Driving Security and Accountability in a Smart Singapore

STP Seminar on the Future of Work

Cybersecurity Group

20 July 2018

Wajeeha Ahmad

Nathaniel Fruchter

Marc Gallet

Peilan He

Jan-Aurel Pfister

Bryan Phee

Yuwen Zhang

Table of Contents

1 Executive summary

Singapore is one of the most connected countries in the world. It has leveraged its expertise in digital and IT technologies to make itself a regional—and worldwide—leader in the integration of technologies into governments, cities, and everyday life. While this provides significant advantages for the country, it also opens it up to many potential cybersecurity threats. These threats will continue to grow as the country pursues its Smart Nation initiatives and adopts cutting-edge Artificial Intelligence (AI) and Internet-of-Things (IoT) technologies into its infrastructure.

While Singapore has made significant strides through the creation of its Cyber Security Agency and adoption of the Cybersecurity Act of 2018, cybersecurity is only as strong as its weakest link. An increasing number of citizens and stakeholders will start bearing responsibility for the country's cybersecurity as Singapore embraces its Smart Nation Programme.[1] As such, upholding good computer security standards is a **shared responsibility** at each level of the society: among the Singaporean population, through the practices of corporations and enterprises, and through government policy.

We propose a framework for accountability with respect to cybersecurity vulnerabilities among those participating in a smart Singapore. We identify key pillars of accountability that can build on existing work by the Singapore government and bridge gaps in current corporate and government policy. Specifically, we discuss a four-part definition of accountability.

First, *accountability through standards and hygiene* recognizes the fact that security is a shared responsibility for citizens and companies. By leveraging the government's role as a standards setter, it can nudge companies providing products and services to integrate a higher amount of security by design into their productions.

Second, *accountability through increased data sharing* acknowledges that stakeholders can increase Singapore's cybersecurity by overcoming the current siloed approach to maintaining data on security incidents. By using the government's convening power and position as a trusted intermediary, it can encourage stakeholders to work together and share valuable security data for the benefit of all.

Third, *accountability for artificially intelligent systems* recognizes that novel threats present themselves for AI-driven systems*.* By targeting research towards threats like adversarial learning and recognizing the presence of potential vulnerabilities in AI systems, Singapore can more safely integrate them into its infrastructure and head off future attacks.

Finally, we must create a *foundation for accountability* by building on existing education and workforce training efforts. Increasing the scope of current cybersecurity education and re-skilling efforts will build a more capable and engaged population at every level of society.

We believe that these four key pillars can help Singapore maintain its leadership on cybersecurity and further establish itself as an example of what a smart, connected nation can look like.

[1] "Smart Nation Singapore." Accessed July 19, 2018. https://www.smartnation.sg/.

2 Introduction

In its relatively short 53 years of growth, Singapore has impressively managed to transform itself from a backward fishing village into the respected Asian powerhouse that it currently is. Today, the Lion City is widely regarded as a leading financial capital and a major transportation hub, with significant air and sea cargo passing through its borders. The status that Singapore enjoys makes it an attractive target for attackers. In fact, the country's infrastructure has already suffered attacks[2]. However, this status also bolsters its potential as a leader in the cybersecurity domain.

2.1 The Singaporean context

Being geographically limited, Singapore has consistently taken appropriate measures to defend itself and deter potential attackers. Such policies include mandatory national service for all Singaporean men aged above 18 to bolster its physical defence forces. As the world steps into an increasingly connected future, Singapore has also digitised its economy and followed suit by kicking off its 'Smart Nation' framework to transform the country through technology.

Singapore is a world leader in connectedness, ranking 1st in the world for the Networked Readiness Index as assessed by the World Economic Forum since 2015. This evolution has also come with a growth in the number of cyber threats locally; in 2017, there were a total of 5,430 reported cybercrimes, corresponding to 16.6% of crimes that took place in Singapore[3]. It is clear that the next generation of attacks will be shifting to the cyberspace; given Singapore's desire to continue building on its connectedness, having suitable cybersecurity measures in place is key to maintaining the resilience and security of the nation as citizens' exposure to cyberattacks increases.

