SURVIVABILITY OF A SMART NATION

by ME6 Calvin Seah Ser Thong

Abstract:

In this age of technology, the trend of cyber attacks is ever increasing and, no nation is spared. Even in Singapore, it has been reported that 16 waves of targeted cyber attacks have been surfaced to the Cyber Security Agency of Singapore from April 2015 to June 2016. More recently, two waves of cyber attacks disrupted StarHub's broadband network in October 2016. On both occasions, subscribers' bug-infected machines turned into zombie machines that carried out distributed denial-of-service attacks on StarHub's network. Following these attacks, security experts have warned that armies of unsecured 'smart' devices like web cameras could become a rising force of disruption. As Singapore embarks on the Smart Nation initiative to transform itself into the world's first true Smart Nation, this could potentially be a Centre of Gravity that could pose as a critical vulnerability. This essay explores this notion by firstly examining Singapore's Smart Nation Initiative. Next, it will look at Clausewitz's Centre of Gravity concept and explore if the Information and Communications Network could become the Centre of Gravity of a 'Smart Nation'. Finally, the essay will propose recommendations to bolster a Smart Nation's security by adopting from Dr David Wilkes' Survivability Onion.

Keywords: Cyber Attacks; Vulnerability; Security; Increasing; Force

INTRODUCTION

> *"Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."*
>
> National Research Council[1]

In February 2016, hackers shut down the internal computer system at the Hollywood Presbyterian Medical Centre for a ransom of almost $3.7 million. The cyber attack forced the centre to revert to paper documentation and to send 911 patients to other hospitals.[2] Communications between physicians and medical staff became bogged down by paper records and doctors' notoriously messy handwriting.[3] Back home, it has been reported that 16 waves of targeted cyber attacks have been surfaced to the Cyber Security Agency (CSA) of Singapore from April 2015 to June 2016.[4] More recently, two waves of cyber attacks disrupted StarHub's broadband network in October 2016. On both occasions, subscribers' bug-infected machines turned into zombie machines that carried out distributed denial-of-service attacks on StarHub's network.[5] Following these attacks, security experts have warned that armies of unsecured 'smart' devices like web cameras could become a rising force of disruption. As Singapore embarks on the Smart Nation initiative to transform itself into the world's first true Smart Nation, could this be a Centre of Gravity that could pose as a critical vulnerability? This essay explores this notion by firstly examining Singapore's Smart Nation Initiative. It would next look at Clausewitz's Centre of Gravity concept and explore if the Information and Communications Network could become the Centre of Gravity of a 'Smart Nation'. Finally, the essay would propose recommendations to bolster a Smart Nation's security by adopting from Dr David Wilkes' Survivability Onion.

SMART NATION INITIATIVE

On 24th November 2014, Prime Minister Lee Hsien Loong launched the Smart Nation Initiative to harness technology to make life better for Singaporeans (*Figure 1*).[7] During the Smart Nation Innovations 2015 event, the Infocomm Development Authority (IDA) of Singapore revealed the development of the Smart Nation Platform consisting of infrastructure and technology to support the roll out of new capabilities to citizens, businesses, and the government. This would eventually enable connectivity across smart, connected devices with applications such as remote health monitoring, remote learning and and even self-driving vehicles.[8] Besides infrastructure and technology, the Big Analytics Skills Enablement initiative has also been announced to equip more people with skills in big data and analytics. As Singapore gears up to be the world's first Smart Nation, it's relying on standards to create a common framework for good practice and to enable innovation. Three key areas that are being trialled are Telemedicine, Urban Living and Urban Mobility. In alignment to the Smart Nation Initiative, MINDEF has also established a committee to chart the way forward to realise our vision of Smart Defence. Within the SAF, data analytics, coupled with predictive engines, will offer sustained sense-making and intelligence to detect security threats to Singapore.

