Cyber Capabilities as Favourable Instruments in the Pacific Century

Francis C. Domingo
Francis.Domingo@nottingham.ac.uk
De La Salle University and University of Nottingham

Paper prepared for the ISA International Conference 2017
University of Hong Kong, 15 to 18 June 2017

Introduction

Pa

Cyber capabilities have emerged as instruments for states to advance their foreign policy interests in the Information Age. States engage in computer network attacks to project a calibrated response to prevailing political and territorial disputes between neighbouring states in the Asia-Pacific Region (Region). Since computer network attacks are more aggressive than diplomatic and economic measures but less consequential than military conflicts, these tactics have been proven useful for states to convey their foreign and security preferences without significantly damaging diplomatic relations and creating instability in the Region (Libicki, 2009, 28-29). Given these considerations, states can exploit the benefits of cyber capabilities when utilised during interstate rivalries or when configured to compliment conventional military capabilities.

Indeed, states have started integrating computer network operations in their military forces to defend against cyber intrusions and to align with capabilities of major allies. The increase in cyber skirmishes is more pronounced in the Region, where the highest number of interstate cyber incidents has been observed in the past fifteen years (Valeriano and Maness, 2015a). Despite of this, there has been no conflict escalation due to of cyber incidents, which suggests that the use of computer network operations encourages less physical harm or damage. The restrained response to cyber conflict raises the question: *what makes cyber capabilities favourable foreign policy instruments in the Asia-Pacific Region?*

The objective of this paper is to explicate the strategic value of cyber capabilities in the Region. It contends that cyber capabilities are favourable foreign policy instruments in the Region because of three strategic advantages: the *nonphysicality* of cyber incidents; the *stealthiness* of cyber intrusions; and the *functionality* of computer network operations. The paper aims to make two contributions to the study of cybersecurity. First, the study

contributes to the literature by clarifying the different foreign policy functions of cyber capabilities. Second, study advances the cybersecurity literature by identifying the strategic advantages of cyber capabilities when these are used as instruments in the Region. The paper is divided into four parts and a conclusion.

The remaining section of the introduction presents the scope and concepts relevant to the paper. The second part examines how states have used cyber capabilities to pursue foreign policy interests. The third part explores how geopolitical constraints contribute to the cyber conflict in the Region. The fourth part explores the strategic advantages of employing cyber capabilities in the Asia-Pacific. The last part recapitulates the main argument of the paper and offers some implications for the cyber strategies of states in the Region.

Scope and concepts

The study of cyber phenomena is extensive and involves several fields of inquiry that transcends the social sciences. This study however, is anchored on the field of International Relations and focuses on the state as the primary unit of analysis because it remains the most powerful actor in cyberspace (Nye, 2011). Lindsay (2013, 403) notes that states have a dominant role in cyberspace because they "have the most experience managing information system complexity through their trials with combined arms force employment and large-scale systems integration…" Meanwhile, Brantly (2014, 465) points out that cyber attacks are a "functional tool of state" since it is capable of influencing "the space between overt diplomacy and overt war." The study therefore, only considers the cyber security capabilities of states as well as the implications of interstate cyber conflict in its assessment.

Given this scope, cyber capabilities are defined as three types of operations: computer network attack, computer network defence, and computer network exploitation. Computer network attack (CNA) is the capability to use computers to "disrupt, deny, degrade, or destroy information" in computers and information systems while computer network defence (CND), on the other hand, is the capability to "detect, analyse, and mitigate threats and vulnerabilities, and outmanoeuvre adversaries." Computer network exploitation (CNE) is the capability to collect intelligence through the use of computer networks to gather data about adversaries (U.S. Department of Defence, 2010).

These operations are considered as general classifications for what states are capable of in cyberspace, however the specific operational instrument or weapon involved in executing cyber attacks are designated as "cyber weapons." This study draws on Rid and McBurney's (2012, 7) work in defining the concept: a cyber weapon is a computer code that is employed with the intention of "manipulating, threatening or inflicting physical, functional, or mental harm to structures, systems, or living beings."

Cyber capabilities as foreign policy instrument

In exploring the utility of cyber capabilities, it is useful to consider these capabilities as foreign policy instruments used by states to pursue their national interests. This idea is based on empirical research that suggests that cyber conflict is predominant between states with existing foreign policy disputes (Valeriano and Maness, 2014). Cyber capabilities are useful instruments for states depending on the type of foreign policy issue they are confronted with and the objectives these states intend to achieve. Following these conditions, there are three ways that states deploy computer network operations for strategic effect: covert action, strategic ambiguity, and deception.