Another factor that contributes to the strong need for a comprehensive cybersecurity strategy in Singapore is the rapidly ageing population that the country is currently facing. Between now and 2030, the number of citizens aged 65 years and above is set to more than double[4]. Studies have shown that a person aged 65 years and above is 35% more likely to be a victim of a financial scam than another person in his or her 40s. In addition, the group of Singaporean people aged 50 years and above registered the highest year-on-year increase in Internet use[5]. Having a population with a disproportionately large group of aged people, combined with the statistics that show that elderly people are more likely to be victims of cyberattacks and the fact that these same elderly people are getting increasingly connected, means Singapore needs to take appropriate measures to ensure accountability among all Singaporeans for the country's cybersecurity.

[2] "Cyber attacks on NUS, NTU: Singapore latest target of ever-growing cyber threat." (2017). https://www.straitstimes.com/tech/singapore-latest-target-of-ever-growing-cyber-threat

[3] CSA. (2017). Singapore Cyber Landscape 2017. Retrieved July 19, 2018, from https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecyberlandscape2017.pdf

[4] Population.sg. (2018). Demographics. Retrieved July 19, 2018, from https://www.population.sg/population-trends/demographics

[5] Fong, J. H. (2017, January 04). Protecting the Elderly from Cyber Attacks. Retrieved July 19, 2018, from https://www.todayonline.com/singapore/protecting-elderly-cyber-attacks

2.2 The challenge

Singapore has already put a lot of thought into cybersecurity; this is demonstrated by its Cyber Security Agency, governmental strategy, and new Cybersecurity Act. However, a challenge presents itself: how can the country *maintain* this advantage as the country's digital footprint grows? Put another way, *how do we ensure accountability for cybersecurity among those participating in a smart Singapore*?

This report answers the challenge by laying out a broad set of findings within several cybersecurity domains relevant to Singapore, including its smart city initiatives, leadership in autonomous vehicles, and efforts to up-skill the nation's workforce. We lay out an accountability-centred framework for cybersecurity in Singapore and provide a set of policy recommendations aimed at enhancing existing government schemes and filling gaps identified in previous sections.

3 Building in accountability

As autonomous vehicles, AI, and smart city technologies continue to be introduced into Singapore, an increasing number of citizens and stakeholders will start bearing responsibility for the country's cybersecurity. How can the country leverage its existing work on cybersecurity while ensuring those participating in a smart Singapore remain ready for future threats?

We provide several policy proposals based on *cybersecurity accountability* to enable this vision. Since all participants in Singapore's smart nation will bear responsibility for its security, our use of accountability reflects the fact that all groups—from individuals to government agencies and corporations—will need to proactively work to maintain and grow their cybersecurity expertise. These responsibilities will need to be checked and enforced throughout their lifecycle.

In this section, we discuss the four pillars of *standards and hygiene, data sharing, security for artificial intelligence,* and *education.* These pillars reflect areas where the government can build upon existing work while maintaining a high impact. They also reflect a need to focus on prominent, high-risk areas of active research and investment.

3.1 High-level cybersecurity strategy

Before diving into accountability, it is important to discuss Singapore's existing view on cybersecurity. The government recognised the need for cybersecurity early and put in place several measures to ensure that the country would be well-protected in the cyber domain. The Cyber Security Agency (CSA) was established in 2015 with the intention to tackle the latest cyber threats as well as oversee long-term policies in the area. Since its inception, CSA has put forth multiple recommendations, which culminated in the Cybersecurity Act introduced in 2018[6]. The former can be summarized in the following points:

- The act designates Critical Information Infrastructure (CII) and provides CII owners with advice on how to protect their systems.

[6] CSA. (2018). Cybersecurity Act. Retrieved July 19, 2018, from https://www.csa.gov.sg/legislation/cybersecurity-act

- The Commissioner of Cybersecurity is empowered to investigate cybersecurity threats and incidents to prevent future attacks.
- CSA is given the power to request, protect and share related cybersecurity information as it deems fit.
- CSA is given the ability to license service providers for penetration testing and security operations centre (SOC) monitoring.

The measures that CSA has implemented has helped Singapore lead the world in terms of cybersecurity; the International Telecommunication Union's Global Cyber Security Index ranked Singapore 1st in the world for 2017.[7] After consideration by the government and selected committee members, the Cybersecurity Strategy was drawn up and published in 2016[8].

3.2 Cybersecurity standards and hygiene

Singapore has provided leadership in the area of cybersecurity standards, but can build on its current work to ensure accountability through standards for smart city products.

3.2.1 Findings

As a part of its Cybersecurity Strategy, the CSA has set up the Singapore Common Criteria Scheme (SCCS) to help companies evaluate the security performance of their IT products that they use in their implementation. These established international Common Criteria (CC) standards are used to promote security-by-design to protect companies from the financial threats posed by cyberattacks.[9] However, this is limited to hardware architectures in the area on which standards are imposed.