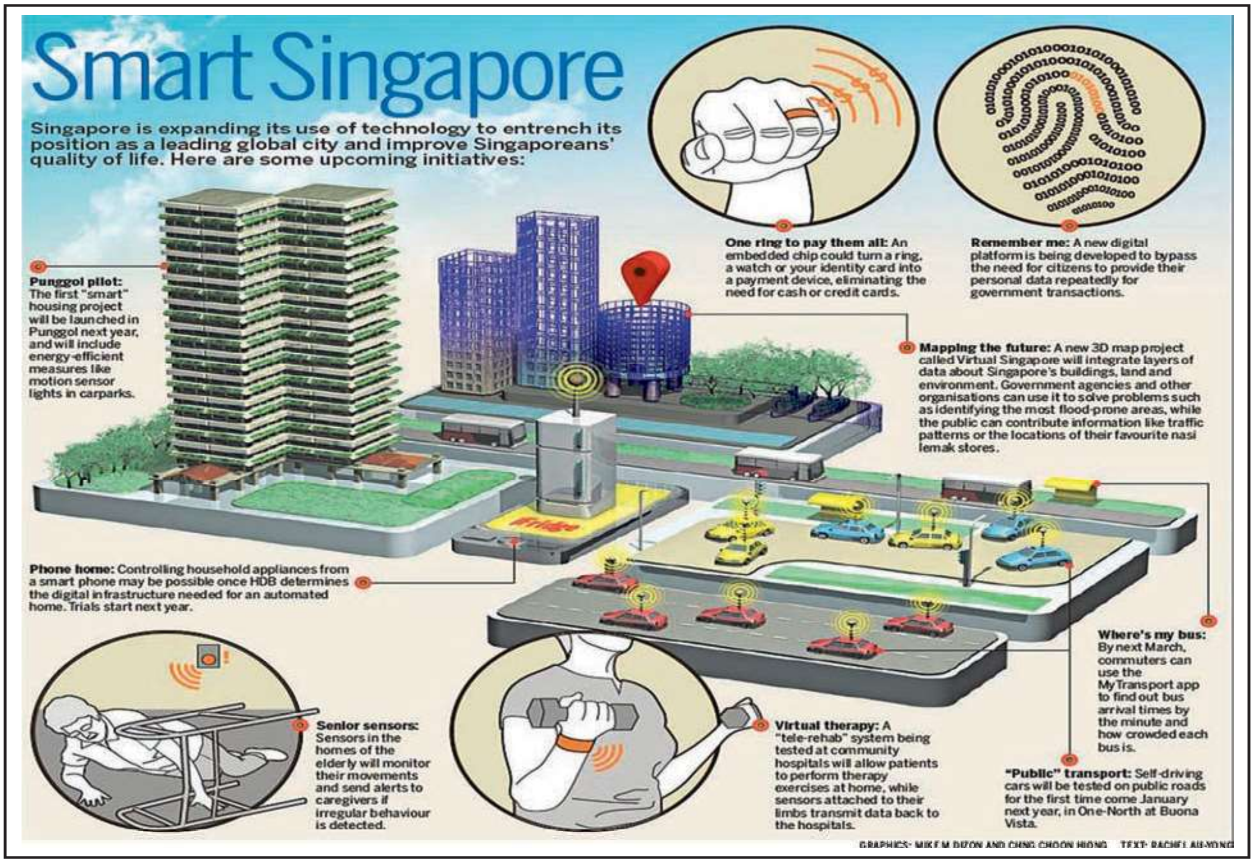

Smart Singapore
Singapore is expanding its use of technology to entrench its position as a leading global city and improve Singaporeans' quality of life. Here are some upcoming initiatives:
One ring to pay them all: An embedded chip could turn a ring, a watch or your identity card into a payment device, eliminating the need for cash or credit cards.
Remember me: A new digital platform is being developed to bypass the need for citizens to provide their personal data repeatedly for government transactions.
Punggol pilot: The first "smart" housing project will be launched in Punggol next year, and will include energy-efficient measures like motion sensor lights in carparks.
Mapping the future: A new 3D map project called Virtual Singapore will integrate layers of data about Singapore's buildings, land and environment. Government agencies and other organisations can use it to solve problems such as identifying the most flood-prone areas, while the public can contribute information like traffic patterns or the locations of their favourite nasi lemak stores.
Fridge
Phone home: Controlling household appliances from a smart phone may be possible once HDB determines the digital infrastructure needed for an automated home. Trials start next year.
Where's my bus: By next March, commuters can use the MyTransport app to find out bus arrival times by the minute and how crowded each bus is.
Senior sensors: Sensors in the homes of the elderly will monitor their movements and send alerts to caregivers if irregular behaviour is detected.
Virtual therapy: A "tele-rehab" system being tested at community hospitals will allow patients to perform therapy exercises at home, while sensors attached to their limbs transmit data back to the hospitals.
"Public" transport: Self-driving cars will be tested on public roads for the first time come January next year, in One-North at Buona Vista.
GRAPHICS: MIKE M DIZON AND CHNG CHOON HIONG TEXT: RACHEL AU-YONG

Figure 1: Towards a Smart Nation.[6]

New applications will help streamline corporate services and raise the productivity of administrative and corporate functions. At the individual level, smart technologies will be employed to improve work life in MINDEF.[11]

THE CENTRE OF GRAVITY

The essence of every profession is expressed in the writings of its unifying theorists. For the military, Prussian writer Carl von Clausewitz is regarded as one of the most influential military theorists whose views on the character of war have held up best over the past two centuries.[12] In his book, '*On War*', Clausewitz defined the Centre of Gravity (CoG) as a focal point that if attacked, causes a loss of overall balance. He derived the idea from 19th century physics and believed that it was the key factor in military planning.[13] He surmised that the CoG represents the point where the forces of gravity converge within an object. Thus, striking at the CoG with enough force can cause the object to lose its balance and fall.[14] So, is there a CoG for a Smart Nation that could be a potential vulnerability?

Currently, the 'Cyber' domain that information technology and communication systems depend on is a source of national power.[15] Unlike the traditional domains of air, sea, land and space, it is man created and does not seem to have physical manifestations. Thus, while the infrastructures in the four traditional domains are distinct CoGs that provide lucrative targets for threat vectors, the 'Cyber' domain seems to be devoid of any CoG. But when we study closer, the Clausewitzean principles of key terrain can still be applied to the 'Cyber' domain as it has physical manifestations such as data centres, internet service providers and undersea cables. In his article, 'The key terrain of cyber,' John Mills demonstrates that the 'Cyber' domain has several elements of key terrain that Clausewitz might not have foreseen but would possibly include if he updated his theory of key terrain.[16]

By identifying the CoGs, we can identify sources of power as well as sources of critical vulnerability. Adapting such a bifocal vantage point for a Smart Nation in the areas of critical infrastructure vulnerabilities and the security of the 'Cyber' domain could enable the development of defence mechanisms.[17] Current reality has shown that the more technologically reliant an actor is, the more susceptible they will be to attacks on their information systems. Actors that become reliant on advanced technology may become increasingly vulnerable to issues of friction and fog of war due to the actions of an aggressor perpetuating a cyber war. Attacks would likely not be limited to only military networks and this complicates an actor's capacity to respond as government or, civilian networks may not be as protected nor have the redundancies built into them for a quick recovery.

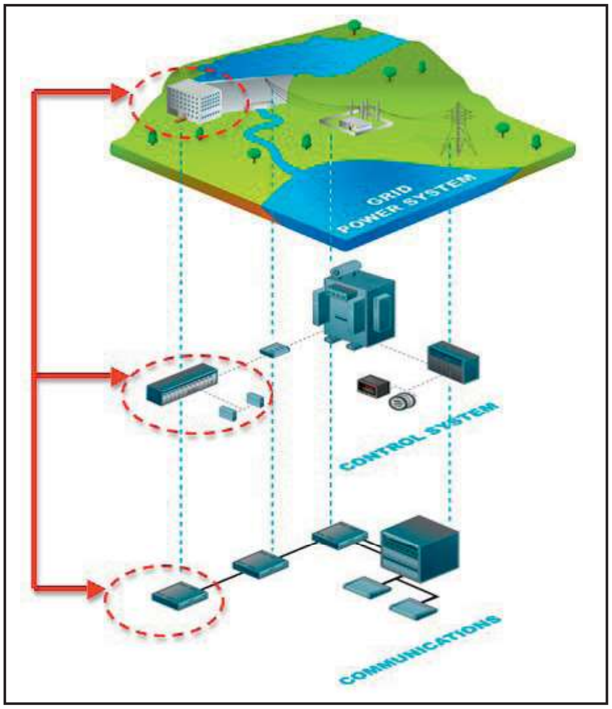


Figure 2: Critical Infrastructure – A potential CoG.[21]

The longer an information based society is disrupted, the greater the damage and public confusion. If the CoG provides for unity within an actor, destroying or degrading this unity can hamper an actor's capacity to engage in effective action within the system.[18] In addition, cyber attacks on national level 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 (*Figure 2*).[19] In Singapore's context, co-ordinated cyber attacks on critical sectors such as energy, banking and telecommunications can potentially cripple the country, and a Smart Nation with its deep reliance on Infocomm Technology (ICT) will definitely be vulnerable.[20] Furthermore, these cyber attacks may be potential precursors to further military action.

