Cyber Attacks and the Roles the Military Can Play to Support the National Cyber Security Efforts

by ME5 Alan Ho Wei Seng

Abstract:

The advent of low cost computing devices and fast access to the Internet has brought forth great convenience to everyday life, but there are also many cyber threats lurking in cyberspace, waiting to exploit system or network vulnerabilities so as to compromise their integrity, availability, and confidentiality. On a national level, cyber attacks can exploit the vulnerabilities of critical infrastructures such as the energy, transportation and communications sectors and seriously undermine military mission success, since the infrastructures are critical in supporting the conduct of military operations. Therefore, there is vested interest for the military to partner with other defence agencies, private sectors and possibly international players to enable a 'whole-of-nation' effort to develop comprehensive cyber security measures in order to mitigate the impact of cyber attacks. This is essential as cyberspace may eventually be commonly accepted as a military domain of conflict.

Keywords: Internet; Cyber Attacks; Compromise; Exploit Vulnerabilities; Vested Interest

INTRODUCTION

> *"We have to consider (cyber security threats) every bit as foundational as we do in our ability to manoeuvre forces as a military construct."*
>
> *- US Navy Admiral Michael S. Rogers*
> *Commander of US Cyber Command*
> *Director of the National Security Agency*
> *Chief of the Central Security Service*[1]

In this Information Age, the technological advancements of the Internet have enabled information to be more accessible to much of the world population, and at an increasing speed.[2] Based on data retrieved from 'Worldometers', the world population stands at 7.2 billion as of end 2014, of which 3 billion or close to 50% of the populace have access to the Internet.[3] As Internet usage continues to expand, cyberspace, which is the national environment that communication over computer networks occurs, will become increasingly woven into the fabric of everyday life across the globe.[4] Hopping onto the cyberspace bandwagon, militaries around the world, like the United States (US), have harnessed onto the good prospects offered to better conduct its operations: logistical support and global command and control of forces, real-time provision of intelligence, and remote operations.[5]

However, we need to be cognisant of this reliance on cyberspace as there are many system or network vulnerabilities, which are weaknesses that allow an attacker to compromise the integrity, availability and confidentiality of the system or network used.[6] Cyber attacks can exploit these vulnerabilities and penetrate the computers or networks of a user, company or even nation, for the purpose of causing damage or disruption.[7] One recent cyber attack incident was what US President Barack Obama termed as an act of 'cyber vandalism': in December 2014, Sony Pictures broadcasted a movie depicting the assassination of the North Korean leader, Kim Jong-un.[8] On a national level, cyber attacks on critical infrastructures such as the energy, transportation and communications sectors could seriously undermine military mission success since the infrastructures are critical in supporting the conduct of military operations.

FROM THE WESTERN CAPITALIST PIGS WHO BROUGHT
NEIGHBOURS AND THIS IS THE END
SETH ROGEN
JAMES FRANCO
이 무식한 미국놈들을 믿지 마십시
THE
INTERVIEW
인터뷰

Wikipedia

Movie poster of 'The Interview', which depicted the assassination of North Korean Leader, Kim Jong-un.

Therefore, there is vested interest for the military to participate in the national effort to develop comprehensive cyber security measures, which could include the legislation of governing policies, implementation of cyber security tools and best practices, as well as the training of appropriate cyber security experts to better safeguard the organisation and user's assets.[9] The importance of cyber security was echoed in the private sectors through an Information Assurance (IA) survey conducted in 2014, of which 75% of respondents named cyber security and privacy as primary concerns.[10] In Singapore, the government is stepping up efforts to strengthen the nation's resilience towards cyber attacks. In order to complement the existing national cyber security efforts, it was reported in 2014 that a new Cyber Security Research Centre will be set up to study and develop capabilities in cyber forensics and mobile security.[11] For the Singapore Armed Forces (SAF), it was reported in 2013 that a new hub has been set up to consolidate its cyber security experts to monitor cyber threats round the clock and muster a sharper response to thwart cyber attacks and digital spies.[12] Cyber security is also gaining traction academically. For example, Nanyang Polytechnic has collaborated with the Centre for Strategic Infocomm Technologies (CSIT) to offer bond-free scholarships to qualified students who enroll into their Diploma in Cyber Security and Forensics.[13]

In summary, this essay looks at the attributes and techniques employed in cyber attacks. It also articulates the impact of cyber attacks on the military, and roles the military can play to support the national cyber security efforts in mitigating the impact of cyber attacks so as to safeguard the nation's cyber well-being.

