The Challenges of Cyber Deterrence

by **MAJ Lee Hsiang Wei**

Abstract:

In the cyber realm, there are three necessary pillars of cyber defence strategy—a credible defence, an ability to retaliate and a will to retaliate. The concept of cyber deterrence builds upon this strategy to alter an adversary's actions for fear of an impossible counter-action. Cyber security is an expensive business and is a difficult strategy to achieve. Despite billions of dollars spent on cyber security, it did not stem the rise in cyber-attacks over the past five years. Cyber deterrence is impractical for most nations given today's technology and the lack of common interpretation of the international law for the cyber domain. This essay presents obstacles such as attribution, diminishing capability to retaliate, unnecessary escalation, involvement of non-state actors and a potential legal issue that make cyber deterrence a less viable strategy to adopt.

Keywords: Cyber Security, Cyber Deterrence, Viability, Technology, Hacker

INTRODUCTION

The threat of cyber-attacks and the ascent of cyberspace as a military domain has gained significant traction over the past three years. The Stuxnet computer worm was discovered in June 2010 and it was found to specifically target Iran's nuclear enrichment centrifuges.[1] The extent and complexity of Stuxnet demonstrated the potential of cyber warfare and the extent it could be used. The use of cyber warfare was also evident in conflicts both in Estonia and Georgia, in 2007 and 2008 respectively, where coordinated cyber-attacks compromised government websites and denial of service attacks crippled the systems of news networks and financial institutions.[2] More recently, the threat of cyber-attacks and subsequent defacement of Singapore government websites by 'The Messiah' in October 2013 showed that Singapore was not spared in the realm of cyber-attacks.[3] The cost of cyber defence has also garnered significant attention with reports of countries spending billions of dollars on cyber defence in a single year.[4] With the increased awareness of cyber-attacks and cyberspace as a military domain, the concept of cyber deterrence has gained traction amongst countries such as the United Kingdom and the United States.[5]

The concept of cyber deterrence builds upon the strategy of cyber defence by incorporating both the ability to retaliate as well as the will to retaliate towards the cyber attacker. This essay will argue that the concept of cyber deterrence is impractical for most nations given today's technology and the lack of a common interpretation of the international law for the cyber domain. While academics have well-articulated the elements of deterrence, in practice there are implementation hurdles and practical problems that would render most proposed cyber deterrence strategies inimical to a nation's interests. A credible cyber defence, though probably more expensive, is a less risky and more practical approach.

What is a Cyber-attack?

One can view a cyber-attack as any action taken to undermine the functions of a computer network for a political or national security purpose.[6] For a cyber-attack to be carried out, it usually requires the target system to have one or more vulnerabilities that the attacker can exploit to manipulate to the system. Some of the vulnerabilities used are known as 'zero-day' as they had not been uncovered or made known to the developers. Stuxnet, for example, was found to use a total of four zero-day vulnerabilities.[7]

What is Cyber Deterrence?

According to conventional deterrence theory, "deterrence, in its broadest sense, means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks."[8] The strategy of deterrence gained prominence in the Cold War model of Mutually Assured Destruction where any nuclear attack would be met with an overwhelming nuclear counter strike that would also destroy the aggressor. Hence, deterrence really is about the ability to alter an adversary's actions by changing the attackers' cost-benefit calculations that includes subjective and psychological assessments, as well as a state of mind brought about by the existence of a credible threat of unacceptable counteraction.[9]

With the increased awareness of cyber-attacks and cyberspace as a military domain, the concept of cyber deterrence has gained traction amongst countries such as the United Kingdom and the United States.

Extending this concept of deterrence to the cyber realm, cyber deterrence seeks to dissuade the attacker from acting for fear of retaliation. It requires preparedness and a degree of retaliatory certainty, which is linked to having an offensive capability.[10] In the cyber realm, there are three necessary pillars in this strategy—*a credible defence, the ability to retaliate and the will to retaliate.*[11] See Figure 1.

