

**Israel National Defence College**

**47th Class 2019-2020**

**Cyber Security and its Influence on Social Resilience**

* **A Singapore Perspective**

Academic Advisor: Prof. Daphna Canetti

Submitted by: Wong Khiong Seng

xx May 2020

**ABSTRACT**

<to be included>

**ACKNOWLEDGEMENT**

<to be included>

|  |  |  |
| --- | --- | --- |
|  | **TABLE OF CONTENT** | **PAGE** |
| **Abstract** | | **1** |
| **Acknowledgement** | | **2** |
| **Table of Content** | | **3** |
|  |  |  |
| **Chapter 1: Introduction** | |  |
| **1.1** | **Background** | **5** |
| **1.2** | **Research Outline** | **7** |
| **1.3** | **Significance of Research** | **8** |
| **1.4** | **Methodology** | **9** |
|  |  |  |
| **Chapter 2: Cyber Terrorism Threats to Singapore** | |  |
| **2.1** | **Evolution of the Cyber Threats** | **10** |
| **2.2** | **The Collateral Consequences from Cyber Attacks** | **12** |
| **2.3** | **The Challenge to Singapore’s Multiculturalism** | **17** |
| **2.4** | **Cyber Vulnerability to Singapore as a Smart Nation** | **19** |
| **2.5** | **Social and Psychological Resilience Defined** | **21** |
|  |  |  |
| **Chapter 3: Singapore’s and Israel’s National Cyber Defence Strategy** | |  |
| **3.1** | **Singapore’s Cyber Security Strategy** | **25** |
| **3.2** | **Digital Defence as part of Singapore’s Total Defence Strategy** | **30** |
| **3.3** | **The Israeli National Cyber Security Strategy** | **32** |
|  |  |  |
| **Chapter 4: Comparative Analysis of Singapore’s and Israel’s National Cyber Security Strategy** | | ~7pp |
| **4.1** | **Comparison Metrics** | **36** |
| **4.2** | **Perception of Cyber Threat** | **36** |
| **4.3** | **Stakeholders Identified And Approach** | **37** |
| **4.4** | **Incident Response Capabilities** | **38** |
| **4.5** | **Capacity Building** | **39** |
| **4.6** | **Policy and Regulations** | **40** |
| **4.7** | **Summary of Comparative Analysis** | **41** |
|  |  |  |
| **Chapter 5: Recommendations** | |  |
| **5.1** | **Communicating a Strong Narrative (raise threat perception in public through exercises involving public also, besides business)**  **Online threats, need bottom approach as well** | **43** |
| **5.2** | **Emphasis on Preparedness (community support) – attack on infra**  **Make use of CEP, communicate threat through this avenue, exercises** |  |
| **5.3** | **Communications in times of crisis** |  |
|  | **Improve media literacy** |  |
| **5.4** | **The Role of Individual Resilience ((Individual level)**   * **Strengthen Community Support to aid Coping and Adapting (Fortify, Resilience)** |  |
| **5.5** | **A Culture of Preparedness (Society Level)**   * **Government Regulation of the Internet** * **Build up Science and Engineering Capital**   **Moving from Whole-of-Government to Whole-of-Society approach (extend to private sector)** |  |
|  |  |  |
| **Chapter 6: Conclusion** | |  |
|  |  |  |
| **Bibliography** | |  |
|  | |  |

**CHAPTER 1**

**INTRODUCTION**

**1.1 BACKGROUND**

The advancements and innovations in computer and communication technologies have resulted in radical improvements in information and communication capabilities. With rapid and widespread assimilation, this cyber phenomenon has led to significant changes in our social way of life and the design of our economy. Humans are now very interconnected via their smartphones and IT gadgets. Smart cities are being created where city infrastructures and services are linked up using interconnected systems for monitoring, control and automation. Within a very short span of time, individuals and companies have harnessed cyberspace to create new industries, a new economic sphere, and a vibrant social space that are intertwined with everyday lives. In this regard, Singapore is also pursuing its ambition to become a Smart Nation by leveraging significantly on the new industrial revolution fuelled by digital technologies. Singapore’s Smart Nation initiative is a whole-of-nation efforts to make its economy more productive and its citizens’ lives more convenient through digital transformation in its economy, government and society.

