in the region, this source of tension is unlikely to ease anytime soon. Friction between China and the Philippines may escalate in the future and lead to open conflict. Chinese literature on warfare indicates the PRC will employ a combination of means to coerce an adversary in the event of conflict, including network warfare. China possesses a potent arsenal of network warfare means and is capable of conducting sophisticated operations against an adversary in the domain of cyberspace. Should the PRC execute a campaign of cyber attacks targeting the Philippines such as those executed by Russia against Estonia and Georgia in 2007-8, the effects would be devastating. Taking financial and government websites offline while isolating Philippine networks from the global internet would paralyze a nation whose economy relies on remittances from overseas workers and business process outsourcing.

Although the Government of the Philippines recognizes the importance of cybersecurity, its information infrastructure is especially vulnerable to attack owing to endemic software piracy as demonstrated by recent, high-profile hacks. As the Philippines is a key U.S. ally in the Asia-Pacific Region per the provisions of a 1951 mutual defense treaty and the 2014 Enhanced Defense Cooperation Agreement, Philippine vulnerabilities to cyber attack and any conflicts with China are very concerning. Given China-Philippines tensions, the significant capabilities of the PRC to conduct network warfare, and Philippine vulnerabilities to cyber attack, United States Pacific Command (USPACOM) should support efforts by America's Filipino allies to improve their cyber defense capabilities through "cyber engagement."

BACKGROUND

Overlapping maritime claims in the South China Sea are a significant source of tension between China and the Philippines. As the primary economic artery between the Indian and Pacific Oceans, the South China Sea is vital to the global economy. Occasionally, it is referred to as a "Second Persian Gulf" due to vast underlying petroleum and natural gas reserves, which are crucial to the continued development of the Philippine economy..[1] The PRC claims virtually all features and waters in the South China Sea. The so-called "nine-dash line" marks the limits of what China claims are historical waters, now considered part of the Sansha City prefecture of Hainan Province established in 2012. Philippine claims in the South China Sea, notably over Scarborough Shoal and the Spratly Islands (called the Kalayaans by Filipinos) conflict with Chinese maritime claims. Philippine claims are based on the definitions of territorial seas and exclusive economic zones per the United Nations Commission on the Law of the Sea (UNCLOS). Although the Permanent Court of Arbitration (PCA) for the UNCLOS struck down Chinese claims in 2016 following an arbitration case brought by the Philippines, in which the PRC declared it would not participate, there is no indication China intends to abide by this ruling. Also, ongoing Chinese efforts to expand South China Sea outposts on features such as Fiery Cross, Subi, and Mischief Reefs make Chinese control a *fait accompli*, indicating the source of friction

[1] Shicun and Hong, *Recent Developments in the South China Sea Dispute*, xv.

associated with overlapping maritime claims between the two nations is likely to persist. Incidents linked to territorial disputes in the South China Sea, which have occurred frequently since 1945, could escalate into a serious conflict between the Philippines and China.

Since the Second World War, at least 19 incidents associated with China-Philippines territorial disputes have occurred in the South China Sea and indicate a propensity for future conflict.[2] These incidents include arrests of fishermen, ship collisions, and firing warning shots. In 2000 during an exchange of fire between the Philippine Coast Guard and Chinese fishermen, the captain of a Chinese fishing vessel was killed. In 2011 off Reed Bank in the Spratlys, Chinese patrol boats attempted to ram Philippine survey vessels conducting seismic surveys of possible undersea energy reserves. In April-May 2012, coast guard vessels from both nations engaged in a stand-off at Scarborough Shoal until a U.S.-brokered de-escalation. These continuing incidents are the symptoms of unresolved territorial disputes and the lack of an agreed upon code of conduct between South China Sea claimants to regulate behavior and provide for an equitable distribution of economic benefits. In 2005, China, the Philippines, and Vietnam signed the Joint Marine Seismic Undertaking, an attempt to cooperate on joint energy exploration projects and a significant first step in implementing a joint development scheme. However, this agreement was never fully implemented due to domestic political disputes in the Philippines.[3] In the absence of an agreement regarding the validity of conflicting maritime claims or an enduring regime to guarantee peaceful conduct by rival claimants and joint exploitation of economic resources, there is no reason to believe

[2] Pham, “The Use or Threat of Force in South China Sea Disputes Since 1945,” 523-539.
[3] Shicun and Hong, *Recent Developments in the South China Sea Dispute*, xv.

tensions will decrease. In fact, it is quite possible that Philippine-China tensions will worsen and escalate into open conflict. Should this occur, it is worthwhile to refer to Chinese writings on warfare on to ascertain what shape such a conflict might take.