THE 'SMART' BATTLEFIELD

Currently, hackers have yet to actively target smart technologies presumably because not enough electronic devices are connected to the Internet for a cyber attack to be worthwhile. But this situation could change by 2020 when the number of smart devices produced hits an estimated 26 billion units based upon the upward trend of smartphones, Personal Computers (PCs) and tablets use. This could provide the lure for cyber-criminals to begin scouring the technology for weaknesses. What is even more troubling is that smaller smart devices are less likely to have encryption and authentication capabilities due to their limited computing power. It is not just individuals who will be targeted by cyber-criminals; organisations too can be vulnerable when employees bring unsecured smart devices to work.[22] A spate of data breaches at United States (US) companies such as JPMorgan Chase, Home Depot, and Target in 2014 has surfaced questions about the effectiveness of the private sector's information security.[23] A malware code associated with the Russian hacking operation dubbed Grizzly Steppe that was discovered within the system of the US electrical grid's Vermont utility in December 2016 underscores the vulnerabilities of a nation's electrical grid.[24] Power cuts that hit the Ukrainian capital, Kiev due to cyber attacks in 2015 and 2016 prove that utilities can similarly be hacked.[25]

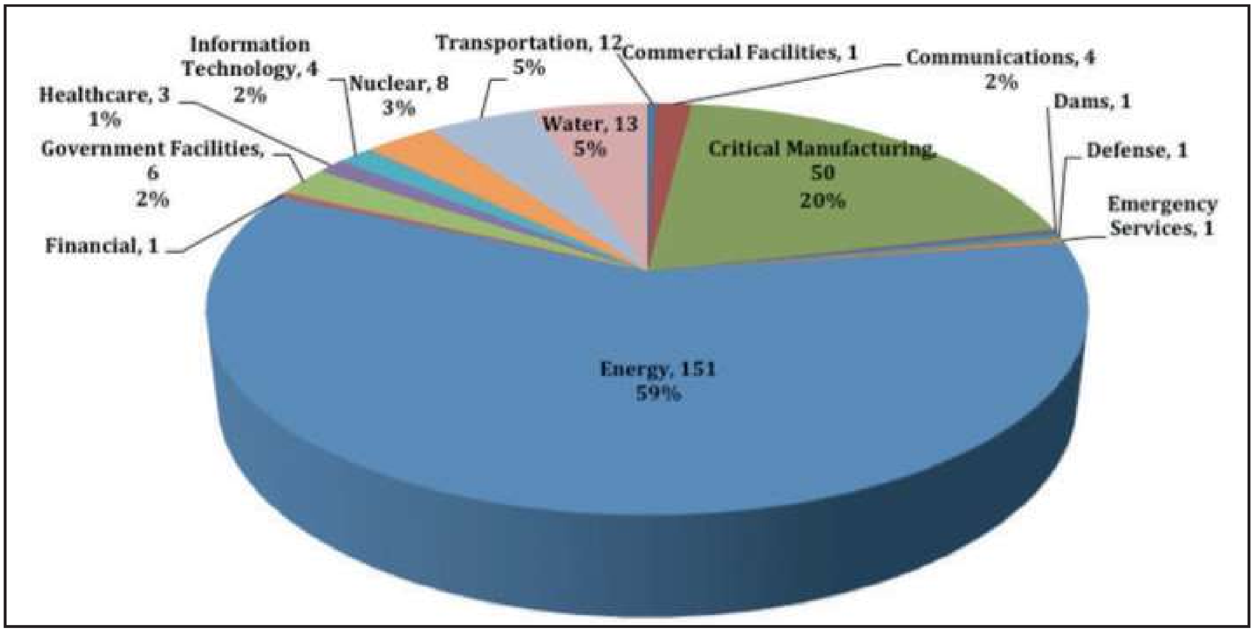


Figure 3: Apportionment of malicious cyber-attacks in 2013.[29]

The cyber attacks on StarHub in October 2016 are reminders of such a reality in Singapore. Following these attacks, security experts warn that armies of unsecured 'smart' devices like web cameras could become a rising force of disruption. Mr Alex Tay, Netherlands-based digital security firm Gemalto's Associations of South East Asian Nation (ASEAN) head of identity and data protection has proclaimed that these Internet-connected devices are especially vulnerable as there are no regulations over their security standards. "The lack of consideration for security controls within such devices is giving hackers the ability to take ownership of them," said Mr Tay.[26] For instance, devices such as routers and network cameras have default credentials and passwords that users rarely change. As such, cyber-criminals can turn them into zombie machines that flood targeted systems in a distributed denial-of-service (DDoS) attack.[28]

In a 2013 Monitor report, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) revealed intensification for brute force attacks against control systems mainly belonging to the energy sector (*Figure 3*).[29] Notwithstanding, cyber attacks can even be performed on national infrastructures such as traffic lights. As demonstrated in 2014, Cesar Cerrudo of global security consultancy IOActive, Inc used his laptop to hack Washington City's traffic system. Like his previous tests in Manhattan and elsewhere, Cerrudo was able to turn red lights green and green lights red. He could have unleashed the following scenarios: gridlocking the whole town, turning a busy thoroughfare into a fast-paced highway, paralysing emergency responders, or shut down all roads to the Capitol.[30] Such threats seem highly plausible and inevitably attractive to cyber-criminals due to the hyper connectivity of a Smart Nation. Chaos and confusion could be caused if critical infrastructure