While the advent of cyberspace as a global phenomenon has offered many opportunities, it has also presented challenges to national security at the same time. As nations and critical infrastructure became more dependent on computer networks for their operation, new vulnerabilities are created. A hostile nation or group could exploit these vulnerabilities to penetrate a poorly secured computer network and disrupt or even shut down critical functions, potentially crippling the country.[[1]](#footnote-2) The cyber attack on Ukraine’s power grid in 2015, which caused disruption to electricity supply and left hundreds of thousands of homes in the Ivano-Frankivsk region of Ukraine without power for at least a few hours in a cold December is one such example.[[2]](#footnote-3) In 2016, a power outage that hit part of Kiev, which amounted to a loss of about one-fifth of Kiev’s power consumption at that time of the night, was also assessed to be attributed to cyber attack.[[3]](#footnote-4) There was also a series of cyber attacks on Ukraine’s banks, postal services, airport systems, hospitals, and government ministries within a single day in June 2017. These incidents highlighted the vulnerability of a nation in a cyber era and the challenges cyber threats poses to national security, as nations becomes ever more dependent on cyberspace for both its most basic and most critical functions.

Cyber terrorism also has adverse effects on the psychological well being of individuals. Increasingly, many financial services and essential government services have become highly dependent on the Internet and other information networks. Cyber attacks on these information systems can disrupt individual’s daily activities, causing increased stress and anxiety in individuals and making them feel insecure, which would in turn undermine the public’s morale and their confidence in economic and political institutions.[[4]](#footnote-5) In 2018, Singapore was hit by one of the worst data breach in its history when SingHealth, Singapore’s largest group of healthcare institutions, had 1.5 million patients’ record stolen by hackers, and that includes the data of its Prime Minister. The breach also stirred up an ensuing discussion on social media where many netizens voiced their frustrations on SingHealth’s handling of the issue, and expressed concerns over the privacy risks resulting from the database compromise.[[5]](#footnote-6)

Every nation must also defend itself against the spread of disinformation on social media as more of its people consume news, receive and share information through this platform. Disinformation, amplified by social media, can cause disunity and dissent among the population, resulting in social divisiveness. A polarisation of communities within a nation state will have protracted effects on society and can lead to its breakdown. Particularly for Singapore, a country that is multi-racial and multi-religious, and being small geographically with an open economy, the relative peace and tolerance among the various religious communities that it currently enjoys is achieved by maintaining social and religious harmony. However, cyber terrorism could polarize this multi-cultural society and create an adverse effect on its social fabric. This would then weaken Singapore’s social resilience as well as degrade its capacity to contain and effectively manage major national crisis, and its abilities to ‘bounce back’ rapidly to restore normalcy.

Therefore, it is imperative that Singapore pro-actively confronts and addresses the security challenges emanating from the evolving cyber threats, and ensure that its abilities to prevent cyber terrorism, as well as its capacity to withstand, respond, and recover from disruptions arising from cyber events stays relevant and effective.

**1.2 RESEARCH OUTLINE**

To this end, this paper seeks to answer the following questions:

1. How Singapore's cyber security strategy influences its social resilience against cyber threats?
2. Are there new policy changes and/or enhancements to the cyber security efforts in Singapore that can be pursued in a bid to strengthen social resilience?

Singapore has long embraced infocomm technologies for economic and social development and its use in Singapore is widespread, both in the public and private sectors. However, the reliance on infocomm technologies makes Singapore vulnerable to cyber threats. Like many countries, Singapore has placed much attention in cyber security to protect its critical infrastructure and also to secure cyberspace for business and communities through the implementation of its Cybersecurity Strategy. The most basic approach to cyber security is based on the idea of ‘resistance’ and it entails building defences against potential cyber attacks. However, a cyber security framework based on defence, or ‘resistance’ alone, is likely to be inadequate due to the high degree of uncertainty and unpredictability associated with cyber threats. Therefore, resilience towards cyber threats will be key. Here, resilience is defined as the ability to recover or ‘bounce back’. Taken together, this is not to say that ‘resistance’ is unimportant but that greater emphasis needs to be placed on ‘resilience’.