Chinese conflict theory indicates the PRC's leaders will make use of a combination of means to triumph over an adversary including those not associated with armed force such as network, or cyber, warfare.[4] The ancient Chinese general and military theorist Sun Tzu wrote in approximately 500 B.C. that, "The supreme art of war is to subdue the enemy without fighting." This quote indicates a preference for using means other than armed force to attain desired ends and manifests in the contemporary era when Chinese leaders employ "gray means" such as a maritime militia to bolster territorial claims in the South China Sea.[5] In their 1999 work *Unrestricted Warfare*, People's Liberation Army (PLA) Colonels Qiao Liang and Wang Xiangsui argued for the employment of "supra-means combinations" to defeat an opponent:

> …if the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time

[4] Sheldon and McReynolds. "Civil-Military Integration and Cybersecurity," 197. The term "network warfare" is used deliberately as the Chinese see warfare in the information domain embracing operations in four discrete sub-domains: electromagnetic, psychological, intelligence, and network (or cyber) - the terms network and cyber are used interchangeably in this paper.

[5] Erickson and Kennedy. "China's Maritime Militia." Gray means are examples of non-lethal force such as presence missions in the vicinity of disputed maritime features, obstructing survey vessels, and transforming reefs or islets into larger installations through development. Such means may not be directly attributable to a state actor, as in the case of Chinese Maritime Militia vessels conducting presence or obstruction missions.

> carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. There is finally the forceful bearing down by the army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty..[6]

The authors list no less than 23 different types of warfare in their work ranging from network warfare to financial warfare to media warfare to atomic warfare, all of which equate to means of applying lethal or non-lethal force. Ancient and contemporary examples of Chinese conflict theory indicate the PRC is certain to employ a variety of means to bend an adversary's will. Given recent Chinese actions and current capabilities, one of these means will certainly be network warfare.

CHINESE NETWORK WARFARE CAPABILITIES

China possesses a robust array of irregular and regular forces capable of engaging in network warfare. Per Chinese military doctrine, network warfare is conducted in one of the four sub-domains of an overarching information domain and consists of the full spectrum of what the U.S. terms computer network operations, this is, computer network attack, exploitation, and defense..[7] The FBI estimates the PRC has a cadre of 30,000 government cyber warriors augmented by ~150,000 cyber personnel residing in the private sector..[8] The

[6] Liang and Xiangsui, *Unrestricted Warfare*, 145.
[7] Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 165.
[8] Brenner, *America the Vulnerable,* 53 and 80.

smaller number of “regular” cyber warriors are full-time government employees and work mainly in the Third Department of the People’s Liberation Army General Staff (3/PLA). This organization is analogous to the U.S. National Security Agency (NSA) and consists of 12 subordinate bureaus capable of sophisticated computer network attack and exploitation operations targeting nations around the globe along with protecting China’s classified networks.[9] The PRC’s “irregular” cyber warriors consist of information warfare militias (also called cyber-militias) representing the advancement of China’s concept of People’s War into the twenty-first century. These militia units consist of part-time cyber warriors typically affiliated with educational institutions or telecommunications companies often operating in support of a military unit.[10] Despite examples of cyber-militias engaging in offensive cyber operations, it seems likely that China views these units mainly as a means to provide economical local network defense through tasks such as upgrading firewalls, replacing damaged systems, or rolling back corrupted systems to their last known good configuration.[11] China has employed its network warfare forces against adversaries on numerous occasions in recent history.