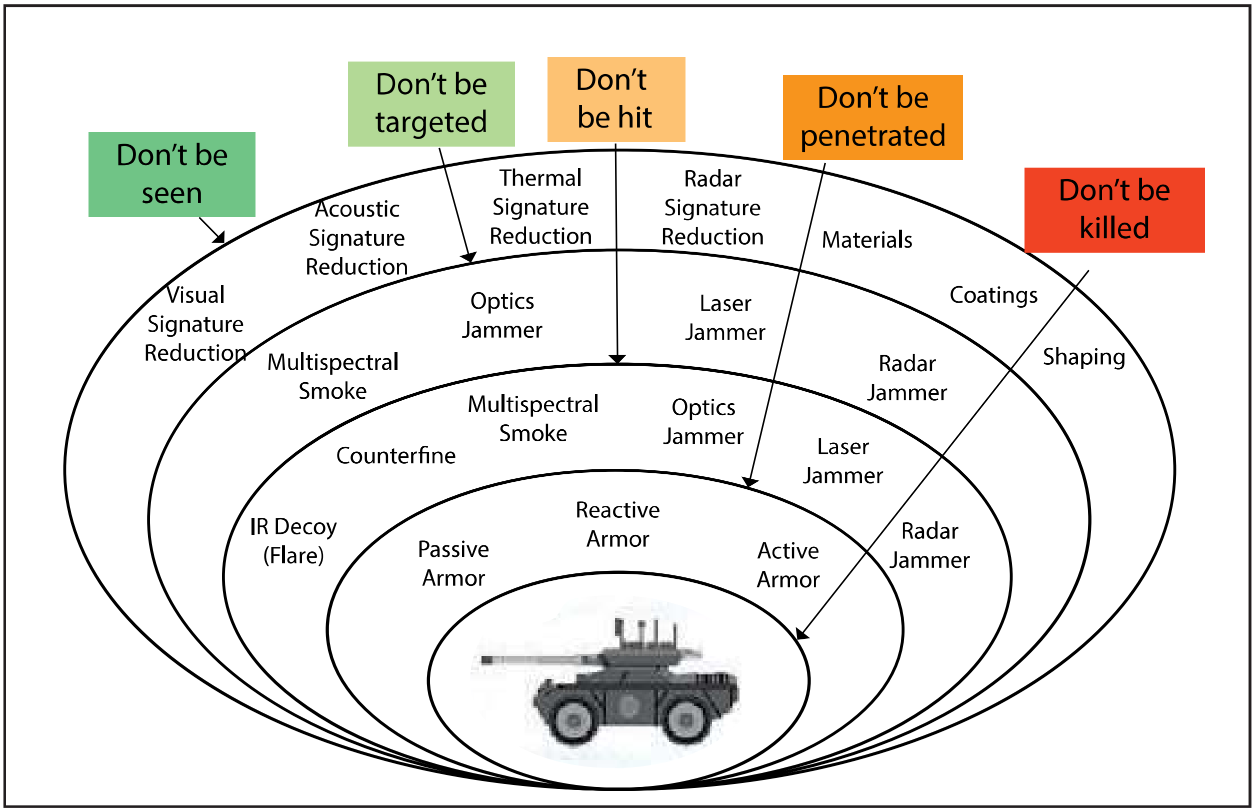


Figure 4: The Survivability Onion.[32]

and systems were to fall into the wrong hands, and spoof messages and transmissions were sent out.[33]

DEFENDING THE 'SMART' BATTLEFIELD

In recognising the threat of cyber attacks to its networks and systems, the SAF had established the Cyber Defence Operations Hub (CDOH) in 2013 to step up its cyber defence capabilities. Defence Minister Dr Ng Eng Hen had also announced that in enhancing cyber defence, the SAF will employ more artificial intelligence and big data analytics to detect and respond to cyber threats. The SAF will also build greater security into software design and network infrastructure to make them more resilient and resistant to cyber attacks. In parallel, cyber engineers and researchers from Defence Science Technology Agency (DSTA) and Defence Science Organisation (DSO) are working on advanced cyber defence solutions for MINDEF and the SAF. They aim to secure its networks, respond to cyber attacks and to safeguard its classified information and systems.[32]

In Singapore's bid to create the Smart Nation, various initiatives have been put in place to defend Singapore's 'Cyber' domain. CSA was set up in 2015 to co-ordinate the country's national efforts in cyber security. The Singapore Government has also embarked on a comprehensive blueprint that maps out Singapore's long-term approach towards securing its cyber space against incursions and to grow the ICT sector locally. Launching the national cyber security strategy at the opening of the first Singapore International Cyber Week in October 2016, Prime Minister Lee recognised that cyber security is 'an issue of national importance' as the country becomes more connected in its mission to become a Smart Nation.[34] One key prong of the strategy is directing more funds into defence against attacks. Mr Lee announced that about 8 per cent of the ICT budget will be set aside for cyber security spending, up from about 5 per cent before. The new proportion is similar to what other countries spend—Israel stipulates that 8 per cent of its total government IT budget must go to cyber

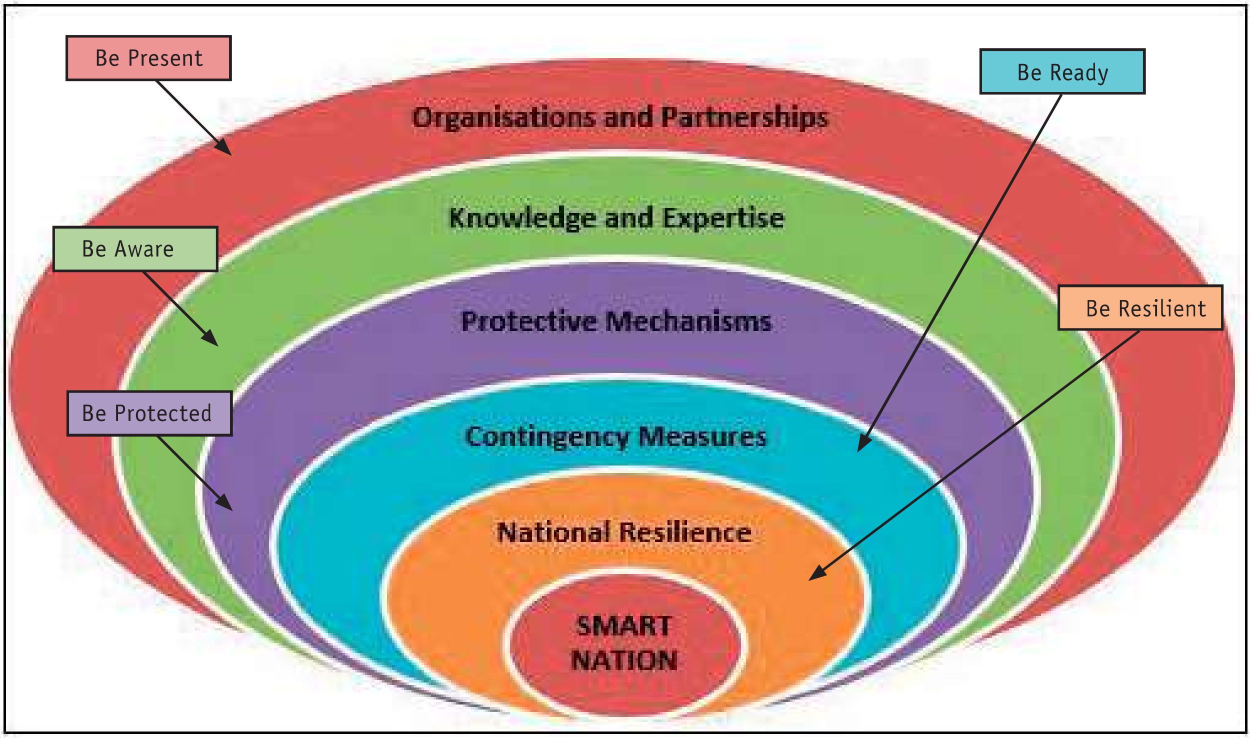


Figure 5: Adapting the Survivability Onion to Defending the Smart Nation

security, while South Korea channels as much as 10 per cent.[35]

