Hype or Reality: Putting the Threat of Cyber Attacks in Perspective

by **CPT Lim Ming Liang**

Abstract:

The potential threat of cyber-attacks has been a subject of concern for military and national security. Especially in the United States, cyber threat is deemed as a crucial problem that could compromise the security of a nation and is regarded as 'acts of war'. There have been known cases of attacks against religious corporate and government groups—formed by non-state cyber groups—and this has further escalated the need for cyber security. The essay also highlighted various findings that question the plausibility for cyber-attacks to compromise national security. This essay will address the levels and measures of cyber threats, its limitations and the strategies against it, as well as instances of cyber-attacks that were being used against states. It will also address the extent of the damage cyber threats can bring and the viability of its impact on national security.

Keywords: Military and National Security, Technology, State Secrets, Impact

INTRODUCTION: CYBER ATTACKS IN POLITICAL AND ACADEMIC DISCOURSE

In 2011, the former United States (US) Secretary of Defence warned the American Senate that "the next Pearl Harbour could very well be a cyber-attack."[1] The language, coupled with the speaker's identity and a budget-approving audience bodes of securitisation.[2] It is, however, beyond the object of this essay to scrutinise why politicising the cyber threat is in the interest of the US Department of Defence and its military. Expectedly, America's securitising of the cyber threat has evoked similar fears among various states as national cyber commands begin to emerge in other technologically-advanced countries. At the same time, non-state cyber groups such as Anonymous, which is notable for high-profile hacks and denial-of-service (DOS) attacks against religious, corporate and governmental groups and the Syrian Electronic Army which consists of hackers supporting Syrian President Bashar al-Assad, are also active in cyberspace. Even more worrisome is the Pentagon's announcement in 2011 that it will categorise hostile acts in cyberspace as acts of war and that the US reserves the right to retaliate with all necessary means, including a nuclear response.[3] This landmark discourse has essentially opened the floodgate for militarising and escalating attacks in the cyber domain.

US Navy Cyber Defense Operations Command Monitor

The hype of cyber security in the political arena is supported with analyses from the security studies academia. A group of scholars advance the cyber revolution thesis which claims that cyber-attacks present a perilous threat to states. Most of these works identify cyber-attacks as possible of being independent of traditional military systems, inherent with the problem of attribution which conceals its perpetrators, having an asymmetric nature with low entry of barriers, hence favouring weak states & non-state actors; and imposing a zero-sum paradox on technologically-advanced states as they are concurrently more vulnerable.[4] Others purport that current cyber operations are primarily offence-dominant and that a serious cyber-attack can bring about catastrophic destruction.[5] In sum, the cyber revolution theorists affirm the securitisation of cyberspace and advance that cyber-attacks revolutionalise warfare and impose an unprecedented vulnerability on states.

Against this backdrop, the virtual peril of the cyber domain is palpable. How secure are states in the advent of widespread cyber-attacks and the rise of both state and non-state cyber groups? Do cyber-attacks really threaten our nation's security? This essay seeks to put the threat of cyber-attacks in perspective and provide an objective answer to the question in the following manner. Firstly, it presents an empirical study of recent cyber-attacks to objectively assess their existing trend and risk profile. This takes the form of a risk assessment and bubble chart plot of recent cyber-attacks based on their threat level, likelihood and frequency. Secondly, it conducts a short case study on two significant cases of cyber-attacks to complement the empirical study. Thirdly, it aggregates the findings of the previous two sections to contest the cyber revolution thesis. Finally, this essay also proposes principles for a tenable cyber strategy. In so doing, it will argue that the cyber threat is overrated and that current cyber-attacks do not yet threaten states' security.

At this point, it is useful to specify the definitions of the state and its security for an objective discussion to avoid conflating the concept of security. Max Weber inspired a means-centric understanding of a state that state theorists described as having born of medieval war-making or "war made the state and the state made war."[6] Christopher Pierson added that the state's central activity of war-making is 'turning outwards' to achieve the ends of defending the state's territorial integrity and its monopoly of (legitimate) force for social order within its territory.[7] According to Pierson, these ends are one of the primary goods that the modern state provides for its citizens, requisite among a host of other economic and social goods. Any discussion of security necessitates first, an identification of its referent object and second, the values that the referent object seeks to be free from threat.[8] In this case, the state is the referent object which desires to maintain a "low probability of damage" to its values of territorial integrity and monopoly of legitimate force.[9] These are plausible definitions that policy-makers and scholars in the security arena can identify with.