History clearly demonstrates China’s willingness to use the means of network warfare waged by irregular groups to target foreign nations. The PRC’s irregular cyber forces, namely its cyber-militias, have conducted offensive cyber attacks against adversaries. In 1998, the first recorded incidence of network warfare executed by China occurred when

[9] Stokes, “The Chinese People’s Liberation Army Computer Network Operations Infrastructure,” 164-5.
[10] Sheldon and McReynolds. “Civil-Military Integration and Cybersecurity,” 203, 206-7, 210.
[11] *Ibid*., 208.

patriotic Chinese hackers formed a cyber-militia called the China Hacker Emergency Meeting Center in response to anti-Chinese race riots in Indonesia. Chinese “hacktivists” launched denial of service attacks on, and conducted defacements of, Indonesian government websites.[12] In 1999, when U.S. aircraft accidentally bombed the PRC’s embassy in Belgrade, Chinese cyber-militias conducted retaliatory cyber attacks on Department of Energy, Department of Interior, and National Parks System websites. The Philippines has also been exposed to cyber attacks that were most likely launched by China. In April 2012 during the midst of the Scarborough Shoal standoff, hackers defaced the University of Philippines’ web page with nationalist slogans claiming Chinese sovereignty over Scarborough. More recently, Philippine banking, defense, and telecommunication industries have been subjected to a series of cyber-espionage attacks over the last several years. Cybersecurity experts believe the “Conference Crew”, a group of hackers sponsored by the PRC government, is behind many of these attacks.[13] These actions, conducted by groups loosely affiliated with or supported by China’s government, are an example of gray zone conflict in which China employs irregular forces against adversaries while maintaining plausible deniability. China also consistently demonstrates the willingness to employ its more capable group of regular cyber forces to target adversaries with sophisticated attacks.

It is reasonable to assume the PRC would employ its sophisticated network warfare capabilities, embodied by a robust suite of regular cyber forces, to coerce adversaries in the future. China’s regular network warfare forces have engaged in a litany of extremely effective cyber attacks against its most sophisticated adversary, the U.S. A series of attacks

[12] Carr, *Inside Cyber Warfare*, 2.
[13] Badilla, "China, Vietnam Behind Cyber Attacks on PH, Asia."

originating in China during 2003 termed “Titan Rain” succeeded in exfiltrating 20 terabytes of data from Department of Defense (DoD) networks, equivalent to almost 20% of the total information residing in the Library of Congress.[14] In January 2010, Google disclosed massive attacks on its networks by Chinese hackers that had succeeded in stealing proprietary source code. This episode was part of a series of cyber espionage attacks termed “Aurora” consisting of coordinated assaults on the networks of thousands of firms in the U.S. and Europe including Morgan Stanley, Yahoo!, Northrop Grumman, Dow Chemical, as well as several oil and gas firms. Among privileged information exfiltrated was “bid data” detailing quantities and locations of oil reserves that cost targeted energy firms millions of dollars to obtain.[15] In 2011, Chinese cyber forces were able to penetrate Lockheed Martin’s network after hacking into RSA Security, a firm that provides secure ID tokens used by companies doing classified work for DoD.[16] Although China’s network operations seem to focus mainly on cyber espionage/computer network exploitation and a systematic thievery of intellectual property, it is logical to expect that cyber forces capable of penetrating sophisticated defenses are also capable of executing advanced cyber attacks that could cripple target networks. Given China’s effectiveness in penetrating the relatively advanced networks of a superpower such as the U.S., its network warfare means could prove devastating when directed against a less advanced nation lacking a viable means of retaliation.

[14] Brenner, *America the Vulnerable,* 53 and 80.

[15] *Ibid.*, 45-46 and 48.

[16] Inkster, “The Chinese Intelligence Agencies,” 42-3.

PHILIPPINE CYBER VULNERABILITIES

It is entirely possible that the Philippines could be targeted by cyber attacks similar to those launched by Russia against its adversaries, which disrupted the provision of internet-enabled services and isolated target nations from communications with the rest of the world. In 2007, a flood of cyber attacks brought daily life in the Baltic nation of Estonia to a halt. Distributed denial of service (DDoS) attacks took government and financial websites off-line and paralyzed daily life. As a state highly reliant on information technology (IT), Estonia proved especially vulnerable to attacks on internet-linked infrastructure.[17] This string of attacks was launched in the wake of a decision to move a memorial dedicated to the Red Army's Second World War dead out of a square in Tallinn, the national capital. Russian cyber-militias, likely supported by the Russian Federation's government, were responsible for the attacks.[18] The following year, Russian cyber-militias struck again, this time in conjunction with Russian military operations executed against the state of Georgia. These cyber attacks also proved effective, virtually isolating Georgia from communication with the rest of the world.[19] Attacks such as these can have grave economic effects on a nation that depends on internet-linked critical infrastructure along with digital financial transactions and communications with the rest of the world. The Philippines, though still classified as a developing nation, is heavily dependent on information communications technology (ICT) to support its economic health and development goals.[20]

[17] Czosseck, Ottis, and Talihärm, "Estonia After the 2007 Cyber Attacks."
[18] Carr, *Inside Cyber Warfare*, 3.
[19] Hollis, "Cyberwar Case Study."
[20] Philippine DICT, *National Cybersecurity Plan* 2022, Message from the Secretary.

