CYBER THREAT – A GLOBAL SECURITY THREAT

by ME5 Seah Ser Thong, Calvin

Abstract:

The technology boom of the 21st century has led to the rapid rise and influence of the Internet on people around the world. Originally created to interconnect laboratories engaged in government research, the Internet has now become a universal information sharing platform that brings people from all walks of life closer together. However, this increased interconnectedness of information sharing has its disadvantages and perils. International hacking groups like 'Anonymous' have increased efforts to obtain information through illegal and unethical means, while cyber threats like the Stuxnet Worm have become increasingly prevalent. As such, an increasing number of countries are investing more into cyber security to combat these cyber threats. This essay will delve deeper into the nature and extent of cyber threats and its impact on the military and potential cyber defence measures.

Keywords: Cyber; Interconnect; Unethical; Security Threats; Information

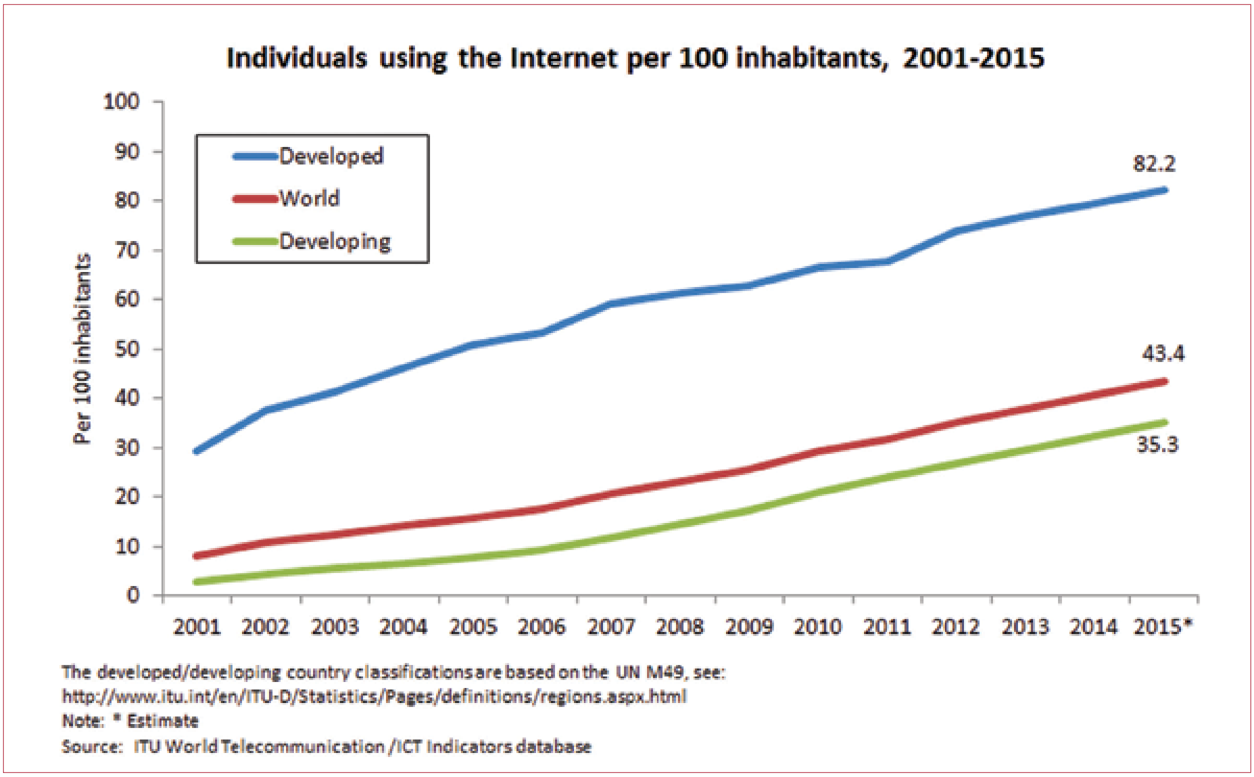
INTRODUCTION

> *"Cyber threat is one of the most serious economic and national security challenges we face as a nation."*
>
> *– Barack Obama, US President*[1]

The Internet is a medium that all of us have gotten so used to. It has grown fast and furious and has seen an increase in usage from 16 million users to 2,937 million users presently since it was created to interconnect laboratories engaged in government research in the 1990s.[2] It has become the universal source of information for people all over the world and has inadvertently become a battlefield for a new kind of warfare, 'Cyberwarfare'. With cyber threats such as the Stuxnet Worm that appeared to have attacked Iran's nuclear programme to the 'Anonymous' international network of hackers, governments around the world have been called to arms to deal with this new threat. In 2011, the United States (US) Department of Defence even designated cyberspace as an 'operational domain' in which US forces will be trained to defend.[3] Closer to home, Singapore Prime Minister Lee Hsien Loong unveiled a $130 million plan in 2013 to enhance the nation's cyber security firepower in the face of a rising tide of global cyber-attacks in 2013.[4] This essay explores the threat posed by cyber threats as well as proposes a framework for cyber defence.