The first is the use of covert action against adversaries. Covert action is a state instrument designed to support foreign policy by influencing political, economic, or military environments overseas without revealing the role of the sponsoring state (Johnson, 1989, 19). A number of activities are included as part of covert action from propaganda to paramilitary activities but the role of computer network operations is still under debate. The discreet and near instantaneous nature of cyberspace however, makes cyber operations an appropriate and distinct activity within the range of covert action.

Like propaganda and paramilitary activities, cyber operations can support foreign policy by influencing outcomes during security dilemmas where diplomacy is not effective and military action is counterproductive (Brantly, 2014, 466). An example of computer network driven covert action is the use of a malicious computer worm (i.e. Stuxnet) by the U.S. and Israel to disrupt the uranium enrichment program of Iran in 2010. The operation was evaluated as low risk because it involved minimal human deployments and was judged useful even if the outcome did not result in consequential damage (Barzashka, 2013, 48).

The second is the use of cyber capabilities to support the policy of strategic ambiguity. This policy is adopted by states to introduce uncertainty in decision-making

process by deliberately not clarifying their involvement in contentious security situations such as the policy of the U.S. towards the Taiwan Strait. The logic of the policy is that since the involvement of the U.S. is uncertain, the conflict between China and Taiwan will not escalate to war (Zhongqi, 2003, 387). Cyberspace is particularly suited for ambiguity because computer network operations are inherently stealthy therefore the risk of detection is low and the probability of retaliation is unlikely (Sheldon, 2015, 288-293). States can therefore pursue their foreign policy interests through cyberspace with minimal risk of involvement or visible commitment to parties engaged in the conflict (Libicki, 2011). The use of this policy has been limited but the proliferation of cyber capabilities makes strategic ambiguity a favourable strategy for states that are entangled in contentious foreign policy dilemmas but is unwilling to commit substantial resources.

The third is using cyber capabilities support foreign policy by deceiving adversaries. Deception through cyberspace is a distinct option that can potentially be employed as a protective strategy for states. While this idea is difficult to test empirically, preliminary research suggests that two advantages can be drawn from using strategic deception (Gartzke and Lindsay, 2015). Deception can improve cyber defensive operations by creating traps such as installing malicious software (malware) in critical databases to trace and subvert attackers after they infiltrate computer systems. Specifically, states may encourage computer network exploitation by allowing access to terabytes of data but deceive perpetrators by attaching sophisticated malware in the stolen data (Singer and Friedman, 2014, 55-59). Another is using deception to improve deterrence in cyberspace. Applying technical countermeasures such as broadcasting beacons that can entrap attackers and trace its location and silent intrusion-detection systems that give clues to attribution, increase the threat of detection and retaliation for perpetrators, thereby discouraging subsequent attacks (McHugh, et al., 2000; Modi et al., 2013).

Geopolitical constraints in Asia-Pacific

The Asia-Pacific is the most active Region for interstate cyber incidents due to pre-existing rivalries that are mostly caused by territorial disputes (Valeriano and Maness, 2015a, 128-129). Studies on interstate conflict suggest that territorial disputes are more war prone than other sources on conflict because “human territoriality encourages the establishment of

borders through aggressive displays" (Valeriano and Vasquez 2010, 3). The implication is that neighbouring states have a higher probability of going to war compared to any other two states if their borders have not been mutually acknowledged. While territorial disputes are a significant factor that fosters the use of cyber capabilities, other factors such as great power rivalry and historical animosities support the prevalence of cyber conflict in the Region since these factors have been part of the rationale of the procurement and upgrade of conventional military capabilities (Tan, 2014, 105-141).

The great power rivalry between China and the U.S. has been a dominant feature of international relations in the twenty-first century however, the extension of the military competition into cyberspace has just escalated during the last decade. While both powers have invested extensively in conventional military capabilities, they have also militarised cyberspace by developing cyber commands, creating doctrines for cyber operations, and rationalising of policies that enable military responses to cyber conflict (Manson, 2011; Domingo 2015). More importantly, these states already have high level of expertise in employing complex computer network operations in support of their respective foreign policy objectives, some of which relate to tensions in the Asia-Pacific (Valeriano and Maness, 2015a, 88).