With national revenues equivalent to almost 20% of national gross domestic product (GDP) originating from sectors that depend on ICT and digital connectivity with the global economy, cyber attacks such as those suffered by Estonia and Georgia would have a catastrophic effect on the Philippine Economy. A veritable army of Filipinos working overseas in nations ranging from the Gulf States to Africa generates a sizable portion of the Philippines' national income in the form of remittances, that is, money transferred from countries in which Filipino expatriates work to family members residing in the Philippines. In 2016, overseas Filipino workers remitted almost $27 billion into the Philippine economy, typically via digital bank transfers. This figure was equivalent to 9.8% of Philippine GDP; GDP is typically used to quantify a nation's total economic output.[21] The Philippines also boasts a strong business process outsourcing sector that provides call center and ICT support to foreign firms. This sector accounts for approximately another 10% of Philippine GDP, three-quarters of which derives from servicing U.S. firms such as Citibank, J.P. Morgan, and Microsoft.[22] An adversary with sophisticated network warfare capabilities and the willingness to employ them, such as China, represents a significant risk to the Philippines. Network warfare could easily be used to disrupt the Philippines' economy as a coercive tool during a conflict deriving from territorial conflicts in the South China Sea. This threat is compounded by the fact that Philippine networks and ICT are especially vulnerable to penetration.

Cybersecurity experts assess the Philippines is twice as susceptible to cyber attacks when compared to other nations. A study found that 30% of surveyed Philippine

[21] Cuaresma, "Digital Banking."

[22] *Philippines Information Technology Report*, 14.

organizations were targeted by advanced cyber attacks in the second half of 2015, compared to a global average of 15%.[23] In 2016, the Philippine government suffered the biggest data breach in world history when hackers exfiltrated data on 70 million voters and posted it to the internet; stolen information included fingerprint records and passport data. The scale of this data breach surpassed the 2015 U.S. Office of Personnel Management hack, which revealed personally identifiable information of 20 million Americans.[24] Also in 2016, malware linked to the theft of $81 million from Bangladesh's Central Bank was found on systems in a Philippine Bank.[25] A major reason behind the vulnerability of Philippine ICT to cyber attack is the ubiquitous use of pirated software. As of 2013, experts estimated that 69% of software used in the Philippines was pirated.[26] This is significant as pirated software does not benefit from periodic critical security updates and fixes provided by developers, making host systems especially vulnerable to exploits that would not affect patched systems. The president of cybersecurity company FireEye Inc. summarized the significance of Philippine vulnerability to cyber attack in 2016:

> The Philippines' cybersecurity gap is an urgent economic and national security concern. Organizations here are frequently targeted by advanced attackers. As geopolitical tensions drive rapid militarization in the West Philippine Sea [South China Sea], it is important we acknowledge the first shots in any conflict will be fired in cyberspace.[27]

[23] Kristyn, "PH More Prone to Cyber Attacks."
[24] BBC, "Philippines Hackers Breach Poll Body Database of Voters, Leak Details - Report."
[25] AAP Finance News Wire, "UK: SWIFT Malware Linked to Philippines Attack."
[26] *Philippines Information Technology Report*, 45.
[27] Kristyn, "PH More Prone to Cyber Attacks."

The Philiipines' vulnerability to cyber attack and the economic effect such an attack could have concern the U.S. given the two nations are key alliance partners.