Other parts of the Strategy are broader than standards concerning hardware.[10] For example, the requirement to protect critical infrastructure led to the enactment of the Cybersecurity Act, where multiple requisites for critical information infrastructure were formulated, such as mandatory incident reporting, audits and risk assessments.[11] Since cybersecurity affects everyone from businesses and governments to individuals and is international in nature, Singapore's strategy aims to create a safer cyberspace and partly do so through strengthening international collaboration and partnerships.[12] However, this strategy only works if stakeholders can be held accountable, and accountability only works if regulators know what to hold people accountable for. This is where we believe the creation of security standards for devices can come in.

[7] Ghosh, N. (2018, March 21). Cyber Security Essential to Singapore's Survival: CSA Chief David Koh. Retrieved July 19, 2018, from https://www.straitstimes.com/world/united-states/cyber-security-essential-to-singapores-survival-says-csa-chief-david-koh

[8] CSA. (2016). Singapore's Cybersecurity Strategy. Retrieved July 19, 2018, from https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

[9] CSA. (2018). CSA Common Criteria. Retrieved July 19, 2018, from https://www.csa.gov.sg/programmes/csa-common-criteria

[10] CSA. (2016). Singapore's Cybersecurity Strategy.

[11] CSA. (2018). Cybersecurity Act.

[12] CSA. (2016). Singapore's Cybersecurity Strategy.

3.2.2 Recommendations

One common problem in cybersecurity is *information asymmetry*, which rises when end users of systems are not able to judge the security of the systems. The SCCS and other non-binding standards provide guidelines. However, this lack of transparency to the end users may render them less effective. Information asymmetry can be tackled through certifying products that comply with various security standards, making it easy for the user to understand the security of the products.

It is important that a device that comes to the market is immune against current attack vectors. Due to the coevolution of cybersecurity and hackers, the software will eventually be breached anyway, leading to the fact that the lifetime of a software is in most cases shorter than the lifetime of a device.[13] Therefore, software maintenance and upgrades should be provided by a manufacturer. These two, together with other variables like efforts to detect vulnerabilities, could be merged into a classification system that evaluates the level of cybersecurity of the software.

1. We propose a classification label with the respective level of cybersecurity based on the guidelines and standards the manufacturers abide by. This could look similar to EU's energy efficiency label (Figure 1). The manufacturers of devices or software that are intended to be used in Singapore are required to obtain the label from the government. The manufacturers should clearly state the guidelines and standards they intend to follow. In the case that the manufacturers refuse to specify the guidelines and standards they follow, the label's lowest level of security could be issued.

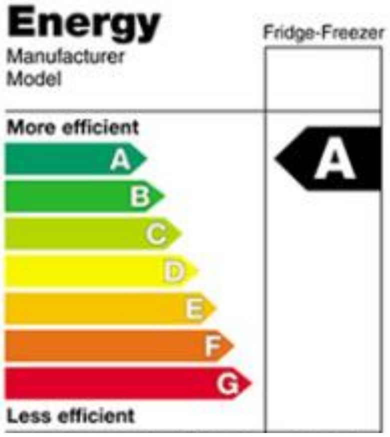

Figure 1. The European Union's energy usage label.

This label should be placed on the products and made visible to consumers. The psychological effect of buying products with better rankings act as a demand-side incentive for manufacturers to offer better cybersecurity.

2. We propose that government agencies and critical infrastructure operators are only allowed to employ certified devices and software that comply to a predetermined minimum standard of cybersecurity. While it may take a longer time to integrate certification and standards into the consumer market, the government can leverage its position to phase in certification processes in these crucial markets.

3. In the event of a cybersecurity incident, the Commissioner appointed by the Cybersecurity Act can investigate whether the manufactures have complied to their declared standards through mandatory incident reporting and the system logs. The Commissioner is then able to punish the

[13] Fu, Kevin, and James Blum. 2013. "Controlling for Cybersecurity Risks of Medical Device Software." Communications of the ACM 56(10): 35.

manufacturers if they did not follow their promised standards, for instance, if the manufacturer did not provide the promised security update.