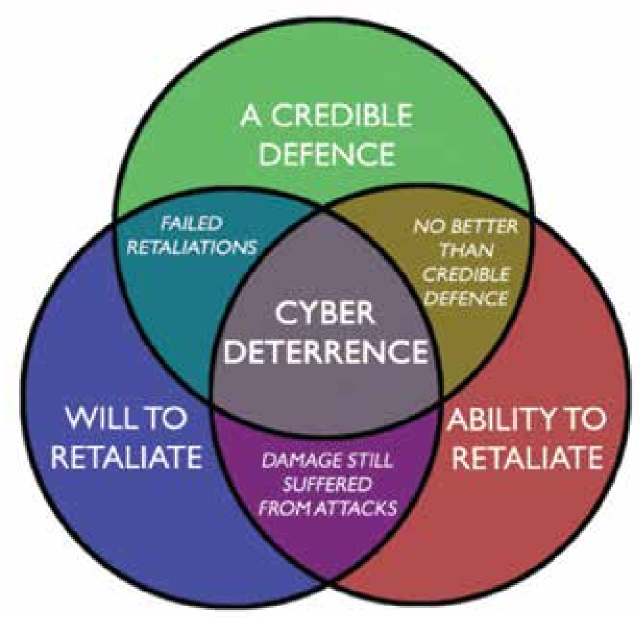


Figure 1: Components of Cyber Deterrence

The first pillar of an effective cyber deterrence strategy is to have a *credible defence*. If the cyber defence of a country is sufficient to make an attack exceedingly difficult, an attacker might decide that he lacks sufficient expertise or choose to give up after multiple failed attempts.[12] In addition to preventing a successful cyber-attack, a credible defence is also about having backup systems to achieve 'defence in depth' such that a single successful attack would not result in a total loss of the system.[13] This goal, although expensive,[14] is a practical solution to the majority of attacks.[15]

The next pillar is *the ability to retaliate*. For this pillar to work, the retaliatory action would need to result in damage greater than that inflicted by the attacker.[16] In the cyber domain, this refers to the ability to carry out cyber-attacks unto the original attacker. Implicit to the ability to retaliate in the cyber domain is the ability to identify the cyber attacker.

The last pillar is *the will to retaliate* against potential cyber attackers. The will to retaliate needs to be an overt policy. For cyber deterrence to work, the cyber attackers need to be dissuaded when they include the possibility of cyber retaliation into their impact calculus. If the perceived possibility of retaliation and the pain from cyber retaliation is high, the cyber attacker may be dissuaded from attacking. As such, the nuancing of the will to retaliate is crucial to the success of a cyber-deterrence strategy. If the message is too indeterminate, hawkish or directed to the wrong party, the will to retaliate may be rendered ineffective.[17]

A Case for Cyber Deterrence?

Given that cyber security is an expensive business and the goal of cyber deterrence would be to reduce the risk of cyber-attacks to an acceptable level at an acceptable cost, cyber defence is expensive.[18] An estimated US$55 billion was spent on cyber security in 2011 and the amount is expected to rise to US$86 billion in 2016.[19] Another study also attempted to place the cost of cyber security into perspective, estimating that an average of US$10 million was invested in cyber defence for every 125 lines of attack code written.[20] Unfortunately, expensive investment did not stem the rise in cyber-attack incidents over the past five years (See Figure 2).[21]

Governments around the world are continuing to commit more dollars in the area of cyber security. Under President Obama, the US had increased the budget for cyber defence by US$800 million to US$4.7 billion in 2014, despite tightening US budget constraints.[22] The Director of the Federal Bureau of Investigation (FBI), James B. Comey, even cautioned in a meeting with the Senate Homeland Security and Governmental Affairs Committee that in the future, "resources devoted to cyber based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats."[23] The Singapore government had done likewise in 2013 with a S$130 million plan to enhance the nation's cyber security.[24]

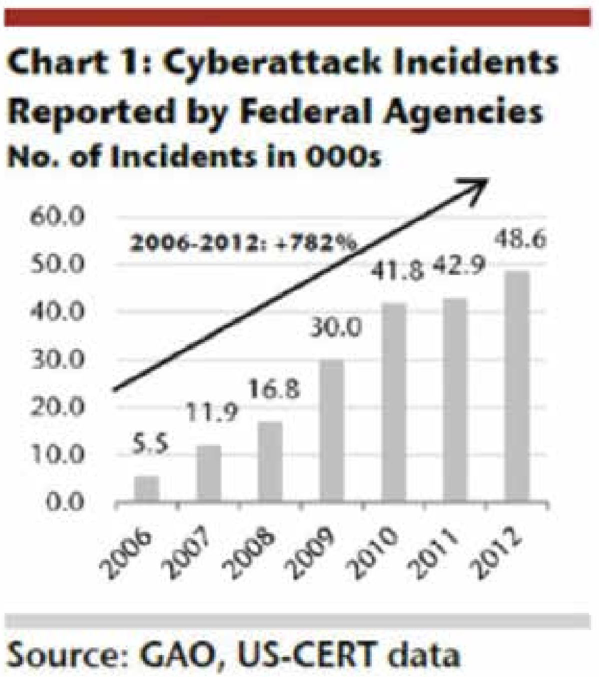


Figure 2: Cyber Attacks Incidents on US Federal Agencies

In addition, there are reports claiming that several countries such as India, China, North Korea as well as Pakistan, are rapidly developing their cyber offensive capability.[25] Some countries,[26] such as Iran,[27] have openly declared similar intentions. The threat of cyber-attacks will continue to increase as more countries develop cyber offensive capabilities.