**1.3 SIGNIFICANCE OF RESEARCH**

The challenge of cyber is global and the rapid assimilation of cyber technologies into the conduct of our daily lives requires a nation to continually examine its evolving impacts, and to develop new ways to deal with the threats presented to national security. As Singapore charts its progress towards becoming a Smart Nation, enabled by a digital economy, government and society, it is even more critical that Singapore continues to have in place a relevant and effective cyber security strategy.

Similar to Israel, Singapore also recognised this lurking cyber threat against social resilience, and has seeded many initiatives and put in place measures to mitigate the cyber risks to society. Learning from best practices adopted by Israel, this paper seeks to explore new approaches that Singapore could pursue to combat cyber threats.

**1.4 METHODOLOGY**

This paper will present a qualitative analysis of Singapore’s cyber security strategy based largely on open-source documents, government official records and news reports. The paper will attempt to provide an overview of the cyber threats to Singapore, drawing the connection of its impacts to Singapore’s national security, especially in the area of societal given its unique social demography. This paper will then provide an in-depth examination of the key challenges of Singapore’s cyber security strategy. The paper will also seek to draw out key lessons on the cyber strategy and approaches from the Israeli experience and use it to make comparisons with Singapore’s digital defence approach. The paper will then conclude with a recommendation on new opportunities or framework that Singapore could adopt to better strengthen social resilience while transforming into a Smart Nation.

**CHAPTER 2**

**CYBER TERRORISM THREATS TO SINGAPORE**

**2.1 EVOLUTION OF THE CYBER THREATS**

Cyber threats have existed in various forms since the proliferated use of the internet. The cyber threats spectrum could range from malicious pranks by individual hackers, small scale cyber crimes by individual criminals looking for monetary gains, organised cyber crimes by criminal groups, cyber espionage by state or non-state actors to gain confidential information, to nation-state cyber attack and warfare.

In the 1990s to early 2000s, the cyber attacks came predominately from hackers as a form of malicious prank or criminal groups committing cyber crime. Software viruses or worms were used by these hackers to infect computers worldwide. The viruses or worms made malicious changes to the infected computers and generated millions of spam-messages which in turn caused slow network connections, network failures or even loss of files. One such example is the My Doom software virus, which had the capability to conduct Distributed Denial-of Service (DDoS) attacks.[[6]](#footnote-7) Criminal groups then capitalised on botnets to commit cyber crimes. These groups, using virus-controlled botnets, conducted DDoS attacks to extort money from businesses as well as phishing attacks to steal someone’s identity for profiteering.[[7]](#footnote-8) According to The Washington Post, a group of phishers, known as the Rock Group, reportedly stole about $150 million from bank accounts using such method.[[8]](#footnote-9)

Cyber attacks by state actors soon came into prominence in the late 2000s. The cyber attacks on Estonia in 2007 could be regarded as a harbinger of future attacks. In the weeks following a decision by the Estonian government to move the Bronze Soldier (a memorial commemorating the Soviet liberation of Estonia from the Nazis) to a lesser prominent location, Estonia suffered DDoS cyber attacks on the websites of its government ministries, major banks, newspapers and broadcasters. Estonian officials accused Russia of perpetrating the cyber attacks, to which the EU and NATO technical experts were unable to find evidences of it after investigation. Such an attack could be interpreted as a mild version of a new form of cyber terrorism where the effect was to disrupt public services, commerce, and government operations, and the intent driven by political purposes and not for commercial gains.[[9]](#footnote-10) Other examples of cyber attacks include the Russian DDoS attack on the Georgian government and local news website just before the Russian military invaded the town of Tskhinvali, a city in South Ossetia, Georgia, during the Russian-Georgian war of 2008; and the Russian DDoS attack on Kyrgyztan in 2009 to pressure it to terminate US’s access to the airbase at Manas, a key logistics centre supporting U.S. military operations in Afghanistan. The ability for nation-states to launch cyber attacks to disrupt or damage critical infrastructure through non-kinetic means could also be seen through the alleged US’s and Israel’s attack on the Natanz nuclear enrichment plant in Iran in 2010 using Stuxnet.[[10]](#footnote-11)

Another form of cyber threat is the proliferation of online falsehoods or fake news. The massive spread of fake news has been identified as a major global risk where propagandists manipulate the public,[[11]](#footnote-12) some with the aim to interfere in elections as well as other democratic process or to sow discord amongst racial and religious communities, while others for financial reasons.