ATTRIBUTES OF CYBER ATTACK

Cyber Attacks are Asymmetric

With the advent of low cost computing devices, cyber attackers can exert an adverse impact disproportionate to their size. They do not require sophisticated weaponry, and neither do they have to build expensive platforms such as stealth fighters or aircraft carriers, in order to compromise the network of interest and pose a significant threat.[14] Besides state actors, there are concerns that terrorists or organised criminal groups could stage cyber attacks that leverage on the low capital outlay required. For instance, it was reported in 2009 that Iraqi insurgents had utilised software available for only US$26 to hack into video imagery relayed by a US drone aircraft, thus allowing them to see what the US military was seeing.[15]

Offense has the Advantage and Speed

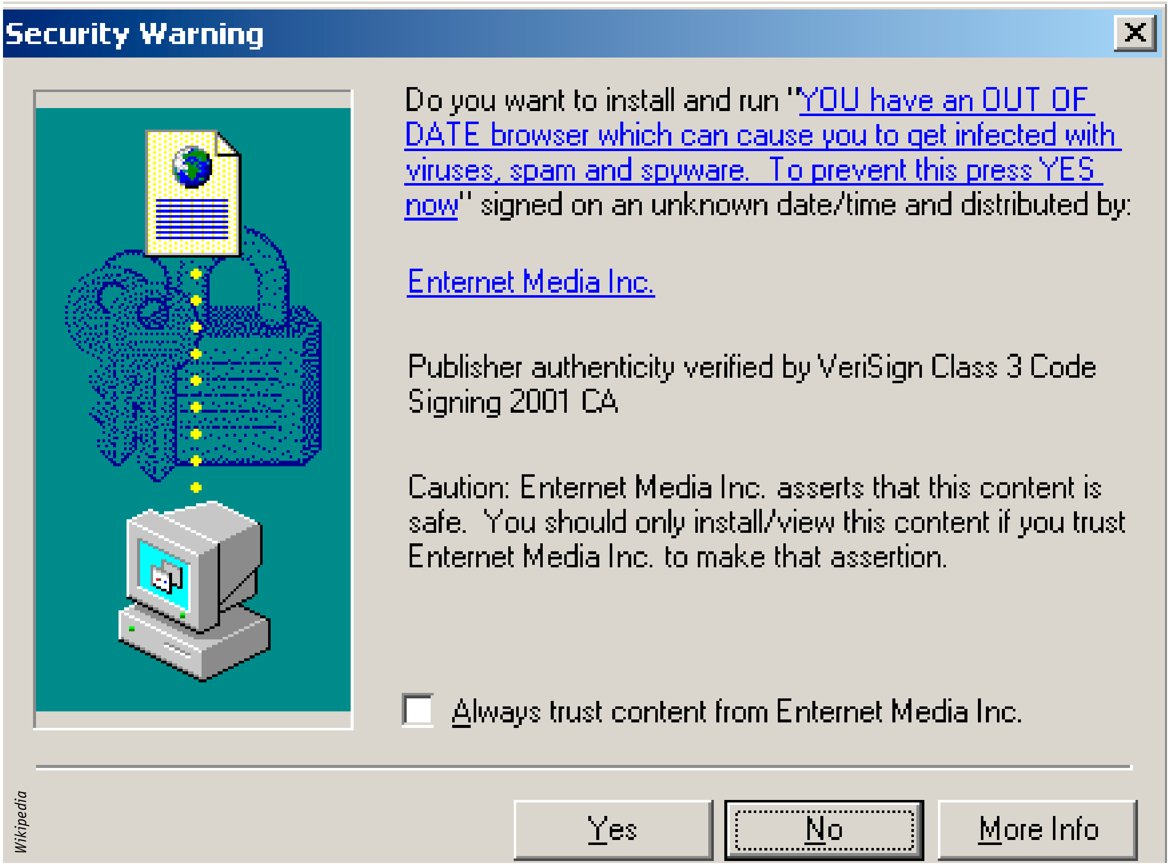
Cyber attacks are like manoeuvring forces where speed and agility matter most, and offense can have the upper hand in an instance. A fortress mentality will not work in an offense-dominant cyberspace environment since there is little to retreat to behind a Maginot Line of firewalls or the user will risk being overrun.[16] Offense has the advantage over defence because the defender must contend with millions of lines of codes, while the attacker only has to find a single vulnerability to quickly destabilise the situation, which is possible to unfold in a few minutes. This is as opposed to conventional warfare, where it would take from, at the very least, minutes to a few hours to carry out, as missiles are fired at targets or aircraft, tanks, and ships are sent into battle.