CYBER THREATS

So, are cyber threats just hype or an overreaction by everyone? A proxy would be searching the Internet using the search key 'cyber threats'. It is telling to see the huge amount of interest in these matters.[5] While hacking and virus-writing began as hobbyist activities not meant to cause serious long-term harm,



The developed/developing country classifications are based on the UN M49, see: http://www.itu.int/en/ITU-D/Statistics/Pages/definitions/regions.aspx.html
Note: * Estimate
Source: ITU World Telecommunication /ICT Indicators database

Figure 1: Internet users' growth[6]

cyber threats have since evolved towards achieving financial and political objectives and have also become destructive in nature.[7] Let us now take a look at some of the incidents and damages posed. It is noteworthy that these incidents are wide-ranging and can be triggered by national governments, organisations and individuals. They also involve cyber-attacks like hacking and even scams and can be represented by the cyber threats spectrum shown in *Figure 2*.

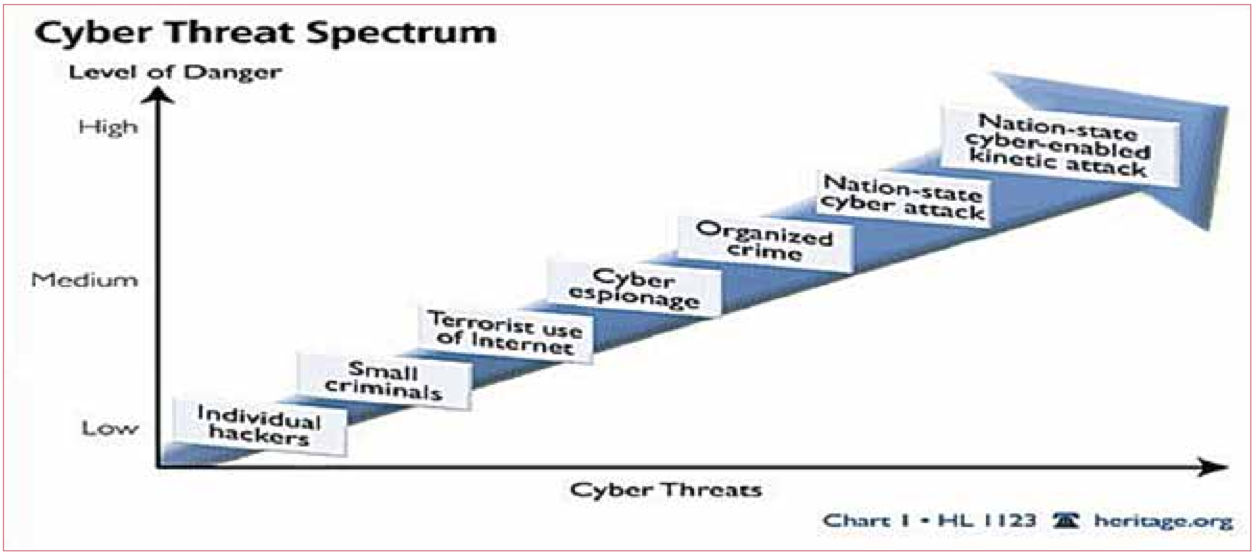
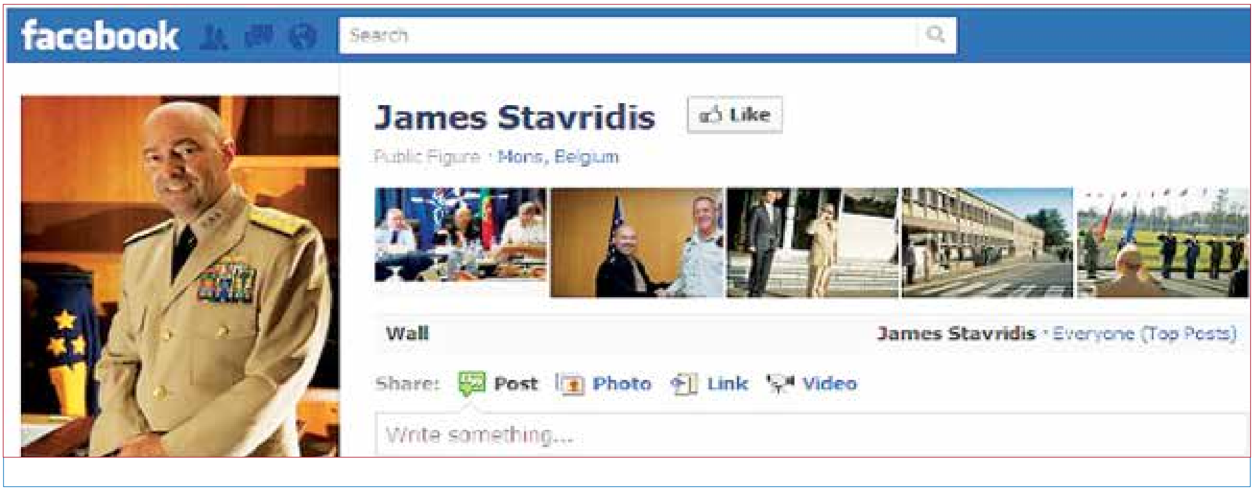