So what more can be done to defend a Smart Nation? It is imperative to note that there never will be a 'one size fits all' solution, thus it is important to consider all possible options together. In his lecture on staying alive in the 21st Century, Dr Wilkes uses the Survivability Onion to demonstrate how risks and threats can be mitigated using a layered approach. Thus, I have adapted the Survivability Onion to protect against all levels of threats through a layered approach (See *Figures 4* and *5*).[36] I would be looking at five layers of defence to mitigate against any potential threats. They are essentially to be 'Present', 'Aware', 'Protected', 'Ready' and 'Resilient'. For the first layer, the Cyber Security Agency is currently already being set up in a whole of government approach as earlier mentioned. In terms of partnership, Singapore is looking to partner with other ASEAN member states and has been deploying 'cyber diplomacy' by building alliances with other countries, both to swop expertise, such as the latest in attack methods, and to regularly exercise and test its defences.[37] These measures ensure that Singapore is ever-present in all aspects of defending our Smart Nation. Next, I would be delving further into the other four layers of Knowledge & Partnerships, Protective Mechanisms, Contingency Measures and National Resilience.

BE AWARE – KNOWLEDGE AND EXPERTISE

Cultivate Cyber Security Experts

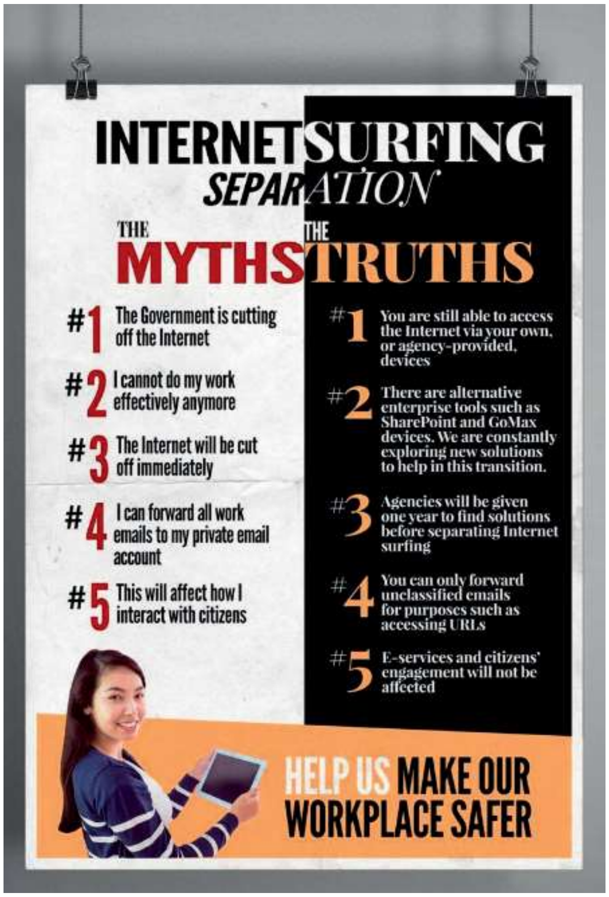
At the core of any cyber security initiative would be the need to build up a core of cyber security experts. It has been predicted that the demand for cyber security expertise will continue to increase. Currently, Singapore's educational institutes are starting programmes and initiatives to attract more talents for the cyber security workforce. The National University of Singapore and the Singapore Institute of Technology are starting undergraduate degree programmes in Information Security. The Nanyang Technological University and the Singapore Management University already have pre-existing cyber specialisation courses and modules while the Singapore University of Technology and Design has plans for a Master's degree in Cyber Security in future.[38] However, with the dire shortage of Cyber Security professionals worldwide, Singapore could consider tapping national servicemen with cyber security skills and knowledge.[39] With the announcement that pre-enlistees would be able to choose from 33 vocations across the SAF, police and civil defence in 2017, cyber security could be added as one of the preferred vocations that pre-enlistees could choose from.[40] Additionally, we could also consider dual vocations for National Servicemen who are already cyber security professionals.

Cyber Security Knowledge

It is not enough to have a group of experts in cyber security as cybersecurity is everyone's business and, a Smart Nation can only be as strong as its weakest link. It is therefore important for cyber security to be taught and shared with the different demographics of people in Singapore. A group that should not be missed would be new citizens, permanent residents as well as foreign workers in Singapore. A case in point would be the five foreign domestic helpers working in Singapore who were radicalised through social media. Thus, the introduction of the security course for all maids intending to work in Singapore is a welcome move. As terrorism has been increasing through the spread of social media and even women and children could be influenced, the launch of the SGSecure

So what more can be done to defend a Smart Nation? It is imperative to note that there never will be a 'one size fits all' solution, thus it is important to consider all possible options together.

programme in 2016 to rally more Singaporeans, foster resilience and prepare them to handle crises in the face of the looming terror threat is an important platform to share and impart cyber security knowledge.[41]



INTERNET SURFING SEPARATION

THE MYTHS	THE TRUTHS
#1 The Government is cutting off the Internet	#1 You are still able to access the Internet via your own, or agency-provided, devices
#2 I cannot do my work effectively anymore	#2 There are alternative enterprise tools such as SharePoint and GoMax devices. We are constantly exploring new solutions to help in this transition.
#3 The Internet will be cut off immediately	#3 Agencies will be given one year to find solutions before separating Internet surfing
#4 I can forward all work emails to my private email account	#4 You can only forward unclassified emails for purposes such as accessing URLs
#5 This will affect how I interact with citizens	#5 E-services and citizens' engagement will not be affected

HELP US MAKE OUR WORKPLACE SAFER

Figure 6: Circular addressing queries over new Net access rules.[42]

BE PROTECTED – PROTECTIVE MECHANISMS

Segregating Secure E-Mail from Internet Systems

There is a need for protective safeguards. One would be to protect secure e-mail systems by segregating them from the internet system. This measure, while inconvenient to users, could guard against cyber attacks over the internet that is possible when the systems are interconnected. Surfing separation will prevent attackers from using the Internet to plant malware to access Government computers or worse, an interconnected Smart Nation. Currently, this practice has already been implemented in the Ministry of Home Affairs (MHA) and MINDEF. However, the IDA has announced that it would be implementing this measure for all public servants come June 2017.[43] Separately, a circular (*Figure 6*) was sent out to address queries over the new Net access rules. It branded claims that the Government is cutting off the Internet for civil servants as a 'myth'. Dr Vivian Balakrishnan, then Minister-in-Charge of the Smart Nation Initiative, has reinforced that cyber security is essential if Singapore is to become a smart nation. Dr Balakrishnan said: "You can't afford a breach of privacy. So, the way I look at it, cyber security is the flip side of the coin of being a Smart Nation."[44]