The rivalry between two powers may not directly initiate cyber conflict but it heightens the uncertainty in the Region through the militarisation of cyberspace and through the use of cyberspace for espionage. The militarisation of cyberspace by great powers contributes to uncertainty because there is insufficient knowledge about cyber operations to determine the relative capabilities of each state (Liff, 2012, 402). While China and the U.S have demonstrated their capabilities through selected cyber incidents, there is no conclusive assessment regarding the capabilities of these states. The ambiguity surrounding the impact of cyber weapons has influenced other states respond to uncertainty by hardening network defences and enhancing situation awareness.

A second aspect that contributes to uncertainty in the Region is that computer network operations are utilised by great powers for espionage. Espionage is a standard and permanent feature in international relations however, the anonymity and ubiquity afforded by cyberspace enables great powers to implement more extensive and invasive espionage activities. Computer network exploitation contributes to uncertainty in the Asia-Pacific because cyber capabilities have been utilised to exploit the communications and computer

networks of both adversaries and allies. For example, China's computer network operations are threatening because they collect massive amounts of classified information and intellectual property from states regardless if these are important trading partners like South Korea, benign neighbours like Malaysia or small states such as Brunei and Singapore (Geers, *et al*., 2014; Boland, 2015). On the other hand, states are distrustful of U.S. since its intelligence agencies were confirmed to be monitoring the communications of world leaders of allied states in Europe, Latin America, and Asia (Easley, 2014; Walsh and Miller, 2016).

Historical animosities involving religion and ethnicity have stimulated the sustained investment in conventional military capabilities in the Region. Some notable examples include conflicts between North and South Korea, China and Taiwan, India and Pakistan, and Singapore and Malaysia. These states are compelled to maintain capable and effective military forces to project a strong strategic posture and ensure a credible military response to adversaries (Tan, 2014, 113-124). Modern military platforms such as the fighter jets and subsystems for air-defence however all run on cyber-enabled technologies and therefore require cyber capabilities to counteract exploitation and prevent systems from being compromised. In this sense, computer network operations have become necessary tools to protect military forces from cyber threats. While enduring animosities between states do not directly contribute to cyber conflict, these conflicts encourage the development of conventional military capabilities that subsequently require cyber capabilities for network defence.

Strategic advantages

The confluence of different geopolitical constraints has contributed to the sustained build-up of conventional military weapons thereby developing an "arms dynamic" that contributes to insecurity between states in the Region (Bitzinger, 2010). While military force can alter the behaviour of states through various ways including compellence, deterrence, and actual military invasion, this particular instrument is not necessarily advantageous in unique geopolitical environments such as the Asia-Pacific. There are two reasons for this assertion.

First, great powers that competing for power and influence are not inclined to initiate a war in the Region because of less destructive alternatives such as power sharing between China and the U.S. (cf. Goh, 2013, Porter, 2013; Goldstein, 2015). This can be

pursued if the U.S. accommodates China's rise by not intervening in disputes that have little strategic value such as the contemporary flash points in the East and South China Seas and "by treating it as a great power" (Goh, 2015). In addition, economic interdependence has enabled less powerful states to hedge between rather than side with one great power, relying on the U.S. for security and China for economic growth (McKinney, 2015, 57). This predicament moderates the conflict between great powers because it diffuses the build-up of allied states that are entangled into the rivalry. Second, Asian societies are culturally oriented towards "applying power to achieve order through consensus rather than to derive it through debate and compromise" (Tow, 1999). Since the use of military force is more aggressive than debate and compromise, this instrument is not a first option for states in the Region. Alternative options are therefore necessary for states in the Region to achieve specific foreign policy objectives.

In this context, this section examines the strategic advantages of cyber capabilities. There are various concepts developed to characterise cyber capabilities, however this paper focuses on specific characteristics that make it attractive for states in the Asia-Pacific. Drawing on the existing literature on cybersecurity, the paper proposes that nonphysicality, stealthiness, and functionality are characteristics of computer network operations that explain the favourability of cyber capabilities that as foreign policy instruments in the Region. Other crucial characteristics of cyber capabilities have been convincingly disputed by cybersecurity scholars and are omitted in this paper: non-attribution, low barriers to entry, offense dominance, and ubiquitousness.[1]

Nonphysicality

The first advantage of utilising cyber capabilities is that these do not directly cause physical damage or harm. The primary instruments used in cyber incidents are cyber weapons or malicious computer codes that are not tangible elements located in the physical domain. This fundamental characteristic of cyber weapons defines the nonphysical nature of computer network operations as well as the possible outcomes that cyber operations can achieve.

