How a Good Offence is not the Best Defence: An Analysis of SAF's Approach to Cyber Warfare

by **LTA Ng Yeow Choon**

Abstract:

Technological advancement has ushered in an era of network-centric warfare where cyberspace plays an instrumental role in military operations. Due to its integral nature to modern militaries, cyberspace offers the ideal platform on which military operators can conduct their missions. Cyber warfare refers to the military doctrines and tactics used by operators in their attempt to gain dominance in the realm of cyberspace. Through the analysis of the offensive and the defensive aspects of cyber warfare, this paper argues that the SAF should invest in cyber-defence rather than cyber-offence. In addition, it suggests that by focusing on cyber-defence, the SAF may not only deter potential military aggressions from state actors but also protect Singapore's civilian infrastructure and institutions from non-state entities.

Keywords: Network-centric Warfare, Technology, Cyber Defence, Deterrence

INTRODUCTION:

Improvements in information technology and the evolution of business organisations have prompted militaries around the world to adopt new processes and take advantage of innovations. Among these innovations, increased connectivity between computer systems and effective coordination across multiple platforms have allowed modern militaries to employ systems holistically instead of individually—a fundamental shift from platform-centric warfare to network-centric warfare.[1]

NETWORK-CENTRIC WARFARE AND CYBERSPACE

The SAF, like other modern militaries in the world, underwent its 3rd Generation Transformation and established itself as a network-centric force.[2] A network-centric force is characterised by two broad themes. First, it involves a shift in focus from the weapons platform, such as the battle tank or the submarine, to the information network. Second, it emphasises a holistic employment of military systems in a dynamic battle environment over deployment by individual military units.[3] The advent of network-centric warfare revolves around the usage of interconnected computer systems and military platforms—every component of network-centric warfare occurs within the sphere of cyberspace. Cyberspace, succinctly defined by the United States (US) Department of Defense, is *"the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."*[4] The more a military identifies itself as a network-centric force, the more connected it is to the cyberspace.

While network-centric warfare offers the obvious advantage of incorporating technology and sound organisation as force multipliers, the accompanying connectedness with cyberspace presents some vulnerability.

A network-centric force is susceptible to disruptions to its command and control mechanism. The enemy can disable key components of a network-

centric force, preventing commanders from issuing orders, units from communicating with one another, or even individual weapon systems from sharing essential information. It is the defence against such cyber-attacks that spurs network-centric militaries to establish teams of cyber experts. The US Cyber Command and the 'Chinese Information Support (Assurance) Base' were established to cope with the realities of this new realm of warfare.[5] These new military units are responsible for doctrines and tactics regarding cyberspace—developing cyber weapons and carrying out cyber-offence operations, while preventing their opponents from doing the same.[6]

Being a small city-state, Singapore has no illusions about the state of the region or the world.[7] Taking cues from the rest of the world, the SAF Cyber Defence Operations Hub was established "to defend MINDEF/SAF military networks against cyber threats."[8] In the light of these cyber threats, be it initiated by aggressive states actors or non-state enttities (like terrorists or rogue hacktivists), how should the SAF position itself in the evolving cyberspace?

This paper explores the offensive and defensive aspects of cyber warfare, and argues that the SAF should invest in cyber-defence rather than cyber-offence. By focusing on cyber-defence, the SAF not only deters potential military aggressions from state actors but also protects Singapore's civilian infrastructure and institutions from non-state entities.

CYBER WARFARE

The US Air Force describes cyber warfare as the ability 'to destroy, deny, degrade, disrupt, and deceive,' while at the same time 'defending' against the enemy's use of cyberspace for the very same purpose. The key instrument in conducting cyber warfare is the computer—it is a military weapon in the same way the sword, the battle tank, or the submarine is.[9] An article published in 2011,entitled *The New Cyber Arms Race,* depicts how cyber warfare might be conducted in the

Analysts and operators showing Minister for Defence, Dr Ng Eng Hen and then-Minister of State for Defence and Education, Mr Lawrence Wong (far right) how the C4 network and intelligence elements aid them during deployments.

future: *"Wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponised computer programmes that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement or troops, the path of jet fighters, the command and control of warships."*[10]