Figure 2: Cyber threat spectrum of the various threats and level of danger posed.[8]



Actual Facebook profile of United States Navy Admiral James Stavridis. The fake account was immediately taken down when Facebook was notified.[9]

Attack on Estonia (2007)

A three-week wave of cyber-attacks was made on Estonia in April 2007 that swamped websites of Estonian organisations, including the Estonian parliament, banks, ministries, newspapers and broadcasters.[10] These were a wave of so-called Distributed Denial of Service (DDoS) attacks, where websites are suddenly swamped by tens of thousands of visits, jamming and disabling them by overcrowding the bandwidths for the servers running the sites. This crisis happened amidst the country's disagreement with Russia about the relocation of the Bronze Soldier of Tallinn. The North Atlantic Treaty Organisation (NATO) had to dispatch some of its top cyber terrorism experts to Tallinn to investigate and to help the Estonians beef up their electronic defences. Estonia is now home to NATO's Cooperative Cyber Defence Centre of Excellence which was established in response to what has become known as 'Web War 1'.[11]

While hacking and virus-writing began as hobbyist activities not meant to cause serious long-term harm, cyber threats have since evolved towards achieving financial and political objectives and have also become destructive in nature.

Stuxnet Worm (2010)

The Stuxnet is a computer worm that infected the Iranian nuclear programme systems in 2010 and apparently set back the Iranian nuclear programme by as much as two years. Reputable experts in the computer security community had labelled Stuxnet *"unprecedented... an evolutionary leap and the type of threat we hope to never see again."*[12] The worm was designed to attack industrial Programmable Logic Controllers (PLCs) and its authorship remains unknown.[13] This is highly significant, as the Stuxnet Worm has resulted in flaws in existing security assumptions and was able to inflict damage on industrial systems that were outside the Internet. It is reported that, unlike Denial of Service (DOS) attacks that could take at most weeks to clear up, Stuxnet-like attacks can set their victims back by many years.[14]

Facebook Sham (2011)

In 2011, senior British military officers, Defence Ministry officials and other government officials were tricked into becoming Facebook friends with someone masquerading as US Navy Admiral James Stavridis.[15] This allowed their information to be compromised. Even though the fake Facebook account was deleted

The government website of Singapore's Prime Minister's office was hacked by Anonymous on 7th November, 2013.[16]

within 24 to 28 hours of being discovered, it was difficult to find the creator of the account. *"There have been several fake supreme allied commander pages,"* a NATO spokesperson said in a statement.[17] *"We recognise that there are vulnerabilities in infrastructure... That's why we see breaches by the thousand every single month. We know that the capabilities of foreign states are substantial and we know the type of information they are targeting,"* said Shawn Henry, an FBI Executive Assistant Director, in a statement.[18] This highlights the real danger in our use of social media.

Singapore Defence Minister, Dr Ng Eng Heng, also pointed out that cyber-attacks could develop into nightmare scenarios where the networks that the SAF relies upon during operations are incapacitated.

Activist group Anonymous (2013)

The government web-site of Singapore's Prime Minister's office was hacked on 7th November, 2013 by apparent members of the activist group 'Anonymous' after Prime Minister Lee Hsien Loong told local journalists that his government would "*spare no effort*" in going after Anonymous members who had threatened to wage a cyber-war against Singapore.[19] "*It's great to be Singaporean today,*" read a mocking headline in a section of the Prime Minister's Office website, next to the group's trademark Guy Fawkes mask - a symbol of anti-establishment defiance worldwide.[20] The defaced section was quickly taken offline after the hacking incident surfaced in a posting on Facebook.

Ukraine conflict (2014)

The hostilities between Ukraine and Russia are currently mirrored by a corresponding cyber war where, as an analysis of internet traffic suggests, both sides have opened up an online front. In one instance, dozens of Ukrainian computer networks, including those run by the Kiev government, have been reportedly infected by the aggressive 'Snake' or 'Ouroboros' virus.[21] The number of cyber-attacks traded between Ukraine and Russia appears to have risen sharply as relations have worsened with the overthrow of the Yanukovych government and the annexation of Crimea. The online struggle is being waged by a mixture of state forces, criminal gangs as well as independent 'patriotic hackers'. Activists and experts have suggested that this sets a pattern likely to be repeated in future conflicts.[22] Greg Day, the Vice-President of FireEye had mentioned that the spread of information technology had widened the arena for conflict and meant combatants no longer had to be heavily armed with expensive weaponry.[23] This could suggest the simultaneous use of military and cyber warfare in future conflicts. It could be a potential vulnerability to watch out for with our dependency on IT systems.

CYBER THREATS VERSUS THE MILITARY

Threats to the Military

In the United Kingdom (UK), it was quoted that a group of Member of Parliament (MPs) had mentioned that the threat of a cyber-assault on Britain is considered so serious that it is being marked as a higher threat than a nuclear attack.[24] Singapore Defence Minister, Dr Ng Eng Heng, also pointed out that cyber-attacks could develop into nightmare scenarios where the networks that the SAF relies upon during operations are incapacitated. These networks support the Singapore Armed Forces' (SAF) surveillance, weapons, engineering, logistics, and most importantly, communication systems.[25]

With enduring cyber threats looming, many countries have actually commenced the setup of cyber defence organisations within their militaries to take them on. Let us take a look at the initiatives taken by various countries' militaries in the war against cyber threats.