[1] The literature is expanding but the most relevant works for these issues are: attribution problem (Clark and Landau, 2011; Rid and Buchanan, 2014), low barriers to entry (Denning, 2009; Nye, 2011), offence dominance (Lindsay, 2013; Slayton, 2017) and ubiquitousness (Gray, 1996; Libicki, 1996).

The nonphysical nature computer network operation is attractive to great powers that have interests in the Region because of two reasons. First, as previously mentioned, great power are not interested in initiating war in the Region. China, Russia, and U.S. have formidable conventional military capabilities but for specific objectives they favour the use of cyber capabilities because of non-lethal nature of cyber weapons. While great powers have a range of foreign policy tools at their disposal, the use of cyber capabilities is an emerging strategic option for great powers. Employing computer network operations is favourable when the objective is limited such as to convey displeasure regarding an adversary's foreign policy or to communicate specific political preferences in the context of an existing rivalry. Moreover, the low risk of escalation to armed conflict is a strong incentive for great powers to utilise computer network operations as a foreign policy instrument.

The strategic value of computer network operations is supported by the existing research that confirms the occurrence of cyber incidents between great powers in the Region. For instance, the U.S. and Russia have engaged in several cyber incidents that can be classified into two categories: espionage and disruption (Valeriano and Maness, 2015b, 102-103). Although espionage is normal aspect of diplomatic relations between U.S. and Russia, disrupting the Eastern power grid through network attacks is not. In this case, the use of computer network operations was useful for Russia because it achieved the limited objectives it set out as well as provoked a diplomatic rather than military response from the U.S. (Gambino *et al.*, 2016). Another example is the geopolitical rivalry between China and the U.S. that has spread into cyberspace, with both states engaged in more than twenty cyber exchanges mostly initiated by China. These incidents are mostly characterised as disruption and espionage operations but the persistence and frequency of the incidents has contributed to the prevailing tension between the two great powers. The use of cyber capabilities have been a favourable for China because while the U.S. has responded with its own cyber operations to counter intrusions, the more decisive response to China's actions is diplomatic: an agreement that facilitates increased cooperation in countering cyber crime, developing appropriate norms of state behaviour in cyberspace, and establishing mechanisms for high-level joint dialogue on cybersecurity (Collins, 2015).

Second, since cyber incidents are nonphysical, these are not automatically considered as military action. This characteristic can be exploited and used against states

that rely on military alliances and defence pacts considering that it is difficult to justify a case for military action against perpetrators of cyber conflict. A prominent case that supports this point is the distributed denial of service attacks (DDoS) against Estonia in 2007. Despite the extensive scope of the DDoS attacks, Estonia was unable to convince the North Atlantic Treaty Organization (NATO) to respond to Russian-based computer network attacks using military force since NATO did not consider the cyber incident as a case of clear military action (Crandall, 2014, 36). While NATO Member States have invested in considerable resources and implemented targeted measures to enhance their respective cyber defensive capabilities, the official response to computer network attacks still remains restrained: "A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis" (North Atlantic Treaty Organization [NATO], 2014).

Stealthiness

The second advantage of using cyber capabilities is the surreptitious nature of computer network operations. The deployment of cyber weapons is difficult to detect because malicious software can pretend to or be integrated within legitimate computer programmes that seem to be non-threatening to users. The stealthy nature of cyber operations is further manifested in the challenge of attributing CNA. Debates about how to address the attribution problem are extensive but a clear strategy to attribute cyber incidents remains elusive.

The stealthiness of computer network operations is advantageous for states engaged in rivalries and disputes in the Region because these can support intelligence operations against adversaries specifically through espionage and sabotage. To be sure, intelligence operations conducted through cyberspace have already been useful for some states. In terms of espionage, China's capacity for CNE is well documented and has proven to be effective enough to infiltrate the most secure networks as well as collect secret information from various government agencies. Indeed, the Asia-Pacific is the most active region for interstate cyber conflict mainly because of Chinese actions: "The Chinese are the most active propagators in cyberspace, and they have initiated cyber incidents with every rival in the Far East region…" (Valeriano and Maness, 2015a, 128).