There are several ways fake news can be used: (a) as a medium for organised disinformation campaigns with the aim of destabilising states through subversion of societies, (b) as viral rumours or false information (semi-truths) either shaping national opinion or affecting the resilience of a polity by actors within a state, without external malign actor involved, (c) as viral falsehoods of an entirely different nature, and (d) as fake stories distributed in order to attain revenue from advertising or swaying sentiments to manipulate the stock market.[[12]](#footnote-13)

State and private actors exploit fake news to advance their agenda. Through the use of fake news, state actors could seek to de-stabilise a nation state by creating racial and religious discord, entrenching divisions within a society and undermining its social cohesion. It could also sway the electoral outcome towards candidates whose policies are more favourable towards them. On the other hand, non-state actors employ fake news usually for financial gains. They circulate sensational and controversial posts or news articles to entice users for views and clicks so as to generate revenue.

**2.2 THE COLLATERAL CONSEQUENCES FROM CYBER ATTACKS**

Cyber attacks, unlike conventional or terrorist attacks, often do not target individuals but infrastructures such as computer networks or facilities. It is only expected that discussions among security experts often centred on defending transportation networks, refineries, dams, military installations, hospitals, banks, and government offices from cyber attack, and making these facilities and its networks resilient to cyber attacks, similar to concerns about defending the same facilities from terrorist bombs or ballistic missiles.[[13]](#footnote-14) However, the effects of cyber attacks are far reaching beyond the direct impact on the computer systems and networks.

Festering within the aftermath of cyber attacks on infrastructure and computer networks, we can expect disruptions to society’s way of lives and the psychological state of individuals being impacted. Research has shown that these cyber attacks can cause social and psychological impacts besides damages to the infrastructure and computer networks.[[14]](#footnote-15) The social impact of a cyber-attack refers to aspects such as the social disruption caused to people’s daily lives, and widespread issues such as anxiety or loss of confidence in cyber or technology. Psychological impact can be informed by social impact, and can include more personal aspects such as an individual’s anxiety, worry, anger, outrage, depression.[[15]](#footnote-16) In Jan 2017, Lloyds Banking Group suffered a DDoS cyber attack over 2 days. At the social and societal levels, millions of bank customers were impacted by the attack. While there was no financial loss by the customers according to reports, the DDoS cyber attack affected the availability of services which left many customers temporarily unable to use services such as checking their balance or sending payments. Several other major British banks were also hit by cyber attacks over a 2 year period between 2015 and 2017 and this prompted British lawmakers to criticize both British banks and regulators for doing insufficient to improve on cyber security.[[16]](#footnote-17) The DDoS cyber attack also impacted the customers psychologically. Many people were angry with the situation and took to social media to vent their frustrations at being blocked from accessing their online accounts.[[17]](#footnote-18)

Another related example is the outbreak of the COVID-19 virus in Jan 20, which has since caused significant global panic based on a survey results by Pharmaceutical Technology.[[18]](#footnote-19) While the COVID-19 is not a cyber attack in itself, it has had a significant impact on popular anxiety surrounding this outbreak from the way information is shared through the cyberspace. The panic was fuelled by misinformation, particularly via ‘social spread’, mainly due to the limited amount of information on the unknown COVID-19. The way information is framed and interpreted, and then reach out unverified through social media to the mass population, can lead to uncertainty and confusion creating other social challenges.[[19]](#footnote-20) Some of the social impacts that have been observed in this COVID-19 episode include a growth of mistrust and racist attitudes towards Chinese people living in other countries: In the UK, there have been reports of anxiety where commuters actively avoided sitting or standing near people of Chinese descent on public transport; Elsewhere, there have been reports of playground bullying, as well as online hashtags and petitions, calling for Chinese people to stay away from schools, universities and out of certain countries. With an inaccurate perception, formed through misinformation, it has also led to anxiety and fear around how deadly and contagious the virus is, and how bad things can get. Psychologically, such anxiety and fear influences adverse individual actions, which in turn have ripple effects on the community and the broader society. When news of the COVID-19 spread broke out in Singapore, online rumors and photos of people emptying shelves and panic buying in supermarkets were also circulated. This anxiety has a knock-on effect where stress and irrationality triggered many other people to also rush to supermarkets to stock up on their personal supply of face, and food supplies.[[20]](#footnote-21)