(1) **US Department of Defence (DoD)**

The US Cyber Command officially began service in October 2009 and aims to protect US military networks, as well as possibly launching digital warfare attacks against rival nations.[26] The department was established by Defence Secretary Robert Gates and marked the first time the US government has ever created such a department. A fivefold increase in the staff of the US Cyber Command in 2013 is indicative of how conflict in cyber space is moving towards centre stage for the US military, a domain similar to land, sea, air and outer space.[27] As reported by Ellen Nakashima in *The Post*, there are three types of forces under the Cyber Command. Two are familiar: 'Combat Mission Forces' to serve in parallel with military units and 'Protection Forces' to defend Pentagon networks.[28] A third area is new: 'National Mission Forces' that seeks to remove threats to critical infrastructure in the US, such as electrical grids, dams and other potential targets deemed vital to national security and are expected to operate outside the US, perhaps launching pre-emptive strikes on adversaries preparing to take down critical US infrastructure.[29]

2) **UK Ministry of Defence (MoD)**

The UK Defence Secretary had announced in 2013 that a new cyber unit would be created to help defend national security with hundreds of reservists recruited as computer experts to work alongside regular forces in the creation of the new Joint Cyber Reserve Unit.[30] The role of the unit is to protect computer networks and safeguard vital data and, if necessary, launch strikes in cyberspace. Conservative Minister, Mr Philip Hammond told the Conservative Party conference that "*the threat is real… and that… Last year… cyber defences blocked around 400,000 advanced, malicious cyber threats to the government secure intranet alone.*"[31] The MoD said the recruitment of reservists will target regular personnel leaving the armed forces, current and former reservists with the required skills and civilians with the appropriate technological skills and knowledge.[32]

(3) **Japan Ministry of Defence (MoD)**

While cyber security in Japan is largely the responsibility of its Self Defence Forces, however, Japan's Ministry of Defence set up Japan's first Cyber Defence Unit on 26th March, 2014 as it reorganised the ministry's hitherto disparate cyber security teams under a single command.[33] The new combined command unit, with a budget of ¥14.1 billion (US $141.9 million) as compared to the previous year's ¥9.1 billion for its cyber teams, will provide integrated 24-hour cyber security monitoring, inspection and analysis, defence, cleansing and training functions for the entire military.[34] It was formed with an initial staff of a hundred to act as a central hub to co-ordinate responses and develop expertise and training. Politically, the government has also established new rules governing the circumstances in which Japan may counter attack against a cyber-threat.[35]

(4) Singapore's Military Response

Back home, Singapore has set up a centralised Cyber Defence Operations Hub in 2013 for more robust defences of its military networks. In announcing the setting up of the operations hub, Defence Minister Dr Ng Eng Hen mentioned that the round-the-clock operations hub will allow the SAF to build up its expertise to not only combat evolving cyber threats, but also disrupt the military's front and back-end systems. The hub is established to defend the Ministry of Defence (MINDEF)/SAF military networks against cyber threats. The hub will partner Singapore Infocomms Technology Security Authority to keep abreast with the latest developments in cyber threats and will also draw on the existing expertise of the SAF and MINDEF, as well as the defence technology community.[36] The SAF has been consistent in its build up to keep abreast with the increasing cyber threats. As mentioned by Dr Ng, the SAF was not starting from scratch, but amalgamating existing SAF-wide resources that deal with cyber-attacks.[37]

CYBER DEFENCE FRAMEWORK

Reflecting on how all international conflicts now have some digital component, the North Atlantic Treaty Organisation (NATO) has updated its cyber defence policy to make it clear that a cyber-attack can be treated as the equivalent of an attack with conventional weapons. The organisation's new cyber defence policy clarifies that a major digital attack on a member state could be covered by Article 5, the collective defence clause. That states that an attack against one member of NATO "shall be considered an attack against them all" and opens the way for members to take action against the aggressor—including the use of armed force—to restore security.[38] That NATO is updating its cyber defence strategy now shows how rapidly cyber warfare has jumped up the agenda.[39] Besides recognising cyberspace as an 'operational domain', and taking actions against potential cyber aggressors, what more could be done by the military to combat cyber threats? What are the challenges that must be faced? I will outline some of the challenges that would need to be considered before implementing any cyber defence strategy.

a. People as the weakest link

While systems can be put in place, people always turn out to be the weakest link. The human tendencies to be trusting and inquisitive make people gullible to the many cyber shams that are out there on the Internet. As such, increased awareness is necessary to ensure that people are not the weakest link.