3.2.2.1 Singaporean context

Singapore is very advanced regarding to cybersecurity awareness and regulation. We intend to leverage these efforts to increase the benefit from existing policies. The Commissioner appointed by the new Cybersecurity Act in 2018 can be leveraged to additionally investigate standards violations. This would constitute a cost-effective use of current resources and provide them with clear judging rules that might increase the efficiency. Furthermore, existing efforts like cybersecurity awareness campaigns and the cybersecurity awareness alliance can be used to familiarize the population, small and medium-sized enterprises, as well as big companies with the certification.

Finally, there is a gap in cybersecurity standards among different countries. It makes it hard to regulate cybersecurity on the international level as Internet is not bounded by the geographic boundaries of countries. Singapore can be the first nation to establish such standards and act as a leader in the future policy development in cybersecurity.

3.3 Data sharing for security

With increasing reliance on digital infrastructure within and outside the government, it is becoming more and more important for organizations to share data on existing cybersecurity vulnerabilities.

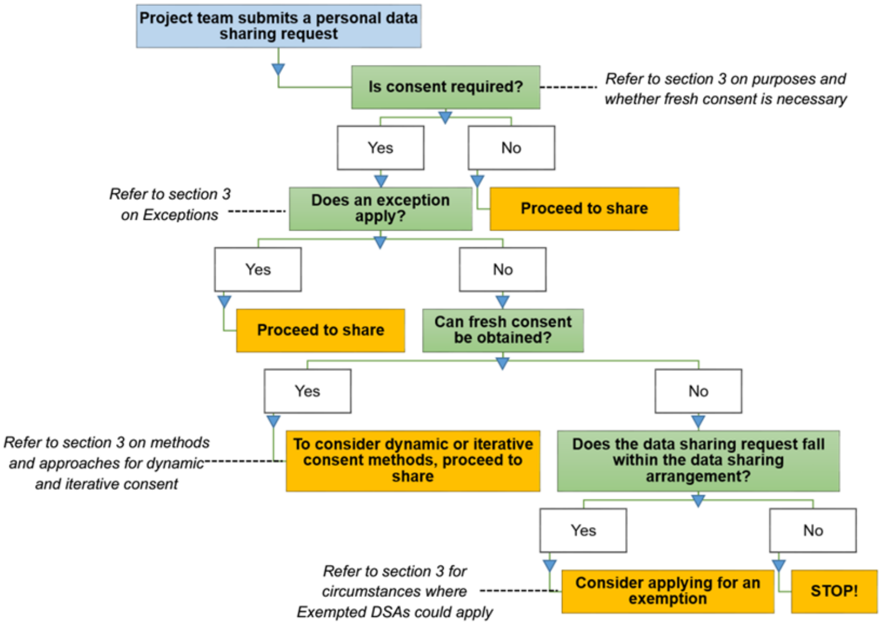
Project team submits a personal data sharing request
Is consent required?
Refer to section 3 on purposes and whether fresh consent is necessary
Yes
No
Refer to section 3 on Exceptions
Does an exception apply?
Proceed to share
Yes
No
Proceed to share
Can fresh consent be obtained?
Yes
No
Refer to section 3 on methods and approaches for dynamic and iterative consent
To consider dynamic or iterative consent methods, proceed to share
Does the data sharing request fall within the data sharing arrangement?
Yes
No
Refer to section 3 for circumstances where Exempted DSAs could apply
Consider applying for an exemption
STOP!

Figure 2. A sample data-sharing workflow that organizations can consider to adapt.

3.3.1 Findings

Data sharing can generate numerous benefits for both organizations and the broader public. For corporations and government agencies, mutual data sharing can significantly reduce the costs of detecting common vulnerabilities; to funders, it makes optimal use of publicly funded research and maximize return on investment; to the public, it reduces the probability of breaches of personal data and prevents damages to heavily relied-upon critical infrastructure.[14] In addition, all information sharing improves cyber incidents or attacks prevention, detection, prediction, response and recovery.

However, many issues should be considered before and during data sharing, especially from the view of cyber security. Singapore has proposed the Personal Data Protection Act 2012 ("PDPA") which applies to the sharing of personal data within and between organizations.[15] It aims to help Data Protection Officer to identify the appropriate approach for sharing personal data in compliance with the PDPA. As Figure 2 illustrates, the PDPA establishes a consent-based approach towards personal data sharing and sets out exceptions where organisations may collect, use or disclose personal data without consent.