In fact, the future is already here. We have witnessed some forms of "weaponised computer programmes [aimed at] disrupt[ing] or destroy[ing] critical industries [and] disable[ing] military networks" in recent history. The employment of Stuxnet is one such example.[11]

CYBER-OFFENCE IN FOCUS: STUXNET

Described as the world's first cyber warfare weapon, Stuxnet was a complex malware designed to physically destroy a military facility.[12] Like any malware, Stuxnet infects a system through an external source like a USB flash drive. However, it only targets controllers from one specific manufacturer – Siemens. These controllers were used by Iran to run centrifuges that enrich nuclear fuel. Stuxnet compromised the logic controllers involved in the system and caused the centrifuges to spin out of control, damaging at least 14 industrial sites in the process, including a uranium-enrichment plant.[13] Due to the level of sophistication involved in the design and targeted execution of the malware against Iran, many observers believe that Stuxnet was created by a team of experts sanctioned by a national government. In other words, Stuxnet may well be a politically motivated cyber weapon used by a state actor against its adversary.[14]

A network-centric force is susceptible to disruptions to its command and control mechanism. The enemy can disable key components of a network-centric force, preventing commanders from issuing orders, units from communicating with one another, or even individual weapon systems from sharing essential information. It is the defence against such cyber-attacks that spurs network-centric militaries to establish teams of cyber experts.

While Stuxnet is an overt example of cyber-offence capabilities, Advanced Persistent Threat (APT) is a covert category of cyber-offensive works carried out by state actors against potential enemies.

ADVANCED PERSISTENT THREAT

APT involves continuous and stealthy hacking activities organised and carried out by governments against a specific target, such as another nation, in order to exploit vulnerabilities for political gains. The high degree of coordination involved in APT, along with its associated political motivation, differentiates it from regular hacking activities. Only state actors, with their resources and pool of expertise, can carry out the drawn-out and sophisticated works of APT as they patiently see the returns of these stealthy activities come to fruition.[15]

APT comprises several teams; each specialised to perform a particular task. First, a surveillance team studies and identifies the key vulnerabilities of the target. This preparation process can take months or years. Thereafter, having gathered enough information about the target, an intrusion team works to breach the system. Once the team has successfully intruded into the system, having gained access to sensitive information, an exfiltration team extracts the information the APT is intended for. Instead of extracting everything it can find, only specific files are retrieved in order to avoid suspicion. Often, victims of APT do not know that they have been targeted until it is too late. Moreover, there is little reliable evidence the victim can use to accuse

Wikipedia

Diagram depicting the life cycle staged approach of an Advanced Persistent Threat (APT) which repeats itself once complete.

the perpetrator.[16] Information gathered through APT can serve as critical intelligence for a military to conduct its onward operations. For instance, battle plans conceived by adversarial political and military leaders can be obtained, allowing pre-emptive actions to thwart possible interventions.[17]

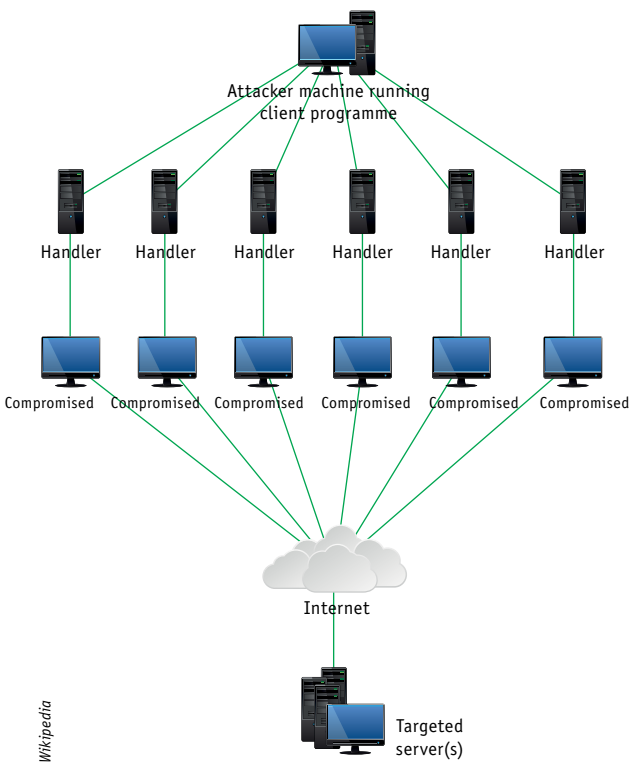
Given the effectiveness of Stuxnet as a cyber-weapon and the potential of APT to collect critical intelligence, investment and potential usage of cyber-offence capabilities may seem to be an obvious choice for the SAF if it wants to remain relevant in the evolving world of cyberspace. After all, obtaining these cyber-offence capabilities might deter potential adversaries of the SAF not just in cyberspace, but also in the conventional political space.