Given the onset of fear, anxiety and confusion within individuals following the aftermath of a cyber terror attacks, herein lies the challenge for states to recover and restore normalcy rapidly. Research has also shown that depending on who the attackers and the victims are, the level of psychological effects of cyber threats may even rival those of traditional terrorism.[[21]](#footnote-22) The impacts of these psychological effects in turn has an influence on the political attitudes towards the cyber security polices and measures implemented by government agencies to prevent future cyber attacks or to recover from an attack. When subjected to a cyber attack, victims react not only with fear, but would also demand government intervention for protection via surveillance and stronger regulations.[[22]](#footnote-23)

**2.3 THE CHALLENGE TO SINGAPORE’S MULTICULTURALISM**

|  |
| --- |
| *"Security threats can be real and physical like terrorism or, just as damaging, can come through the cyber world… Malicious malware can cripple our systems. Fake news can cause racial riots and divide our people."*  *- Dr Ng Eng Hen, Feb 2019*  *Singapore’s Minister of Defence*  *(message uploaded on his Facebook)* |

Singapore has an ethnically plural society comprising a Chinese majority (about 76 percent), a substantial minority of Malay/Muslims (about 15 percent) and a smaller percentage of Indians and other ethnic groups[[23]](#footnote-24). As such, Singapore’s social and ethnic fabric is a unique blend of cultures and people. However, Singapore’s multi-culturalism and multi-racialism also offer opportunities for its potential adversaries to exploit and magnify differences and inevitable tensions between groups. This could lead to the undermining of national values and disruption of social harmony and stability.

Singapore's diverse society provides fertile ground for insidious "slow drip" falsehoods to cause longer-term damage to society.[[24]](#footnote-25) Addressing the media during the release of a committee report regarding its findings and recommendations on the issue of combating fake news in Singapore, Committee Chairman Charles Chong said online falsehoods are "pervasive and can affect different aspects of our country: national security, racial harmony, democratic processes, social cohesion and trust in public institutions".[[25]](#footnote-26) In the report, it also said that the "low-level" falsehoods, which could be about a particular ethnic, religious or immigrant group, could raise tensions little by little, fanning emotions on issues which may not be high initially.[[26]](#footnote-27) In Singapore, there is a noticeable shift towards increased use of social media as a source for news and information. As a result, misrepresentation or misinterpretation of information, deliberate or unintended, amplified through social media could be one such way to lead to confusion, distrust and social divisiveness. With the wide reach and influence of social media, cyberhate against a particular ethnic group or religion can also be incited by accentuating the negative effects of inaccurate sentiments circulated online, and the content online can go viral and gets circulated rapidly.

Online falsehoods is increasingly undermining Singapore's social fabric and unity. Fake news campaigns and cyber attacks can exploit the fault lines in its increasingly diverse multi-ethnic, multi-religious society to create polarisation in the social fabric. Singapore Foreign Affairs Minister, Vivian Balakrishnan also noted that digital media has created ideological echo chambers in which people can affirm their views - no matter how mistaken or biased they are - and this leads to a more fractious and divided society.[[27]](#footnote-28) As Singapore’s social resilience is founded on its policy of multiculturalism, there is a need to strengthen its unity, resilience and resolve in face of cyber threats.[[28]](#footnote-29) The leaders in Singapore’s government consistently stress the importance of social harmony, where the various ethnic groups are able to live in harmony. However, the risk of netizens obtaining only superficial understandings of issues and then spreading misinformation, and the threat posed by fake news and cyberhate continue to underscore significant challenges for Singapore.[[29]](#footnote-30)

**2.4 CYBER VULNERABILITY TO SINGAPORE AS A SMART NATION**

As a global banking, maritime, and aviation hub, Singapore plays a vital role in facilitating the transactions incurred within the digitised economies it operates in. Singapore is also a conduit for a significant proportion of the world’s freight, air traffic, and financial capital and this puts it as an attractive target of cyber attacks.