3.3.2 Policy recommendations

While the Government of Singapore has made efforts towards the sharing of personal data with and between organizations, more efforts need to be directed towards the sharing of data for cybersecurity incidents to enhance the resilience of critical and digital infrastructure. Many stakeholders have identified barriers to sharing crucial security data and we believe the government can incentivize a smoother sharing process.

1. **A phased approach to increasing data sharing among companies.** We recommend a phased approach towards data sharing of cybersecurity vulnerabilities between government agencies and corporations. To start with, the government should consider mandating the disclosure of cybersecurity vulnerabilities for vendors who provide technology for critical infrastructure such as smart city sensors for the Land Transport Authority (LTA). The United States has led in the creation of coordinated vulnerability disclosure schemes, which Singapore could take inspiration from.[16]

2. Reducing friction for sharing security data. In addition, the government should also consider the development of incentive structures to enable companies to disclose vulnerabilities and significantly reduce the costs incurred by companies and citizens of detecting and facing the consequences of software vulnerabilities. Singapore could consider structures like those proposed by the European Union's network security agency, ENISA.[17]

[14] See, for example, "ISAOs: The benefits of sharing security information." https://searchsecurity.techtarget.com/tip/ISAOs-The-benefits-of-sharing-security-information

[15] "Personal Data Protection Act 2012 - Singapore Statutes Online." Accessed July 19, 2018. https://sso.agc.gov.sg/Act/PDPA2012.

[16] For example, see "ICS-CERT Vulnerability Disclosure Policy," https://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy.

[17] "Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches." ENISA. December 2015.

3. Embrace bug bounties. Bug bounty programs encourage the discovery of cybersecurity vulnerabilities. While Singapore Ministry of Defence has recently launched a Bug Bounty Programme[18], there exists significant room to both increase the payout amounts to encourage broader participation and extend this effort towards other government agencies and developers of critical infrastructure.

3.4 Artificial intelligence and cybersecurity

In this section, we focus on cybersecurity challenges associated with adoption of artificial intelligence (AI) technologies.

3.4.1 Findings

3.4.1.1 Technical context

AI technologies underpin many of the advances in smart city and autonomous vehicle infrastructure being implemented in Singapore. Specifically, deep neural networks (DNNs) are vulnerable to so-called adversarial examples. Adversarial examples are inputs such as images which have deliberately been modified to produce a desired response by a DNN. A recent paper by MIT students showed how easy it is to trick an AI-based vision system into wrongly classifying 3D objects, when a 3D-printed turtle was identified as a rifle.[19] Numerous other examples have also shown that real-world video imaging is now vulnerable to adversarial attacks.[20] The adversarial images may look the same to humans, but changing a few pixels can cause computer vision systems to make completely different decisions. Among the most striking versions of an adversarial attack is the one-pixel attack in which changing one pixel can throw these systems off completely.[21]

As Figure 3 illustrates, adversarial attacks pose a real threat to the deployment of AI systems in security critical applications[22]. Virtually undetectable alterations of images, video, speech, and other data have been crafted to confuse AI systems. Such alterations can be crafted even if the attacker doesn't have exact knowledge of the architecture of the DNN or access to its parameters. Even more worrisome, adversarial attacks can be launched in the physical world: instead of manipulating the pixels of a digital image, adversaries could defeat visual recognition systems in autonomous vehicles (AVs) by sticking patches to traffic signs.

[18] "Fact Sheet: Ministry of Defence (MINDEF) Bug Bounty Programme 2018 Results." Accessed July 19, 2018. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2018/february/21feb18_fs.

[19] "Fooling Neural Networks in the Physical World." labsix. Accessed July 19, 2018. http://www.labsix.org/physical-objects-that-fool-neural-nets/.

[20] Akhtar, Naveed, and Ajmal Mian. "Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey." *ArXiv:1801.00553 [Cs]*, January 2, 2018. http://arxiv.org/abs/1801.00553.

[21] Su, Jiawei, Danilo Vasconcellos Vargas, and Sakurai Kouichi. "One Pixel Attack for Fooling Deep Neural Networks." *ArXiv:1710.08864 [Cs, Stat]*, October 24, 2017. http://arxiv.org/abs/1710.08864.

[22] Ackerman, Evan. "Slight Street Sign Modifications Can Completely Fool Machine Learning Algorithms." IEEE Spectrum: Technology, Engineering, and Science News, August 4, 2017. Images from Eykholt et al., "Robust Physical-World Attacks on Deep Learning Models." https://arxiv.org/abs/1707.08945.