OBSTACLES IN ACHIEVING CYBER DETERRENCE

On a conceptual level, the pillars needed to support the strategy of cyber deterrence may seem intuitive. However, the implementation and execution of the cyber deterrence strategy is inherently problematic. These obstacles affect *the will to retaliate* and *the ability to retaliate* in the cyber domain.

Problem of Attribution

The notion that retaliation can only take place after the attacker is identified tends to be trivialised as identification of the attacker is assumed to be fairly straightforward in traditional warfare. In the cyber domain however, tracing the source of cyber-attacks can be a significant hurdle. General Keith Alexander, Commander of the United States Cyber Command, mentioned in a testimony to the US Congress in 2010 that even in the foreseeable future, attribution of cyber-attacks will likely remain "costly and comparatively rare."[28]

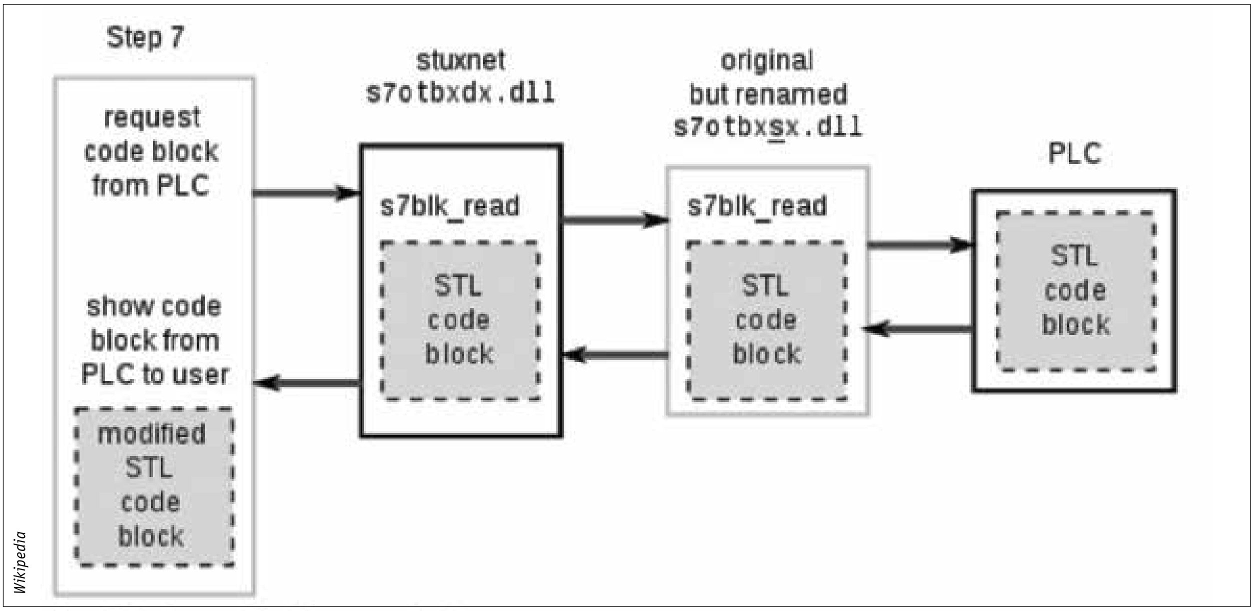
The Stuxnet computer worm that targeted Iran's nuclear centrifuges in 2010, exemplifies the difficulty in determining who the actual attackers were. Although the US and Israel were widely believed to be behind Stuxnet, there had not been any concrete evidence supporting this assertion.[29] Most of the allegations stemmed from weak circumstantial hypotheses. An example of such weak links is concerning the use of the term ‘myrtus’ in the Stuxnet code.[30] The term ‘myrtus’ can either be linked to a story of a Persian plot against the Jews in the Bible’s Book of Ester or simply an abbreviation for ‘my Remote Terminal Units’ (my-RTUs). Even after months of in-depth analysis by established security firms such as Symantec, Kaspersky Labs and F-Secure, the attacker behind the Stuxnet malware could not be definitively identified. Even while Edward Snowden had indeed claimed in an interview that Stuxnet was a collaborative effort between the United States and Israel, there has not been any further evidence available to back up the claim.[31]

The main reason why identifying a cyber-attacker is often times challenging is because almost anyone could be the culprit.

The main reason why identifying a cyber-attacker is often times challenging is because almost anyone could be the culprit. The equipment needed to launch a cyber-attack is easily accessible and inexpensive. Also, cyber-attacks can be launched from almost anywhere—an open Wi-Fi access point, a compromised third party computer or even a stolen mobile phone and routed through multiple servers before reaching the intended target. As such, attribution is often guesswork. Even with the improving ability to trace the source of cyber-attacks in recent years, computer security experts acknowledge that it is still difficult to identify the cyber attacker with total certainty.[32]

For deterrence to work, potential attackers must be sufficiently concerned that their identity would be exposed and retaliation carried out on them. Misattribution and incorrect retaliation not only weakens the logic of deterrence, but possibly results in a new enemy. The prospect of facing one cyberwar against the original attacker would have evolved to two cyberwars against both the original attacker and the misattributed party.[33]

The ability to correctly attribute the source of a cyber-attack is a key element of the cyber deterrence strategy. If a nation has doubts over the accuracy of the attribution, it would negate the will to retaliate. Retaliating against an innocent party would run the risk of unwanted escalation. If a nation is unable to confidently identify the attacker, there is no way



Wikipedia

Overview of the Stuxnet hijacking communications a retaliatory attack can be launched and hence the ability to retaliate will be effectively nullified.