In terms of disruption, North Korea's cyber operations against the U.S. and South Korea interests have been persistent, inflicting DDoS attacks against websites and processes

of government agencies, private companies, and civil society groups (Haggard and Lindsay, 2015; Jun, *et. al.* 2015). A prominent incident involving the U.S. was the network intrusions against Sony Pictures Entertainment (SPE) in 2014. North Korea did not fully succeed in its objective to abandon the release of *The Interview* but it did manage to change the behaviour of SPE by inflicting financial losses and destabilised its leadership (Sharp, 2017, 20). South Korea's case is more problematic since it has been a more frequent target of computer network attacks by its neighbour with at least nine disruptive incidents in since 2009 (Jun, *et al.* 2015). A commonly cited example is the "10 Days of Rain" incident that involved DDoS attacks against multiple targets in South Korea such media outlets, financial institutions, and government agencies including the website of United States Forces Korea (USFK) (McAfee, 2011). The objective of these attacks was to undermine the government services as well as business operations in South Korea, highlighting the geopolitical tension between the two states (Jun *et al.*, 2015).

Functionality of cyber capabilities

The third advantage pertains to functionality or the range of actions that can be undertaken through computer network operations. Conventional military weapons such as missiles, guns, and bombs are specifically designed to inflict or defend against physical attacks. In this sense, cyber capabilities are functional because these capabilities are useful in supplementing conventional weapons through three non-lethal strategic functions that are vital in military operations.

The first and the most fundamental function is that computer network operations are essential for protecting military networks. Modern military command and control systems are managed through cyber-enabled technology therefore cyber capabilities are necessary to prevent disruptions and counter infiltrations that can compromise military operations. Since states are in the process of upgrading their military capabilities, securing computers and network is now a fundamental challenge for military forces in the Region.

The second function is that cyber capabilities can be utilised offensively by disabling command and control systems during military readiness exercises and maritime operations in the Region. The objective of this action is to communicate protest or express disapproval against military force projection of adversaries. This move is effective because attributing computer network attacks is difficult and escalation to conventional military conflict is

improbable (Valeriano and Maness, 2015a). Another offensive function of cyber capabilities is the suppression of an adversary's air defence systems by infiltrating and disabling them. An example is the case of *Operation Orchard* in 2007. The Israeli Air Force facilitated the bombing of a Syrian nuclear facility by exploiting the Syria's military computer networks and deactivating its air defence systems (Miller, 2016, 3). The outcome of the operation was the successful destruction of the Al Kibar plant, a facility that contributed Syria's nuclear weapons development.

The third is that these capabilities maybe used for defence by disrupting computer systems of hostile military forces when they breach air defence identification zones or operate close maritime territorial boundaries. The objective of this measure is to defend a state's national security by dissuading adversaries from operating near territorial boundaries. This measure has been considered by China as part of their anti-access/anti-denial strategy to counter U.S. military power in the Region. Existing assessments suggest that the People's Liberation Army is likely to "Conduct cyber attacks against US battle networks aimed at disrupting logistics, corrupting C2 systems, degrading fire control radars, denying essential services, and degrading US counter-space control, space situational awareness and space ground control stations." (Van Tol, *et al.*, 2010, 20).

In addition to supporting conventional operations, the other dimension of functionality is the transitory nature of cyber weapons. Transitory in the context of cyber weapons refers to "the temporary ability to access a computer system or network to cause harm or damage to living and material entities" (Smeets, 2017, 5-6). This contributes to the functionality of cyber capabilities because unlike conventional military weapons, the effectiveness and impact of cyber weapons decreases relatively quickly because patches can be installed and vulnerabilities closed within an average of 312 days (Smeets, 2017, 5). In this sense, cyber weapons are functional particularly for powerful states because they states can afford to maximise the deployment sophisticated cyber weapons within its decay period and achieve their objectives with less risk of inflicting physical damage or harm.

Cyber Capabilities as the New Normal

Cyber capabilities are emerging foreign policy tools that states have utilised to signal strategic preferences in the context of specific security challenges. States have so far exploited the cyberspace for covert action, strategic ambiguity, and deception all of which are operations to achieve limited strategic objectives. Cyber capabilities are particularly useful for states in the Asia–Pacific Region because of the enduring geopolitical circumstances shaped by territorial disputes, great power rivalry, and historical animosities.

In this context, this paper argued that computer network operations are favourable foreign policy instruments because of the strategic advantages that these capabilities offer. The unique nonphysicality of cyber weapons limits the potential for conflict escalation and gives more incentives for great powers to make use of computer network operations as a response to specific foreign policy issues. The stealthiness of computer network operations is a strong compliment to existing intelligence operations of states, and another incentive for them to consider cyber operations as an instrument. The functionality of cyber capabilities is a third incentive. Cyber weapons can be useful because these can supplement conventional military weapons by disabling, disrupting, and exploiting adversaries' command and control systems.