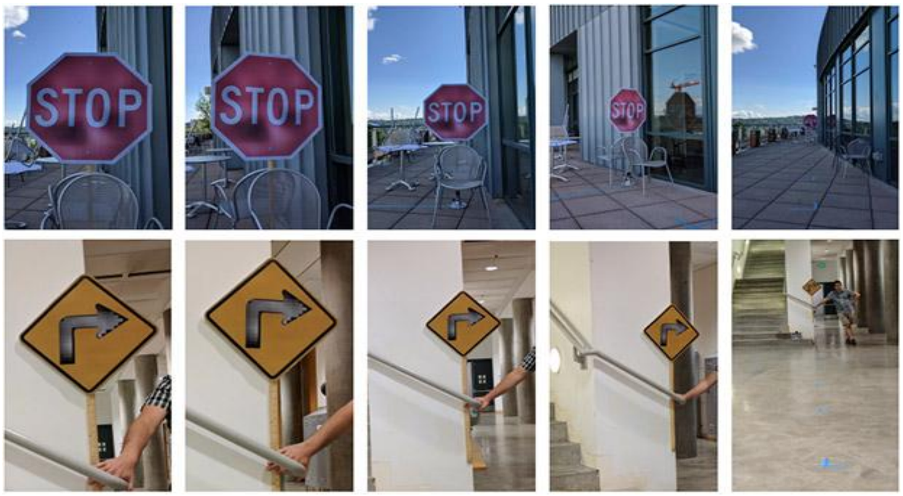

Figure 3. Subtle perturbations cause a neural network to misclassify stop signs as speed limit 45 signs, and right turn signs as stop signs.

3.4.1.2 Singaporean context

Singapore has made significant strides towards becoming a global AI powerhouse. Launched in May 2017, AI Singapore is a five-year, S$150 million national program to enhance Singapore's capabilities in AI.[23] Additionally, Singapore's Land Transport Authority has a dedicated autonomous vehicle initiative that plans to make Singapore the first large-scale test-bed for autonomous vehicle technology.[24] The modern autonomous vehicle is arguably the "smartest" consumer electronic device on the market.

The incredible power, efficiency, and safety potential that accompanies this AI-powered innovation is shadowed by the risks of exploitation. It is imperative that efforts towards the widespread adoption of AI technology in Singaporean society is also accompanied by comprehensive efforts to combat security challenges associated with mission-critical and life-critical AI systems. Consider the effects of an adversarial attack on a fleet of autonomous vehicles, a surveillance camera system in a city, or a fleet of autonomous drones delivering packages. In all of these instances, the car, drone, or camera is dependent on the AI vision system to correctly identify a road sign, a drop off location, or faces to ensure the correct working of a system. Therefore, all such instances could have catastrophic consequences if directed and comprehensive efforts are not made to tackle various adversarial attacks.

3.4.2 Recommendations

Potential defense methods for adversarial examples such as different types of adversarial training methods have also been widely studied.[25] A growing area of research is looking into thwarting such adversarial attacks, changing the algorithms themselves, and making them more robust to such attacks.[26] Overall, we

[23] AI Singapore. Accessed July 19, 2018. https://www.aisingapore.org/.

[24] "Singapore Autonomous Vehicle Initiative | Land Transport Authority." Accessed July 19, 2018. https://www.lta.gov.sg/content/ltaweb/en/roads-and-motoring/managing-traffic-and-congestion/intelligent-transport-systems/savi.html.

[25] Tramèr, Florian et al. "Ensemble Adversarial Training: Attacks and Defenses." ArXiv:1705.07204 [Cs, Stat], May 19, 2017. http://arxiv.org/abs/1705.07204; Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy. "Explaining and Harnessing Adversarial Examples." *ArXiv:1412.6572 [Cs, Stat]*, December 19, 2014. http://arxiv.org/abs/1412.6572.

[26] Guo, Chuan, Mayank Rana, Moustapha Cisse, and Laurens van der Maaten. "Countering Adversarial Images Using Input Transformations," February 15, 2018. https://openreview.net/forum?id=SyJ7ClWCb.

are still a long way from finding the optimal defense strategy against these adversarial examples, and we are looking forward to exploring this exciting research area. In light of this, we make two main proposals.

1. Government initiatives such as AI Singapore should support collaborations amongst both researchers and developers in defending Deep Neural Networks (DNNs) against adversarial attacks and thereby making AI systems more secure.