The technology to accurately attribute cyber-attacks may exist outside of the open-source realm and is by extension, a closely guarded secret. The existence of such undisclosed ability to accurately attribute the cyber-attack does not play a role in deterring potential cyber attackers. Firstly, the cyber attacker, without knowing the defender's ability to attribute accurately, would not be otherwise deterred from attacking. Secondly, if the attacker believes the retaliator is just guessing or that the retaliator has ulterior motives for retaliating, the conclusion may be that carrying out further attacks will have no effect on whether or not it will face further punishment.[34] The strategy of cyber deterrence would have failed in both scenarios.

Diminishing Capability to Retaliate

Unlike a nuclear retaliatory attack, it is difficult to imagine an act of cyber retaliation that is so overwhelming that no potential cyber attacker would run the risk of being hit. Hence, repeated cyber retaliation may sometimes be necessary to enforce cyber deterrence. Computer vulnerabilities are often patched and removed expeditiously after their discovery.[35] It is unlikely for a vulnerability to go unpatched for extended periods especially after a malware has inflicted damage on well-defended systems. Even if the cyber attacker is able to produce variants of the malware, the defender would be attuned to detection and the variants would have far less effect. Academics at RAND Corporation have even gone as far as to call cyber-attacks a 'one use weapon.'[36] This characteristic is detrimental to achieving cyber deterrence as a successful retaliation may not be convincing if the attacker, who would perform the necessary security updates, believes it will be less vulnerable the next time around.

While it may be argued that since cyber retaliation is in itself a form of cyber-attack and the diminishing returns on successive offensive actions affect both parties—the original attacker and the defender, it is important to recognise that the luxury of time to uncover and accumulate multiple vulnerabilities in the target system lies with the attacker rather than the defender carrying out cyber retaliation.

Unlike a nuclear retaliatory attack, it is difficult to imagine an act of cyber retaliation that is so overwhelming that no potential cyber attacker would run the risk of being hit. Hence, repeated cyber retaliation may sometimes be necessary to enforce cyber deterrence.

Conceptually, for a nation to maintain the ability to retaliate timely, it first has to be able to identify the list of potential cyber attackers and then collate and continuously update an associated library of vulnerabilities. The library of vulnerabilities may be large due to the number of countries with cyber offensive capabilities themselves. Publicly available information shows 46 countries with military cyber programmes, with 11 counttries having offensive cyber capabilities in 2012, up from four in 2011. Many more countries could well have military programmes but do not admit to them.[37] Since vulnerabilities are constantly being discovered and corrected, the useful life of an exploit may be limited. As such, maintaining a potentially large library of vulnerabilities could place undue strain on intelligence requirements.[38]

Avoiding Escalation

The aftermath of a successful retaliation against an initial cyber-attack is difficult to predict or control. A mistimed or misinterpreted action could well result in the escalation of the situation, resulting in more cyber-attacks. The timing, choice, scope and nature of the retaliation would affect the perceived message by the attacker.

Adding to this complexity in messaging, the difficultly in tracing the source of the cyber attacker can take up to several months. This will result in a delay between the attack and the retaliatory action. The act of cyber retaliation may itself take months to execute before the effects are felt and noticed by the attacker. By the time the retaliatory cyber-attack is discovered, the retaliation could possibly seem both arbitrary and unrelated to the original incident.

If the messaging had indeed been misinterpreted, the defending nation would run the risk of the attacker responding by escalating the matter to an armed conflict. If the attacker becomes convinced that he would lose the cyber tit-for-tat, the option to counter retaliate in a different domain becomes an inviting proposition.[39] In 1998, it was reported that Russia, being concerned about their ability to control 'information warfare,' was openly declaring that it reserved the option to react to a strategic cyber-attack with the choice of any weapon in its arsenal, which included their nuclear arsenal.[40]

Faced with such difficulties in determining the outcome of the cyber retaliatory attacks and the uncertainties surrounding the reactions of the attacker, nations may choose to forego the option to conduct cyber retaliation. In consequence, this undermines the will to retaliation and compromises the strategy of cyber deterrence.