The ability of cyber attacks to reach the desired targets without the need for mass deployment of troops, delivery vehicles or weapons, or foreign bases, coupled with its sheer velocity represents a new dimension to warfare that could dramatically increase the need for immediate and possibly risky decision-making by governments under attack.[17] Former US Secretary of Defense Leon Panetta previously commented on the reaction of US to cyber attack, that "the US may consider preemptive strikes if it detects imminent threat of an attack that will cause a significant physical destruction in the US or kill American citizens."[18] To stay ahead, it is imperative to constantly adjust and improve cyber security measures.

With the advent of low cost computing devices, cyber attackers can exert an adverse impact disproportionate to their size. They do not require sophisticated weaponry, and neither do they have to build expensive platforms such as stealth fighters or aircraft carriers, in order to compromise the network of interest and pose a significant threat.

Difficult to Detect and Attribute

It is hard to deter if you cannot punish, and you cannot punish without first knowing who is behind an attack. For the military, the traditional deterrence model of assured retaliation when attacked will be difficult to execute in cyberspace because it will be challenging to identify the ownership of an attack accurately.[19] This is because a missile will likely come with a distinct signature, but the same cannot be said for a computer virus if the digital footprints are well-covered. Furthermore, the preparations for cyber attack are far less visible than that for conventional warfare. For the latter, preparations are usually evident through a military build-up and mobilisation order which are easily detectable, but there are no visible signs of preparations when it comes to cyber attacks.[20] Even so, if there was a heavily masked attack employing dynamic proxies and routing that spans across many countries where jurisdiction over cyber security could differ or be lacking, it could potentially compound the inability to attribute an attack swiftly, let alone obtaining its intent.



Security Warning

Do you want to install and run "YOU have an OUT OF DATE browser which can cause you to get infected with viruses, spam and spyware. To prevent this press YES now" signed on an unknown date/time and distributed by:

Enternet Media Inc.

Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA

Caution: Enternet Media Inc. asserts that this content is safe. You should only install/view this content if you trust Enternet Media Inc. to make that assertion.

□ Always trust content from Enternet Media Inc.

Wikipedia

A malicious website trying to install spyware on readers' computers in the past. The technology to do so today is much more sophisticated.

Even in a fortunate case whereby an attack could be attributed to the attacker, if it is a non-state actor, such as a terrorist group, it may not have any assets against which the nation can retaliate. To gain easier access and evade detection, attackers can also target defense contractors and subcontractors, whose networks tend to be less secured than the military which they are supporting.[21] These attacks often rely on socially engineered emails, or 'spear phishing', which are made to look authentic to the recipient, and when opened will install a remote-access tool for the attacker.[22] This heightens the necessity to protect the computer network of defence contractors and subcontractors, indirectly offering better protection for the military which they are supporting. One way to mitigate this could be to ensure that the attacks are fruitless by developing resilient systems that are able to withstand serious technical compromises and adapt to changing their Standard Operating Procedures (SOPs) when required, instead of investing resources to find the source to inflict a direct penalty on the attackers, which could potentially be a dead-end.[23]

TECHNIQUES OF CYBER ATTACK AND THEIR IMPACT TO THE MILITARY

Underpinned by the wealth of information available on cyberspace and low cost computing devices, cyber attackers are becoming more tech-savvy and able to launch sophisticated intrusions into the networks that control the national infrastructures. One such intrusion is the Distributed Denial of Service (DDOS) that floods the systems (of

Cyberwar Defense team of the US Air Force monitoring cyber threats at a workstation.

the national infrastructures) with multiple requests, more than they could respond to and paralysing them consequently. DDOS is usually executed by 'botnets' comprising networks of computers that have been hijacked by remote users, often without the owner's knowledge.[24] Other than networks, software and hardware are also at risk of being tampered with even before they are linked together in an operational system. 'Logic bombs' are rogue software programming codes that can cause sudden malfunctions when developed, while hardware can have 'kill switches' and hidden 'back doors' written into the computer chips that allow remote-access by unintended users.[25] Computer-induced failures of national infrastructures could cause massive physical damage and economic disruption. The military strength of a nation ultimately depends on her economic vitality, so cyber vulnerabilities could erode both the nation's military effectiveness and its competitiveness in the global economy, if the attacks are pervasive and persistent.