Herein, any attempt that aims or results in the direct compromise of the state's monopoly of force within its national borders or diminishes its ability to preserve its territorial integrity constitutes a threat to a state's security.

Herein, any attempt that aims or results in the direct compromise of the state's monopoly of force within its national borders or diminishes its ability to preserve its territorial integrity constitutes a threat to a state's security. In this spirit, a foreign cyber-attack that disables or damages a squadron of a state's air force remotely, for example, is considered to have threatened the security of said state as its monopoly of force within its territory has been diminished.

RISK PROFILE OF RECENT CYBER ATTACKS

In the face of a burgeoning discourse on the dangers of cyber-attacks, an empirical study of these attacks presents an objective approach to discern between hype and reality. The Centre for Strategic and International Studies (CSIS) list of "Significant Cyber

	Moderate Risk	Moderate Risk	High Risk	High Risk	High Risk
	Moderate Risk	Moderate Risk	Moderate Risk	High Risk	High Risk
Threat	Low Risk	Low Risk	Moderate Risk	Moderate Risk	High Risk
	Low Risk	Low Risk	Low Risk	Moderate Risk	Moderate Risk
	Low Risk	Low Risk	Low Risk	Low Risk	Moderate Risk
			Likelihood		

Table 1: 5x5 Risk Assessment Matrix

Incidents Since 2006" recorded 153 cases of high profile attacks on government agencies, defence and technology companies as well as economic crimes with losses of more than a million dollars.[10] Of these, 90 out of the 153 incidents targeted government agencies. This study will exclude the other 63 cases of civil and corporate cybercrime and attacks which is consistent with the definition of security proposed earlier.

Methodology

In this study, each of these cases will be coded with a 'threat' and a 'likelihood' score. These factors are functions of a simplified risk equation (Risk = Threat x Likelihood), as other information such as vulnerability is unavailable.[11] This formula produces a risk assessment 5x5 matrix that can reasonably determine risk. *Table 1* shows the matrix that the study uses with each cell colour-coded with red, yellow or green to indicate the respective level of risk – high, moderate or low.[12]

For each of the incidents in the CSIS List, the 'threat' score is ordinally measured on a five-point scale which determines the consequential severity of an attack where a score of 'one' denotes the types of attack with the least impact and a score of 'five' denotes a cyber-war with catastrophic consequences. The five-threat levels and their corresponding type of attack and description are summarised in *Table 2*. 'Likelihood' operationalises the sophistication required and scale of the cyber-attack on a five-point ordinate measure where a score of 'one' denotes a high-technology and high-cost, usually state driven effort while a score of 'five' denotes a low cost and easily

Score / Type of Attacks	Threat Description
1 Disruption	Cyber penetration, or disabling of systems (including denial-of-service attacks)
2 Subversion	Penetration with modifications or vandalism of websites to undermine or challenge authority or society (including hacktivism)
3 Espionage	Penetration for purposes of extracting sensitive or protected information
4 Sabotage	Penetration leading to physical damage, malfunction or destruction of critical systems or infrastructure
5 Cyber War	Loss of lives and infrastructure as a result of cyber attacks

Table 2: Ordinate Measurement for Threat

Score	Likelihood Description
1 Least Likely	When state-directed, invested and highly-sophisticated agencies can launch attacks
2 Less Likely	When state-directed individuals or groups can launch attacks
3 Likely	When skilled and organised non-state actors or groups, with or without state sponsorship can launch attacks
4 More Likely	When skilled non-state actors or individuals with commercially available or open software can launch attacks
5 Most Likely	When civilians with basic computer skills can launch such attacks (i.e. internet URLs on web forums for overloading websites)

Table 3: Ordinate Measurement for Likelihood

perpetrated attack – the level of likelihood increases with its score. The five levels of likelihood and their description are presented in *Table 3.*