First Responders

Next, first responder teams would need to be formed. An example is found in local power company Singapore Power which has a 'multi-faceted' approach to defending, detecting, responding and recovering from cyber attacks in place. A Singapore Power spokesperson has stated that there is a dedicated team on the lookout for 'unusual activities' on the grid around the clock. The company also hires external companies to conduct tests on its systems. "Our measures are tested and evaluated on a regular basis internally and also by professionals who perform audits and tests to ensure that our systems and procedures remain relevant and robust," the spokesperson said.[45] The company's comments come after a Western Ukraine power company Prykarpattyaoblenergo suffered an outage on 23rd Dec 2015, causing 700,000 people and half the homes in the Ivano-Frankivsk region in Ukraine to be without electricity for several hours.[46] To enhance Singapore's overall response to any cyber emergency, teams from various companies could partner with the National Cyber Incident Response Teams (NCIRT) that are part of the national cyber response plan to enable a nationwide response.[47]

Cyber Security Range

In the military, wargaming is rudimentary in developing nascent operation concepts and processes, since they can be clinically tested without massive resources, as compared to the actual manoeuvring 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. An example of such a facility is the National Cyber Range that was developed by the US Department of Defense in 2012 to allow co-operation with other US government agencies, and potentially non-US government partners to rapidly create numerous models of network. This was intended to enable the military and others to simulate cyber space operations and test new technologies and capabilities, promoting collaboration and critical info sharing, in support of a 'whole of nation' effort.[48]

BE READY – CONTINGENCY MEASURES

Ensuring Redundancy

Network Redundancy is an industry best practice to prevent critical network failure and improve stability. For example, if a point-of-failure occurs within the network infrastructure, the network redundancy will redirect data traffic to maintain a functional network and prevent widespread interruption of service. There are many different tools and hardware available to help create a redundant network. Hardware that has 'hot-swappable' components is especially helpful, as the network can be kept online while replacing failed components. Redundant hardware, such as battery backup systems, extra routers, switches and servers are also essential in the event of power failures or complete failure of essential devices. Beyond hardware, there are also protocols and software programmes that can maintain a stable network by autonomously detecting, addressing and alerting technicians of problems.[49]

Scenario and Contingency Planning

It is important to prepare for the worst and therefore it is vital to threat model all sorts of scenarios. The traditional scenario planning methodology, pioneered by Royal Dutch Shell, emphasises that scenarios are not intended to present definitive predictions about the future. Rather, scenarios help to articulate the risks and opportunities present in a range of plausible futures and serve as a discussion tool to stimulate debate about strategies to shape the future. Scenario planning was first introduced into MINDEF in the late 1980s and has since been approved by the government as a tool for long-term policy and strategic development.[50] Currently, the Singapore Government produces a set of National Scenarios every three to five years to spark discussion and fresh thinking about issues related to Singapore's future. The National Scenarios are complemented by Focused Scenarios, which are in-depth studies into specific topics, such as climate change or new media.[51] However, it is now critical to also add 'what if' scenarios for cyberattacks.

Table Top Exercise

Once the different contingency plans have been formulated, table top exercises can help to test the theoretical responses during an emergency and are important for reviewing plans without the need to exhaust huge resource. In 2016, the CSA mounted its first multi-sector exercise, Exercise Cyber Star. The exercise comprises a series of scenario planning sessions, workshops and table-top discussions focusing on cyber incident management processes. The final exercise brought together over 100 participants, comprising sector leads and Critical Information Infrastructure owners from four sectors, namely Banking and Finance, Government, Energy and Infocomm. The exercise scenario covered different types of cyber attacks including web defacement, wide-spread data exfiltration malware infections, large-scale DDoS attacks and cyber physical attack.[52] However, besides the CSA, more agencies should partake in such exercises so as to keep their response plans warm and to establish key linkages.

It is not enough to have a group of experts in cyber security as cybersecurity is everyone's business and, a Smart Nation can only be as strong as its weakest link.

BE RESILIENT – NATIONAL RESILIENCY

Psychological Defence

Apart from building in multiple layers of failsafe and redundancy, the government will need to promote national resilience so that when technical malfunctions do strike, the country can swiftly bounce back and return to normalcy. Rather than aim for a perfect system that never fails, this might indeed be a more realistic approach.[53] The larger dangers arising from cyber attacks are public fear, panic and the corrosion of public trust in the things we often take for granted as being secure and reliable, such as public utilities, cloud computing and electronic transactions. In the wake of a cyber attack, our critical infrastructure and systemic response must be resilient, enabling our society to bounce back so that normalcy is restored without undue delay and unnecessary detriment. Rather than the security breach itself, much damage flows from an inadequate response to it.[54] Equipping the community with the knowledge and skills of basic and psychological first aid has another less overt benefit: it empowers people. It is a foil against that debilitating feeling of helplessness that may follow a catastrophe, and strengthens resilience that comes from that sense of preparedness in the face of unpredictable threats.[55] Thus, as part of Total Defence, the SGSecure movement is an important platform to continue to involve every Singaporean in playing a part, individually and collectively, to build a strong, secure and cohesive nation.

Psychological Preparation

There is a need for psychological preparedness to fight against terror threats. It has been opined that (1) Singaporeans may not be able to react with resilience and unity in the event of a terror attack due to the peace and security they experience daily; (2) the psychological impact of an attack may be overlooked as it may not be as obvious as physical impacts. Therefore, Singaporeans must be trained to deal with unpredictable events like terror attacks and help one another. Citizens and businesses need to learn how to respond to cyber security emergencies, preparing for cyber drills as we do in fire drills. For example, if our computers or mobile devices are taken over by ransomware, will we have backup plans or will we panic? Many countries—from Singapore to Estonia to Zambia—conduct cyber drills, which see government agencies and key businesses planning responses to cyber attacks. But such attacks would also affect thousands of citizens and small businesses, destroying their work or personal data, or disabling communication for days or weeks. They, too, need to be brought into this ecosystem of preparation.[56]

Apart from building in multiple layers of failsafe and redundancy, the government will need to promote national resilience so that when technical malfunctions do strike, the country can swiftly bounce back and return to normalcy.

CONCLUSION

Singapore's bid to become a Smart Nation is a journey that can provide many opportunities and benefits for the Singapore population. However, it is one that is also fraught with challenges. With the possibility that the networks and connectivity in the Smart Nation become a CoG and an acute vulnerability, it is important that we put in measures to counter the threat of cyber attacks which are becoming a norm. Just like the common catchphrase used to portray the existential threat of terrorism, 'a matter of when, not if,' it is crucial that a layered defence is taken against cyber attacks.[57] Thus, this essay has recommended adapting from the survivability onion to look at a layered defence to mitigate any potential threats faced and to ultimately make this Smart Nation 'Secure'.

ENDNOTES

1. National Research Council, Computers at Risk, (*National Academy Press*: Washington DC, 1991).

2. Balakrishnan, Anita "The hospital held hostage by hackers," *CNBC*, 16 February 2016, http://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html

3. Skinner, Curtis "Los Angeles hospital paid hackers $17,000 ransom in bitcoins," *Reuters*, 18 February 2016, http://www.reuters.com/article/us-california-hospital-cyberattack-idUSKCN0VR085

4. Kwang, Kevin, "Singapore can't be a Smart Nation if systems are vulnerable: CSA chief," *Channel Newsasia*, 9 June 2016, http://www.channelnewsasia.com/news/singapore/singapore-can-t-be-a/2858650.html

5 Tham, Irene "StarHub: Cyber-attacks that caused broadband outages came from customers' infected machines," *The Straits Times*, 26 October 2016, http://www.straitstimes.com/tech/starhub-cyber-attacks-that-caused-broadband-outages-came-from-customers-infected-machines

6. Au-Yong, Rachel, "Technology will also help Singapore to keep pace with world's top cities," *The Straits Times*, 25 November 2014, http://www.straitstimes.com/singapore/vision-of-a-smart-nation-is-to-make-life-better-pm-lee

7. Tegos, Micheal "IDA wants to make Singapore a Smart Nation. Here's what you need to know," *Tech In Asia*, 22 April 2015, https://www.techinasia.com/singapore-smart-nation-2015

8. Loke Kok Fai, "Singapore needs to stay ahead while pursuing Smart Nation vision: Vivian Balakrishnan," *Channel NewsAsia*, 12 April 2016, http://www.channelnewsasia.com/news/singapore/singapore-needs-to-stay/2688112.html

9. SPRING Singapore, "Setting the standard worldwide: intelligent city, Smart Nation," *Enterprise Singapore*, 3 August 2015, http://www.spring.gov.sg/Inspiring-Success/Enterprise-Stories/Pages/Setting-the-standard-worldwide-intelligent-city-Smart-Nation.aspx

10. Lui Tuck Yew, "Speech by Second Minister for Defence Mr Lui Tuck Yew at the MINDEF Pride Day 2015 Award Presentation Ceremony at Singapore University of Technology & Design," *MINDEF*, 2 September 2015, http://www.mindef.gov.sg/content/imindef/press_room/official_releases/sp/2015/02sep15_speech.html

11. Scales, Robert "Clausewitz and World War IV," *Armed Forces Journal*, 1 July 2006, http://armedforcesjournal.com/clausewitz-and-world-war-iv/

12. *TTW Asia*, "Innovation Driven Initiatives pave the way for Singapore's Smart Nation Vision", 27 April 2015, http://www.ttwasia.com/news/article/innovation-driven-initiatives-pave-way-singapores-smart-nation-vision/

13. Evans, Michael "Centre of Gravity Analysis in Joint Military Planning and Design: Implications and Recommendations for the Australian Defence Force," Security Challenges, Vol. 8, No. 2 (*Winter*, 2012): 81-104, http://www.regionalsecurity.org.au/Resources/Files/vol8no2Evans.pdf

14. Echevarria, Antulio J. II "Clausewitz's Center of Gravity: Changing our Warfighting Doctrine – Again!", *Clausewitz*, September 2002, http://www.clausewitz.com/readings/Echevarria/gravity.pdf

15. Laasme, Haly, "The role of Estonia is developing NATO's Cyber Strategy," *Cicero Foundation*, December 2012,http://www.cicerofoundation.org/lectures/Laasme_%20Estonia_NATO_Cyber_%20Strategy.pdf

16. Mills, John R. "The Key Terrain of Cyber," *Georgetown Journal of International Affairs*, 23 March 2013, http://journal.georgetown.edu/wp-content/uploads/2015/07/gj12712_Mills-CYBER-2012.pdf

17. Boyd, Robert "Secure Technology, Centers of Gravity and Homeland Security," *TinMore Institute*, December 2014.

18. Greathouse, Craig "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?" Cyberspace and International Relations, *Springer-Verlag Berlin Heidelberg*, 2014.

19. ME5 Ho Wei Seng, Alan, "Cyber Attacks and the roles the military can play to support the National Cyber Security Efforts," *POINTER*, Vol. 42. No.3 (2016).

20. Tan Teck Boon, "Building a Smart Nation: A Nuanced Understanding of Hyper-Connected Singapore," *International Policy Digest*, 26 August 2015, http://intpolicydigest.org/2015/08/26/building-a-smart-nation-a-nuanced-understanding-of-hyper-connected-singapore/

21.http://www.tiaonline.org/policy/securing-network-cybersecurity-recommendations-critical-infrastructure-and-global-supply

22. Tan Teck Boon, "Building a Smart Nation: A Nuanced Understanding of Hyper-Connected Singapore," *International Policy Digest*, 26 August 2015, http://intpolicydigest.org/2015/08/26/building-a-smart-nation-a-nuanced-understanding-of-hyper-connected-singapore/

23. Walters, Riley, "Cyber Attacks on U.S. Companies in 2014," *The Heritage Foundation*, 27 October 2014, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

24. Eilperin, Juliet and Entous, Adam, "Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say," *The Washington Post*, 30 December 2016, https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html

25. *BBC*, "Ukraine power cut 'was cyber-attack'," 11 January 2017, http://www.bbc.com/news/technology-38573074

26. Tham, Irene, "StarHub outage: Experts sound alarm on attacks by 'smart' devices," *The Straits Times*, 27 October 2016, http://www.straitstimes.com/tech/experts-sound-alarm-on-attacks-by-smart-devices

27. Bellinger, Lee, "Cyber attacks. Impacting everything.", *Independent Living News*, https://independentlivingnews.com/2015/01/21/202478-cyber-attacks-impacting-everything-from-the-national-grid-to-pacemakers-yet-the-government-remains-obsessed-with-climate-change/