Cyber security is a discipline that requires national effort, and it is not something that the citizens and private companies can expect to outsource to the military.

On the impact of cyber attacks to the military, the exploitation of vulnerabilities in military cyber systems could result in weapons blueprint, operational plans and surveillance data being compromised, which could seriously undermine national security. For instance, a rogue programme that was introduced by an infected flash drive inserted into a US military laptop at a Middle East base was able to gain access to information within networks operated by the US Central Command.[26] Cyber attack techniques that can infiltrate military systems can be made stealthy to ensure that rogue programmes, when introduced, remain undetected. They could establish a digital 'beachhead' from which these programmes operate silently to stealthily exfiltrate sensitive military operational plans to unintended servers under foreign control. Noting the gravity of a cyber attack, the US has asserted the belief that such an attack could be regarded as an act of war, and that the US could respond using traditional military force.[27]

THE ROLES THE MILITARY CAN PLAY TO SUPPORT THE NATIONAL CYBER SECURITY EFFORTS

Cyber security is a discipline that requires national effort, and it is not something that the citizens and private companies can expect to outsource to the military. Any nation that depends heavily on the military for cyber security will reduce the incentives for the private sector, especially Multinational Corporations (MNCs) who possess adequate resources for the necessary Research and Development (R&D), to develop cyber wellness provision.[28] Furthermore, few private sectors are likely to welcome hands-on assistance from the military since the former would be better poised to defend their own networks, business data privacy concerns aside.[29]

Therefore, a partnership is one position which the military can consider—collaborating with other government departments/agencies, and the private sector (including defence contractors) to enable a 'whole-of-nation' cyber security strategy, albeit there is still the lingering question for a neat way to rationally and effectively divide the national cyber security responsibilities between the military, and the rest.[30] The following are four initiatives in which the military can play such supportive roles, collectively working as a team with other defence agencies, private sectors and possibly international players.

Cyber Security Governance and Practices

The teams can collaborate and enact policies to govern cyber security through standardising operating procedures in cyberspace so as to better protect classified networks which could house sensitive information and enable crucial war-fighting, diplomatic, counter terrorism, law enforcement, intelligence and homeland security operations. The sharing of best practices for cyber security amongst the team members can provide operational norms to deal with cyber threats and incident responses, especially those that could cause exceptionally grave damage to the national security. The developed cyber security governance and practices must be enduring against the fast-paced cyberspace, and aimed at building an approach to cyber defence strategy that deter interference and attack in cyberspace. The cyber defence strategy can be further enhanced by improving warning capabilities, articulating roles for private sector and international players, and developing appropriate responses for both state and non-state actors.[31]

Since the nation depends on a variety of privately owned and operated critical infrastructures to carry out the public's businesses, the team can help define its role by advocating and extending cyber security governance and practices into the critical infrastructures domains. In the US, there is existing and ongoing partnership between the Federal Government, the public and private sector owners and operators of Critical Infrastructure and Key Resources (CIKR) in addressing security and information assurance efforts across the cyber infrastructure to increase resiliency and operational capabilities.[32] It also includes a focus on public-private sharing of information regarding cyber threats and incidents in both government and CIKR.[33]

Cyber Threat Research and Warning

It is essential to know the current state of play in cyber threats in order to develop appropriate cyber security governance and policies to address them. Similar to mapping the threat landscape of a military adversary, the team can collaborate in researching emerging cyber threats and developing measures/technologies to forewarn imminent cyber attacks. This involves mapping the entire cyber landscape that the nation is operating in, establishing a healthy baseline of cyber well-being, and determining the threshold in which, when that baseline is crossed, it could indicate a possible cyber attack. In addition, the team can research and provide an understanding to the relationship between recovery time and value of a cyber attack, assuming an attacker is less motivated to take down a network, if the victim can quickly restore it to operation.[34]

Also, against the fast-paced cyber threat landscape, it is imperative for cyber security experts to keep abreast of the adversary, if not at least staying alongside, through continuous learning and regular currency checks, to help shape an open, vibrant and stable cyberspace, which the public can use safely.