Thereafter, these data are transferred onto a table which counts the frequency of each threat-likelihood combination. For example, there were 10 incidents with a 'likelihood' score of two and a 'threat' score of one. This table enables the graphing of the bubble chart with the 'threat', 'likelihood' and 'frequency' variables. 'Threat' and 'likelihood' are plotted on the vertical and horizontal axises respectively, while

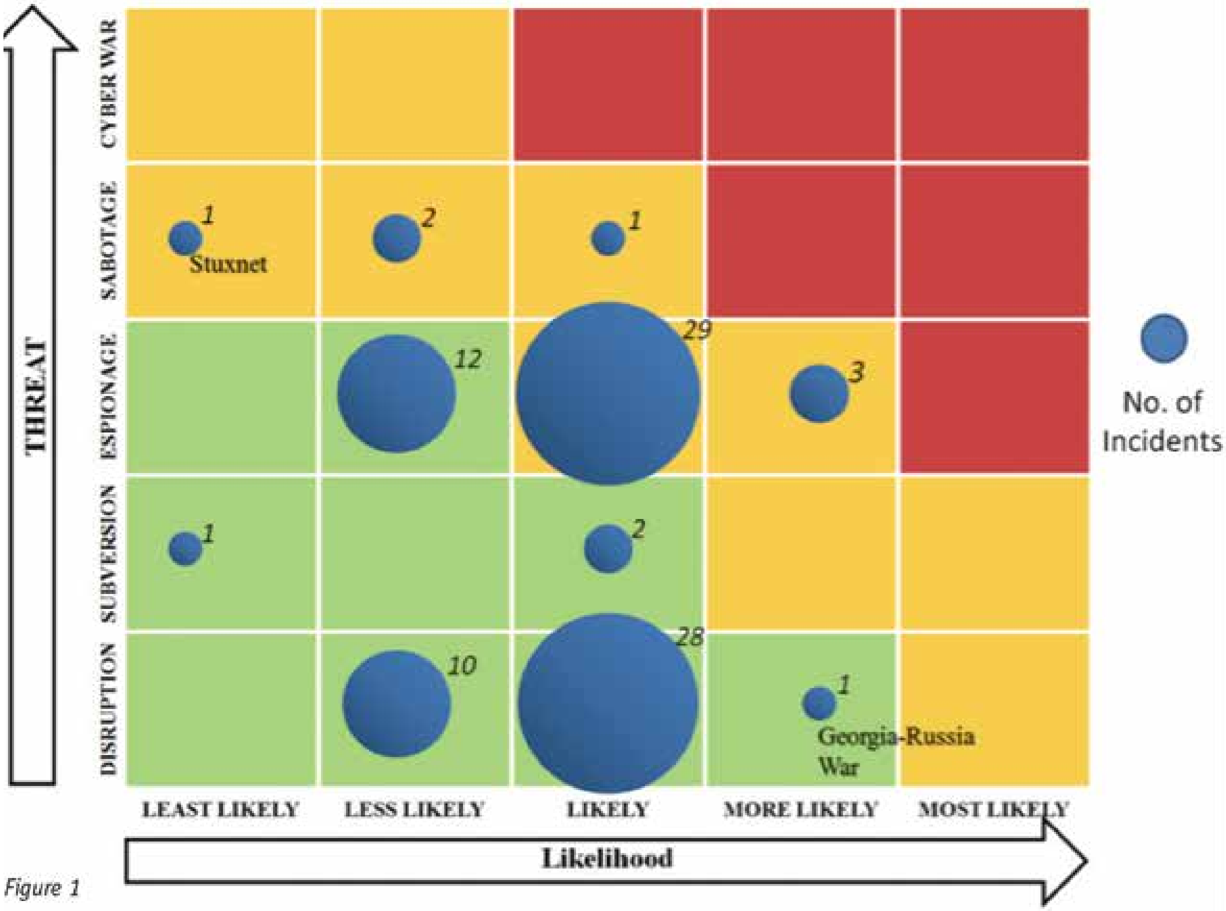

Figure 1

frequency is represented by the size of the bubbles. The bubble chart provides a bird's eye view of the trend of the significant cyber-attacks in recent years and identifies the risk profile of the most prevalent attacks.