In recent years, Singapore has faced growing cyber attacks against government and non-government entities. In Oct 2016, two waves of cyber attacks disrupted the broadband network of one of its telco, StarHub. Subscribers’ machines were infested with bugs, turning them into zombie machines to carry out distributed denial-of-service attacks on StarHub’s network.[[30]](#footnote-31) Singapore suffered another cyber attack in 2018, which saw 1.5 million SingHealth patients’ personal information illegally accessed and copied. The same year, [Singapore’s Cyber Security Agency](https://www.businessinsider.sg/businesses-in-singapore-lost-nearly-s58-million-to-cyber-attacks-last-year-csa-report/) reported an overall increase in the number of cybercrimes from 2017. [[31]](#footnote-32) In the report, it also noted that there was a shift from profit-motivated attacks towards those aimed at causing massive disruptions, such as the WannaCry ransomware campaign.[[32]](#footnote-33) Cyber threats on Singapore’s critical infrastructure can have significant impact on Singapore’s society and economy. Successful cyber attacks on national critical infrastructure that run utility plants, transportation networks, hospitals and other essential services will result in disruptions which could cripple economies or lead to loss of life. For example, a cyber attack on Singapore’s financial institutions could undermine consumer confidence and spark a run on bank deposits, leading to economic losses. Whereas a cyber attack on Singapore’s water supply control system leading to disruptions or water shortage can create stress and unrest in individuals and society given the scarce water resource situation in Singapore.

Further, under its Smart Nation initiative, Singapore has laid out mutually-reinforcing plans to build a Digital Economy, Digital Government and Digital Society, involving the public, private and people sectors. Central to Singapore's Smart Nation goals is the adoption of advanced technologies in an increasingly connected society. This means digital transformation in key domains, such as health, transport, urban solutions, finance, and education. 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, infrastructure and technology to support the roll out of new capabilities to citizens, business, and the government. This would eventually enable connectivity across smart, connected devices with applications such as remote health monitoring, remote learning and even self driving to make lives better in a Smart Nation.[[33]](#footnote-34) In this context, a Smart Nation with deep reliance on Infocomm Technology will definitely be even more vulnerable to cyber attacks. At a social/societal level, cyber attacks in key services sector such as energy, transportation and communications will definitely cause disruptions to Singaporeans’ daily life. It can also create negative perception of technology or a drop in confidence in organisations affected by the cyber attacks.

As a developed, highly-networked country which is connected to the world by air, sea and the Internet to serve as a hub for air travel, shipping, finance and trade, Singapore is particularly vulnerable to cyber attacks. Coupled with its Smart Nation program and quest to become a data hub, it will have a larger cyber threat landscape than other small states, making it and its government systems more vulnerable to cyber threats made by other states.[[34]](#footnote-35) These risks necessitate an immense responsibility to actively protect and make resilient the cyber infrastructure that forms the foundation of its economic activities.

**2.5 SOCIAL AND PSYCHOLOGICAL RESILIENCE DEFINED**

Disruptive events such as cyber attacks can have impacts both at the societal and psychological level. Building social and psychological resilience is therefore key in responding to and recovering from a cyber attack that has caused disruptions to daily life or loss of lives. Social resilience is the capacity of a society to prepare itself, to contain and effectively manage major national crises, to react in accordance with their severity and magnitude, and to “bounce back” expeditiously to an enhanced functioning.[[35]](#footnote-36) Resilient societies and communities demonstrate readiness to face a grand crisis, without giving up on national and strategic objectives.[[36]](#footnote-37) Individual resilience pertains to the person's strength and coping behaviors that sustain individuals during stressful life events.[[37]](#footnote-38) Resilient persons can continue to function normally under adverse circumstances and revert back to their original state when the stressing factors end.[[38]](#footnote-39)

Research has also shown that individual resilience is integral to social and national resilience.[[39]](#footnote-40) Studies have pointed out that most people are resilient to the negative effects of post-traumatic stress disorder, anxiety, and fear, even though these symptoms increase after disruptive events.[[40]](#footnote-41) Key to this is the strong psychological resilience within individuals. Psychological resilience is deﬁned as the ability to maintain stable and healthy levels of psychological and physiological functioning after disruptive events.[[41]](#footnote-42) People with higher psychological resilience can more easily navigate themselves around stress and adversity, stay positive, and pursue resilient outcomes.[[42]](#footnote-43)