The cyber threat research is contingent on a robust relationship with internal defence agencies, private sectors and also international players to share intelligence on threat signatures/actors, analytic and collaborative technologies in order to maximise the advantage of each organisation's unique capabilities and provide timely and accurate assessments to support the nation's decision makers. For instance, the National Cyber Security Center (NCSC) within the Department of Homeland Security plays a key role in securing US Government networks and systems by co-ordinating and integrating information from all relevant agencies to provide cross-domain situational awareness, analysing and reporting on the state of US networks and systems, and fostering inter-agency collaboration and coordination.[35] It is unlikely for a single entity to be aware of the overall nation's cyber security efforts, so the team can also help to co-ordinate the nation's R&D in cyber security and redirect efforts to where they are needed. This initiative is critical in eliminating redundancies, identifying research gaps and prioritising R&D efforts, in order to justify the usage of public money in strengthening the nation's cyber well-being.

Cyber Security Measures and Implementation

In the military, war gaming is rudimentary in developing nascent operation concepts and processes, since they can be clinically tested without massive resources, as compared to the actual maneuvering of forces. One possible cyber security measure and implementation is in developing a Cyber Range/Simulation system to enable the development and testing of cyber tools, best practices, policies for robustness in core system architecture. This could force the redesign or retrofit of hardware, Operating System (OS), and computer languages with cyber security in mind, and the same set of consideration should also be extended to the systems of defence contractors to build unified cyber security architectures.[36] The military could lend their war gaming experiences and facilities to simulate how technical systems might respond to various attacks and provocations, how cyber attacks could escalate out of control, and lastly, which games of co-operation might best thwart attacks.[37] All these can be done within the safe confines of the war gaming centres.

One such facility is the National Cyber Range that was developed by the US Department of Defense (DOD) in 2012 to allow co-operation with other US government agencies, and potentially non-US government partners to rapidly create numerous models of network, intended to enable the military and others to simulate cyberspace operations and test new technologies and capabilities, promoting collaboration and critical info sharing, in support of the 'whole-of-nation' effort.[38] One possible simulation could be studying the 'lethal radius' of a cyber weapon. Every bomb has a 'lethal radius', and any given target that lies outside of said radius is likely to be unharmed. This knowledge can help military planners minimise collateral damage. What, if any, is the cyber analogy of 'lethal radius' for cyber attacks?[39]

In addition, the team could consider developing a unified Intrusion Detection System (IDS) harnessing sensor across the military, the other defence agencies, and private sectors. In the US, the IDS called upon 'EINSTEIN 2', which uses passive and signature-based sensors from a vital part of the US Government network defences to identify when unauthorised users attempt to gain access to those networks. It also inspects Internet traffic entering Federal systems for unauthorised accesses and malicious content as well.[40] Most importantly, 'EINSTEIN 2' is capable of alerting the United States Computer Emergency and Readiness Team (US-CERT) in real-time to the presence of malicious or potentially harmful activity in federal network traffic and provides correlation and visualisation of the derived data. Consequently, due to the capabilities of 'EINSTEIN 2', US-CERT analysts have a greatly improved understanding of the network environment and an increased ability to address the weaknesses and vulnerabilities in Federal network security, enhancing overall situation awareness. There are plans to develop the next generation system, dubbed the 'EINSTEIN 3', that will draw on commercial and government technologies to conduct real-time, deep packet inspection and threat-based decision-making on network traffic entering or leaving key networks, with the goal of identifying and characterising malicious network traffic so as to enhance cyber security analysis, situation awareness and security response.[41]

Cyber Security Training and Awareness

With massive capital invested on new technologies to secure the cyberspace, it is the people with the right knowledge and skills to implement those technologies that will make the difference and achieve mission success. The team can propose options to invest in human capital and collaborate with leading institutions that specialise in cyber security related fields to develop courses to train a cadre of cyber security experts to tackle the increasing cyber threat landscape. The US Federal Government aims to develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees, which will adopt a national strategy, similar to the effort to upgrade science and mathematics education in the 1950s, to meet this challenge.[42]

Also, against the fast-paced cyber threat landscape, it is imperative for cyber security experts to keep abreast of the adversary, if not at least staying alongside, through continuous learning and regular currency checks, to help shape an open, vibrant and stable cyberspace, which the public can use safely. Separately, it is essential to proliferate basic cyber security hygiene awareness for both the cyber security work force and the population that rely on IT systems so that everyone can contribute towards a secure future for cyberspace and the users.