Findings

The final chart is set out in *Figure 1* with the frequency listed numerically beside each bubble for convenient reference. By mapping the bubble chart over the risk assessment matrix, several conclusions are clear. Firstly, a majority of the cyber-attacks are low risk incidents, while the rest are in the region of moderate risk. Additionally, there have been no incidents of real cyber war yet. Secondly, skilled and organised non-state or state-sponsored actors mostly conduct espionage and disruption activities which are the most prevalent attacks against states. Thirdly, as attacks become more threatening, they are also less likely to happen as evidenced by the sparse frequency in the top left area of the chart. Finally, and most importantly, current cyber-attacks have not reached the region of high risk where perpetration of attacks is easy and effects are catastrophic at the same time.

Limitations

While these conclusions seem comforting at first sight, there are some limitations to this empirical approach. Firstly, the CSIS list of cyber incidents include only attacks which are deemed 'significant' and is thus, incomprehensive. It provides no clarification on what constitutes significance and there are expectedly numerous other incidents that have been omitted—either because those attacks failed to achieve their objectives or that they were less publicised. Also, states are not inclined to reveal every attack experienced as it may expose their vulnerabilities or impair investigation efforts. Secondly, the difficulty of attributing the perpetrators behind cyber-attacks imposes the difficulty of ascertaining accurately the 'likelihood' scores of the 90 incidents. As a result, several incidents were accorded a 'likelihood' score of three and deemed to be perpetrated by highly-skilled and organised non-state or state-sponsored actors. Nonetheless, this is a reasonable estimate due to the complexity and scale of those attacks. Thirdly, the data measures only incidents and not the number of discrete attacks. Some incidents were composed of several discrete attacks, sometimes amounting to millions of executed attacks such as the hacks against Israeli websites during the 2008-2009 Gaza War. Thus, it is virtually impossible to measure attacks singularly. Furthermore, the various attacks in a specific incident can vary in their threat level, thereby complicating measurement. In such cases, the incident will be accorded a 'threat' score based on its most severe attack. One such incident was the cyber-attacks launched against Georgian government websites during the Georgia-Russia War.[13] In order to circumvent the limitations of the quantitative approach, the next section presents two case studies, each of the most likely and most threatening cyber incidents.

CASE STUDIES: THE GEORGIA-RUSSIA WAR AND STUXNET

This section complements the previous section in assessing the hype of cyber-attacks with analyses from two cases of cyber incidents—the cyber-attacks during the Georgia-Russia War and Stuxnet. These cases were chosen as they each lie on the extreme end of the 'threat' and 'likelihood' spectrum separately. A summary of the significant tenets of these cases will precede an analysis of their lessons.

The Georgia-Russia War

The Georgia-Russia War, against the backdrop of historical geopolitical tensions and other complexities, broke out as a result of Georgia's attack on the Russian-aligned South Ossetian militia. Russia retaliated with an armoured advance, amphibious assault and an intensive artillery bombardment on a Georgian town. In addition, the kinetic assaults were accompanied with a series of cyber operations which in fact, preceded the conventional assaults.[14]

The cyber incidents during the Georgia-Russia War comprised three main types of attacks.[15] The first was a subversion campaign which defaced Georgian government websites—the most prominent vandalism involved collages of the photographs of Adolf Hitler with the Georgian President for Russian propaganda purposes. The second was a series of distributed denial-of-service attacks that brought down several government, media and corporate websites. The third, and most significant operation involved the setting up of an 'Attack Georgia' website which encouraged the Russian public to download tools as rudimentary as PING utility, which are normally used to test the accessibility of IP addresses, to flood the Georgian cyberspace.[16] A cyber campaign of this scale necessitated preparation, reconnaissance and even war-games. Russian intelligence infiltrated Georgian military and government networks three weeks before the ground campaign to scour for information while cyber militia conducted 'probing attacks' against specified targets in preparation for the actual campaign.[17] Interestingly, Russian cyber militias also attacked a Georgian hacker forum—seemingly as a pre-emptive strike to stem the possibility of a Georgian hackers' retaliation.[18] Furthermore, the cyberspace operations appeared coordinated with Russian conventional ground campaign as hackers attacked local Georgian websites in areas where the military planned on shelling.[19] The Georgia-Russia War is significant as it is a first of its kind where a conventional war was 'integrated' with a cyber-campaign with mass participation.

