CYBER SECURITY IN SINGAPORE

Policy Report
December 2016

Cung Vu

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Policy Report

CYBER SECURITY IN SINGAPORE

Cung Vu
December 2016

EXECUTIVE SUMMARY

From the development of the integrated circuit, which gave rise to the computer and the evolution of the internet today, we have witnessed the way technology has transformed our way of life. Now, we are moving to the Internet-of-Things, where everything will be connected because of the presence of cheap and readily available sensors. To harness the potential of the information communication technology (ICT) to drive the economy and to simultaneously address the issues that Singapore is facing, such as providing healthcare for an increasingly aging population, meeting energy demand, and urban development, Prime Minister Lee Hsien Loong has launched a Smart Nation Initiative for Singapore in November 2014. As we enjoy the increased benefits, we also become more and more dependent on ICT, therefore making us more vulnerable. Singapore is one of the countries in the Asia-Pacific region with the most advanced ICT; therefore it is no surprise that it is also facing the most cyber security challenges. As a small population with not enough critical mass, it is difficult for Singapore to defend against well-thought out cyberattacks. With the launch of the Smart Nation Initiative, Singapore has recognised the challenges in cyber space, established the Cyber Security Agency in April 2015 and released its Cybersecurity Strategy in October 2016. It is heading in the right direction to make the best out of its manpower constraints. This paper will examine the issues and challenges that Singapore is facing in cyber security at the strategic level and propose some policy recommendations.

INTRODUCTION

From the development of the integrated circuit, which gave rise to the computer and the evolution of the ARPA-net transforming into the internet today, we have witnessed the way technology has transformed our way of life. Within the last decade, the advancement in portable devices, such as the smart phone, has added another dimension to our freedom, allowing us to conduct most, if not all, businesses while on the move, virtually anytime and anywhere. Vast quantities of information are now available literally at our fingertips, and that has increased our capacity for social interactions exponentially. Companies, such as Facebook and Twitter, now have billions of users and this has tremendously changed the way we interact, communicate, and think. Now we are moving to the Internet-of-Things, whereby everything will be connected because of the presence of cheap and readily available sensors. We have also seen the birth of smart cities, and in Singapore, a smart nation.

Information communication technology (ICT) has improved our quality of life, and has helped us to meet our basic needs, including food, water, medicine, environment and energy. Advancements in bio-informatics and genetics have allowed scientists to improve agricultural crop yields, minimise the use of pesticides, and make crops more resistant to draught or disease. ICT facilitates the technologies used in water purification and sanitisation and also streamlines the way we manage healthcare. It enables the harnessing of clean energy to provide energy in remote areas and to reduce the greenhouse gas effect.

Overall, ICT has undeniably provided more comfort and convenience in our daily life. For instance, in the past, a car was simply a mean of transportation from point A to point B, but with the utilisation of the Bluetooth, we now can make or receive phone calls without taking our hands off the steering wheel. Also, GPS provides us with driving directions, advising us to take the best route to avoid congested traffic. Many features inside a car are controlled by computer chips responsible for monitoring the engine performance, sensing the surroundings to avoid collision, governing the anti-lock brake, and so on. In recent car models, there are numerous microprocessors to enhance security and help the car to self-drive. As computer chips are getting cheaper and cheaper, the devices in our home will start to include sensors, which can communicate with one another.

Some of such devices have been used for a long time, including motion sensing for lighting and thermostat for temperature control, but each of these devices work independently. Now in a smart home, they can seamlessly communicate the knowledge of our presence and our preferences to pre-emptively adjust various settings like temperature, light intensity, and sound

volume. In doing so, they not only help save energy but also increase our physical comfort. Appliances such as the water heater, washer, dryer, dishwashers, home security devices are automatically monitored and controlled.

In addition, architects and builders have taken advantages of our natural environment to minimise energy usage, by taking into consideration the presence of natural draft, the direction of sunlight, and by incorporating renewable energy such as wind, solar power to lessen the demand on utility usage and energy consumption. In doing so, their buildings can provide maximum comfort while requiring minimum energy.

To harness the ICT potential to drive the economy and to simultaneously address the issues that Singapore is facing (such as provision of healthcare for an increasingly aging population, meeting energy demand, and urban development), Prime Minister Lee Hsien Loong launched a Smart Nation Initiative for Singapore in November 2014[1].

[1] Smart Nation Singapore, http://www.smartnation.sg/

DISCUSSION

As the age-old saying goes, nothing is free. As we enjoy increased benefits, we also become more and more dependent on ICT, therefore making us more vulnerable. In the Asia-Pacific region, Japan, Korea, Singapore, Australia, and New Zealand are countries with the most advanced ICT, so it is no surprise that they are also facing the most cyber security challenges[2].

Such vulnerability could be exploited by cyber attackers to serve their purposes, which could include cyber theft, cyber crimes, cyber attacks, influencing public perceptions, or terrorism.