CONCLUSION

Cyber security includes protecting military networks against cyber threats. Cyberspace is a network of networks that includes countless computers across the globe, therefore no state or organisation can unilaterally maintain effective cyber security. Close co-operation and timely sharing of cyber events, threat signatures of malicious code, and information about emerging actors/threats, allies and international players can improve collective cyber security standards. The military should continue to explore possible ways to defend its networks from malicious threats, and invest in people, technologies and R&D to create and sustain the cyberspace capabilities that are vital to national cyber security. This is essential as cyberspace may eventually be commonly accepted as a military domain of conflict, and it will be no different to allocating resources to procure sophisticated weaponry and developing the people to better serve in the Services and the overall Armed Forces for conventional warfare.

ENDNOTES

1. "The NSA's new look at cyber security," (*Armed with Science - The Official U.S. Defense Department Science Blog*, 2014) http://science.dodlive.mil/2014/06/16/the-nsas-new-look-at-cybersecurity/

2. Nazli Choucri and Daniel Goldsmith, "Lost in cyberspace: Harnessing the Internet, international relations and global security", (*Bulletin of the Atomic Scientists 68*, 2012), n._2, 70-77 http://bos.sagepub.com/lookup/doi/10.1177/0096340212438696

3. "Current world population", (*Worldometers*, 2014) http://www.worldometers.info/world-population/

   "Internet users in the world - distribution by world regions 2014 Q2" (*Internet World Stats*, 2014) http://www.internetworldstats.com/stats.htm

4. "Definition of cyberspace", *Oxford Dictionary* http://www.oxforddictionaries.com/us/definition/american_english/cyberspace

5. Lynn III and William J., "Defending a new domain", (*Foreign Affairs 89*, 2010), n._5, 97-108 http://eds.a.ebscohost.com/eds/detail/detail?sid=7c7a6fed-8f6c-4a05-bd0f-6095da13331e%2540sessionmgr4005&vid=0&hid=4110&bdata=JnNpdGU9ZWRzLWxpdmU%253d#db=bth&AN=52957873

6. "Definition of cyber vulnerability", (*Microsoft Corp*, 2014) http://msdn.microsoft.com/en-us/library/cc751383.aspx

7. "Global Security Outlook", (*Singapore Defence & Security Report*, 2011), n._1 http://connection.ebscohost.com/c/articles/57525657/global-security-outlook

8. "North Korea goes offline for 10 hours", (*Today Newspaper*, 2014)

9. "Definition of cyber security", (*International Telecommunication Union* (ITU), 2014) http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

10. Peter Rawlings, "Survey: Cyber security tops IA compliance agenda", (*Business Source Complete*, 2014) http://eds.a.ebscohost.com/eds/detail/detail?sid=62058abe-4f9f-47a5-8a8a-d478465c275d%2540sessionmgr4005&vid=2&hid=4110&bdata=JnNpdGU9ZWRzLWxpdmU%253d#db=bth&AN=97337568

11. "New Cyber Security Centre to Defend Singapore's Smart Nation Systems", (*Strait Times*, 2014) http://www.straitstimes.com/news/singapore/more-singapore-stories/story/new-cyber-security-centre-defend-singapores-smart-nation#sthash.EgWBc8i3.dpuf

12. "SAF sets up New 'Cyber Army' to Fight Digital Threats", (*Strait Times*, 2013) http://www.straitstimes.com/breaking-news/singapore/story/saf-sets-new-cyber-army-fight-digital-threats-20130630#sthash.deTt6Stu.dpuf

13. "Be a CSIT-Nanyang Scholar," (*Today Newspaper*, 2015)