b. Lack of Cybersecurity Competency

While casual users of the Internet are aplenty, there is a lack of 'cyber talent', and this could be a gap that provides a possible vulnerability.[40] This is partly due to a massive global demand that stretches an already small, existing pool of people.[41] The Cisco 2014 Annual Security Report has reinforced this gap with its estimation that by 2014, the industry will still be short of more than a million security professionals across the globe.[42]

c. Lack of attribution of Cyber Attacks

There is a challenge to attribute attacks to specific perpetrators in cyberspace as identities can

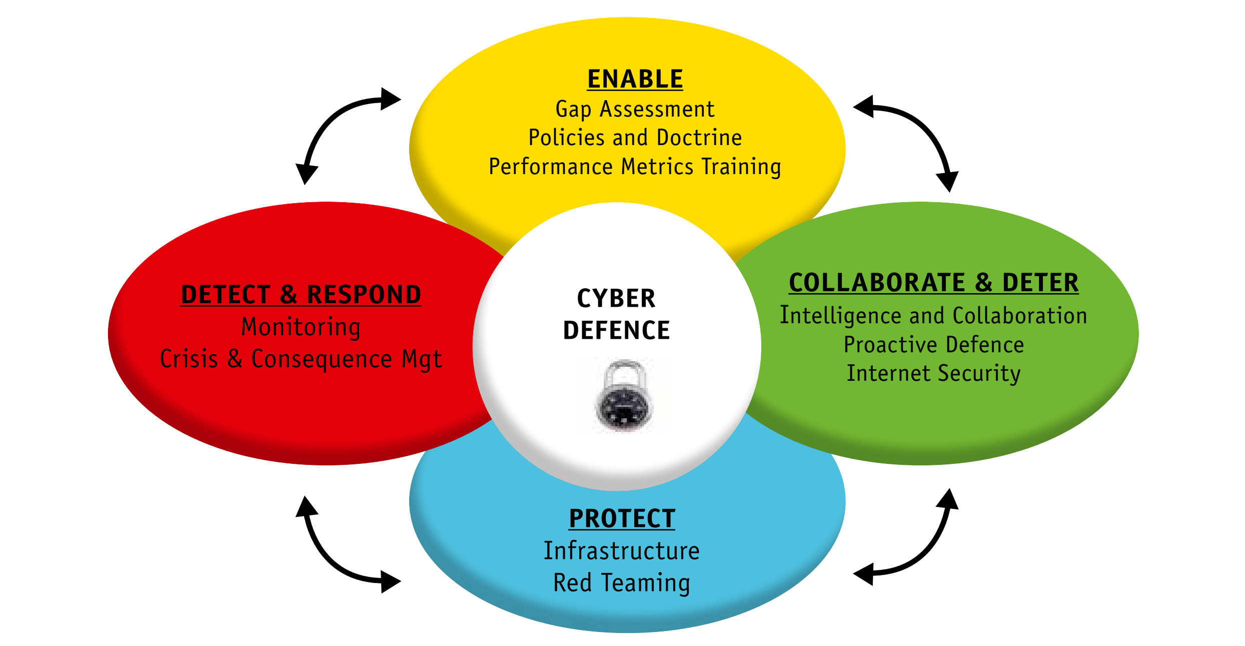


Figure 3: Proposed Cyber Defence Framework

be easily masked. Even if that is possible, there is the added difficulty in determining if he is a representative of a state, a state-sponsored actor, a terrorist or just a prankster. As governments cannot be easily made liable for cyber-attacks done by private hackers working individually, retaliation becomes an unlikely scenario. Consequently, if the attacker is misidentified, there is a possibility of harming innocent individuals or targeting the wrong place.[43]

d. **Dilemma of Individual Privacy Versus National Security**

In ensuring cyber security, the above-mentioned would be a common tussle. The revelation by former Central Intelligence Agency (CIA) technical worker, Edward Snowden, in June 2013 that the National Security Agency (NSA) was collecting millions of telephone records and monitoring internet data to track individuals suspected of terrorism and spying highlights this fragile balance.[44] In response, US President Barack Obama defended the surveillance programme as a modest encroachment on privacy and necessary to protect the US from terrorist attacks. Therefore, while individuals value their privacy, it may have to give way in the interest of national security.

e. **Lack of boundaries in Cyber space**

Cyber space has no boundaries which would mean that national boundaries are not deterrents as perpetrators can conduct attacks from anywhere as long as they have access to the Internet. This increased interconnection in the world as well as the speed of proliferation of new technological products offers increased opportunities for cyber-attacks.

I seek to propose a cyber defence framework that could be undertaken along the key tenets of Enable, Collaborate and Deter, Protect and Detect & Respond. It is important that a defence-in-depth approach is taken so as to provide overall resilience against any cyber threats.

A. Enable

This tenet is about understanding and improving the current state of preparedness against any cyber threats.

(1) *Gap Assessment*

The start state would be to make an assessment of the cyber security maturity and identification of areas of vulnerability as well as technological readiness. Comparison with the industry regulations, standards and best practices would be the start state for such an assessment. Even after the establishment of a cyber security system, vulnerability assessments which help to identify and prioritise network vulnerabilities should still be conducted periodically and after security updates. The outcomes would be to generate comprehensive reports and databases identifying known vulnerabilities that can be exploited.[45]

NATO's defence clause states that an attack against one member of NATO "shall be considered an attack against them all" and opens the way for members to take action against the aggressor—including the use of armed force—to restore security.