Engineering such a sophisticated and specific weapon like Stuxnet is no mean feat. Reconnaissance is necessary to map out the target facility's networks and configuration. Intensive technological, programming and engineering prowess are required to design the malware's propagating ability and adaptability.

Stuxnet

The second case study was another game changer as it was the first instance where a cyber-attack resulted in physical destruction.[20] Stuxnet was a highly sophisticated malicious software that was planted in the network of an Iranian nuclear facility in Natanz and designed to gradually deteriorate centrifuges used for uranium enrichment. Natanz functioned on a Microsoft Windows operating system and a Siemens Industrial Control System, but had an 'air gap' which meant that its computers were not connected to the internet.[21] Most likely, Stuxnet had to be inserted into the networks by an unsuspecting staff with an infected thumb drive. Once inserted, Stuxnet was like a living worm. It can propagate and adapt itself in the network; changing its characteristics to avoid detection by antivirus software and firewalls; replicating itself till it identifies the Programmable Logic Controller (PLC) that controls the centrifuges; as well as sending situation reports to its control servers.[22] Stuxnet was to lie dormant until it identifies a PLC connected to a frequency converter that runs the motors of the centrifuges. Thereafter, Stuxnet will begin a sequence to inject a payload designed to disrupt the frequencies of the motors to damage the centrifuges slowly.[23] Meanwhile, the malware is capable of sending deceptive feedback to the human operators to give the impression that the centrifuges were still functioning normally. Nevertheless, the Iranians eventually reached out to open-source security researchers and neutralised Stuxnet. The software vulnerabilities that Stuxnet exploited were quickly patched by Microsoft and Siemens.[24] In the end, Stuxnet only managed to delay Iranian centrifuge programme by a year.[25]

Engineering such a sophisticated and specific weapon like Stuxnet is no mean feat. Reconnaissance is necessary to map out the target facility's networks and configuration. Intensive technological, programming and engineering prowess are required to design the malware's propagating ability and adaptability. Extensive financing is necessary to obtain testing equipment, similar centrifuges and a mock facility for trials and rehearsals. Finally, intelligence networks are

An example of the Siemens Simatic S7-300 PLC CPU that was infected by Stuxnet.

required to plant the malware into the target network. These resources indicate a strong state's involvement. Allegedly, the US National Security Agency and an Israeli intelligence group known as 8200 collaborated to design Stuxnet since the Bush administration.[26] Together, Stuxnet and the cyber incidents in the Georgia-Russia War provide new perspectives on the threat of cyber-attacks against states.

Contesting the Half-Truths of Cyber Attacks

The cyber revolution thesis and political discourse seems to purport that cyber threats can severely threaten nations' security. While there are merits to and advantages of that perspective, it is necessary to balance its half-truths with objective and evidence-based analyses to avoid spiralling threat conflation. The research in this essay suggests that as yet, the threat of cyber-attacks to states is overrated.

One of the tenets of the cyber revolution thesis asserts that cyber-attacks can take place independently of traditional military systems. While this is possible, my findings suggest that attacks that take place solely in the cyber domain may only marginally compromise a state's monopoly of legitimate force at best, but are unable to infringe upon a state's territorial integrity. The case of the Russia-Georgia War demonstrates the importance of 'boots-on-the-ground' to overpower the opponents' militaries and occupy territories. While the accompanying cyber campaign was impressive, they were nothing but cyber vandalism and a nuisance. Stuxnet demonstrates the case of a standalone cyber-attack which damaged physical infrastructure—a case of an arguably significant threat to a state. Yet, for a highly invested and sophisticated cyber weapon to only achieve a limited effect of destroying 11.5% of the 8,500 Iranian centrifuges, barely above the centrifuges' typical breakdown rate, this more than adequately proved that cyber-attacks independent of traditional military systems can only marginally compromise a state's monopoly of violence.[27]

Perhaps the most accepted claim of the cyber revolution thesis is the difficulty of attribution and the anonymity of cyber-attacks. While I concur with the claim, attribution is not entirely impossible. In fact, most cyber-attacks remain anonymous because they are 'an inconsequential nuisance' that do not warrant a full-scale investigation.[28] On the other hand, most incidents with a 'threat' score of four on the bubble chart can be attributed. The circumstantial evidence of Stuxnet for example, inadvertently points to possible US and Israeli collaboration. Additionally, anonymity can be a burden for its perpetrators. Actors intending to initiate cyber-attacks must undertake considerable measures to maintain anonymity. As the complexity and intended threat of an attack increases, the risk of attribution increases consequently as states are also more likely to investigate incidents of greater significance.

Another claim advances the asymmetric nature of cyber-attacks and its low entry barriers which facilitate its exploitation by non-state actors or weak states. As the Stuxnet case study demonstrates, cyber-attacks on the higher end of the 'threat' spectrum are contrary to the asymmetric claim. Effective cyber weapons are costly and impose high technology barriers beyond the reach of non-state actors such as terrorist groups. Furthermore, they often do not guarantee success and are surgical and 'one-shot' in nature. Hence, it is more rational for non-state actors to resort to conventional tactics with higher rates of success at much lower costs.

Cyber-attacks are also cited as inherent with a zero-sum paradox where technologically advanced states are empowered and vulnerable at the same time. The findings in this essay however, demonstrate that the paradox is exaggerated. As the bubble chart shows, disruption and espionage are the most prevalent cyber-attacks to plague the most technologically advanced states; but they do not threaten the state's territorial integrity and monopoly of legitimate force. Furthermore, vulnerability in cyberspace is less severe than in the physical domain. Stuxnet shows that disruption or damages as a result of cyber-attacks can be quickly recovered or replaced, unlike the irreversible destruction that kinetic force inflicts.

In the long run, cyber offence cannot keep up with defence as defenders learn the modus operandi of cyber-attacks.

Cyber revolution theorists also highlight that cyberspace is primarily offence-dominant but my findings suggest that defence will be increasingly easier. Firstly, while cyber disruption and espionage are relatively easier to conduct, cyber operations with physical offensive implications such as sabotages are still few and costly. Yet, while strong states can reasonably afford to produce costly and complex cyber weapons for offensive purposes, the costs of defence and recovery for the defending state is significantly lower.[29] Stuxnet for example, had enthusiastic technological corporations rushing to patch and neutralise on behalf of their Iranian clients. Additionally, the codes of several malicious cyber weapons, including Conficker and Stuxnet, are presently available on the internet along with instructions for repair and recovery. In the long run, cyber offence cannot keep up with defence as defenders learn the modus operandi of cyber-attacks.[30]

Most alarmingly, the academic and political discourse is interspersed with claims that cyber threat is catastrophic. As yet, the bubble chart shows that current cyber incidents have not reached the region of high risk and are unable to inflict widespread infrastructural damages and civilian casualties. If Stuxnet can be benchmarked as the most threatening cyber weapon currently, it would take astronomical investments and massive collaboration to wage an entire cyber war capable of deposing a sovereign state's monopoly of force. Intuitively however, conventional military forces are still necessary to breach its territorial integrity and occupy territories. Of course, this is a purely deductive conjecture as cyber-attacks may still be in their infancy.

DEFENCE AS A TENABLE CYBER STRATEGY?

The findings in this essay provide some principles for a tenable cyber strategy. The bubble chart and risk assessment reveal disruption and espionage activities as the most prevalent attacks. While the case studies suggest that disruption activities are merely cyber nuisance, espionage is an already prevalent phenomenon that is merely facilitated by the cyber domain but definitely falls short of revolutionary. Additionally, recovery and defence is faster and more cost-effective than offensive tactics in the absence of catastrophic cyber war which, as evidenced by Stuxnet, would require astronomical cost and effort with no guarantee of success. Without conventional military force, cyber-attacks are unable to effectively diminish a state's monopoly of force or compromise its territorial integrity. Therefore, a tenable cyber strategy in the near term should primarily be defence-oriented. Firstly, the establishment of rapid recovery capabilities can minimise the impact of disruption and subversion activities, while attribution capabilities can potentially deter aggressors. Next, deceptive counter-intelligence and management discipline of human operators—the weakest link in the entire cyber infrastructure—can mitigate cyber espionage. Last but not least, reconnaissance and other intelligence activities are useful for early warnings as both Stuxnet and the Georgia-Russia War demonstrated that rehearsals do take place before major cyber-attacks.

CONCLUSION

This essay has demonstrated that the hype asserting that cyber-attacks threaten the security of states is overrated. The empirical study of recent cyber-attacks show that the risk profile of these attacks are in the region of low to moderate risk—mostly disruption and espionage activities—and that no incidents of cyber war has occurred. The case studies countered the claims of the cyber revolution thesis and showed that they mostly portray half-truths. While the cyber domain indeed presents new challenges and difficulties for the security of states, in reality cyber-attacks do not yet possess the capacity to effectively depose a state's monopoly of force or infringe on its territorial integrity. Feeding the hype and frenzy of catastrophic cyber-attacks will engender unnecessary fears and perceived vulnerabilities, leading to greater militarisation of cyberspace and ironically, increased and perhaps irrational insecurity. In this vein, a defensive cyber strategy focused on recovery and attribution capabilities, counter-intelligence and personnel discipline and reconnaissance is rational and tenable in the short term.

BIBLIOGRAPHY

Adams, J. "Virtual Defence." *Foreign Affairs,* 80(3), (2001).

Albright, D., Brannan, P., and Walrond, A. C. "Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant?" *Institute for Science and International Security* (2010).

Baldwin, D. A. The Concept of Security. Review of International Studies, (1997), 5-26.

Buzan B., Wæver, Ole, and Wilde, Jaap De. Security: A New Framework for Analysis (Boulder: Lynne Rienner Publishers, 1998).

Cox, L.A. "What's Wrong with Risk Matrices." *Risk Analysis* 28, n._2 (2008), 497-512. Data Exchange Agency. "Cyber Attacks Against Georgia." *Ministry of Justice of Georgia,* 2011.

Haddick R. "This Week at War; Lessons from Cyber War 1." *Foreign Policy,* 2011. http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i.

Hollis, D. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal,* (2011).

Keizer, G. "Russian Hacker 'Militia' Mobilises to Attack Georgia." Computer World, accessed November, 2013. http://www.computerworld.com/s/article/9112443/Russian_hacker_militia_to_attack_Georgia

Krepenevich, A. F. Cyber Warfare: A "Nuclear Option"? *Centre for Strategic and Budgetary Assessments,* 2002.

Lindsay, J. R. "Stuxnet and the Limits of Cyber Warfare," *Security Studies,* (2013).

MITRE. *Risk Management Tools.* http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-management-tools

Panetta, L. "CIA Chief Leon Panetta: Cyber Attack Could is 'Next Pearl Harbour'." *Huffington Post,* June, 2011. http://www.huffingtonpost.com/2011/06/13/panetta-cyberattack-next-pearl-harbor_n_875889.html.

Pierson, C. The Modern State (London: Routledge), 1996.

Rid, T. "Cyber War Will Not Take Place." *The Journal of Strategic Studies* 35, n._1, (2012), 5-32.

Sanger, D. E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (New York: Crown), 2012.

Schreier, F. "On Cyberwarfare." *DCAF Horizon 2015 Working Paper No. 7,* n.d.

Shimeall, T., Williams, P., and Dunlevy, C. "Countering Cyber War." *NATO Review 49,* n._4, (2001): 16-18.

Tabansky, L. "Basic Concepts in Cyber Warfare." *Military and Strategic Affairs* 3, n._1 (2011): 75-92.

Tilly, C. The Formation of National States in Western Europe (Princeton: Princeton University Press), 1975.

L. Valeri, and M. Knights. "Affecting Trust: Terrorism, Internet and Offensive Information Warfare." *Terrorism and Political Violence* 12, n._1 (2000), 15-36.

Wall Street Journal. "Cyber Combat: Act of War," May 21, 2011. http://online.wsj.com/news/articles/SB10001424052702304563104576355623135782718.

Weber, M. "Politics as a Vocation". in H. H. Garth, and C.W. Mills. *Essays in Sociology.* (New York: Macmillian, 1946), 26-45.

Wolfers, A. "'National Security' as an Ambiguous Symbol." *Political Science Quarterly* 67, n._4 (1952), 481-582.

ENDNOTES

1. Panetta, Leon. *Cyber Attack Could be 'Next Pearl Harbour'*. Huffington Post, June 2011. http://www.huffingtonpost.com/2011/06/13/panetta-cyberattack-next-pearl-harbor_n_875889.html.

2. Barry Buzan, Ole Wæver, and Jaap De Wilde, *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998.

3. Wall Street Journal, *Cyber Combat: Act of War,* May 2011. http://online.wsj.com/news/articles/SB1000142405270230456310457635562313578 2718.

4. L. Tabansky, *Basic Concepts in Cyber Warfare,* Military and Strategic Affairs 3, n._1, 2011; F. Schreier, *On Cyberwarfare,* DCAF Horizon 2015 Working Paper No. 7, n.d.

5. Schreier, *On Cyberwarfare;* A. F. Krepenevich, *Cyber Warfare: A "Nuclear Option"?* Centre for Strategic and Budgetary Assessments, 2002.

6. M. Weber, *Politics as a Vocation,* in H. H. Garth, and C.W. Mills, *Essays in Sociology,* (New York: Macmillian), 26-45;

7. C. Pierson, *The Modern State,* (London: Routledge, 1996).

8. B. Buzan, *People, States and Fear: The National Security Problem in International Relations,* (North Carolina: University of North Carolina Press, 1983).

9. D. A. Baldwin, "The Concept of Security", *Review of International Studies* (1997), 13.

10. Centre for Strategic and International Studies, *Significant Cyber Incidents Since 2006,* accessed November, 2013. The list is a work in progress subjected to regular updates by the CSIS and the data used in this essay is correct as of the accessed date.

11. L. A. Cox, "What's Wrong with Risk Matrices," *Risk Analyses* 28, n._2 (2008). While risk assessment matrices vary according to organisations and contexts, the threat and likelihood matrix is a widely used tool in organisations such as the American Federal Aviation Administration among other applications such as for terrorism risk analyses, climate change risk management and military safety and risk management.

12. MITRE, *Risk Management Tools* http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-management-tools.

13. T. Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, n._ 1 (2012), 13.

14. D. Hollis, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal* (2011).

15. T Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, n._ 1 (2012).

16. Data Exchange Agency, *Cyber Attacks Against Georgia,* Ministry of Justice of Georgia, 2011, 11.

17. R. Haddick, "This Week at War; Lessons from Cyber War 1,"Foreign Policy, 2011, http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i; Hollis, "Cyberwar Case Study".

18. G. Keizer, *Russian Hacker 'Militia' Mobilises to Attack Georgia,* Computer World, November, 2013. http://www.computerworld.com/s/article/9112443/Russian_hacker_militia_mobilizes_to_attack_Georgia.

19. D. Hollis, "Cyberwar Case Study: Georgia 2008." *Small Wars Journal,* (2011).

20. J. R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies* (2013).

21. T. Rid, *Cyber War Will Not Take Place,* The Journal of Strategic Studies 35, n._ 1 (2012), 18.

22. J. R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies* (2013), 382.

23. Ibid., 384.

24. Ibid., 394.

25. Ibid., 390.

26. D. E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power,* New York: Crown, 2012.

27. D. Albright, P. Brannan, and A. C. Walrond, *Did Stuxnet Take out 1000 Centrifuges at the Natanz Enrichment Plant?,* Institute for Science and International Security, 2010.

28. J. R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies* (2013), 401.

29. Ibid.

30. T. Shimeall, P. Williams, and C. Dunlevy,"Countering Cyber War", *NATO Review* 49, No. 4, 2001.

CPT Lim Ming Liang is an Armour Infantry Officer by vocation and is currently a Staff Officer in HQ Armour. He received the SAF Academic Scholarship and graduated from the National University of Singapore with a Bachelors of Social Sciences (Honours) in Political Science.