At the moment, the incidents or attacks have been increasing on a daily basis with no levelling off in sight. It is very difficult to retaliate since the cyber attackers are anonymous, and they could be state or non-state sponsored. Furthermore, attacks are often routed through many countries where global governance has yet to be agreed upon, due to differences in cyber powers.

According to the Symantec (a cyber security firm) 2016 Internet Security Threat Report[3], there were nine mega-breaches in 2015, and the reported number of exposed identities totalled around 429 million. There were over one million web attacks against people each day in 2015, but the main problem was that more companies chose not to reveal the full extent of their data breaches.

The McAfee (another cyber security firm) Labs Threats Report (March 2016)[4] disclosed that more than 157 million daily attempts were made (via emails, browser searches, etc.) to entice its customers into connecting to risky URLs (internet addresses). The report also stated that more than 353 million infected files were exposed to its customers' networks, 71 million potentially unwanted programs attempted installation or launch on its customers' systems, and 55 million attempts were made by its customers to connect to risky IP addresses (or those addresses attempted to connect to customers' networks).

Besides technical vulnerabilities (hardware and software), there are other challenges in cyber security:

(i) There is no international governance to dictate the law, the rules of engagement, the norms, or tell us our responsibility and accountability.

---

[2] Asia-Pacific Defense Outlook 2016, Deloitte, January 2016, http://www2.deloitte.com/global/en/pages/public-sector/articles/gx-asia-pacific-defense-outlook.html

[3] Internet Security Threat Report, Symantec, April 2016, https://www.symantec.com/security-center/threat-report

[4] Threat Reports, McAfee Labs, March 2016, http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf

Without governance, our rights are in jeopardy and our lives are not protected.

(ii) Big corporations are reluctant to adopt common standards since that would erase their own competitive edge achieved through new designs, patents, and trade secrets. The situation also makes it more difficult for smaller companies in one country to develop the necessary know-hows to interact with a device made in another country.

(iii) As old equipment is replaced with the new ones, it is often done in phases due to budget constraints or physical difficulties in replacing old infrastructure (because the old security measures were not planned with the new security environment in mind).

(iv) The main goal of corporations is to make money for their shareholders. They focus on developing new products or services to quickly enter the market; and the time spent in perfecting their products or services is not considered well-spent and would not benefit the bottom line. Instead, they aim to be the first to capture the market and then buy time to resolve other issues such as security at a later stage. At the present, we receive new updates almost daily on our personal devices or computers, as cyber security may not be the top priority in the producers' business strategies.

(v) Critical infrastructures, such as power grids, were designed to provide power to the public, and water plants to provide water, etc. They could be overdesigned to take care of overloads or peak demands, but were not planned with cyber security in mind since cyberspace did not exist then. For example, chemical plants were designed solely to manufacture chemicals. Their health and safety requirements were established to meet the air and water environment requirements, so accidental release could be controlled and minimised, but the plants were never designed to ward off a massive cyber attack.

CYBERSECURITY IN SINGAPORE

Cybersecurity is critical. More than 75 countries[5] have set it as their top priority to address, and they have developed their own national cyber security agendas.

Recognising the challenges, Singapore has developed the Infocomm Security Master Plan (2005-2007), followed by the Infocomm Security Master Plan II (2008-2012), and recently, the National Cyber Security Master Plan 2018 (NCSM2018)[6], which was launched in 2013. As cyber security problems increase, on top of Singapore's goal to become a smart nation, the Cyber Security Agency (CSA)[7] was established in April 2015 to oversee and coordinate activities as well as strengthen Singapore's cyber security. It is a national agency under the Prime Minister's Office and administered by the Ministry of Communications and Information (MCI).

CSA has taken over the Singapore Infocomm Technology Security Authority (SITSA) from the Ministry of Home Affairs to oversee operational IT security and the Singapore Computer Emergency Response Team (Sing CERT), which had belonged to the Infocomm Development of Authority (IDA).

The key responsibilities of CSA are in Strategy and Policy Development, Cyber Security Operations, Industry Development, and Outreach. In Strategy and Policy Development, the aim is to strengthen cyber security of Singapore's critical sectors: government, infocomm, energy (power), land transport, maritime, civil aviation, water, security and emergency, banking and finance, and health. In Cyber Security Operations, the main focus is to ensure effective coordinated operations in response for cyber attacks, and in Industry Development, the goal is to develop a robust ecosystem equipped with proper manpower to respond to and mitigate cyber attacks. Lastly, in Outreach, CSA aims to foster relationships with local and global industries and thought leaders, through public outreach activities enhancing cyber security awareness.