Overcoming Potential Legal Issues

The current set of international laws can only be applied indirectly to cyber warfare and they are deficient as a legal framework in addressing cyber-attacks.[41] Under international law, it is clear that if Nation A fires a missile at a military base in Nation B, Nation B has the right to defend itself with lethal force. However, it is not so clear if Nation A uses a cyber-attack to cause an explosion at a military base in Nation B, whether Nation B can still exercise its inherent right to self-defence by firing missiles at a military target in Nation A or even launching its own cyber-attack on Nation B.[42]

The legal issues surrounding offensive or retaliatory cyber-attacks are still being widely debated. While there are efforts to define the legal framework for cyber warfare such as the *Tallinn Manual on the International Law Applicable to Cyber Warfare,* the interpretation of the current set of international laws on cyber warfare differs across various nations. As many of the differences in interpretation stem from the disagreements in key definitions, academics opine that an international treaty or agreement would be necessary to overcome the legal issues on cyber warfare.[43]

As such, maintaining a potentially large library of vulnerabilities could place undue strain on intelligence requirements.

The unclear legal status of cyber warfare and retaliation in the cyber domain presents a challenge in enforcing the will to retaliate. Communicating the will to retaliate or the execution of the cyber retaliation may appear unnecessarily aggressive or even to be contravening international law by some countries. This adds to the pressures faced by the defending nation from amongst the international community.

Involvement of Non State Actors

Cyber-attacks could either be the work of state actors as well as non-state actors. The barrier to entry to carrying out cyber-attacks is low. From a resource perspective, a small group or even an individual can amass enough resources to develop the necessary skills sets and acquire the necessary hardware to carry out cyber-attacks with relative ease.[44] The low barrier of entry was highlighted in a report released by the United States Joint Forces Command in 2010, citing that it would complicate the ability to deter threats.[45]

Blackhat computer groups such as *LulzSec* and *Anonymous* are examples of non-state actors carrying out cyber-attacks, targeting both companies and states.[46] To date, *LulzSec* and *Anonymous* has targeted public websites of US government entities and publicly released stolen data on the Internet.[47]

The involvement of non-state actors in cyber-attacks complicates the strategy of cyber deterrence. These non-state actors may have little worth hitting, thereby raising the question if cyber retaliation is even worthwhile.[48] Even if cyber retaliatory attack is successful in damaging all the computer systems of the non-state attacker, the low barrier to entry would see the attackers be re-equipped quickly.

To make matters worse, if the non-state actor is deliberately shielded and hosted by another country, it may not be legally clear if the state can be even held responsible.[49] Choosing to carry out cyber retaliatory attacks may result in the host country carrying out its own 'cyber retaliation,' pitting the defending nation against both the host country and the non-state actor.

CONCLUSION

Cyber deterrence is a difficult strategy to achieve. The obstacles such as problems in attribution, diminishing capability to retaliate, unnecessary escalation, involvement of non-state actors as well as the potential legal issues, make cyber deterrence an unviable strategy in practice. The risks of misattribution, incurring widespread condemnation and unnecessary escalation would dissuade many nations from adopting this strategy.

The obstacles described in this essay weaken the *will to retaliate* as well as diminish the *capability to retaliate,* both of which are necessary to employ a strategy of cyber deterrence. Adopting a cyber-deterrence strategy is both problematic and risky. Unless new technology allows for speedy attribution to occur or until international norms on cyber-attacks are established, cyber deterrence may remain just an academic construct. In this regard, given today's technology, having a credible and robust cyber defence is the only viable approach.

BIBLIOGRAPHY

Alexander, Keith. US Department of Defence, "Statement Of General Keith B. Alexander Commander United States Cyber Command before the House Committee on Armed Services 23 September 2010."

http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC Command Posture Statement_HASC_22SEP10_FINAL _OMB Approved_.pdf.

Ashford, Warwick. Computer Weekly, "Cyber attack retaliation a bad idea, says international panel."

http://www.computerweekly.com/news/2240206279/Cyber-attack-retaliation-a-bad-idea-says-international-panel.

Campbell, Matthew. *The Sunday Times,* "'Logic bomb' arms race panics Russia."

http://cryptome.org/jya/ru-panic.htm.

Capaccio, Tony. *Bloomberg News,* "Pentagon Five-Year Cybersecurity Plan Seeks $23 Billion." April 09, 2009.

http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html

Chng, Grace. *The Straits Times,* "Singapore's cyber defence firepower gets $130m boost." http://www.straitstimes.com/breaking-news/singapore/story/singapores-cyber-defence-firepower-gets-130m-boost-20131026.

Dorothy Denning, "Barriers to Entry," *IO Journal* (2009): 6-10, http://faculty.nps.edu/dedennin/publications/Denning-BarriersToEntry.pdf

Egan, Matt. *Fox Business,* "As Cyber Threats Mount, Business is Booming in the Security World."

http://www.foxbusiness.com/technology/2013/03/12/as-cyber-threats-mount-business-is-booming-in-security-world/

Fryer-Biggs, Zachery. *Defence News,* "U.S. Military Goes on Cyber Offensive." March 24, 2012.

http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive.