THE U.S.-PHILIPPINE RELATIONSHIP

The U.S.-Philippine Alliance obliges the U.S. to help the Philippines confront an enemy in time of war and establish a credible defense capability to deter adversary aggression; this later obligation certainly includes engagement activities aimed at improving Philippine cyber defenses. The two nations signed a mutual defense treaty in 1951 and are bound by Article IV to meet the common dangers associated with an armed attack on either party in the Pacific Area. Article V of the treaty defines an armed attack as an, "…attack on the metropolitan territory of either of the Parties, or on the island territories under its jurisdiction in the Pacific Ocean, its armed forces, public vessels or aircraft in the Pacific." The Enhanced Defense Cooperation Agreement (EDCA) of 2014, which was upheld by the Philippine Supreme Court in 2016, reaffirmed the relationship between the two nations and obliges the U.S. to assist the Armed Forces of the Philippines (AFP) address short-term capability gaps while also promoting long-term modernization. These bilateral agreements commit the U.S. to assist the Philippines in defending its sovereignty. Although neither agreement specifically addresses conflict in the cyber domain, the EDCA's language regarding the promotion of AFP modernization can easily be interpreted to include building the capacity of the Philippine Military to operate in cyberspace. Furthermore, it is reasonable to assume any armed conflict between the Philippines and China would include Chinese employment of its robust network warfare capabilities. In such a case, the U.S. would clearly be obligated to help the Philippines confront the dangers associated with cyber attacks on its

ICT. A recent rapprochement between the two nations has not eliminated the possibility of a future China-Philippine conflict, which would certainly involve the U.S.

Despite a recent easing of tensions between the Philippines and China, enduring territorial disagreements over maritime claims in the South China Sea make China a likely adversary with which the Philippines may come into open conflict. Following an agreement between Philippine President Duterte and his PRC counterparts, Filipino fishermen are now permitted to access Scarborough Shoal. In addition, China and the Philippines are major trading partners; in 2015 the PRC was the largest single source of Philippine imports accounting for 12.9% of all imports while China was the third largest export market for the Philippines absorbing 12.4% of Philippine exports. Nevertheless, these realities do not change the fact that both nations have unresolved, conflicting territorial claims in the South China Sea. Absent an agreed upon code of conduct to regulate the behavior of rival claimants in the area and the division of economic benefits, there is no reason to expect this source of China-Philippines tension to vanish. China's refusal to participate in the UNCLOS PCA case brought by the Philippines also indicates the chance of conflict between the two states over conflicting territorial claims will persist. With the enduring specter of conflict between China and an ally that is particularly vulnerable to cyber attacks, the U.S. has a moral obligation to help bolster Philippine cyber defenses via cyber engagement.

IMPROVING PHILIPPINE CYBER DEFENSES

The Philippines recognizes the importance of cybersecurity and the U.S. must take note of steps its ally has taken to improve its cyber defense capabilities and ensure USPACOM cyber engagement activities complement Filipino efforts. The Department of Information and Communications Technology Act of 2015 (Republic Act 10844) established the Department of Information and Communications Technology (DICT) and defined the role of this new government agency. In addition to planing, developing, and promoting the Philippines' national ICT development agenda through efforts such as developing a national broadband plan, the DICT is charged with ensuring "…the security of critical infrastructure, including information assets and data of the government, individuals, and businesses…" in collaboration with key stakeholders including the Philippine Cybercrime Investigation and Coordination Center as well as the Department of National Police..[28] The DICT took a key first step in discharging these responsibilities by publishing *National Cybersecurity Plan 2022* in May 2017. This plan mandates several concrete actions that will lead to improved Philippine cybersecurity such as mandating government agencies update software and apply security patches; requiring national cyber drills and exercises in which government activities must participate; and directing the establishment of a network of government, military, and private sector computer emergency response teams (CERTs) to respond to network intrusions under the cognizance of a national CERT..[29] USPACOM can easily complement and reinforce some of these efforts to help the Philippines improve its cyber defenses.

Supporting Philippine initiatives to improve national cybersecurity is an attractive cyber engagement option for USPACOM. The combatant commander could quantifiably contribute towards the Philippine *National Cybersecurity Plan 2022*'s goal of a network of CERTs by supporting the development of the Department of Defense's CERT as well as those of the AFP's regional unified commands such as Northern Luzon Command (responsible for Scarborough Shoal) and Western Command (located on Palawan and

[28] Philippine DICT, *National Cybersecurity Plan* 2022, 2.
[29] *Ibid*., 36-7.

responsible for the Spratly/Kalayaan Islands). With its ally's concurrence, USPACOM should incorporate cyber events into major bilateral/multilateral exercises such as the *Balikatan* series and even synchronize the execution of such exercises with Philippine national cyber drills mandated by *National Cybersecurity Plan 2022*.[30] USPACOM could also encourage and support Philippine efforts to improve national cybersecurity in conjunction with new initiatives.