(2) *Policies and Doctrine*

There is a need to build up the policies and doctrines to manage and respond to cyber threats. It would be necessary to develop an overarching cyber security doctrine rather than a patchwork of policies and agencies dealing with cyber threats. The doctrine could define several aspects of cyber security, including defence against attacks, steps taken to deter attacks, safe usage of the networks as well as the kinds of attacks that will be responded to.[46] This process should include a review, update and enforcement of security policies and legislation as well as the establishment of baseline control over network access and usage protocols.

(3) *Performance Metrics*

While it may not be possible to measure in the beginning, it is necessary to develop metrics to assess the operational effectiveness of cyber defence measures as a function of time. This would enable better decision making about the cyber defence investments required. Such measurements can also help decide on the continuation or termination of cyber defence measures, as well as providing important hindsight. It is noteworthy to consider benchmarking. However, proxies may be necessary as the information gathered would inherently be classified in nature.

(4) Training

There would be a need to institutionalise the training of personnel. Sustaining a continued pool of trained personnel who are technologically skilled and cyber-savvy would be essential. More importantly, they must have hands-on skills and not just academic knowledge. The launching of the first and only Cyber Security Academy amongst the Institutes of Higher Learning by Singapore Polytechnic in December 2013 could be one such avenue to cater to this training demand.[47]

B. Collaborate & Deter

This tenet would involve deterring would-be perpetrators through establishing collaborative networks as well as establishing a proactive threat defence.

(1) *Intelligence and Collaboration*

Intelligence is a key component of this tenet and there is a need for defence agencies to work closely with local and regional counterparts to monitor and disrupt possible threats as well as to identify and pre-empt emerging threats. Feedback should be gathered from all available means and 'live' information sharing among counterparts should be established to enhance situational awareness and collaboration against cyber threats. Such alliances and defences must be on 24/7 alert to ensure constant vigilance, as well as to deter would-be perpetrators. Besides deterring external threats, there is a need to deter and mitigate against possible insider threats. This could be done through strengthening workforce communications, workforce accountability, internal monitoring and information management capabilities.[48]

(2) *Proactive Defence*

Besides the setup of a responsible agency for cyber defence as a deterrent, there may also be a need to deploy proactive threat defences to deter potential adversaries. One such mechanism looked into by the US Air Force is the use of cyber deception capabilities to trick and manipulate cyber attackers. It is intended to be used solely on Defence Department networks and be concealed from adversaries, all while impeding attackers by increasing the costs of their actions while providing increasingly limited gains.[49]

(3) *Internal Security*

Besides external deterrence, there is also a need to protect against insider threats. As people are the first line of defence in sustaining good cyber 'hygiene' and reducing internal threats, there is a need for constant communication as well as the need to impose security restrictions. Existing security classifications as well as punishment for offences may have to be increased due to the sensitivity of information in this domain.

C. Protect

This tenet would involve designing and implementing a cyber defence infrastructure so as to deny any possibility of an attack.

(1) *Infrastructure*

As mentioned by former US Deputy Defence Secretary William Lynn, *"If an attack will not have its intended effect, those who wish us harm will have less reason to target us through cyberspace in the first place."*[50] An important part of this build up would be applying Disruption-Tolerant Network (DTN) technologies for both centralised and decentralised networks. DTN architecture revolves around a data-centric model and not the traditional network-centric model and helps ensure that data is protected at all times and not only in transmission.[51]

(2) *Red Teaming*

As part of the build-up of a cyber defence infrastructure, the employment of white-hat hackers to perform red teaming could be used to perform security evaluations of hardware security, software security and procedural security as well as to uncover potential vulnerabilities. Red teams are one of the only qualitative metrics in today's system technology discipline, thus playing an essential role.[52] The overall goal of employing the red teams is to improve system defences.

D. Detect & Respond

This tenet is about the response as well as the investigation of any cyber threats.

(1) *Monitoring*

To be able to respond, you have to first be able to see the adversary. There is therefore a need to build detection and analytical capabilities. One way would be the inclusion of anomaly detectors to spot irregular traffic and report the findings. A truly sound security prototype will employ anomaly-based detectors alongside signature-based detectors, as neither type of detector, by itself, is fool proof. Using the two systems together properly and in serial will drastically improve a network's security posture.[53]

(2) *Crisis and Consequence Management*

Besides containing the effects of cyber-attacks, there is a need to ensure a quick recovery. Formalising the business processes for response and recovery will help to build resilience. Cyber gaming on various scenarios can also be performed to test and improve personnel response capabilities. One example of a large scale cyber exercise is 'Cyber Storm', a pseudo cyber-attack coordinated through the US Department of Homeland Security's National Cyber Security Division which tested how senior leaders of the US government would respond to a cyber incident of national significance. The first 'Cyber Storm' was conducted over five days in 2006 and involved more than 100 public and private organisations in five different countries.[54]

CONCLUSION

While we may never know when a cyber threat will ever strike, we do know that the trends are on a perennial increase and thus necessitate continued vigilance. We need to adopt an attitude where we presume that the adversary is constantly on the networks. As seen by the various examples, it is hard to pinpoint likely threats as cyber threats can be unleashed by nations, organisations or even individuals. As such, the recommended framework is proposed to ensure a swift response to any cyber threat. In conclusion, I quote the following which highlights our strong commitment to cyber defence:

> *"You may think you are anonymous. We will make that extra effort to find out who you are."*
>
> *– Singapore Prime Minister, Lee Hsien Loong*[55]

ENDNOTES

[1] Barrack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," *The White House*, (2009), https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

[2] Internet World Stats, "Internet Growth Statistics," http://www.internetworldstats.com/emarketing.htm.