Gartner Inc, . *Infosecurity Magazine,* "Global security spending to hit $86B in 2016." http://www.infosecurity-magazine.com/view/28219/global-security-spending-to-hit-86b-in-2016/.

Hathaway, Oona, Rebecca Crootof, and Philip Levitz. "The Law of Cyber Attack." *California Law Review.* n._4 (2012), 826.

http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf

Hayley, Christopher. Georgetown Journal of International Affairs, "A Theory of Cyber Deterrence."

http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/.

Hoffman, Stefanie. CRN, "Russian Cyber Attacks Shut Down Georgian Websites." August 12, 2008.

http://www.crn.com/news/security/ 210003057/russian-cyber-attacks-shut-down-georgian-websites.htm.

Kelly, Brian. Boston University Law, "Investing In A Centralized Cybersecurity Infrastructure: Why “Hacktivism” Can And Should Influence Cybersecurity Reform."

http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume92n4/documents/KELLY.pdf.

Kushner, David. IEEE Spectrum, "The Real Story of Stuxnet." December 26, 2013. Accessed February 23, 2014. http://spectrum.ieee.org/telecom/ security/the-real-story-of-stuxnet/.

Lee, Ferran. *ABC News,* "Edward Snowden: U.S., Israel ‘Co-Wrote’ Cyber Super Weapon Stuxnet."

http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/.

Libicki, Martin. RAND Corporation, "Brandishing Cyberattack Capabilities." Last modified 2013.

http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR175/RAND_RR175.pdf.

LiveSquare Security, "Cyber Warfare: the good, the bad, the ugly."

http://www.arizonatele.com/atic/docs/ATIC_Cyber_Warfare_Presentation_11_17_11.pdf.

Maher, Heather. RFERL, "New Manual Explains Laws Of Cyberwarfare

http://www.rferl.org/content/new-manual-rules-cyberwarfare/24944686.html.

Markoff, John, and David Sanger. The New York Times, "In a Computer Worm, a Possible Biblical Clue."

http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?pagewanted=all&_r=0.

Martin Libicki, *Cyberdeterrence and Cyberwarfare,* (Santa Monica: RAND Corporation, 2009), xvi.

Mearsheimer, John. Conventional Deterrence. (Ithaca, New York: Cornell University Press, 1983).

Melzer, Nills. United Nations, "Cyberwarfare and International Law."

http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

Miller, Greg. *Washington Post,* "FBI director warns of cyberattacks; other security chiefs say terrorism threat has altered."

http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html.

Murchu, Liam. "Stuxnet Using Three Additional Zero-Day Vulnerabilities." Symantec Connect (blog), September 14, 2010. http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities

Norton-Taylor, Richard. *The Guardian,* "Britain's Defense Policy Adds Cyber Deterrence to Nuclear Deterrence." September 30, 2013.

http://www.theguardian.com/uk-news/defence-and-security-blog/2013/sep/30/cyber-gchq-defence.

Paget, Francis. McAfee Labs, "Hacking Summit Names Nations With Cyberwarfare Capabilities."

http://blogs.mcafee.com/mcafee-labs/hacking-summit-names-nations-with-cyberwarfare-capabilities.

Patrick Morgan, *Proceedings of a Workshop on Deterring CyberAttacks:* Informing Strategies and Developing Options for U.S. Policy, (Washington DC: The National Academies Press, 2010), 55-76.

Rehn, Steven. U.S. Army War College, "Don’t Touch My Bits or Else! – Cyber Deterrence." http://handle.dtic.mil/100.2/ADA560247.

Robinson Neil, and Walczak Agnieszka, *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)*, (Santa Monica: RAND Corporation, 2013), 10.

RSIS, *Effective and Credible Cyber Deterrence,* (Singapore: Centre of Excellence for National Security, 2013).

http://www.rsis.edu.sg/cens/PDF/CENS_Cyber_Security_Workshop_Effective_&_Credible_Cyber_Deterrence.pdf

Secunia, "Time to Patch for All Products," *Vulnerability Security Review* (2014). http://secunia.com/vulnerability-review/time_to_patch.html.

Singer, Peter, and Allan Friedman. Armed Forces Journal, "What about deterrence in an era of cyberwar?"

http://www.armedforcesjournal.com/what-about-deterrence-in-an-era-of-cyberwar/.

Sullivan, Andy. Reuters, "Obama budget makes cybersecurity a growing U.S. priority." Last modified April 11, 2013. http://www.reuters.com/ article/2013/04/11/us-usa-fiscal-cybersecurity-idUSBRE93913S20130411

Tan, Jeanette. *Yahoo News Singapore,* "Hacker 'The Messiah' claims attack on Singapore govt sites, repeats ‘Anonymous’ cyber threat." November 05, 2012. http://sg.news.yahoo.com/hacker--the-messiah--claims-attack-on-singapore-govt-sites-repeats-‘anonymous’-cyber-threat-090023141.html.

Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia." The Guardian, May 17, 2007. http://www.theguardian.com/ world/2007/may/17/ topstories3.russia

UK Parliment, "2 MoD networks, assets and capabilities ."http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/10605.htm

Waqaas, . Hackread, "Israeli Think Tank Acknowledges Iran as Major Cyber Power, Iran Claims its 4th Biggest Cyber Army in World."

http://hackread.com/iran-biggest-cyber-army-israel/.

Weisanthal, Joe. *Business Insider,* "Notorious Hacker Group LulzSec Just Announced That It's Finished."

http://www.businessinsider.com/lulzsec-finished-2011-6?IR=T&.

Worstall, Tim. *Forbes*, "Stuxnet Was a Joint US/ Israeli Project." http://www.forbes.com/sites/timworstall/2012/06/01/stuxnet-was-a-joint-us-israeli-project/.

ENDNOTES

1. Kushner, David. IEEE Spectrum, "The Real Story of Stuxnet." December 26, 2013. http://spectrum.ieee.org/telecom/ security/the-real-story-of-stuxnet/.

2. Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia." The Guardian, May 17, 2007. http://www.theguardian.com/ world/2007/may/17/ topstories3.russia

   Hoffman, Stefanie. CRN, "Russian Cyber Attacks Shut Down Georgian Websites." August 12, 2008. http://www.crn.com/news/security/ 210003057/russian-cyber-attacks-shut-down-georgian-websites.htm.

3. Tan, Jeanette. *Yahoo News Singapore,* "Hacker 'The Messiah' claims attack on Singapore govt sites, repeats 'Anonymous' cyber threat." November 05, 2012. http://sg.news.yahoo.com/hacker--the-messiah--claims-attack-on-singapore-govt-sites--repeats-'anonymous'-cyber-threat-090023141.html.

4. Capaccio, Tony. *Bloomberg News,* "Pentagon Five-Year Cybersecurity Plan Seeks $23 Billion." April 09, 2009. http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html.

5. Norton-Taylor, Richard. *The Guardian,* "Britain's Defense Policy Adds Cyber Deterrence to Nuclear Deterrence." September 30, 2013. http://www.theguardian.com/uk-news/defence-and-security-blog/2013/sep/30/cyber-gchq-defence

   Fryer-Biggs, Zachery. *Defence News,* "U.S. Military Goes on Cyber Offensive." March 24, 2012. http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive.

6. Hathaway, Oona, Rebecca Crootof, and Philip Levitz. "The Law of Cyber Attack." *California Law Review,* n._4 (2012), 826. http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf

7. Murchu, Liam. "Stuxnet Using Three Additional Zero-Day Vulnerabilities." Symantec Connect (blog), September 14, 2010. http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities

8. Mearsheimer, John. Conventional Deterrence (Ithaca, New York: Cornell University Press, 1983).

9. Singer, Peter, and Allan Friedman. Armed Forces Journal, "What about deterrence in an era of cyberwar?." http://www.armedforcesjournal.com/what-about-deterrence-in-an-era-of-cyberwar/.

10. RSIS, Effective and Credible Cyber Deterrence, (Singpaore: Centre of Excellence for National Security, 2013). http://www.rsis.edu.sg/cens/PDF/CENS_Cyber_Security_Workshop_Effective_&_Credible_Cyber_Deterrence.pdf

11. Hayley, Christopher. *Georgetown Journal of International Affairs,* "A Theory of Cyber Deterrence." http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/.

12. Ibid.

13. UK Parliment, "2 MoD networks, assets and capabilities." http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/10605.htm.

14. Martin Libicki, *Cyberdeterrence and Cyberwarfare,* (Santa Monica: RAND Corporation, 2009), xvi.

15. Ibid., 73.

16. Rehn, Steven. U.S. Army War College, "Don't Touch My Bits or Else! – Cyber Deterrence." http://handle.dtic.mil/100.2/ADA560247.

17. Patrick Morgan, *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy,* (Washington DC: The National Academies Press, 2010), 55-76.

    RSIS, *Effective and Credible Cyber Deterrence,* (Singapore: Centre of Excellence for National Security, 2013). http://www.rsis.edu.sg/cens/PDF/CENS_Cyber_Security_Workshop_Effective_&_Credible_Cyber_Deterrence.pdf

18. Ibid., 16, 32.

19. Gartner Inc, . Infosecurity Magazine, "Global security spending to hit $86B in 2016." http://www.infosecurity-magazine.com/view/28219/global-security-spending-to-hit-86b-in-2016/.