---

[5] Cyber Security Strategy Documents, NATO, August 2016, https://ccdcoe.org/cyber-security-strategy-documents.html

[6] National Cyber Security Masterplan 2018, July 2013, https://www.ida.gov.sg/~/media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf

[7] CSA Singapore, https://www.csa.gov.sg/

In October 2016, Singapore launched its Cybersecurity Strategy[8] which encompasses the four pillars:

(i) Building a resilient infrastructure to strengthen the critical infrastructures by working closely with private sectors and cyber security community;
(ii) Creating a safer cyberspace by promoting involvement from not only government but also industry and the public;
(iii) Developing a vibrant security ecosystem by working with industry and academia to grow the cyber security workforce; and
(iv) Strengthening international partnerships, especially among the ASEAN members, to address transnational cyber security issues.

[8] PM Lee Launches Singapore's Cybersecurity Strategy, https://www.csa.gov.sg/news/press-releases/pm-launches-singapore-cybersecurity-strategy

PONDERING POINTS

With the establishment of the CSA and the launch of Singapore's Cybersecurity Strategy, the following questions remain: Does Singapore have enough resources to fend off intentional attackers? Does Singapore have enough muscle to force the key developers to set up standards? Does Singapore have enough manpower to address these cyber security issues?

According to the 2016 Singapore budget, it is estimated that 234 million SGD has been allotted to the Administration Programme which includes both the Cyber Security Agency and the Design Singapore Council, in addition to the 393 staff members in this section[9]. Would that be sufficient? In October 2015, Dr Yaacob Ibrahim, Minister of MCI, announced that Singapore would consider spending eight to ten percent of its IT budget on cyber security to be in line with Korea (ten percent) and Israel (eight percent across the government)[10].

It is hard to say whether it is sufficient, since Singapore has yet to develop the implementation plan for its Cybersecurity Strategy; without the roadmap and milestones, we do not know how many programmes or the level of resources that are required. For reference, the UK published its National Cyber Security Strategy in 2011, and in April 2016, it announced its investment of 1.9 billion pounds over five years[11]. Australia released its Cyber Security Strategy in April 2016 which states that it intends to spend 230 million AUD over four years[12]. The U.S. released its first national strategy to secure cyberspace in 2003, and in 2015, it included cyber security as a part of the national security strategy. Between 2015 and 2016, the U.S. released many cyber security initiatives and strategies, both at national and departmental levels. President Obama also proposed the cyber security budget in 2017 to be 19 billion USD[13] - 5 billion more than in 2016 - out of the 79 billion for its IT budget (twenty-four percent of the IT budget). Even though the number of cyber attacks is on the rise, the actual cost per incident is difficult to determine due to the lack of metrics or standards.

---

[9] Singapore Budget 2016, Annex to Expenditure Estimates, Ministry of Communications and Information, http://www.singaporebudget.gov.sg/data/budget_2016/download/40%20MCI%20Annex%202016.pdf

[10] Minister MCI Opening Speech at govware2015, CSA, https://www.csa.gov.sg/news/speeches/min-opening-speech-at-govware2015

[11] The UK Cyber Security Strategy 2011-2016, April 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

[12] Australia's Cyber Security Strategy, April 2016, https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

[13] The President's Budget for Fiscal Year 2017, https://www.whitehouse.gov/omb/budget

It is unlikely that Singapore could convince IT corporations to adopt common security standards. For example, the U.S. government could not convince Apple to modify their iOS operating system to allow the law enforcers to access to evidence believed to be stored in an Apple iPhone in the San Bernardino terrorist case.

The biggest challenge for Singapore might be the fact that there are not enough critical mass and people with appropriate skills in the workforce. As published in the NCSM2018, less than one percent of infocomm professionals are working in the cyber security area. In 2015, the infocomm workforce totaled around 173 thousand. What Singapore needs is to increase the number of people in the workforce and also, the percentage of cyber security professionals in the infocomm area.

At the moment, more than 75 countries have published their national security strategies. Most of these cyber security strategies take the whole government approach, which includes economic, education, social, and military consideration. The goals are to drive economic prosperity while protecting critical assets against cyber attacks by:

(i) Building a robust and resilient infrastructure to deal with attacks;
(ii) Developing public-private partnerships, which also includes international collaboration;
(iii) Building a skilled workforce; and
(iv) Supporting economic growth

The differences lie in the way they execute their strategy, focusing on their own perceived cyber threats and opportunities. This will determine the level of effort and resources required.

For example, the Comprehensive National Action Plan (CNAP) released in the U.S. in February 2016[14] focuses on three key areas: raising the cyber defences, countering malicious cyber actors, and improving the responses to cyber incidents.

The first area is to improve both public and private network defences. This means changing the way cyber risk is managed as a nation - for example, working with industry to develop best practices and cybersecurity standards.

Although defence is necessary, it is not sufficient, so the second area focuses on deterring and disrupting malicious actors. The U.S. has stated publicly that nothing is off the table and they will use whatever means of national power necessary to deal with cyber threats or attacks, be it diplomacy, economic strategy, or cyber offense.