[3] David Alexander, "Pentagon to treat cyberspace as "operational domain," *Reuters*, (2011), http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714.

[4] Grace Chng, "Singapore's cyber defence firepower gets $130m boost," *The Straits Times*, (2013), http://news.asiaone.com/news/singapore/singapores-cyber-defence-firepower-gets-130m-boost.

[5] Pierluigi Paganini, "Cyber threats from military sector to business," *Security Affairs*, (2012), http://securityaffairs.co/wordpress/1575/security/cyber-threats-from-military-sector-to-business.html.

6. Mary Johnston, "High Density Power Requirement -Can your Data Center Support it?? *DataSite*, (2014), http://datasitecolo.com/wp-content/uploads/2014/12/IoT-Graphic.png

7. Tyler Thia, “Country-to-country cyberattacks deemed OK by users,” *ZDNet Asia News*, (2011), http://www.zdnetasia.com/country-to-country-cyberattacks-deemed-ok-by-users-62202005.htm.

8. T O’Connor, “The Cyberterrorism Threat Spectrum,” (2011), http://www.drtomoconnor.com/3400/3400lect06a.htm.

9. Emil Protalinski, “Chinese spies used fake Facebook profile to friend NATO officials,” *ZDNet*, (2012), http://www.zdnet.com/blog/facebook/chinese-spies-used-fake-facebook-profile-to-friend-nato-officials/10389?tag=content;siu-container.

10. Ian Traynor, “Russia accused of unleashing cyberwar to disable Estonia,” *The Guardian*, (2007), http://www.theguardian.com/world/2007/may/17/topstories3.russia.

11. The Economist, “War in the fifth domain,” (2010), http://www.economist.com/node/16478792.

12. Paulo Shakarian, “Stuxnet: Cyberwar Revolution in Military Affairs,” *Small Wars Journal*, (2011), http://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf.

13. Ibid.

14. Peter Bright, “Stuxnet apparently as effective as a military strike,” *ARS Technica*, (2010), http://arstechnica.com/tech-policy/news/2010/12/stuxnet-apparently-as-effective-as-a-military-strike.ars.

15. Emil Protalinski, “Chinese spies used fake Facebook profile to friend NATO officials,” *ZDNet*, (2012), http://www.zdnet.com/blog/facebook/chinese-spies-used-fake-facebook-profile-to-friend-nato-officials/10389?tag=content;siu-container.

16. AFP News, Singapore PM's website hacked by Anonymous, (2013),https://sg.news.yahoo.com/singapore-pms-website-hacked-anonymous-175123528.html.

17. Ibid.

18. Ibid.

19. AFP News, Singapore PM's website hacked by Anonymous, (2013),http://news.asiaone.com/news/singapore/singapore-pms-website-hacked-anonymous

20. Ibid.

21. Tony Morbin, “Russia suspected of Ukraine cyber attack,” *SC Magazine*, (2010), http://www.scmagazineuk.com/russia-suspected-of-ukraine-cyber-attack/article/337578/.

22. Ben Farmer, “Ukraine cyber war escalates alongside violence,” *The Telegraph*, (2014), http://www.telegraph.co.uk/news/worldnews/europe/ukraine/10860920/Ukraine-cyber-war-escalates-alongside-violence.html.

23. Ibid.

24. Sky News, “Cyber Defence Unit Set Up By UK Military,” (2013), http://news.sky.com/story/1147919/cyber-defence-unit-set-up-by-uk-military.

25. Rachel Lim, “New hub to defend against cyber threats,” *Cyberpioneer*, (2013), http://www.mindef.gov.sg/content/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2013/jun/30jun13_news2updated.html#.VBGpOXlxmcw.

26. Michael Barkoviak, “US Military Creates Cyber Defense Department,” *Daily Tech*, (2009), http://www.dailytech.com/US+Military+Creates+Cyber+Defense+Department/article15513.htm.

27. The Washington Post, “Cyberwar, out of the shadows,” (2013), http://articles.washingtonpost.com/2013-02-03/opinions/36728784_1_forces-national-mission-cyber-command.

28. The Washington Post, “Pentagon to boost cyber security force”.

29. Ibid.

30. BBC News, “UK to create new cyber defence force,” (2013), http://www.bbc.com/news/uk-24321717.

31. Ibid

32. Ibid

33. Paul Kallender-Umezu, “Experts: Japan's New Cyber Unit Understaffed, Lacks Skills,” *DefenseNews*, (2013), http://www.defensenews.com/article/20130709/DEFREG03/307090007/Experts-Japan-s-New-Cyber-Unit-Understaffed-Lacks-Skills.