HOW A GOOD OFFENCE IS NOT THE BEST DEFENCE

In assessing the usefulness of cyber-offensive warfare to the SAF, it is important to note the core purpose of the SAF: "to enhance Singapore's peace and security through deterrence and diplomacy, and should these fail, to secure a swift and decisive victory over the aggressor."[18] Both overt cyber-offence (Stuxnet) and covert cyber-offence (APT) do not support the SAF's ability to ensure a swift and decisive victory. In addition, cyber-offence creates destabilising effects

in the political arena—the SAF will be better off focusing its resources elsewhere.

The development of sophisticated cyber weapons like Stuxnet requires a great deal of expertise and long periods of planning. Yet, the intended consequences, however carefully designed, are not always clear. There is difficulty in assessing the outcome of cyber-offence because the damage caused is not immediately apparent, unlike the use of conventional weapons. In the case of Stuxnet, recent research has suggested that the cyber weapon was ineffective and had caused negligible setback to Iran's nuclear programme—this is in direct contradiction to the widely-acclaimed success Stuxnet was thought to have achieved. Overall, the effects of Stuxnet were short-lived and Iran managed to overcome the cyber-attacks by 2010.[19] There might be unintended effects of cyber-offence as well. Besides Iran, Stuxnet infected over 60,000 computers from countries including China, United States, the United Kingdom and Australia.[20]



Distributed Denial-of-Service (DDoS) Stacheldraht attack diagram involved in the cyber-attack.

Regardless of the origin of Stuxnet, the uncontrollable spread of such cyber weapons might cause harm to the very nation it is meant to protect. Because cyber-offence involves uncertainty in delivering its intended payload, coupled with the long process it takes to materialise, it will not be able to ensure the swift and decisive victory desired by the SAF.

The stealthy nature of covert cyber-offence hinders trust between countries and hampers diplomacy. Even though cyber-attacks are meant to be stealthy, they are never absolutely undetectable because potential victims can follow the traces left behind by the cyber-attackers. When the *New York Times* suspected that its networks had been compromised, it worked with a computer security company and tracked down the cyber-attack. They found out that the attack was attributed to the Chinese military.[21] Revelations of such incidents have strained the diplomatic relationship between US and China. The US has blamed China for the theft of intellectual property and repeated attempts to gain a strategic advantage through cyber-attacks.[22] China has likewise made similar accusations against the US.[23] The political fallout resulting from cyber-offence continues to mar discussions between the two major powers, resulting in unintended destabilising effects to the international political arena at large. Cyber-offence carried out between US and China has invariably bred suspicions and hampered diplomatic efforts. As seen, both overt and covert forms of cyber-offence are counter-productive and undermine the SAF's role "to ensure peace and security through… diplomacy."[24] In the context of cyberspace then, a good offence is not the best defence; cyber-defence, not cyber-offence, is key.[25]

SINGAPORE'S VULNERABILITES AND IMPORTANCE OF CYBER-DEFENCE

The significance of cyber-defence for a nation that is heavily dependent on cyberspace cannot be overemphasised. Singapore, among the most wired countries in the world,[26] is dependent on cyberspace for many critical administrative processes like its e-government initiative.[27] Its increased connectivity

in cyberspace has resulted in an accompanying rise in vulnerabilities.[28]