[14] FACT SHEET: Cybersecurity National Action Plan, February 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Details of the third area were released in July 2016[15] to establish a framework to coordinate national efforts in response to cyber incidents or attacks. It defines the key responsibilities of each federal agency. The Federal Bureau of Investigation (FBI) (similar to the Internal Security Department (ISD) of the Ministry of Home Affairs of Singapore) will take the lead in terrorism cases by coordinating responses to the threat, from gathering evidence and collecting intelligence information to attributing attacks and bringing the cyber culprit to justice. The Department of Homeland Security (DHS) (similar to the Ministry of Home Affairs of Singapore) will take the lead in assisting organisations facing the cyber attacks and preventing them from spreading elsewhere. The Office of Director of National Intelligence (ODNI) (similar to the National Security Coordination Secretariat (NSCS) of Singapore) will take the lead in integrating intelligence, analysing threats, and identifying opportunities to mitigate and disrupt any.

Another country worth looking at is Israel. It is a small country of 8 million people but has become one of the most powerful countries in the area of cyber security. According to the Israeli National Cyber Bureau[16], Israel exported 6 billion USD in 2014 in cyber security solutions. Israel represents only 0.1 percent of the world's population but 10 percent of global investments in cyber security. In fact, the oldest Israeli cyber security company, Check Point, now has a market cap of over 15 billion.

Israel has built ecosystems to promote learning and mastering of technology. It has used its national service as a pipeline to supply skilled workforce to the security area - especially the 8200 intelligence unit[17] - by training its recruits in cyber intelligence. It is understood that Israel is constantly under military and cyber threat from its neighbouring countries.

To foster innovation, Israel encourages people to take risks and constantly seek improvement. This culture is rarely seen in Asia, as people tend to be risk-averse, afraid of failure, and hesitant to challenge the status quo. This combination of traits has the unfortunate tendency to siphon off any innovative minds.

---

[15] Presidential Policy Directive -- United States Cyber Incident Coordination, July 2016, https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[16] Israeli Cyber Exports Double in a Year, Barbara Opall-Rome, June 2015, http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/03/israel-cyber-exports-double/28407687/

[17] Inside Israel's Secret Startup Machine, Richard Behar, May 2016 http://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#4f4c9e43157d

CYBER SECURITY ACTIVITIES IN SINGAPORE

This paper now reviews the activities that have developed since the launch of Singapore NCSM2018 and the CSA.

Building a robust and resilient infrastructure

As published in the Singapore NCSM2018, Singapore has established the Critical Infocomm Infrastructure (CII) Protection Assessment programme to assess the security of infocomm systems that are critical to the operation of CII in Singapore, ensuring that CIIs remain secure and resilient. It was then followed by the Critical Infocomm Infrastructure Security Assessment (CII-SA) to appraise the infocomm security readiness of Singapore's CIIs and ascertain the adequacy of infocomm protection measures, implemented by infrastructure owners and operators. The Secure and Resilient Internet Infrastructure Code of Practice (SRII-CoP), aligned with international standards and best practices, has been issued by the IDA to designated internet service providers. It conducted exercises (through the National Cyber Security Exercise programme) to assess the capability and readiness of critical sectors, aiming to improve the overall resilience of the national infrastructure and services against significant cyber attacks at the national level. The enhanced Cyber Watch Centre (CWC) was created to improve the overall effectiveness of security monitoring for the public sector, leveraging on advanced tools and techniques. The enhanced Threat Analysis Centre (TAC) was also established to utilise state-of-the-art analytical tools to assess larger volumes of data from a wider range of sources, provide public agencies with detailed cyber threat analysis, and give recommendations so that timely preventive actions can be taken.

Building a skilled workforce

Since the launch of the Singapore NCSM2018, Singapore has developed the National Cybersecurity R&D Programme[18] to promote research and development and build more cyber security expertise. Its goal is to promote collaboration among agencies, academia, research institutes, and the private sector. It involves the National Research Foundation (NRF), Ministry of Defence (MINDEF), Ministry of Home Affairs (MHA), National Security Coordination Secretariat (NSCS), Infocomm Development Agency (IDA) and Economic Development Board (EDB). Its 5-year budget of 130 million SGD is used to fund research in both technological and human-science aspects of cyber security, complemented by studies in cyberspace governance and policy research.

[18] National Cybersecurity R&D Programme, National Research Foundation, http://www.nrf.gov.sg/about-nrf/programmes/national-cybersecurity-r-d-programme

The IDA initiated the Company-Led Training (CLT) Programme for young professionals in collaboration with CLT Partners. CLT goals are to recruit, mentor, and train young professionals in areas and technologies to meet the requirements of local infocomm industry. Trainees receive fundamental training in infocomm security in the CLT Partner's business unit by working on real life problems. The goal of CLT is to foster young infocomm security professionals and train them to be able to fill specialist-level positions.