34. Ibid

35. Adam Baddeley, “Regional Cyber: Defence and Offence,” (2012), http://www.asianmilitaryreview.com/regional-cyber-defence-and-offence/.

36. Ellyne Phneah, “Singapore creates operations hub to beef up cyberdefense,” *ZDnet*, (2013), http://www.zdnet.com/singapore-creates-operations-hub-to-beef-up-cyberdefense-7000017521/.

37. Rachael Lim, “New hub to defend against cyber threats” *ZDnet*, (2013), http://www.zdnet.com/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict-7000031064/.

38. Steve Ranger, “NATO updates cyber defence policy as digital attacks become a standard part of conflict,” *ZDNet*, (2014) http://www.zdnet.com/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict-7000031064/.

39. Ibid

40. Warwick Ashford, “NAO details progress and challenges of UK cyber security strategy,” *ComputerWeekly.com*, (2013), http://www.computerweekly.com/news/2240177866/NAO-details-progress-and-challenges-of-UK-cyber-security-strategy.

41. Brian Leonal, “Cybersecurity Skills Shortage Poses Threat in Singapore,” *Bloomberg*, (2014), http://www.bloomberg.com/news/2014-06-22/cybersecurity-skills-shortage-looms-in-singapore-southeast-asia.html.

42. Cisco, “Cisco 2014 Annual Security Report,” http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

43. Dimitar Kostadinov, “The Attribution Problem in Cyber Attacks,” *Infosec Institute*, (2013), http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/.

44. Glenn Greenwald, Ewen MacAskill and Laura Poitras, “Edward Snowden: the whistleblower behind the NSA surveillance revelations,” *The Guardian*, (2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

45. Spirent Communications, “Achieving Cyber Security Readiness Within an Evolving Threat Landscape,” *White Paper*, (2013)

46. IDG Reporter, “Experts call for cyber security doctrine from US government,” *CNME*, (2012), http://www.cnmeonline.com/news/experts-call-for-cyber-security-doctrine-from-us-government/.

47. Special Report, “Singapore Poly launches Cyber Security Academy,” *iN.SG*, (2014), http://www.ida.gov.sg/blog/insg/special-reports/singapore-poly-launches-cyber-security-academy/.

48. US Department of Defense, “Department of Defense Strategy for Operating in Cyberspace,” (2011)

49. Joey Cheng, “Air Force looks to get proactive on cyber defense,” Defense Systems, (2014), http://defensesystems.com/articles/2014/08/12/air-force-cyber-resilience.aspx.

50. David Alexander, “Pentagon to treat cyberspace as "operational domain", (2011) http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714.

51. COL Bruce D. Caulkins, “Proactive Self Defense in Cyberspace,” *The Land Warfare Papers*, (2009), n._72 http://www.ausa.org/publications/ilw/ilw_pubs/landwarfarepapers/Documents/LWP72.pdf.

52. Bradley J. Wood, O. Sami Saydjari and Victoria Stavridou, “A Proactive holistic approach to Strategic Cyber Defense,” *SRI International, Cyber Defense Research Center, Systems Development Laboratory*, http://www.cyberdefenseagency.com/publications/A_Proactive_Holistic_Approach_to_Strategic_Cyber_Defense.pdf.

53. COL Bruce D. Caulkins, “Proactive Self Defense in Cyberspace,” *The Land Warfare Papers*, (2009), n._72 http://www.ausa.org/publications/ilw/ilw_pubs/landwarfarepapers/Documents/LWP72.pdf.

54. Heidi Price, “Cyber Attack Scenarios Test Responses,” *SEI*, (2008), http://www.sei.cmu.edu/library/abstracts/news-at-sei/03feature200803.cfm.

55. Jermyn Chow, “No effort spared to find hackers: PM Lee,” *The Straits Times*, (2013), http://www.straitstimes.com/breaking-news/singapore/story/singapore-spares-no-effort-hunt-down-cyber-threats-pm-lee-20131106.

ME5 Seah Ser Thong, Calvin is currently attending the 46th Goh Keng Swee Command and Staff Course. He is an Army Engineer by vocation. ME5 Seah holds a Bachelors of Engineering in Mechanical & Production Engineering from NTU, the Nanyang Technological University Masters of Science in Industrial and Systems Engineering from the National University of Singpaore (NUS) as well as a Masters of Science in Defence Technology and Systems from NUS, obtained under the SAF Postgraduate Award. He is a Business Excellence Assessor, National Innovation and Quality Circle Assessor as well as an American Society of Quality Judge. He was a winner of the 1st and Merit Prizes for his co-written essays at the 2013/2014 Chief of Defence Force Essay Competition and a winner of the Commendation Award at the 15th Chief of Army (COA) Essay Competition in 2014. His co-written article, 'Learning from Mother Nature: Biomimicry for the Next Generation SAF,' was recently published in the August issue of the Australian Defence Force (ADF) Journal.