This can be done via setting up institutional partnerships or programs with a focus on defense efforts, including supporting the development of an open-source software library to support researchers and developers in creating novel defense techniques, as well as in deploying practical defenses of real-world AI systems. An example of a similar initiative is the Adversarial Robustness Toolbox released by IBM Research Ireland, which provides interfaces supporting the composition of comprehensive defense systems using individual methods as building blocks.[27] A similar program in Singapore that create a vibrant ecosystem of contributors both from industry and academia will enable researchers to benchmark novel defenses against the state-of-the-art in making autonomous vehicles and other AI technologies resilient to adversarial examples.

There is a need for continued systemic investigations in this area that stimulate research and development around adversarial robustness of DNNs, and advance the deployment of secure AI in real world applications. This is especially important since adversarial threats keep advancing with "counter-counter" measures being adopted by adversarial algorithms.

2. Since the existence of adversarial threats poses significant questions about the robustness of AI vision algorithms and their readiness, comprehensive risk assessments should be undertaken. The fact that one pixel could throw off a stop sign classifier in a self-driving car is a major cause for worry and suggests that Level 4 and Level 5 automation should perhaps come with a safety warning.

3.5 Education and workforce development

Cybersecurity is ever changing: tomorrow's threats will be different from the ones we know today. Consequently, security recommendations evolve over time and it is a challenge to keep every individual up to date. These challenges are faced by everyone, from individuals to large corporations.

3.5.1 Findings

In the general population, the main issue is a lack of awareness about cybersecurity. Few have attended any courses or training on the subject, yet the vast majority of the population owns and/or works with a computer or smartphone. As attacks are often invisible, most don't feel the need to care for this topic on a day-to-day basis. This lack of visibility means that people don't often seek education in the area. In addition, people usually react only after they have been affected by an attack and, before that, tend to think that this only happens to others. Finally, training people about cybersecurity once is not enough. It is a continuous process which needs to be repeated regularly to not only keep up to date, but also keep the level of awareness sufficiently high.

[27] "IBM/Adversarial-Robustness-Toolbox" Accessed July 18, 2018. https://github.com/IBM/adversarial-robustness-toolbox.

In companies, cybersecurity risks can be classified into two categories: (i) threats impacting the company's own IT systems, whose failure can affect the company's ability to do business or impact its revenues, and (ii) threats emanating from the products that the company produces (these products can be software/online services or devices with embedded software which may be vulnerable or not secured enough).

In the first case, the risk is increased if the company lacks the resources and/or talent to properly secure the company's IT infrastructure or lack properly defined and enforced IT security procedures. Because any employee could be the vector leading to a security incident, regular in-house training is needed. The second case arises when the company fails to include sufficient security consideration in the design of their products. This can be the result of the higher cost and time required to market a product with appropriate cybersecurity measures, but can also result from a lack of expertise. While we consider the second case in a previous section (see *Standards*), in both cases, industry has expressed concerns regarding the chronic shortage of human capital skilled in cybersecurity and that it is difficult to hire the right people and to retain them.[28]

3.5.2 Recommendations

As a small nation, the impact of a cyberattack on the general populace could be particularly critical. Singapore regularly attempts to educate the general population via boards and posters in public spaces (such as bus stops and MRT stations) and has already launched two cybersecurity campaigns.[29] However, we believe more targeted campaigns can build on this work.

1. For the general public, include more basic cybersecurity courses in the curriculum of primary, secondary and post-secondary education. This could take different forms depending on the age of students. The goal of this recommendation is that, over time, a mindset of caring about cybersecurity percolates from the young people into the population. While the Ministry of Education already has "Cyber Wellness Education" in the formal curriculum, which includes education on anti-bullying efforts,[30] this curriculum could be expanded to include other digital threats, including but not limited to recognizing trusted sources and links on the Internet and not clicking on links from untrusted sources.

2. The government of Singapore and local universities should direct further efforts to both increase specialised offerings in cybersecurity and increase the number of students in specialized degrees in the field of cybersecurity.

[28] "IT Talent in Short Supply amid Smart Nation Push, Manpower News & Top Stories - The Straits Times.". https://www.straitstimes.com/singapore/manpower/it-talent-in-short-supply-amid-smart-nation-push; "Singapore Taking Lead in Fighting Cybercrime, but Expertise Remains in Shortage - Channel NewsAsia." https://www.channelnewsasia.com/news/singapore/singapore-taking-lead-in-fighting-cybercrime-but-expertise-9235890.