To prepare cyber security professionals in the ability to detect and respond to cyber attacks, the DigiSAFE Cyber Security Centre was opened in June 2014. The Centre offers highly sophisticated operations-centric cyber security training and provides young professionals with the opportunity to be trained in handling simulated real-world attacks.

The CSA and IDA jointly launched an initiative called the Cyber Security Associates and Technologists (CSAT) Programme. By collaborating with partnering companies, the CSAT Programme trains young ICT professionals and mid-career professionals in cyber security areas. Trainees receive hands-on training in both local and overseas assignments.

The ICT Industry and academic institutions also play an active role in the training of students and professionals in the cyber security areas. For example, Temasek Polytechnic launched a IT Security and Forensics Hub, and offers two types of Diplomas in Cyber Security and Forensics, equipping students with industry-relevant skills by collaborating with industry partners such as IBM, Cisco Systems, and others.

Singtel launched the Singtel Cyber Security Institute to develop new cyber security products and services to train enterprises to protect their operations against cyber attacks using a state-of-the-art facility that replicates real ICT environments. The Institute also provides advanced education and training in cyber threat awareness, risk management, business continuity planning, and crisis communications preparation.

Singapore University of Technology and Design (SUTD) and ST Electronics launched the ST Electronics-SUTD Cyber Security Laboratory. The laboratory's goals are to advance new cyber security technologies and build next generation solutions and products to address both current and future cyber security challenges. The laboratory is funded by the National Research Foundation Singapore.

Public-private partnership

In the area of Public-Private partnership, the Singapore NCSM2018 has launched the Cyber Security Awareness and Outreach programme to explore new avenues that offer wider coverage and reach to users, the Cyber Security Awareness Campaign to reinforce security awareness messages to Government, business and the public, and the National Infocomm Security

Competition (NISEC) to educate the public about cyber security and secure online practices. NISEC has also held competitions to engage the younger generations, ranging from primary to tertiary levels.

The CSA has also worked with the Personal Data Protection Commission of Singapore (PDPC) to produce guides for small and medium enterprises (SME) to protect their company's data from cyber threats and help them develop a data breach management plan.

The CSA conducted its first Cyber Security Table-top Exercise for the banking and finance sector by partnering with the Monetary Authority of Singapore (MAS), a statutory board that leads the banking and finance sector. The exercise provided a good platform to test the capabilities of participating financial institutions in preparing for, responding to, and recovering from cyber attacks.

To build cyber security capability and work on key areas of interest, the CSA signed the Memoranda of Understanding (MOU) with Singtel, Check Point Software Technologies, and FireEye[19]. Singtel will help the CSA develop training and certifications that meet the requirements and demand for cyber security. The CSA leverages Check Point's expertise to bring advanced solutions to Singapore while growing local capabilities to provide these solutions. It also works with FireEye to strengthen information-sharing on cyber crimes, cyber threats, and indicators of cyber breaches. In addition, the CSA also signed a Memorandum of Intent (MOI) with CREST International and the Association of Information Security Professionals (AISP), introducing CREST certification that serves as a competency baseline for practicing professionals and service providers.

International collaboration

According to the NCSM2018, Singapore has participated in ASEAN TELMIN[20], ASEAN-Japan Annual Engagements, Asia Pacific CERT (APCERT), FIRST (Forum of Incident Response and Security Team), and Meridian Process. The CSA has continued this trend of expanding the collaborations with international partners[21].

The CSA and its French counterpart, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), signed a Memorandum of Understanding (MOU) in May 2015 to strengthen national cybersecurity capabilities through the sharing of best practices and efforts to develop cyber security expertise.

---

[19] CSA inks partnerships with local and foreign industry players, October 2015, https://www.csa.gov.sg/news/press-releases/csa-inks-partnerships-with-local-and-foreign-industry-players

[20] ASEAN Telecommunications and IT Ministers Meeting (TELMIN), http://asean.org/asean-economic-community/asean-telecommunications-and-it-ministers-meeting-telmin/

[21] Press Releases, 2015-2016, CSA, https://www.csa.gov.sg/news/press-releases

The CSA signed a MOU on Cyber Security Cooperation with the Cabinet Office of the United Kingdom in July 2015 to cover cooperation in four key areas, including cyber security incident response and cyber security talent development. There will also be joint cyber research and development collaboration between the UK and Singapore, with funding being doubled from 2.5 million to 5.1 million SGD over three years.

The CSA signed a MOU with the Department of Electronics and Information Technology of India in November 2015 to establish cooperation between the Singapore Computer Emergency Response Team (SingCERT) and the Indian Computer Emergency Response Team (CERT-In). The MOU focuses on five key areas of cooperation covering a formal framework for professional dialogue, operational readiness and response, cyber security technology and research related to smart technologies, exchange of best practices, and human resource development exchanges.