What do these advantages mean for states in the Asia-Pacific? Three implications can be drawn from the analysis in this paper. The first implication is that cyber conflict between states will be come a fundamental feature in international relations. Since information and communications technologies (ICTs) are vital for every aspect of state interaction from diplomacy to military force, computer network vulnerabilities will constantly be exploited to achieve specific foreign policy interests in the Region. In fact, cyber operations have influenced foreign trade negotiations between powerful states (Lindsay, 2015), motivated the capacity development in region institutions (Heinl, 2013), disrupted the operations of transnational corporations (Knapp and Boulton, 2006), and facilitated espionage between competitors (Valeriano and Maness, 2015a). Although there are persistent regional efforts to manage cybersecurity issues, these exchanges will not end because the prevailing geopolitical environment fosters competition and uncertainty between states.

The second implication is the necessity for states to adjust their national security and military strategies to incorporate cyber capabilities. While highly networks states such as Singapore, New Zealand, and South Korea were ahead in upgrading their infrastructure and

developing cyber strategies, a number of states such as Brunei and the Philippines continue fall behind in terms of cyber capability development (Feakin *et al.*, 2016). While this imbalance can be attributed to the digital divide or the "the gap in access to or use of ICT devices" (Ayanso, *et al.*, 2010, 304) between states, the rapid diffusion of ICTs has situated states with limited, underdeveloped capabilities in a weak position, making them vulnerable to computer network attacks by other states (Gamreklidze, 2014, 204-205). In this regard, it is vital for developing states in the region to revaluate their strategies to incorporate cybersecurity as a national security priority as well as measures such as strengthening national computer emergency repose teams to mitigate computer network attacks by adversaries (Heinl, 2016).

The third implication is that a "cyber arms race" is unlikely in the region. The contest between states is considered an arms race when the phenomenon satisfies the following conditions: (i), the existence of two or more states, both conscious of antagonism, (ii) states must focus the development of their armed forces on the participants of the arms race, (iii) state competition must be in terms of quantity (men and weapons) and quality (men, weapons, organisations, doctrine, deployment); and (iv) states must increase or enhance their military weapons at a rapid rate (Gray, 1971, 41). Following these conditions, recent studies have argued that the increased investment of states in capabilities for computer network operations has initiated an active competition for military superiority in cyberspace (cf. Collins and McCombie, 2012; Limnéll, 2016; Kshetri, 2016, 5-7). These studies however are incomplete at best because the authors did not present any evidence that measures the increase of cyber weapons in the framing of military build-ups (Valeriano and Maness, 2015a). Furthermore, there are two reasons why a "cyber arms race" is improbable in the Asia-Pacific Region.

Firstly, the most powerful states in cyberspace have few incentives for revealing the scope and range of their cyber capabilities. Disclosure of what a state can do in cyberspace is necessary for establishing the credibility of its capabilities. Unfortunately, sharing information regarding cyber capabilities diminishes the advantages derived from employing these capabilities because unlike conventional military weapons, cyber weapons are "highly transitory" or their "ability and effectiveness to cause harm" has an expiration date (Smeets, 2017,7). For instance, once a zero-day vulnerability is exploited, its takes an average 312 days before patches are installed and vulnerabilities are closed (Bigle and Dumitras, 2012).

In this case, a cyber arms race is not possible because states are not aware of each other's capabilities. Secondly, there is no reason for less powerful states to "race" towards developing cyber capabilities because these capabilities can only achieve limited strategic outcomes (Gray, 2013, 44). Middle and small powers are therefore building-up cyber capabilities in a gradual rather than rapid manner, thereby making a cyber arms race doubtful in the Region.

Bibliography

Ayanso, A. Cho, D.I., and Lertwachara, K. (2010). The Digital Divide: Global and Regional ICT Leaders and Followers. *Information Technology for Development,* 16(4), 304–319.

Barzashka, I. (2013). Are Cyber-Weapons Effective? *RUSI Journal*, 158(2), 48-56.