Like Singapore, Estonia is also one of the world's most wired nations.[29] Most Estonians carry out administrative functions, such as banking transactions and paying taxes, online.[30] As such cyber warfare poses a real threat to its critical infrastructure and institutions. In 2007, Estonia experienced a massive cyberattack that threatened its national security. The cyber-attack involved distributed denial of service (DDoS) attacks that overwhelmed websites with a surge of requests that crippled the underlying network of servers. As a result, the functioning of government, banks, media and important institutions were brought to a halt.[31] Despite calls from Estonian officials for an international retaliation against the Russian government—whom they believe were the source of the attack—insufficient evidence existed to accuse Russia of staging these attacks.[32]

While Singapore has not seen cyber threats at the scale experienced by Estonia, it saw similar threats initiated by ill-intentioned individuals. In 2013, Singapore encountered a series of cyber-attacks initiated by the hacktivist organisation 'Anonymous'—a loose coalition comprising individuals who conduct hacking activities and defacement of websites, among other cursory works.

Singapore has much to learn from this incident. While the SAF Cyber Defence Operations Hub was established to defend the SAF's military networks against cyber threats, cyber-attacks need not necessarily target military installations to achieve a crippling effect to the nation's normal functioning. Cyber-attacks on critical civilian infrastructure can threaten national security just as in the case of Estonia. It is useful to note that cyber-offence in Estonia's case had no effect on protecting or repelling further cyber-attacks from its adversary; only cyber-defence could perhaps deny the adversary the ability to successfully intrude and cripple its computer networks. Effective cyber-defence could also block many additional cyber-attack attempts and weaken the will of adversaries, prompting them to stop trying. In comparing cyber-offence with cyber-defence, it is clear that the latter would be able to achieve a more tangible and stabilising effect—it could better protect critical infrastructure and ensure national security.

While Singapore has not seen cyber threats at the scale experienced by Estonia, it saw similar threats initiated by ill-intentioned individuals. In 2013, Singapore encountered a series of cyber-attacks initiated by the hacktivist organisation 'Anonymous'—a loose coalition comprising individuals who conduct hacking activities and defacement of websites, among other cursory works. The perpetrator, who went by the alias 'The Messiah,' temporarily disabled up to nineteen government websites.[33] Although the impact of these cyber-attacks was nothing more than fear mongering, the incident underlined the inherent vulnerability Singapore faces given its heavy dependence on cyberspace. Despite the SAF's focus on cyber-defence exclusively aimed at protecting military installations and infrastructure, the processes and organisations developed in enhancing its cyber security can be transferred to civilian operations. Singapore as a whole can then benefit as a result of the SAF's strengthening of cyber-defence capabilities on non-military infrastructure.

BOOSTING CYBER-DEFENCE

In order to create a robust cyber-defence structure, defenders can target three main points of entry cyber-attackers typically exploit: Confidentiality, Integrity, and Availability—collectively known as the CIA triad. Confidentiality means that no information is revealed to unauthorised personnel—only individuals with the rights and privileges are given access to such

information. Integrity refers to the intactness of information as it is transmitted and then received —data integrity assures that information is not compromised. Availability means that resources and access to information are unimpeded.[34] In the case of the cyber-attacks by 'Anonymous' on the Singapore government in 2013, which involved the defacement and temporary shutdown of websites, integrity and availability were compromised.

That said, the country's robust cyber-defence structure was able to recover quickly and websites were back up and running within hours following the attacks, partially due to the low calibre and uncoordinated nature of the attack by 'Anonymous'. Such is a demonstration of another hallmark of good cyber-defence—resilience. A resilient cyber-defence structure has the capacity to work under degraded conditions and if compromised, is able to recover quickly. Also referred to as intrusion-tolerant,'[35] a resilient cyber-defence structure is only as strong as the human component undergirding it.

In terms of system measures, careful issuance and monitoring of access control ensure that the overall cyber-defence structure prevents not only external threats but internal ones as well. It is crucial to acknowledge that sometimes the danger comes from the inside.