Supporting the establishment of a regional, cooperative cybersecurity framework in Southeast Asia under the Aegis of the Association of Southeast Asian Nations (ASEAN) or other umbrella is another engagement option for USPACOM. Following its 2004 accession to the North Atlantic Treaty Organization (NATO), Estonia proposed the creation of a cyber defense center of excellence for the alliance. Thirteen years later, the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) serves as a hub for cooperation, information sharing, and capability development within the field of cyber defense for the alliance's members and partners.[31] Since 2010, the Tallinn-based center has hosted Locked Shields, an annual cyber defense exercise which has become the largest and most advanced exercise of its kind in the world with over 800 participating nations, industry partners, and educational institutions.[32] The Philippines has explored cooperation with its ASEAN partner Malaysia in the field of cybersecurity. Expanding such exploratory initiatives into a full-fledged, multi-lateral cyber defense cooperative is an attractive option for bolstering the capacity of U.S. allies in Southeast Asia. Such a cooperative would help member nations defend against the

[30] *Balikatan* (Shoulder to Shoulder in Tagalog) is an annual U.S.-Philippine bilateral military exercise.
[31] "About Cyber Defense Center," NATO CCDCOE.
[32] "Locked Shields," NATO CCDCOE.

network warfare capabilities of adversaries through the sharing of best practices and combined research..[33] Furthermore, such an initiative is a logical extension of a Philippine proposal adopted by the ASEAN Defense Ministers Meeting Plus (ADMM-Plus) forum in 2016 to form a cybersecurity working group that will serve to exchange knowledge regarding cybersecurity amongst member states..[34] The U.S. should also consider how its ally will access offensive cyber capabilities.

Unfortunately, passive network defensive operations alone are insufficient to deter adversaries from employing network warfare means..[35] In order to deter an adversary, a nation must possess a viable offensive capability to demonstrate that an opponent will face retaliation in the event of conflict. To deter China's employment of its offensive network warfare capabilities, the Philippines must either possess like capabilities or have a commitment by an ally to deploy such capabilities on its behalf in the event of conflict. The U.S. and Philippines must consider this reality and ensure leaders address it during future dialogue. Whether the Philippines will pursue its own offensive cyber capabilities or choose to rely on an explicitly stated agreement that the U.S. is willing to employ computer network attack means on its ally's behalf during a conflict should be point of discussion. Ultimately, the Philippines and U.S. need to determine how their alliance pertains to the employment of offensive cyber capabilities to ensure the former partner has access to such means to effectively deter an opponent.

[33] Estopace, "Malaysia, Philippines Eye Cybersecurity Cooperation."
[34] Parameswaran, "ASEAN Defense Chiefs Agree to New Cybersecurity Group."
[35] Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 176.

CONCLUSION

The fact that the Philippine Government officially terms the South China Sea the "West Philippine Sea" is indicative of the fact that the Philippines intends to stick to its territorial claims in the region, especially now that they have been bolstered by an UNCLOS PCA ruling. Furthermore, China's island building campaign in the Spratlys along with aggressive acts by its maritime militia and coast guard indicate the PRC will remain intransigent regarding its overlapping maritime claims. With no code of conduct or agreement to share economic benefits between rival claimants, this source of tension between the two nations will persist and likely escalate. Any conflict between China and the Philippines will certainly see the later nation subjected to attacks by network warfare means that have proved sophisticated enough to penetrate even the relatively robust network defenses of an advanced nation such as the U.S.

In a lopsided conflict against an adversary whose networks are especially vulnerable, Chinese network warfare attacks could digitally isolate the Philippines and directly disrupt income streams equivalent to at least 20% of GDP. The U.S. is bound to help build the capacity of one of its key allies to defend against such offensive action. As the combatant command responsible for the Philippines, USPACOM is in a unique position to conduct cyber engagement activities that augment initiatives the Philippines outlined in its recently published National Cybersecurity Plan. USPACOM is also in a position to support efforts to build a regional, cooperative cyber defense architecture in Southeast Asia similar to the NATO's CCDCOE. Helping the Philippines to improve its defenses in cyberspace will make a key ally more resilient and better able to resist coercive actions taken by an adversary in the domain of cyberspace. The U.S. should remember that more capable allies are better able to deter adversaries on their own, thus decreasing the likelihood of open conflict and hence American involvement on behalf of an ally.