Bigle, L. and Dumitras, T. (2012, October 16-18). *Before We Knew It An Empirical Study of Zero-Day Attacks In The Real World* Paper Presented at 2012 ACM Conference on Computer and Communications Security, Raleigh, North Carolina, United States. doi.10.1145/2382196.2382284

Bitzinger, R. A. (2010). A New Arms Race? Explaining Recent Southeast Asian Military Acquisitions. *Contemporary Southeast Asia,* 32(1), 50-69.

Boland, B. (2015). Southeast Asia: An Evolving Cyber Threat Landscape. Milpitas, CA: FireEye, Inc.

Brantly, A. F. (2014). Cyber Actions by State Actors: Motivation and Utility. *International Journal of Intelligence and CounterIntelligence*, 27(3), 465-484.

Clark, D. D., & Landau, S. (2011). Untangling Attribution. *Havard National Security Journal.* 2(2), 1-30.

Crandall, M. (2014). Soft Security Threats and Small States: the Case of Estonia. *Defence Studies,* 14(1), 30-55.

Collins, S. and McCombie, S. (2012). Stuxnet: The Emergence of a New Cyber Weapon and its Implications, *Journal of Policing, Intelligence and Counter Terrorism*, 7:1, 80-91.

Collins, W., Lawrence, S.V., Rennack, D.E., and Theohary, C. A. (2015). *U.S.–China Cyber Agreement.* Washington D.C.: U.S. Congress Research Service.

Denning, D. E. (2009). "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal* 1(1), 6-10.

Domingo, F. (2016). Conquering a New Domain: Explaining Great Power Competition in Cyberspace. *Comparative Strategy* 35 (2), 154-168.

Easley, L. (2014). Spying on Allies. *Survival* 56(4), 141-156.

Feakin, T., Woodall, J., and Nevill, L. (2016). *Cyber Maturity Index 2016*. Canberra: Australian Strategic Policy Institute.

Gambino, L., Siddiqui, S. and Walker, S. "Obama expels 35 Russian diplomats in retaliation for US election hacking" *The Guardian*, Retrieved from: https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack

Gamreklidze, l. (2014). Cyber security in Developing Countries, A Digital Divide Issue. *The Journal of International Communication*, 20(2), 200-217.

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, 24(2), 316-348.

Gartzke, E. (2013). The Myth of Cyberwar Bringing War in Cyberspace Back Down to Earth. *International Security,* 38(2), 41-73.

Geers, K., et al. (2014) *World War C: Understanding Nation-State Motives Behind Today's*

Advanced Cyber Attacks. Milpitas, CA: FireEye.
Goh, E. (2013). *The Struggle for Order: Hegemony, Hierarchy, and Transition in Post-Cold War East Asia*. Oxford, UK: Oxford University Press.
Goldstein, L. (2015) *Meeting China Halfway: How to Defuse the Emerging US-China Rivalry.* Washington, DC: Georgetown University Press, 2015.
Gray, C.S. (1971). The Arms Race Phenomenon. *World Politics* (24) 1, 39-79.
Gray, C. S. (1996). The Continued Primacy of Geography. *Orbis* 40(2), 261-274.
Gray, C. S. (2013). *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Carlisle, PA: U.S. Army War College Press.
Haggard, S. and Lindsay, J. (2015). North Korea and the Sony Hack: Exporting Instability Through Cyberspace. *AsiaPacific Issues* No. 117.
Heinl, C. (2016). Regional Cybersecurity Policy Developments in Southeast Asia and the Wider Asia Pacific in Shashi Jayakumar (Eds.) *State, Society and National Security Challenges and Opportunities in the 21st Century* (233-245). Singapore: World Scientific.
Johnson, L. K. (1989). *America's Secret Power: The CIA in a Democracy Society* Oxford: Oxford University Press.
Jun, J., LaFoy, S., & Sohn, E. (2015). *North Korea's Cyber Operations: Strategy and Responses* Washington D.C.: Center for Strategic and International Studies.
Knapp , K. J., & Boulton, W. R. (2006). Cyber-Warfare Threatens Corporations: Expansion Into Commercial Environments. *Information Systems Management,* 23(2), 76-87.
Kshetri, N. (2016). *Quest for Cyber Superiority* Switzerland: Springer International Publishing.
Libicki, M. C. (1996). The Emerging Primacy of Information. *Orbis* 40(2), 261-274.
Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica, California: RAND Corporation.
Libicki, M. C. (2011). The Strategic Uses of Ambiguity in Cyberspace. *Military and Stratgic Affairs,* 3(3), 3-10.
Liff, A.P. (2012). Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies* 35(3), 401-428.
Limnéll, J. (2016). The Cyber Arms Race is Accelerating – What are the consequences? *Journal of Cyber Policy,* 1(1), 50-60.
Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies,* 22(3), 365-404.
Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security*, 39(3), 7-47.
Manson, G. P. (2011). Cyberwar: The United States and China Prepare for the Next Generation of Conflict. *Comparative Strategy*, 30(2), 121–133.
Mahnken, T. G. (2011). Cyberwar and Cyber Warfare in Kristin M. Lord and Travis Sharp (Eds.) *America's Cyber Future: Security and Prosperity in the Information Age, Volume II* (55-64). Washington, DC: Center for a New American Security.
McKinney, J. (2016) "Four Questions for the Improbable War. *Asian Security*, 12 (1), 53-61.
McAfee. (2011). *Ten Days of Rain: Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea* Santa Clara, CA.: McAfee.
McHugh, J., Allen, J., & Christie, A. (2000). Defending Yourself: The Role of Intrusion Detection Systems. *IEEE Software*, 17(5), 42-51.