20. Ibid., 5, 12.

21. Egan, Matt. *Fox Business,* "As Cyber Threats Mount, Business is Booming in the Security World." http://www.foxbusiness.com/technology/2013/03/12/as-cyber-threats-mount-business-is-booming-in-security-world/.

22. Sullivan, Andy. Reuters, "Obama budget makes cybersecurity a growing U.S. priority." http://www.reuters.com/article/2013/04/11/us-usa-fiscal-cybersecurity-idUSBRE93913S20130411.

23. Miller, Greg. Washington Post, "FBI director warns of cyberattacks; other security chiefs say terrorism threat has altered." http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html.

24. Chng, Grace. *The Straits Times,* "Singapore's cyber defence firepower gets $130m boost." http://www.straitstimes.com/breaking-news/singapore/story/singapores-cyber-defence-firepower-gets-130m-boost-20131026.

25. Paget, Francis. McAfee Labs, "Hacking Summit Names Nations With Cyberwarfare Capabilities." http://blogs.mcafee.com/mcafee-labs/hacking-summit-names-nations-with-cyberwarfare-capabilities.

26. Robinson Neil, and Walczak Agnieszka, *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)*, (Santa Monica: RAND Corporation, 2013), 10.

27. Waqaas, . Hackread, "Israeli Think Tank Acknowledges Iran as Major Cyber Power, Iran Claims its 4th Biggest Cyber Army in World." http://hackread.com/iran-biggest-cyber-army-israel/.

28. Alexander, Keith. US Department of Defence, "Statement Of General Keith B. Alexander Commander United States Cyber Command before the House Committee on Armed Services 23 September 2010." http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC Command Posture Statement_HASC_22SEP10_FINAL _OMB Approved_.pdf.

29. Worstall, Tim. *Forbes,* "Stuxnet Was a Joint US/ Israeli Project." http://www.forbes.com/sites/timworstall/2012/06/01/stuxnet-was-a-joint-us-israeli-project/.

30. Markoff, John, and David Sanger. *The New York Times,* "In a Computer Worm, a Possible Biblical Clue." http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?pagewanted=all&_r=0.

31. Lee, Ferran. *ABC News,* "Edward Snowden: U.S., Israel ‘Co-Wrote’ Cyber Super Weapon Stuxnet." Last modified July 09, 2013. Accessed March 3, 2014. http://abcnews.go.com/ blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/.

32. Ashford, Warwick. *Computer Weekly,* "Cyber attack retaliation a bad idea, says international panel." http://www.computerweekly.com/news/2240206279/Cyber-attack-retaliation-a-bad-idea-says-international-panel.

33. Ibid., 16, 43.

34. Ibid., 16, 41.

35. Secunia, "Time to Patch for All Products - *Vulnerability Security Review* (2014) http://secunia.com/vulnerability-review/time_to_patch.html.

36. Libicki, Martin. RAND Corporation, "Brandishing Cyberattack Capabilities." http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR175/RAND_RR175.pdf.

37. Ibid., 27.

38. Ibid., 16, 58.

39. Ibid., 16, 69.

40. Campbell, Matthew. *The Sunday Times,* "'Logic bomb' arms race panics Russia." http://cryptome.org/jya/ru-panic.htm.

41. Ibid., 8.

42. Maher, Heather. RFERL, "New Manual Explains Laws Of Cyberwarfare." http://www.rferl.org/content/new-manual-rules-cyberwarfare/24944686.html.

43. Melzer, Nills. United Nations, "Cyberwarfare and International Law." http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

44. LiveSquare Security, "Cyber Warfare: the good, the bad, the ugly." http://www.arizonatele.com/atic/docs/ATIC_Cyber_Warfare _Presentation_11_17_11.pdf.

45. DorothyDenning,"BarrierstoEntry,"IOJournal(2009),6-10, http://faculty.nps.edu/dedennin/publications/Denning-BarriersToEntry.pdf

46. Weisanthal, Joe. Business Insider, "Notorious Hacker Group LulzSec Just Announced That It's Finished." http://www.businessinsider.com/lulzsec-finished-2011-6?IR=T&.

Kelly, Brian. Boston University Law, "Investing In A Centralized Cybersecurity Infrastructure: Why “Hacktivism” Can And Should Influence Cybersecurity Reform." http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume92n4/documents/KELLY.pdf.

47. Ibid., 46.

48. Ibid., 16, 70.

49. Ibid., 16, 58.

MAJ Lee Hsiang Wei is currently a Senior Policy Officer in the Defence Policy Office, MINDEF HQ. A Helicopter Pilot by vocation, MAJ Lee was previously an operational pilot in 126 SQN. MAJ Lee was a recipient of the SAF Overseas Scholarship in 2004 and graduated from Cornell University with a Masters of Engineering and a Bachelors of Science in Electrical and Computer Engineering. MAJ Lee also won the 2nd prize in the annual Chief of Defence Force Essay Competition in both 2012 and 2014.