The CSA and the National Cyber Security Centre (NCSC) of the Netherlands signed a MOU in July 2016 to commit to working together to foster a secured cyber space. Both parties commit to regular bilateral exchanges, sharing cyber security best practices and strategies in protecting critical information infrastructures as well as access to training and workshops.

The CSA signed a MOU with the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security (DHS) of the U.S. in August 2016. The MOU includes cooperation in CERT-CERT information exchanges, coordination in cyber incident response, and sharing of best practices on Critical Information Infrastructure protection and cyber security trends. Both sides also commit to conducting joint cyber security exercises, collaborating on building regional cyber capacity, and increasing cyber security awareness.

National coordination

According the NCSM2018, National Infocomm Security Committee (NISC) of Singapore comprises of senior leadership from multiple government agencies including the Agency for Science, Technology and Research (A*STAR), IDA, MCI, MHA and its agencies, as well as MINDEF and its agencies, Ministry of Finance (MOF), NSCS, and NRF. Besides being the national platform that formulates infocomm security policies and sets strategic directions for Singapore, NISC also guides the development and implementation of the NCSM2018. The CSA took over this coordination role when it was established in April 2015.

RECOMMENDATIONS

Singapore has gained admiration from around the world due to its ease of doing business, competitiveness, transparency, and motivated workforce. However, as a small population with not enough critical mass, it is less likely that Singapore could defend against well-thought out cyberattacks. Recent breaches, such as in the Office of Personnel Management or the claimed hacking into the National Security Agency's system, illustrate that even with huge manpower and financial resources, the U.S. still could not prevent these well-planned and executed attacks. Now with the launch of the Smart Nation Initiative, Singapore has recognised the challenges in cyber space, established the Cyber Security Agency and released its Cybersecurity Strategy. It is heading in the right direction to make the best out of the manpower constraints. In an attempt to alleviate some of the issues and challenges, this report addresses the critical issues at a strategic level and skips the operational/tactical details, such as governance, protocols, single point of failure, privacy, social media, for examples, since many of these topics deserve detailed and separate studies. The following recommendations (Tables 1 & 2 below) are proposed:

Table 1:
General recommendations to enhance cyber security in Singapore

General recommendations		Key points
1.	Develop a national cyber security strategy implementation plan	• Develop an implementation plan. Without the roadmap and milestones, it is not possible to determine how many programs and level of resources are needed.
2.	Build a Global Cyber Security Community of Interest (GCSCOI)	• Embrace stakeholders from government, academia, private sectors, the public, and international partners; • Conduct regular meetings to bring the stakeholders together to build trust and international norms; • Create an on-line bulletin on cyber that the global stakeholders could participate in; and • Continue to actively participate in workshops, conferences and establish a Global Cyber Security Forum, if feasible.

3.	Improve information/ intelligence sharing	• Identify and resolve issues inhibiting information-sharing through interagency and international collaboration; • Involve intelligence, which will steer the effort to focus on certain areas of vulnerability; and • Develop a software platform architecture to share information at different levels of classifications.
4.	Conduct risk assessment and priorities analysis	• Conduct detailed risk assessment studies for Singapore's eleven critical sectors; and • Assign appropriate priority which will dictate the required manpower and financial resources.
5.	Advocate science and technology	• Understand the implications of emerging cyber technologies to produce new cyber threats or to offer new opportunities to enhance cyber security.

Table 2:
Specific recommendations to enhance cyber security in Singapore

Specific recommendations		**Key points**
1.	Foster interdisciplinary research	• Support more interdisciplinary research in addition to computer science and engineering areas.
2.	Build a workforce by leveraging National Service	• Leverage on the National Service to provide pipeline to or rapidly expand the cyber security workforce similar to the Israeli model.
3.	Enhance interface between policy makers and technologists	• Bridge the understanding gap between the decision and policy makers, and the academic or technical community.
4.	Expand international engagements	• Continue to engage existing international partners and expand to others such as APEC TELMINWG, and IGF.
5.	Take the lead using existing mechanisms	• Use existing mechanisms that RSIS has to provide regional leadership in cyber security, similar to the APPSMO and APPSNO programmes.

General recommendations

(i) National cyber security strategy

Now that Singapore's Cybersecurity Strategy has been released, CSA should develop, launch an implementation plan to develop a roadmap and execute it. Without the roadmap and milestones, it is not possible to determine how many programmes and level of resources are needed. From the milestones, it will then be possible to understand the prioritisation methodology and to evaluate the results against anticipated metrics. These will dictate the level of resources required to achieve different milestones.

(ii) Global Cyber Security Community of Interest (GCSCOI) development

The CSA should be proactively identifying new partners, discussing shared requirements, and creating opportunities for collaboration. This includes all the stakeholders from government, academia, private sectors, the public, and international partners. The CSA should have regular monthly meetings to share information, expand the network, and build trust. In these meetings, the CSA would chair the meetings and speakers would be invited from the GCSCOI stakeholders. The topics would vary among technology, policy, governance, and so on. Domestically, this would be a process not only to build public-private partnership, but also to increase the trust from the public to address potential privacy and cyber security issues. Internationally, Singapore can address potential governance issues, by promoting "norms" in cyber space to deter attackers. This would also alleviate the trust issue wherein private sectors do not want to share information of their attack incidents with the government.