28. Tham, Irene, "StarHub outage: Experts sound alarm on attacks by 'smart' devices," *The Straits Times*, 27 October 2016, http://www.straitstimes.com/tech/experts-sound-alarm-on-attacks-by-smart-devices

29. Paganini, Pierluigi, "ICS-CERT Surge In attacks against Energy Industry," *Security Affairs*, 2 July 2013, http://securityaffairs.co/wordpress/15820/security/ics-cert-surge-in-attacks-against-energy-industry.html

30. Perlroth, Nicole, "Traffic Hacking: Caution Light Is On," *New York Times*, 10 June 2015, http://bits.blogs.nytimes.com/2015/06/10/traffic-hacking-caution-light-is-on/?_r=0

31. Chan Yeng Kit, "Speech by Mr Chan Yeng Kit, Permanent Secretary (Defence), at Cyber Defenders Discovery Camp Awards Ceremony 2016," *MINDEF*, 6 June 2016, http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2016/06jun16_speech.html

32. Wilkes, David, "The survivability onion: how to stay alive in the 21st century," *Yorkshire Philosophical Society*, 2007,

https://www.ypsyork.org/events/the-survivability-onion-how-to-stay-alive-in-the-21st-century/

33. Chan Yeng Kit, "Speech by Mr Chan Yeng Kit, Permanent Secretary (Defence), at Cyber Defenders Discovery Camp Awards Ceremony 2016," *MINDEF*, 6 June 2016, http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2016/06jun16_speech.html

34. Tham, Irene, "Singapore cyber security strategy launched, half of public agencies separate Web surfing from work computers," *The Strait Times*, 10 October 2016, http://www.straitstimes.com/singapore/singapore-cyber-security-strategy-launched-half-of-public-agencies-separate-web-surfing

35. Tham, Irene, "Singapore rolls out high-level cyber security strategy," *The Straits Times*, 11 October 2016, http://www.straitstimes.com/singapore/spore-rolls-out-high-level-cyber-security-strategy

36. Ibid.

37. Lim Yan Liang, "Singapore's weapon: cyber diplomacy," *The Straits Times*, 23 October 2016, http://www.straitstimes.com/singapore/spores-weapon-cyber-diplomacy

38. Chan Yeng Kit, "Speech by Mr Chan Yeng Kit, Permanent Secretary (Defence), at Cyber Defenders Discovery Camp Awards Ceremony 2016," *MINDEF*, 6 June 2016, http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2016/06jun16_speech.html

39. Jayakumar, Shashi and Benjamin Ang. "Smart Nation, but will we be secure?", *The Straits Times*, 14 October 2016, http://www.straitstimes.com/opinion/smart-nation-but-will-we-be-secure

40. Koh, Fabian, "NS pre-enlistees can pick from 33 vocations," *The Straits Times*, 9 September 2016, http://www.straitstimes.com/singapore/ns-pre-enlistees-can-pick-from-33-vocations

41. Royston Sim, "SG Secure to equip people for crises," *The Straits Times*, 19 March 2016, http://www.straitstimes.com/singapore/sg-secure-to-equip-people-for-crises

42. *Channel NewsAsia*, "Govt's move is not to cut off Internet access for public servants: Vivian Balakrishnan," 10 June 2016, http://www.channelnewsasia.com/news/singapore/govt-s-move-is-not-to-cut/2861356.html

43. *Channel NewsAsia*, "No Internet access for public officers' work computers by next June," 8 June 2016, http://www.channelnewsasia.com/news/singapore/no-internet-access-for/2854528.html

44.*Software Defines Everything*, "海外分行的规劃實務", September 8 2016, https://vmshare.blogspot.com/2016/?view=classic

45. *Channel NewsAsia*, "Measures to fend off cyber attacks tested regularly: Singapore Power," 6 January 2016, http://www.channelnewsasia.com/news/singapore/measures-to-fend-off/2402694.html

46. Ibid.

47. *Cyber Security Agency of Singapore*, "Singapore's Cybersecurity Strategy," 2016, https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

48. ME5 Ho Wei Seng, Alan, "Cyber Attacks and the roles the military can play to support the National Cyber Security Efforts," *POINTER*, Vol.42. No.3 (2016).

49. Melancon, Joe "Network Redundancy," *Smart City Networks*, 10 March 2015, https://www.smartcitynetworks.com/network-redundancy/

50. *Public Service Division*, "Conversations for the Future," Singapore's Experiences with Strategic Planning (1988–2011), 2011.

51. *Centre for Strategic Futures and Civil Service College*, "Fore Sight – A Glossary."

52. *Cyber Security Agency of Singapore*, "CSA marks operational milestone with Exercise Cyber Star," 22 March 2016, https://www.csa.gov.sg/news/press-releases/exercise-cyber-star

53. Tan Teck Boon, "Building a Smart Nation: A Nuanced Understanding of Hyper-Connected Singapore," *International Policy Digest*, 26 August 2015, http://intpolicydigest.org/2015/08/26/building-a-smart-nation-a-nuanced-understanding-of-hyper-connected-singapore/

54. Tan, Eugene "Multi-stakeholder approach needed to tackle cyberthreats," *Today Online*, 10 October 2016, http://www.todayonline.com/singapore/multi-stakeholder-approach-needed-tackle-cyberthreats

55. Chong Siow Ann, "After the terror, winning the psychological war," *The Straits Times*, 8 October 2016, http://www.straitstimes.com/opinion/after-the-terror-winning-the-psychological-war

56. Jayakumar, Shashi and Ang, Benjamin, "Smart Nation, but will we be secure?", *The Straits Times*, October 14, 2016, http://www.straitstimes.com/opinion/smart-nation-but-will-we-be-secure

57. *Today Online*, "Attack on Singapore a matter of when, not if, says Shanmugam," 23 March 2016, http://www.todayonline.com/singapore/unless-we-turn-city-prison-not-possible-counter-every-terror-attack-shanmugam

ME6 Calvin Seah Ser Thong is currently on secondment to the Land Transport Authority's Rail Asset, Operations and Maintenance Group. He is an Army Engineer by vocation and was previously a Section Head in HQ Maintenance and Engineering Support. ME6 Seah holds a Bachelors of Engineering in Mechanical & Production Engineering from the Nanyang Technological University (NTU), a Masters of Science in Industrial and Systems Engineering from the National University of Singapore (NUS) and a Masters of Science in Defence Technology and Systems from NUS obtained under the SAF Postgraduate Award. He also attained a Masters of Science in Human Capital Management from NTU under the SAF-NTU Continuing Education Masters Programme and was placed on the Nanyang Business School's Dean's List. For this essay, ME6 Seah was awarded the Second Prize at the 2016/2017 CDF Essay Competition.