[29] "Cyber Security Awareness Alliance." Cyber Security Agency. Accessed July 19, 2018. http://www.csa.gov.sg/gosafeonline; "CSA Launches Second National Cybersecurity Awareness Campaign - 'Cyber Tips 4 You.'" Cyber Security Agency. Accessed July 19, 2018. http://www.csa.gov.sg/news/press-releases/csa-launches-second-national-cybersecurity-awareness-campaign.

[30] "Cyber Wellness." Accessed July 19, 2018. https://www.moe.gov.sg/education/programmes/social-and-emotional-learning/cyber-wellness.

Singapore already has a program for lifelong skill training into place called SkillsFuture,[31] and various local universities and private training providers already have course offerings related to cybersecurity.[32] Current efforts are a good start and should be continued.

3. Finally, for the workforce, we recommend expanding outreach campaigns specifically aimed at cybersecurity threats in the workspace. This could build upon the existing Employee Cyber Security Kit[33] and extend it with more freely and readily available resources on workplace cybersecurity that can be easily distributed to the employees in companies that do not have the time and manpower required to develop an employee education programme. Materials should also be translated and adapted to be accessible and available to Singapore's large foreign workforce, an integral part of the country's employee base.

4 Conclusion

The Government of Singapore has clearly demonstrated its leadership in the cybersecurity domain. This report demonstrates that this leadership can be built upon by recognizing that security is a shared responsibility at each level of the society: among the Singaporean population, through companies' practices, and through government policy.

This report's four pillars of accountability identify gaps and opportunities for growth in current policy in the areas of standards, data sharing, AI, and education. It recommends implementing risk-based and compliance-based policies to increase accountability. These measures, especially in the area of standards, are designed to be phased in with a short-term focus on critical infrastructure. By staying proactive, the Singaporean government can maintain its leadership on cybersecurity and further establish itself as a smart and secure nation.

[31] "SkillsFuture - Home." Accessed July 19, 2018. http://www.skillsfuture.sg/.

[32] "NUS Computing - Masters in Infocomm Security." Accessed July 19, 2018. http://www.comp.nus.edu.sg/programmes/pg/misc/; "Cybersecurity | School of Information Systems (SMU)." Accessed July 19, 2018. https://sis.smu.edu.sg/initiatives/cybersecurity; "Master of Science in Security by Design." Information Systems Technology and Design (ISTD). Accessed July 19, 2018. https://istd.sutd.edu.sg/education/master-science-security-design/; Cybersecrrity courses, NTU Learning Hub, https://www.ntuclearninghub.com/cyber-security-courses-boost-career/

[33] "Employee Cyber Security Kit." Cyber Security Agency. Accessed July 19, 2018. http://www.csa.gov.sg/gosafeonline/resources/employee-cyber-security-kit.

5 Appendix 1: Summary of Recommendations

5.1 Standards

Create a classification label for cybersecurity based on the guidelines and standards the manufacturers abide by. This can drive demand among consumers for better security.

Make government agencies and critical infrastructure operators employ certified devices and software. The government can use its leverage to drive certification for this critical area.

In the event of an incident, the Commissioner appointed by the Cybersecurity Act can investigate whether the manufacturers have complied. Compliance can be assessed through system logs and mandatory incident reporting.

5.2 Data sharing

Phased approach towards data sharing of vulnerabilities between government agencies and corporations. Consider mandating vulnerability disclosure for those who provide critical infrastructure such as smart city sensors for the Land Transport Authority.

Make it easier to share security data. Consider the development of incentive structures to enable companies to disclose known cybersecurity vulnerabilities and significantly reduce the costs incurred doing so.

Extend bug bounty programmes. Build on the Ministry of Defence's bounty to increase payout amounts and extend this effort to other government agencies and infrastructure providers.

5.3 Artificial intelligence

Government initiatives such as AI Singapore should support collaborations among researchers and developers in defending neural networks against novel attacks. Adversarial attacks are one example of a research area that can be promoted.

Consider vulnerabilities like adversarial attacks before deployment of systems. The presence of these attacks should encourage risk assessment before deployment.

5.4 Education and workforce

Include more basic cyber security courses in the curriculum of primary, secondary and post-secondary education. Having a full pathway is crucial to developing awareness and talent.

Expand outreach campaigns specifically aimed at cybersecurity threats in the workspace. Existing government toolkits could be leveraged to provide a curriculum for small and medium-sized enterprises unable to develop an education programme for their own employees.