The CSA should raise the level of awareness of cyber security by having a clearing house to publish and disseminate information. A cyber security bulletin could be a way to collect and share information from news sources, articles on cyber security, and contributions by the GCSCOI. The bulletin should be available online to develop broad readership around the globe, while also enhancing the global community's perception of Singapore on cyber security. Again, this is a tool to promote public-private partnership and public trust.

The CSA should continue to support seminars, workshops, and conferences, by organising them in Singapore or actively participating in international events. It would be ideal if the CSA could establish a Global Cyber Security Forum to be held annually, in similar fashion to the well-respected Shangri-La Dialogues to bring world leaders to discuss cyber security issues.

(iii) Improve information/intelligence sharing

Information-sharing is critical and the CSA should take the lead when it comes to information-sharing coordination in cyber security. Information is not useful when it is not shared; it should be shared at the national level through interagency ministries and departments, and also with the government, private sectors, the public and international partners.

The CSA needs to identify and resolve issues inhibiting information-sharing through interagency and international collaboration.

The CSA should establish an interagency coordinating committee to coordinate interagency technical and sub-technical working groups. As Singapore senior-level executives wear multiple hats due to manpower constraints, each agency should have a senior-level champion who sits in on regular meetings (at least quarterly). Additionally, the middle-level managers should attend monthly meetings conducted within the government as well as interact with the public.

Intelligence must be part of the whole-of-government approach. Intelligence will steer the effort to focus on certain areas of vulnerability. The Security and Intelligence Division (SID) and the Internal Security Department (ISD) should participate in the interagency coordinating committee.

The CSA should promote a software platform architecture to share information at different levels of classifications. This will allow information to be shared with people of different clearance levels, especially those who belong to a number of critical infrastructures residing outside the government. This will also allow information to be shared with the public and international cyber community.

(iv) Conduct risk assessment and priorities analysis

The CSA should conduct detailed risk assessment studies for Singapore's eleven critical sectors which include government, infocomm, energy (power), land transport, maritime, civil aviation, water, security and emergency, health, banking and finance. It should also assign appropriate priority to defence (protecting the sectors and providing resilience in case of attacks). The assessment and analysis will dictate the required manpower and financial resources.

(v) Advocate science and technology

Science and technology also play an important role. The CSA should have a group of technical people to engage the academia, think tanks, private sector, and foreign partners. The CSA needs to be up-to-date on the understanding of the implications of emerging cyber technologies that

have the ability to produce new cyber threats or challenges in cyber space, as well as those that offer new opportunities to enhance cyber security.

Specific recommendations

(i) The National Research Foundation should fund more interdisciplinary research, in addition to computer science or engineering. It should focus on the interface among policy, legal, cyber technologies (computer hardware and software), financial (banking industry), medical (health care), environmental (water infrastructure), chemical (chemical industry, energy infrastructure), civil, and mechanical (transportation infrastructure) disciplines since people with these types of interdisciplinary skills can develop solutions to new, yet-to-be-considered types of attack in the future.

(ii) While leveraging on the existing pool of international experts (Check Point, FireEye, CREST, and others) in the short term, Singapore should grow local talents as quickly as possible. Singapore has the national service and it can take advantage of this to supply a pipeline of skilled workforce into cyber security. For example, in Israel, students can request a deferred conscript to obtain a technical degree, taking three to four years based on the area of study. Upon finishing, the students have to join the national service and can serve in their career profession for five years (three-year compulsory and additional two years if the Army sees fit)[22]. In this case, the students already have eight or nine years in their chosen career when they get out of the national service. If Singapore can copy this model and allow students who excel in math and science to study cyber security, by the time they finish their deferred conscription and serve the mandatory time, they would have gained a broad experience in the cyber security areas and be ready to join the main workforce in public. This would quickly expand the current cyber security workforce of less than 17300 (less than one percent of the current workforce according to NCSM2018). At the turn of the century, Singapore has 50,000 full time National Servicemen and the Operationally Ready National Servicemen of 300,000 - a huge resource pool, which should not be ignored[23].