Miller, S. (2016). Cyber-attacks and 'Dirty Hands': Cyberwar, Cyber-crimes or Covert Political Action? in Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser (Eds.) *Binary Bullets: The Ethics of Cyberwarfare* (229-250). Oxford: Oxford University Press.
Modi, C., Patel , D., Bhavesh, B., Patel, H., Patel , A., & Rajarajan, M. (2013). A survey of Intrusion Detection Techniques in Cloud. *Journal of Network and Computer Applications*,

36(1), 42-57.
North Atlantic Treaty Organization Wales Summit Declaration, 2014. Retrieved from http://www.nato.int/cps/ic/natohq/official_texts_112964.htm
Nye, J. S. (2010). *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard University.
Nye, J. S. (2011). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly*.5(4), 18-38.
Nye, J. S. (2011). *The Future of Power*. New York: PublicAffairs.
Porter, P. (2013) *Sharing Power? Prospects for a U.S. Concert-Balance Strategy* Carlisle, PA: Strategic Studies Institute, U.S. Army War College Press.
Rid, T. & McBurney, P. (2012). Cyber-Weapons. *RUSI Journal* 157(1), 6-13.
Rid, T. & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies* 38(1-2), 4-37.
Sheldon, J. B. (2015). Rise of Cyber Power. In J. Baylis, J. J. Wirtz & C. S. Gray (Eds.), *Strategy in a Contemporary World* (4th ed.) (303-322). Oxford: Oxford University Press.
Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar*. Oxford: Oxford University Press.
Smeets, M. (2017). A Matter of Time: On the Transitory Nature of Cyberweapons. *Journal of Strategic Studies,* 1-28.
Tan, A.T.H. (2014). *The Arms Race in Asia: Trends, Causes and Implications*. London: Routledge.
Tow, W. (1999) Strategic Cultures in Comparative Perspective in K. Booth, and R. Trood (Eds.), *Strategic Cultures in the Asia-Pacific Region* (323-338). London: Palgrave Macmillan.
U.S. Department of Defence. (2010). *Joint Terminology for Cyberspace Operations* Washington D.C.: Vice Chairman of the Joint Chiefs of Staff.
Valeriano, B., & Maness, R. (2015a). *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* Oxford: Oxford University Press.
Valeriano, B., & Maness, R. (2015b). *Russia's Coercive Diplomacy Energy, Cyber, and Maritime Policy as New Sources of Power.* London: Palgrave Macmillan.
Valeriano, B., & Maness, R. (2014). The Dynamics of Cyber Conflict Between Rival Antagonists, 2001- 2011. *Journal of Peace Research,* 51(3), 347-360.
Valeriano, B. & Vasquez, J. A. (2010). Classification of Interstate Wars, *The Journal of Politics*. 72 (2), 1–18.
Van Tol, J., et al. (2010). *AirSea Battle: A Point-of-Departure: Operational Concept.* Washington D.C.: Center for Strategic and Budgetary Assessments.
Walsh, P. & Miller, S. (2016). Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden. *Intelligence and National Security* 31 (3), 345-368.
Yost, D.S. (2010). NATO's evolving purposes and the next Strategic Concept *International Affairs* 86(2), 489–522.
Zhongqi, P. (2003). US Taiwan Policy of Strategic Ambiguity: A Dilemma of Deterrence. *Journal of Contemporary China* 12(35), 387-407.