14. Lynn III and William J., "Defending a new domain", (*Foreign Affairs* 89, 2010), n._5, 97-108 http://eds.a.ebscohost.com/eds/detail/detail?sid=7c7a6fed-8f6c-4a05-bd0f-6095da13331e%2540sessionmgr4005&vid=0&hid=4110&bdata=JnNpdGU9ZWRzLWxpdmU%253d#db=bth&AN=52957873

15. "Global Security Outlook", (*Singapore Defence & Security Report*, 2011), n._1 http://connection.ebscohost.com/c/articles/57525657/global-security-outlook

16. Ibid., 97-108

17. Ibid., 31

18. Adam Segal, "The code not taken: China, the United States, and the future of cyber espionage", (*Bulletin of the Atomic Scientists* 69, 2013) n._5, 38-45 http://bos.sagepub.com/lookup/doi/10.1177/0096340213501344

19. Ibid., 97-108

20. Ibid., 31

21. D. Dieterle, "Chinese hackers steal designs for top US Military Tech - Now What," (*Cyber Arms - Computer Security*, 2013) http://cyberarms.wordpress.com/2013/05/29/chinese-hackers-steal-designs-for-top-us-military-tech-now-what/

22. Ibid., 38-45

23. Alexander Klimburg, "National Cyber Security Framework Manual", (*NATO Cooperative Cyber Defence Center of Excellence*, 2014) http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

24. "The NSA's new look at cyber security," (*Armed with Science - The Official U.S. Defense Department Science Blog*, 2014) http://science.dodlive.mil/2014/06/16/the-nsas-new-look-at-cybersecurity/

25. Lynn III and William J., "Defending a new domain", (*Foreign Affairs 89*, 2010), n._5, 97-108 http://eds.a.ebscohost.com/eds/detail/detail?sid=7c7a6fed-8f6c-4a05-bd0f-6095da13331e%2540sessionmgr4005&vid=0&hid=4110&bdata=JnNpdGU9ZWRzLWxpdmU%253d#db=bth&AN=52957873

26. Ibid., 97-108

27. Ibid., 31

28. Ian Wallace, "The Military Role in National Cyber Security Governance", (*Seoul Defense Dialogue*, 2014) http://www.brookings.edu/research/opinions/2013/12/16-military-role-national cybersecurity-governance-wallace

29. Ibid.

30. "Department of Defense Strategy for Operating in Cyberspace", (*United States of America Department of Defense*, 2011) http://www.defense.gov/news/d20110714cyber.pdf

    Thomas C. Wingfield and Robert Sharp, "Tanks in Cyberspace", (*International Policy Digest*, 2014) http://www.internationalpolicydigest.org/2014/04/14/tanks-cyberspace

31. "The Comprehensive National Cyber Security Initiative", *Executive Office of the President of the United States of America*, 2014) http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

32. Ibid.

33. Ibid.

34. Peter J. Denning and Dorothy E. Denning, "The Profession of IT - Discussing Cyber Attack", (*Communications of the ACM 53*, (2010), n._9, 29-31 http://portal.acm.org/citation.cfm?doid=1810891.1810904

35. Ibid.

36. Ibid., 97-108

37. Ibid., 29-31

38. "Department of Defense Strategy for Operating in Cyberspace", (*United States of America Department of Defense*, 2011) http://www.defense.gov/news/d20110714cyber.pdf

    "Cyber guard exercise tests people, partnerships", (*U.S. Cyber Command News Release*, 2011) http://www.defense.gov/news/newsarticle.aspx?id=122696

39. Herbert Lin, "Why computer scientists should care about cyber conflict and U.S. National Security Policy", (*Communications of the ACM 55*, (2012), n._6, 41-43 http://dl.acm.org/citation.cfm?doid=2184319.2184334

40. "The Comprehensive National Cyber Security Initiative", (*Executive Office of the President of the United States of America*, 2014) http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

41. Ibid.

42. Ibid.

ME5 Alan Ho Wei Seng is a recipient of the SAF Academic Scholarship. He graduated from the University of Queensland in 2006 with a Bachelors of Information Technology with 1st Class Honours and a Masters of Philosophy in Information Technology. In 2013, ME5 Ho received the SAF Postgraduate Award (SPA) and he graduated from Cranfield University with a Masters of Science in Forensic Computing. Following his SPA studies, ME5 Ho is presently a Deputy Branch Head. He was also a winner of the Commendation Award at the 2014/2015 Chief of Defence Force Essay Competition.