(iii) People with skills obtained in academia or industry are available, however, not many have governmental experience. Singapore could initiate some programmes to entice young engineers and scientists to join the public

[22] Military Service, 7th Edition, 2016, http://www.moia.gov.il/Publications/idf_en.pdf

[23] Defence Challenges in the 21st Century, MINDEF, 2000, https://www.mindef.gov.sg/dam/publications/eBooks/More_eBooks/ds21.pdf

service to provide technical insight to the policy makers. Singapore could develop programmes similar to the ones in the U.S., where professional societies like the American Association for the Advancement of Science (AAAS)[24] or the Institute of Electrical and Electronics Engineers (IEEE)[25] provide stipends or fellowships and the recipients work in government on a term-limit appointment. This plan would provide a technical workforce pipeline for government. It is possible that a professional organisation, such as the Institution of Engineers Singapore[26] (IES) could provide this service for Singapore. For seasoned academicians, Singapore could also leverage on their career expertise to serve the policy or decision makers. For example, the Jefferson Fellowship[27] provides a mechanism for well-respected members of academia to serve in the government for a year (the university pays for the salary and the government pays for all the expenses within the temporary position). After their term, the academicians return to their home universities and work as a consultant for government for five years.

(iv) The CSA should expand its network to participate in the Internet Governance Forum[28] (IGF) of the United Nations. The IGF serves to bring people together from various stakeholders to discuss public policy issues relating to the Internet. The IGF facilitates a common understanding of how to maximise Internet opportunities, and addresses risks and challenges that arise. As Singapore tries to take the lead in the ASEAN TELMIN, it should also try to take the lead in the APEC TELMIN working group[29].

(v) Singapore should take the lead in ASEAN to train regional leaders on cyber security issues, similar to the programmes that RSIS conduct (such as the Asia Pacific Programme for Senior Military Officers (APPSMO)[30] or the Asia-Pacific Programme for Senior National Security Officers (APPSNO). The new cyber training programmes will enable the ASEAN's cyber security stakeholders to learn about issues and requirements, establish networks, and build relationships, all of which would be very useful for international interactions and collaborations.

---

[24] Science & Technology Policy Fellowships, https://www.aaas.org/program/science-technology-policy-fellowships

[25] IEEE-USA Engineering & International Development Fellowship, http://www.ieeeusa.org/policy/govfel/ieee-usausaidfellowship.asp

[26] The Institution of Engineers, Singapore, https://www.ies.org.sg/#&panel1-1&panel2-1

[27] Jefferson Science Fellowship Program, http://sites.nationalacademies.org/PGA/Jefferson/

[28] The Internet Governance Forum, United Nations, http://www.intgovforum.org/cms/

[29] APEC Telecommunications and Information Working Group, Strategic Action Plan 2016-2020, http://www.apec.org/~/media/Files/Groups/TEL/20150331_APEC%20TEL%20Strategic%20Action%20Plan%202016-2020.pdf

[30] Asia Pacific Programme for Senior Military Officers (APPSMO), http://www.rsis.edu.sg/networking/asia-pacific-programme-for-senior-military-officers-appsmo/

CONCLUSION

Although Singapore has done an excellent job in providing a vibrant ecosystem to attract foreign investors and has grown its economy exponentially over the 50-year history of its nation, it remains very vulnerable. Even with vast intellectual resources, as a small country, it could face sudden attacks, including cyberattacks, and lose the trust or confidence of its people and foreign investors, if it is not resilient enough to recover quickly. It needs to leverage on its international partners, collaborations, and external expertise in the short term and groom local talents in the long term. It must continue to use its political capital to expand and lead networking in the Asia-Pacific region in the cyber security areas. It is less likely that Singapore would be the main target for cyber attacks, but it could still get entangled and become collateral damage in a global conflict.

With the government's concerted effort in strengthening cyber security, Singapore could prepare for potential attacks, protect their cyber assets, gain public trust, and develop some niche technologies and skills. By leveraging these technologies and skills to provide service to its neighbours, the ASEAN community, and the rest of the world, Singapore could fuel its economic growth and maintain its stability.

ABOUT THE AUTHOR

Cung Vu is a Visiting Senior Fellow at the Rajaratnam School of International Studies (RSIS), Nanyang Technological University. Dr Vu is also an independent consultant, following his retirement from the US government. Prior to his retirement, he served as Associate Director at the Office of Naval Research Global in Singapore. He acted as a technical broker linking the Office of Naval Research (ONR), the Naval Research Enterprise with international scientific community. Dr Vu also served as Chief Science and Technology Advisor at the National Maritime Intelligence-Integration Office (NMIO) where he advised the Director of NMIO on the implications of emerging technologies in the maritime domain. He fostered engagement and information sharing amongst the NMIO stakeholders (Federal, State, Local Government, Academia, Private sector, and Foreign Partners) focusing on S&T. He is a chemical engineer with 35 years of experience in industries, academia and government. He received his Ph.D. in Chemical Engineering from Monash University, Australia and his B.S. in Chemical Engineering with Honours from University of Sydney, Australia.

ABOUT THE S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

The S. Rajaratnam School of International Studies (RSIS) is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS' mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-Traditional Security, International Political Economy, and Country and Region Studies. RSIS' activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information about RSIS, please visit www.rsis.edu.sg.

RSiS Nanyang Technological University | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg