AWAKEN THE CYBER DRAGON: CHINA'S CYBER STRATEGY AND ITS IMPACT ON ASEAN

Miguel Alberto N. Gomez
De La Salle University, Taft
College of Computer Studies
Room 102-A Gokongwei Hall
2401 Taft Avenue
1004 Manila, Philippines
miguel.gomez.n@gmail.com

ABSTRACT

The increase in frequency of cyber attacks launched against the Association of South East Asian Nations (ASEAN) regional bloc that have been attributed to the People's Republic of China (PRC) sets a precedent for the future of low impact cyber conflicts. While the calls for mutual defense of cyberspace and regional cooperation have been highlighted in the ASEAN ICT Masterplan 2015, conflicting interests between members and the nature of the ASEAN principles suggests that any eventual cyber defense policies can only be framed within the context of individual state interests. This lack of cohesion paves the way for low impact cyber attacks that, while not targeting critical infrastructure, can enable the aggressor to influence the different instruments of national power within the region and serves as a viable tool to project power and influence with minimal risk of escalation as opposed to traditional approaches. While this moves against the current predictions that suggests targeted and debilitating attacks aimed at crippling critical infrastructure, the lack of instances of such lends weight to the assumption that these are unlikely for the time being. On the other hand, the recent events that have taken place in the ASEAN bloc has shown that the PRC has, and continues to, utilized low impact cyber attacks. By taking advantage of the problem of attribution coupled with the lack of knowledge regarding its true cyber capabilities and the threat of kinetic retaliation, the PRC has found itself able to operate freely. This study aims to discuss how the PRC has adopted this strategy in response to recent disputes with members within ASEAN, in particular, the Republic of the Philippines. The paper highlights the low impact approach that the PRC has chosen as a means of exerting its influence in ongoing disputes with the Republic of the Philippines and to a greater extent, the rest of the region. The study discusses the underlying factors that allow the PRC to operate freely by taking advantage of the fundamental weaknesses of ASEAN as a platform for establishing a cyber defense mechanisms within the region and goes on to caution as to the long term repercussions of such.

KEYWORDS

Cyber Defense, Cyber Warfare, Cyber Strategy, Cyber Policies, Information Security

1. INTRODUCTION

The appearance of several high-profile cyber security incidents the past year has brought the possibility of cyber war into mainstream consciousness. Incidents such as last year's *Stuxnet* outbreak and related malware *Duqu* and *Flame*, as well as the recent compromise of the oil firm Saudi Aramco has prompted commentary regarding the implications these threats have on global security. So much so that in October 2012, United States Defense Secretary Leon F. Panetta has been quoted saying that the United States faces an impending cyber-Pearl Harbor that would be capable of crippling the nation's critical infrastructure [1]. While discourse such as this is not novel, the frequency with which doomsday scenarios have been proposed is increasing. The question that faces policy makers, military leaders, and security professionals alike is whether or not these events signal a future trend in warfare. While acknowledging the possibility of significant damage caused by attacks against existing and future cyber infrastructure, a study of current cyber conflicts demonstrate that the impact of most have been imperceptible or significantly milder than what has previously been claimed; influencing public perception and national policy rather than causing damage to key infrastructure. To validate this argument, the study uses the case of the People's Republic of China (PRC) – whose cyber capabilities have been acknowledged by analysts in the field – and its recent territorial conflicts with members of the ASEAN regional bloc, namely the Republic of the Philippines (PHL).

To support these claims, the study is divided into 4 sections. The first provides a distinction between cyber war and cyber conflict. The distinguishing factors between the two serve as a fundamental point to explain the PRC's current approach. The second and third section explores how cyber conflicts, and Low Impact Cyber Conflicts (LICC) in particular, contribute to the PRC's cyber strategy and foreign policy. Finally, the last section covers ASEAN's how inherent weaknesses are exploited when the PRC's cyber strategy is put to bear as a means to support on-going policies and disputes. All discussions within this study are viewed from the perspective of the activities that take place between the PRC and ASEAN. This, however, does not mean that conclusions derived from this study are not applicable to other regions or situations. So long as the initial conditions that lead to LICCs are present, the proponent believes that the thesis should hold true.

For the succeeding sections of this paper, the term cyber conflict is used in place of cyber warfare. This distinction is crucial, as the proponent of this study does not believe that events that have occurred and continue to transpire in cyber space are true forms of warfare as per the definition used by Clausewitz. Further discussion regarding this distinction is made in the second section of this study.

2. CYBER WAR VS. CYBER CONFLICT

Existing literature and popular media have labeled recent cyber attacks as being instances of cyber war. While parallels have been drawn between kinetic warfare and that of cyber warfare, these two cannot be taken or viewed on equal footing due to inherent differences between them. This point is emphasized if one were to take the definition of war as established by Clausewitz wherein he provides three characteristics that must first exist, these are its: violent character, instrumental character, and political nature. The first refers to the violent characteristics of warfare, this is crucial as this is viewed to be present in all forms of conflict that have been labeled as war and not merely in the metaphorical sense of the word. Second, war is said to be instrumental, as it must serve as a means to an end. While war is violent, this merely acts as a vehicle to reach the goals set by the aggressor – which is typically to force the other party to concede to the aggressor's will or to act in a manner which it would otherwise avoid. Lastly, all conflict deemed to be war is political in nature. *"War is a mere continuation of politics by other means,"* as Clausewitz is most often quoted as saying clearly illustrates this point. While the violence displayed in war is clear, it is never a single act. Rather, these actions all serve to further political interests of the aggressor that would otherwise be unattainable through other means. While events in cyberspace have exhibited these traits, none of these have, at present, been shown to demonstrate all three simultaneously. Consequently, the claim that cyber warfare is simply warfare moved to cyber space cannot easily be made as past events that, branded as cyber warfare, have only displayed two of the three characteristics highlighted above [2] [3].

If the assumption that cyber warfare is simply warfare transplanted to cyberspace is maintained, additional distinction may be made with regards to whether or not such actions are visible to the general populace. Two classifications are available in this regard; that cyber warfare may either be *subrosa* or *non-subrosa* with the former indicating that actions are, for the most part unknown, while the later is highly visible. While most incidents discussed in existing literature are documented or at least known to the general public, a compelling case exist for discrete forms of cyber warfare. This being the threat of retaliation against an aggressor and subsequent escalation should their identity be revealed. It should be noted that despite the advantages gained in actions conducted within cyberspace, a level of deterrence exists between involved parties. Take the hypothetical case of a disruptive attack launched against a nation's power grid. Should a rival launch a cyber attack against it, and knowledge of such an attack is revealed to the general public; the threat of escalation may increase with calls for the affected party to retaliate in kind. Inversely, should knowledge of the attack be kept or at least attributed to a more begin cause, the respective governments of the rival parties are given the opportunity to arrange for a de-escalation of the hostilities without further escalation. In theory, this gives the aggressor the ability to launch attacks with a reduced fear of escalation – assuming that the parties involved react as expected [4].

The ability to control information, particularly regarding disruptive events that affect a significant portion of the population, is difficult at best. In line with this, revealing crucial information after-the-fact affects a government's credibility and would move them towards full disclosure instead of re-attribution or deception. Disclosure, while risking escalation, is perhaps the best option as it provides the affected party with more liberty to respond with or without retaliation (legal action, diplomacy, etc) [4]. While this sounds counter-intuitive or even reckless, a recent study of past cyber attacks launched between states has shown these to be innocuous in nature. From this it can be assumed that such attacks may actually form the status-quo in terms of cyber relations between states. Consequently, so long as an attack does not lead to massive loss of life or significant damage, the threat of escalation is minimal and the actions are tolerated to a certain degree [2].

With these points in mind, the study posits that cyber warfare does not exist primarily in light of the fact that parties cannot or are not willing to commit to the first characteristic of warfare, violence, as it risks escalation and mitigates advantages obtained by operating in cyberspace to begin with. In its place, the term cyber conflict is suggested as a means to label conflicts that regularly exists between states within cyber space. From this, two further subcategories are established: low-impact cyber conflicts (LICC) and high-impact cyber conflicts (HICC). The former refers to cases of cyber conflicts that are aimed towards influencing or shaping public opinion within the target state while the later refers to attacks that cause damage to specific cyber infrastructure of the target state. However, due to the risk of going beyond the established threshold of cyber relations, the proponent believes that HICCs are unlikely as these increase the likelihood of escalation. Consequently, it can be postulated that current and future incidents are likely to be in the form of LICCs.

3. CHINA'S CYBER STRATEGY

As the previous section has established, incidents that have taken place in cyber space are not true forms of warfare but rather instances of what the study has termed as low-impact cyber conflicts. With this in mind, the feasibility of such needs to be established beyond the realm of intellectual discourse and must be analyzed against the backdrop of current events. To achieve this, the study takes note of the recent conflicts between the PRC and ASEAN members such as Vietnam and the Republic of the Philippines as a means to demonstrate the existence of low-impact cyber conflicts as part of a continuing conflict. Prior to discussing this point further, the concept of cyber strategy as it relates to the PRC must first be established. From there, the process of low-impact cyber conflict may then be presented.

Cyber strategy is defined as *"the development and employment of strategic capabilities to operate in cyber space, integrated and operated with other operational domains, to achieve or support the achievement of objectives across the elements of national power in support of national security strategy"* [5]. From this it can be deduced that cyber strategy can be utilized to support different instruments of power aside from military power. Most notable amongst these is economic power that can be gained through the theft of proprietary information from rivals (not necessarily between states) [6]. In the case of the PRC, strategy is defined as, *"the analytical judgment of such factors as international conditions, hostilities in bilateral politics, military economics, science and technology, and geography as they apply to the preparation and direction of the overall military/war plan"* [5]. Complementary to this, China views cyber strategy as, *"the use of information, a crucial component of cyber processes, to influence or control the direction of an opponent's decision making activities"*.

From these definitions, two crucial points in the PRC's cyber strategy may be established. The first is its willingness to utilize multiple instruments of national power as a means to determine the most appropriate military option – if one should be used at all. Second is the end goal of influencing an adversary's decision making activities rather than confronting them in direct action. To quote the Chinese strategist Li Bingyan, *"How do you get a cat to eat a hot pepper? You can stuff it down his throat. You can put the pepper in cheese ad make him swallow it. Or you can ground the pepper up and spread it on his back, which makes the cat lick himself and receive the satisfaction of cleaning up the pepper"*. From these statements, it can be posited that the PRC's cyber strategy aims to influence an adversary's decision as a means to minimize escalation while achieving its desired result. Niu, Li, and Xu emphasize this point when they cited several stratagems that the PRC may utilize to achieve information supremacy and to seize the initiative in the event of conflict. From these, four can be linked to establish the study's view of the PRC's cyber strategy. These are: thought directing, intimidation through momentum-building, information-based capability demonstration, and releasing viruses to muddy the flow [5].

Thought directing functions by manipulating the cognitive processes of an adversary such that an incorrect decision, from their part, is reached. This may be achieved by releasing factious information that an adversary may mistake as true. Consequently disguising the true intention of its initiator. Intimidation through momentum building is the process of generating psychological pressure directed towards an adversary through intimidation. Information-based capability is another form of intimidation, though this is achieved through the perceived unintentional demonstration of one's capabilities. These two differ in terms of the perceived attempt on the part of the initiator. For the former, the initiator would intentionally perform actions or release information to cause discord and distress on the part of the adversary. The latter is performed under the guise of a routine action that is not intentionally meant to intimidate but would do so nonetheless. Lastly, releasing viruses as a means to muddy the flow pertains to the corruption of information, thus denying an adversary access to resources to assist in their decision-making processes. This process would perhaps be the most straightforward and intrusive of those previously discussed as it attempts to intentionally cause the corruption of an adversary's information resources [2] [5].

Taken collectively, the evidence that points to the PRC's cyber strategy supports the concept of low-impact cyber conflicts. This is achieved by its calls for an "influenced-based" approach rather than that of a direct violent conflict. While the stratagems provided by Niu, Li, and Xu also entertains the possibility of more violent and damaging actions, recent actions on the part of the PRC and its foreign policy demonstrates otherwise.

4. CHINA THREAT THEORY AND CYBER CONFLICT

Recent articles discussing the impending cyber threat that the global community faces have often cited the PRC's liberal use of such tools to further its political aims. While there is no disputing that evidence collected in the aftermath of recent incidents have highlighted the possibility of the PRC's involvement[1], the question is whether or not claims of the PRC's cyber capabilities and their intention to use these pose an actual threat. This requires objective analysis of their foreign policy through the lens of their cyber strategy that was

[1] Attribution of cyber attacks does not provide certainty due to the nature of cyberspace

discussed in the previous section.

While it would not be possible to divine the PRC's true intentions, the perceived threat posed can be traced to the China Threat Theory. Through this, claims of the PRC's hegemonic ambitions are used as a basis to justify the impending threat posed by an emerging China in the form of economic, military, and ideological/political aggression and expansion. This theory, while appealing in light of its current events, may be drawn into question on the grounds that it stands on two fundamental and simplistic assumptions: (1) the PRC has ambitions to dominate the region or the world and (2) it has the capacity to develop capabilities that will allow it to challenge the United State's hegemony [7] [8]. While a substantial amount of literature has been formulated to discuss the validity of this perspective, little to no consensus has been made in this regard. So as to be balanced in terms of providing an explanation on the situation, defining the PRC as either a *status quo* or *revisionist* power is highly dependent on the environment in which it exists.

Taking into consideration Chinese history, the shift between *status quo* and *revisionist* has been driven by external political, economic, and ideological factors. Focusing on its contemporary history, during its "opening up" period between 1970's and early 2000's, China has found it necessary to shift its focus from military, political, and territorial security issues into that of a more "cooperative" and comprehensive approach that emphasized the need to maintain stability and participation in the global political economy [8]. This need to adhere to the status quo is, however, dependent on the relatively benign global conditions that were present during the PRC's rise to power. At present, however, with the global economic crisis in both the United States and the European Union and the PRC's dependence on the stability of this system forces it to reassess and act in order to maintain and/or expand its position both regionally and globally. Consequently, it can be said that the PRC is revisionist in this sense, but not to the extent and capabilities ascribed to it by proponents of the China Threat Theory. Its peaceful rise is possible, but only through careful consideration of its actions [8].

Within the context of this cautious approach, the existence of LICCs lends themselves well to further the PRC's attempts to consolidate its power – specifically within South East Asia – through the use of the traditional instruments of power: Political, Informational, Military, and Economic [9]. This is due in part to the pervasiveness of Information and Communication Technologies (ICT) that not only comes to support these but have also been a cornerstone of development within the region [10]. Corollary to this, the nature of low-impact cyber conflicts minimizes the possibility of escalation if used as an instrument of power or as a supportive tool. To further the point, Buzan has mentioned that China's rise within the region is dependent on its ability to assume a benign posture towards its neighbors. The ambiguity provided by LICCs and the minimal damaged caused by these would dissuade or limit retaliatory action against the PRC for fear of escalation brought about by rash or incorrect action [6]. Consequently, this places it in an advantageous position to push for its interests with little fear of damaging the benign image it continually attempts to present to the international community.

5. ASEAN VULNERABILITY TO LOW-IMPACT CYBER CONFLICTS

While instances of the PRC's cyber capabilities have been suggested to occur at a global scale, analysis of its use within the ASEAN regional bloc is of particular interest as it has coincided with the on-going territorial dispute in the South China Sea. Specifically, the cyber attacks launched against the Philippines are of particular interest.

For the Philippines, cyber attacks were initiated by suspected PRC nationals in April 20, 2012 with the defacement of the University of the Philippines website. A day later, on April 21, 2012, Filipino hackers associate with Anonymous Philippines retaliated with the defacement of PRC websites. In response to rising tensions, the Philippine government calls for a cessation of aggression between the different parties involved. While these calls were made publicly on multiple mediums, neither side yielded to the call; suggesting that, at least from the Philippines, the attacks were not state sponsored. Despite such calls, cyber attacks between suspected PRC hackers and the Philippines continued until May 11, 2012. The attacks launched against the Philippines included Distributed Denial-of-Service (DDoS) attacks against public and private organizations as well as the disclosure of sensitive information [11].

It is important to point out that none of the activities that have transpired during this period could be dubbed as cyber warfare as was established in earlier sections. That is to say, potential targets such as critical infrastructure which cyber warfare advocates often cite as crucial targets were not at all affected. The act of defacing websites (in particular government websites), denying access to them, and releasing sensitive information to the public are, for the most part, a demonstration of capacity and intimidation rather than outright destruction – this was identified in previous sections as a component of the PRC's cyber strategy. While it would be easy to dismiss this as a result of a lack of "suitable targets", it should be pointed out that ICT serves as a crucial component of the Philippine's economic development [12].

A recent report has indicated that the Philippines' Business Process Outsourcing (BPO) industry – one that is heavily reliant on ICT – grows annually at a rate of 20% with its projected value to be 25B PHP by 2016 [15]. This figure does not, as of yet, include the dependency of MSMEs on ICT to support their operations – these include retail, financial services, and telecommunications, etc. Corollary to this, a recent survey by the Economist Corporate Network has shown that 35% of its respondents have indicated that the Philippines is an attractive service provider for IT-BPO services [14]. Clearly, should direct damage to the Philippines have been desired there was no shortage of targets. With the Philippines still identified as an emerging economy, it remains to be highly dependent on the presence and revenue generated from these investments. Attacks against these would impact economic activities within the country and would, in the long run, reduce confidence in the Philippine's ability to protect foreign investments.

While it would be convenient to categorize this exchange as an isolated case for the Philippines, similar cyber attacks have been observed against Vietnam that followed the same form. Interestingly enough, the triggering factor that initiated cyber attacks in that case were also territorial disputes concerning the South China Sea [15]. Besides these, a study conducted by Dell SecureWorks has shown an increase in the number of cyber attacks that may be categorized as LICCs within the ASEAN bloc (Vietna, Brunei, and Myanmar). The question though is what makes ASEAN particularly vulnerable to this form of cyber attack?

By analyzing the different historical, political and social conditions within the ASEAN bloc, its particular vulnerability may be explained through the Socio-Political Cohesion framework provided by Buzan as a means to analyze how nation states view threats to their security relative to their current socio-economic and military power (refer to Table 1) [16]. While a through analysis of Buzan's model would prove interesting, this is beyond the goals of this study. To briefly explain the proposed framework, nation states are categorized based on their socio-political cohesion and power, which in this case refers to military power. From this, four categories may be established: Weak P/Weak SP, Weak P/Strong SP, Strong P/Weak SP, and Strong P/Strong SP. Nation states for each category would view threats in a significantly different manner from each other. For example, a state that is viewed as Weak P/String SP – which is characteristic of the tigers of ASEAN such as Malaysia – lacks significant military power but boasts a formidable economy. These would view direct military action as threats to its security. States that are identified as being Strong P/Weak SP, such as the authoritarian regime of Myanmar, would view and internal destabilizing factors as a threat. According to an earlier study conducted by Buzan, most of ASEAN (with the exception of Singapore) may be labeled as weak. While significant political and economic developments have been made since, none of the ASEAN members have reached the 4th quadrant. That is to say, would fall under the 1st, 2nd, and 3rd quadrants of the table. This situation leads to a disjointed view of threats within the region [17].

Table 1. Vulnerabilities and Types of States [16]

		Socio-Political (SP) Cohesion	
		Weak	Strong
Power (P)	Weak	Highly vulnerable to most types of threats	Particularly vulnerable to military threats
	Strong	Particularly vulnerable to political threats	Relatively invulnerable to most types of threats

Table 2. Mapping to cyber threats [17]

		Socio-Political (SP) Cohesion	
		Weak	Strong
Power (P)	Weak	De-stabilizing political actions in cyberspace, attacks on Internet infrastructure, criminal activities	DDoS and other major attacks on critical infra-structure
	Strong	De-stabilizing political actions in cyberspace	Criminal activities in cyberspace

Table 2 illustrates how the framework may be mapped to threats presented in cyberspace relative to the type of state based on the factors explained earlier. With the 1st and 2nd quadrants being the best representations for the Philippines and Vietnam, the attacks that were assumed to have been initiated by the PRC match those predicted by the framework.

A second, and related, factor that contributes to ASEAN's vulnerability is the *ASEAN Way*. Stemming from the region's collective experience as colonies of the major powers during the late 19th century to the mid 20th century, this regional set of values espouse, among others, non-interference in internal affairs and consensus-based decision making. While ideal, these two traits of the regional bloc have historically proved themselves to be limiting when addressing security threats within the region [18] [19].

From the perspective of cyber attacks and analyzing these through the lens of the framework provided earlier, the *ASEAN Way* is a major hindrance in developing a feasible mechanism to collectively address these threats – regardless of its origin. First, the need for a consensus-based decision prior to passing any resolution is flawed. Given that the region is composed of members with varying levels of economic and military power, the heterogeneous nature of the region would not permit any form of consensus on security matters. This has been shown at different points of ASEAN's history [20].

Second, actions on the part of members that suggest interference with internal affairs may limit the efficacy of attempts to determine the true nature of a cyber attack. The appeal of using cyberspace as political tool or for criminal activities is the inherent anonymity that it provides. Part of this anonymity is achieved through the use of proxies[2] to redirect the source of the attack; consequently disguising the actual source from the intended target. To mitigate this, those wishing to identify the origin of the attack would typically require the cooperation of the proxies involved. For this study, we can view these as simply the states through which the cyber attack passed through prior to reaching its final target. This situation is unavoidable due to the interconnected nature of cyberspace and its most popular manifestation, the Internet. Unwillingness on the part of the proxies to cooperate would limit the amount of information gathered regarding the attack and would in turn severely limit the decisions to be made due to lack of information.

[2] This is not used in its technical sense rather simply as a reference to mediators of a particular act.

A hypothetical scenario that may be used to illustrate this challenge would be a case in which a cyber attack from the PRC passes through Cambodia prior to reaching Vietnam. While the proponent is not aware of any such case, the current political climate in which Cambodia appears to be favoring Beijing's policies [21] can introduce difficulties in obtaining their cooperation if such an event were to take place. A similar issue that has occurred – though outside the region in this study – is that of the attacks against Estonia in 2007. A postmortem of the events identified the initial source of attack as being a computer located within Russia. But without further cooperation from Russia, the presumed source of the attacks, the allegations remained as such – allegations of possible Russian involvement with the incident [22].

Taken together, the unbalanced power distribution within South East Asia and the inherent limitations of the ASEAN regional bloc in the form of non-interference and consensus-based decision making restricts the possibility of a unified defense against cyber attacks aimed at individual member states or the region as a whole. From the perspective of the PRC's assumed cyber strategy, it allows actions in cyber space – particularly low-impact cyber attacks – to go unanswered. Considering the changing political alliances within the region, it is also possible that such attacks may be tolerated to maintain stability within the region while at the same time allowing the PRC to extend its influence through the cyber domain unchallenged.

6. CONCLUSION

While this study presents a cross-section of the current developments within cyberspace concerning both ASEAN and the PRC, it does not attempt to predict with complete with certainty the future of cyber conflict within the region. Based on the form and nature of cyber conflicts attributed to the PRC that has taken place within the region, the likelihood of a "cyber Perl Harbor", at least within ASEAN, remains highly unlikely. Even though the analysis presented has shown the PRC to be a revisionist power at this point in time, its dependence on international structures and their stability minimizes the likelihood of any form of conflict with grave destabilizing capabilities. On the other hand, activities that limit damage and demonstrate or imply the capabilities of the PRC have been observed, as in the case of the Philippines and Vietnam, to be commonplace. These forms of low-impact cyber conflicts, while not at the scale and ferocity that most have claimed, are capable to extending the PRC's influence towards issues that occur outside cyberspace while at the same time limiting the threat of escalation and retaliation.

For ASEAN, the varying level of socio-economic and military power between members continues to challenge attempts at establishing a unified view of security threats to the region. Rather, threats to regional security and stability are addressed at a national level or, at best, through bilateral agreements among member states with similar socio-economic and military characteristics. This situation is further aggravated by the fact that the *ASEAN Way* may limit the amount and quality of information gathered from each other on the basis that this might be perceived as interference.

It is widely known that ASEAN is developing into a global economic focal point that is highly dependent on ICT for its operations. This is best illustrated with the establishment of the ASEAN ICT Masterplan that lays the groundwork that aims to further enhance the use and adoption of ICT within the region [10]. At the same time, the PRC has, in the last three decades, established itself as a formidable entity that is willing to project and expand its power and influence through non-traditional mediums such as cyberspace. The vulnerability of ASEAN as a whole marks itself as the perfect platform on which the PRC can demonstrate and practice with efficiency its current cyber strategy. To mitigate this threat, while taking into consideration the constraining factors, the best solution would be for individual states, at present to strengthen or develop their respective cyber defense policies and practices as a means to limit the impact of attacks that are currently being attributed to the PRC.

While this is strictly a stopgap solution, it would minimize the impact of certain forms of LICCs. Programs such as strengthening existing cyber crime legislation, information security awareness, and private-public partnerships to assist in securing government assets are all viable ways to lessen the impact of these forms of conflict. These, however, would only serve to rebuff attacks rather than provide a constant deterrence that may only be achieved if a more open and cooperative environment were to exist within the region when it comes to addressing cyber conflicts. As a first step, the respective members of the ASEAN bloc, particularly those with underdeveloped or nonexistent cyber legislation, should take proactive steps to develop the necessary laws to curb these threats at the home front. Initially, this would require close collaboration between the public sector and that of the private sector that posses a significant amount of expertise in addressing cyber threats. For its part, the public sector has the manpower and resources required to apply this expertise at a national level [17] [23]. As an example of this form of cooperation, consultation may be conducted between national governments, respective national Computer Emergency Response Teams (CERT), and the telecommunications industry. Once this has been achieved, steps can then be taken to improve information exchange and assistance programs between member states when it comes to cyber attacks [23] [24]. The need for this has already been established in the ASEAN ICT Masterplan. Unless these measures, or some form of them are taken, it is the proponent's belief that the form of aggression which is assumed to originate from the PRC will continue so long as the factors that render it an attractive option continues to persist within South East Asia.

7. REFERENCES

1. Bumiller, E., & Shanker, T.: Panetta Warns of Dire Threat of Cyberattack on U.S., http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0 (2012).
2. Valeriano, B., & Maness, R.: Cyberwar and Rivalry: The Dynamic of Cyber Conflict Between Antagonists, 2001-2011, http://tigger.uic.edu/~bvaler/Cyberwar%20and%20Rivalry%20Dyanamics%20of%20Cyber%20Conflict%20JPR.pdf (2011).
3. Rid, T.: Cyber War Will Not Take Place. Journal of Strategic Studies, 5--32 (2012).
4. Libicki, M.C.: Sub Rosa Cyber War. In: Proc. 2009 CCDCOE Conference on Cyber Warfare (2009).
5. Thomas, T.L.: Nation-state Cyber Strategies: Examples from China and Russia. In: Kramer, F.D., Starr, S.H., Wentz, L. (eds.), Cyberpower and National Security. 465--487. Potomac Books Inc, Washington D.C. (2009).
6. Hjortdal, M.: China's Use of Cyber Warfare: Espinage Meets Strategic Deterrence. Journal of Strategic Security 4, 1--24 (2011).
7. Al-Rodhan, K.E.: A Critique of the China Threat Theory: A Systematic Analysis. Asian Perspective 31, 41--66 (2007).
8. Kwok, O.: China's Foreign Policy: Harmonious World. Is it a Mere Strategem, or an Abiding Policy the World can Trust. In: Robinson, M. (ed.), The Defence Academy Yearbook 2011: A Selection of Commended Essays. 116--138. Defence Academy of the United Kingdom (2011).
9. Tuthill, D.: Reimagining Waltz in a Digital World: Neorealism in the Analysis of Cyber Security Threats and Policy. Dissertation, University of Kent (2012).
10. ASEAN: ASEAN ICT Masterplan 2015. Association of South East Asian Nations (ASEAN). Proposal, ASEAN (2011).
11. Passeri, P.: Philippines and China, on The Edge of a New Cyber Conflict?, http://hackmageddon.com/2012/05/01/philippines-and-china-on-the-edge-of-a-new-cyber-conflict/ (2011).
12. CICT: The Philippine Digital Strategy Transformation 2.0: Digitally Empowered Nation. Proposal, Republic of the Philippines, Commission on Information and Communication Technology (2011).
13. Noda, T.: IT-BPO sector eyes $25B target in 2016, http://www.philstar.com/breaking-news/795644/it-bpo-sector-eyes-25b-target-2016 (2012).
14. Hamlin, M.: Economist: Philippines is Number One, http://www.mb.com.ph/articles/360743/economist-philippines-is-number-one#.UMROV5NetH8 (2012).
15. Vietnam and China hackers escalate Spratly Islands row, http://www.bbc.co.uk/news/world-asia-pacific-13707921 (2011).
16. Buzan, B.: People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era . European Consortium for Political Research Press (2008).
17. Kuehl, D.: From Cyberspace to Cyberpower: Defining the Problem. In: Kramer, F.D., Starr, S.H., Wentz, L.K. (eds.) Cyberpower and National

Security. 24--43. Potomac Books, Inc., Washington D.C. (2009).

18. Sokolsky, R., Rabasa, A., Neu, R.: The Role of Southeast Asia in U.S. Strategy Towards China. Technical Report, RAND Corporation (2001).

19. di Floristella, A.: Building Security in the South East Asian Region: The Role of ASEAN. Technical Report, The European Consortium for Political Research (2010).

20. Jong, K.: ASEAN Way and Its Implications and Challenges for Regional Integration in Southeast Asia. Journal of Southeast Asian Studies 12 (2010).

21. Strangio, S.: Cambodia as divide and rule pawn, http://www.atimes.com/atimes/Southeast_Asia/NG18Ae03.html (2012).

22. Anderson, N.: Massive DDoS attacks target Estonia; Russia accused, http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/ (2007).

23. Tikk, E.: Ten Rules for Cyber Security. Survival 53, 119--132 (2011).

24. Cyber Storm II Final Report. U.S. Department of Homeland Security. Technical Report, Department of Homeland Security (2009).