In 2008, the US military suffered an unprecedented compromise of its classified military computer networks because an unauthorised flash drive carrying a malware was carelessly inserted into an official computer in the Middle East.[36] The damage done encompassed confidentiality and integrity —the enemy who implanted the malware knew classified information about the US military and communication lines within the US military no longer ensured data integrity. All these because one soldier made the mistake of not scanning the flash drive for malware before inserting it into the computer.[37]

Ensuring the compliance of personnel regarding cyber-defence matters is critical in maintaining the robustness of safeguards already put in place. The SAF employs cryptographic integrity checks to ensure the secure communication of classified information. These work in tandem with personnel's efforts to maintain information security. This includes refraining from introducing unauthorised external devices to internal computer networks.

In terms of system measures, careful issuance and monitoring of access control ensure that the overall cyber-defence structure prevents not only external threats but internal ones as well. It is crucial to acknowledge that sometimes the danger comes from the inside. The sensational leaks of classified information in cases like Edward Snowden and Bradley Manning show that failure in access control can result in a devastating compromise of the entire cybersecurity architecture.[38] Edward Snowden, a low-level defence contractor working for the CIA, was given high-level access to classified documents which he would later leak to the press. Access control was too lax and provided the loopholes which whistleblowers like Snowden exploited. The sheer amount of information that he was able to sneak out of supposedly highly-secure computer systems is unfathomable. Learning from these incidents, the SAF should constantly review its access control processes and ensure shortcomings are rectified. Only then can the possibility of leakages be minimised, and confidentiality of information maintained. On top of looking outward for external cyber-attacks, a robust cyber-defence structure must look inward to prevent internal sabotage.

CONCLUSION

The SAF has entered a new era of warfare where cyberspace plays an integral role in military operations and national security. The discovery of cyber weapons like Stuxnet, the reality of APT and the unfolding of international crises like the cyber-attacks on Estonia, all point to the need for the SAF to continually adapt and evolve itself to cope with cyber threats. With the establishment of the SAF Cyber Defence Operations Hub

which focuses on strategies, tactics and doctrines to cope with cyber warfare, the SAF needs to assess the current development and capabilities of both cyber-offence and cyber-defence and decide how much of each it should focus on. Through the analysis of the offensive and defensive aspects of cyber warfare, this paper has shown that the SAF should invest in cyber-defence rather than cyber-offence. By putting emphasis on cyber-defence, the SAF not only deters potential military aggressions from state actors but also protects Singapore's civilian infrastructure and institutions from non-state entities.

ENDNOTES

1. Arthur K. Cebrowski and John J. Garstka. "Network-centric warfare: Its origin and future." *US Naval Institute Proceedings* 124, n._1 (1998), 28-35.
2. MINDEF (Singapore). "3rd Generation SAF." http://www.mindef.gov.sg/imindef/key_topics/3rd_generation_saf.html

   Claire Apthorp. "Singapore Leads The Way." *Defence Review Asia* 4, issue 6 (2010): 22.
3. Michael Dillon, "Network society, network-centric warfare and the state of emergency." *Theory, Culture & Society* 19, n._4 (2002), 71-79.
4. US Department of Defense Joint Publication 1-02. *Dictionary of Military and Associated Terms:* 141.
5. US Army Cyber Command. "Organization." http://www.arcyber.army.mil/org-uscc.html

   Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Project 2049 Institute. https://project2049.net/publications.html
6. Mazanec, M. Brian. "The art of (cyber) war." *Journal of International Security Affairs* 16 (2009), 84.
7. Ministry of Foreign Affairs (Singapore). "Foreign Policy." http://www.mfa.gov.sg/content/mfa/overseasmission/manila/about_singapore/foreign_policy.html
8. MINDEF (Singapore). "Clarification of the role of the SAF Cyber Defence Operations Hub (CDOH)." http://www.mindef.gov.sg/imindef/press_room/clarification/11Nov13_clarification.html#.UzA7s61dW9o
9. Peter W. Singer and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* (Oxford: Oxford University Press, 2013), 128.
10. Mark Clayton. "The New Cyber Arms Race." *The Christian Science Monitor.* http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race.
11. David Kushner. "The real story of Stuxnet." *Spectrum, IEEE 50,* n._3 (2013), 48-53.
12. Ralph Langner. "Stuxnet: Dissecting a cyberwarfare weapon." *Security & Privacy, IEEE 9,* n._ 3 (2011), 49-51.
13. David Kushner. "The real story of Stuxnet." *Spectrum, IEEE 50,* n._3 (2013), 48-53.
14. Sascha Knoepfel. "Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War." *Cyberspace and International Relations.* Springer Berlin Heidelberg, 2014, 117-124.
15. Colin Tankard. "Advanced Persistent threats and how to monitor and deter them." *Network Security,* n._8 (2011), 16-19.
16. Peter W. Singer, and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2013), 56-60.
17. Adam Taylor. "By banning YouTube, has Turkey revealed just how damning today's leaked recording is?" *Washington Post.* http://www.washingtonpost.com/blogs/worldviews/wp/2014/03/27/by-banning-youtube-has-turkey-revealed-just-how-damning-todays-leaked-recording-is/
18. MINDEF (Singapore). "Mission." http://www.mindef.gov.sg/imindef/about_us/mission.html
19. Ivanka Barzashka. "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme." *The RUSI Journal* 158, n._2 (2013), 48-56.
20. James P. Farwell and Rafal Rohozinski. "Stuxnet and the future of cyber war." *Survival* 53, n._1 (2011), 23-40.
21. David E. Sanger, David Barboza and Nicole Perlroth. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *New York Times*

    http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all

22. Sanger, David E. "U.S. Blames China's Military Directly for Cyberattacks." *New York Times*. http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?_r=0

23. Jacob Davidson. "China Accuses U.S. of Hypocrisy on Cyberattacks." *Time*. http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/

24. MINDEF (Singapore). "Mission." http://www.mindef.gov.sg/imindef/about_us/mission.html

25. Peter W. Singer, and Allan Friedman. "Cult of the Cyber Offensive: Why belief in first-strike advantage is as misguided today as it was in 1914." *Foreign Policy,* January 15, 2014. http://www.foreignpolicy.com/articles/2014/01/15/cult_of_the_cyber_offensive_first_strike_advantage

26. Bloomberg. "Most Wired in the World: Countries." http://www.bloomberg.com/visual-data/best-and-worst/most-wired-in-the-world-countries

27. Singapore Government. "About eGov: Introduction." http://www.egov.gov.sg/about-egov-introduction

28. Beidleman, W. Scott. "Defining and Deterring Cyber War." *U.S. Army War College Carlisle Barracks* PA, 2009.

29. Jacob Davidson. "China Accuses U.S. of Hypocrisy on Cyberattacks." *Time,* July 1, 2013. http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/

30. Christopher Rhoads. "Politics & Economics: Estonia Gauges Best Response to Cyber Attack." *The Wall Street Journal,* 2007.

31. Joshua Davis. "Hackers Take Down the Most Wired Country in Europe." *Wired Magazine,* issue. 15.09 (2007).

32. Michael Lesk. "The new front line: Estonia under cyberassault." *IEEE Security & Privacy* 5, n._4 (2007): 76-79.

33. F.C. "Hacking in Singapore: Messiah complicated." *The Economist*. http://www.economist.com/blogs/banyan/2013/12/hacking-singapore

34. Baumann, Rainer, Stéphane Cavin, and Stefan Schmid. "Voice over IP-security and SPIT." *Swiss Army, FU Br* 41 (2006), 1-34.

35. Yves Deswarte, Laurent Blain, and J-C. Fabre. "Intrusion tolerance in distributed computing systems." *IEEE Symposium on Security and Privacy,* Oakland, California (1991), 110-121.

36. Lynn, J.William. "Defending a new domain: The Pentagon's cyberstrategy." F*oreign Affairs* (2010), 97-108.

37. P.W. Singer and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2013). 64.

38. Glenn Greenwald, Ewen MacAskill, and Laura Poitras. "Edward Snowden: the whistleblower behind the NSA surveillance revelations." *The Guardian* 9 (2013).

LTA Ng Yeow Choon is a Fighter Pilot by vocation. He was awarded the SAF Merit Scholarship in 2012 and is currently pursuing his Bachelors of Arts in Economics at New York University. LTA Ng received a Commendation Award at the Chief of Defence Force Essay Competition 2013/2014.