RECOMMENDATIONS

- USPACOM support development and maturation of the Philippine Department of Defense’s CERT.
- USPACOM support development and maturation of AFP regional unified command CERTS, focused initially on Northern Luzon Command and Western Command.
- In conjunction with Philippine partners, USPACOM explore incorporation of cyber events into bi/multilateral military exercises and, if possible, synchronize such events with Philippine national cyber drills organized by the DICT.
- USPACOM support development of a regional, cooperative cybersecurity framework in Southeast Asia along with a regional cybersecurity center of excellence similar to NATO’s CCDCOE.

BIBLIOGRAPHY

AAP Finance News Wire. ”UK: SWIFT Malware Linked to Philippines Attack." May 27, 2016. https://search.proquest.com/docview/1791479692?accountid=322.

“About Cyber Defense Center.” NATO Cooperative Cyber Defense Center of Excellence. Accessed October 6, 2017. https://www.ccdcoe.org/about-us.html

Badilla, Nelson. “China, Vietnam Behind Cyber Attacks on PH, Asia." *TCA Regional News*, May 26, 2017. https://search.proquest.com/docview/1902161312?accountid=322.

BBC Monitoring Asia Pacific. ”Philippines Hackers Breach Poll Body Database of Voters, Leak Details - Report.” April 21, 2016. https://search.proquest.com/docview/1782392753?accountid=322.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. London: Penguin Books Ltd., 2011

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly Media Inc., 2012.

Cuaresma, Bianca. "Digital Banking: The Future of Lower Remittance Costs." *Business Mirror*, March 15, 2017. https://search.proquest.com/docview/1877957120?accountid=322.

Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. “Estonia After the 2007 Cyber Attacks: Legal, Strategic, and Organisational Changes in Cyber Security.” NATO Cooperative Cyber Defence Centre of Excellence (2011). http://www.ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_the_2007_Cyber_Attacks.PDF.

Erickson, Andrew and Conor Kennedy. “China’s Maritime Militia.” adrewerickson.com. Last modified 2016. http://www.andrewerickson.com/2016/02/trailblazers-in-warfighting-the-maritime- militia-of-danzhou.

Estopace, Eden. "Malaysia, Philippines Eye Cybersecurity Cooperation." *SMB World Asia* (Online), October 24, 2016. https://search.proquest.com/docview/1831443098?accountid=322.

Hollis, David M. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal*, January 2011. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Inkster, Nigel. “From *The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace*.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon Lindsay, Tai Ming Cheung, and Derek Reveron, 29-50. Oxford: Oxford University Press, 2015.

Kristyn, Nika M. "PH More Prone to Cyber Attacks." *TCA Regional News,* April 14, 2016. https://search.proquest.com/docview/1780639300?accountid=322.

Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare*. Translated by the Foreign Broadcast Information Service. Beijing: PLA Literature and Arts Publishing House, 1999.

“Locked Shields.” NATO Cooperative Cyber Defense Center of Excellence. Accessed October 6, 2017. https://ccdcoe.org/locked-shields-2016.html.

Parameswaran, Prashanth. “ASEAN Defense Chiefs Agree to New Cybersecurity Group.” *The Diplomat,* June 1, 2016. https://thediplomat.com/2016/06/asean-defense-chiefs-agree-to-new-cybersecurity-group.

Pham, Van. “From *The Use or Threat of Force in South China Sea Disputes Since 1945: A Timeline.*” In *Power Politics in Asia’s Contested Waters: Territorial Disputes in the South China Sea*, edited by Enrico Fells and Truong-Minh Vu, 523-39. Cham: Springer, 2016.

Philippine Department of Information and Communications Technology. *National Cybersecurity Plan* 2022. May 2, 2017.

Philippines Information Technology Report Q3 2017. London: BMI, 2017.

Sheldon, Robert and Joe McReynolds. “From *Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias.*” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon Lindsay, Tai Ming Cheung, and Derek Reveron, 188-222. Oxford: Oxford University Press, 2015.

Shicun, Wu, and Nong Hong. *Recent Developments in the South China Sea Dispute: The Prospect of a Joint Development Regime*. New York: Routledge, 2014.

Stokes, Mark. “From *The Chinese People’s Liberation Army Computer Network Operations Infrastructure.*” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon Lindsay, Tai Ming Cheung, and Derek Reveron, 163-87. Oxford: Oxford University Press, 2015.