Resilience has become a concept that has increasingly informed political and policy discussions around disaster planning and preparedness.[[43]](#footnote-44) For Singapore, its Total Defence concept is a comprehensive defence strategy involving all Singaporeans to respond to threats and challenges threatening Singapore’s independence and well being. The Total Defence concept which comprises six key pillars - Military, Civil, Economic, Social, Digital and Psychological Defence,[[44]](#footnote-45) of which building social resilience centres along the three key pillars of Psychological Defence, Social Defence and Civil Defence. “Psychological Defence” is about "Being a resilient person", having the fighting spirit, the will, the resilience in overcoming a crisis. "Social Defence" is about "Living harmoniously and looking out for one another", with emphasis on respecting and being sensitive to the needs and religious and cultural practices of others so as to keep the social fabric strong for Singaporeans to live in social cohesion and harmony regardless of race or religion. "Civil Defence" is about "Taking care of our family, friends, and people around us in times of crisis", and knowing what to do in times of crisis or disaster.

Research also showed that the interface between national security and resilience is rooted in individuals’ perceptions and attitudes toward institutions and leadership.[[45]](#footnote-46) It suggests that individuals exposed to cyber attacks show an increase in cyber-induced stress, which exacerbates perceptions of violent threat and personal insecurity,[[46]](#footnote-47) leading to fear. Fear appeals are a proactive method for motivating people to act.[[47]](#footnote-48) Fear appeals are also vital in prompting people’s resilient behaviours and support for government policies, which could proactively minimize the impact of cyber terrorism.[[48]](#footnote-49) When it comes to societal resilience, trust in institutions is also one of the central elements of functioning societies.[[49]](#footnote-50) Institutional trust indicates how people value the ability of their institutions to protect society from disruptive events and prevent future attacks. Gaining citizens’ support and trust in government’s cyber security policy, a key element in obtaining national resilience against cyber threats, will thus have a vital and even critical effect on the ability of the state to deal with cyber terrorism.

**CHAPTER 3**

**SINGAPORE’S AND ISRAEL’S CYBER SECURITY STRATEGY**

**3.1 SINGAPORE’S CYBER SECURITY STRATEGY**

Recognising the cyber threats and challenges to national security, Singapore took deliberate steps to enhance its cyber security, beginning with its first Infocomm Security Masterplan (ISMP) that was initiated in 2005. The three-year strategic roadmap focused on building basic cyber defence capabilities within the public sector to mitigate and respond to cyber threats.[[50]](#footnote-51) This was followed by the launch of a new five-year Infocomm Security Masterplan 2 (MP2) in 2008, which focused on enhancing existing measures to secure Singapore's critical infrastructure including utility and telco networks, promoting the use of cyber security technologies among businesses, and increasing cyber security manpower.[[51]](#footnote-52) The new five-year National Cyber Security Masterplan (NCSM) 2018, launched in 2013, built on the efforts of two earlier masterplans and strove to reinforce Singapore’s cyber security by intensify efforts in the Government and Critical Information Infrastructure (CII) as well as the wider cyber security ecosystem which includes businesses and individuals.[[52]](#footnote-53)

The Cyber Security Agency of Singapore (CSA), formed in Apr 2015, brought all agencies and initiatives related to cyber security under its charge. As the central agency, CSA oversees and coordinates all aspects of cyber security for Singapore, which includes developing and enforcing cyber security regulations, policies, and practices. In Oct 2016, following the establishment of CSA, Singapore launched its Cyber Security Strategy, which encompasses the four pillars: (1) *Building a Resilient Infrastructure* to strengthen and secure its Critical Information Infrastructure (CII); (2) *Creating a Safer Cyberspace* by promoting involvement from not only the government but also industry and the public to counter cyber threats, combat cyber crime and protect personal data; (3) *Developing a Vibrant Cyber Security Ecosystem* by working with industry and academia to grow the cyber security workforce; and (4) *Strengthening International Partnerships*, given that cyber threats is transnational.[[53]](#footnote-54)

**3.1.1 Pillar #1: Building a Resilient Infrastructure**

The first pillar on Building a Resilient Infrastructure seeks to enhance the protection of Critical Information Infrastructure (CII) and improve cross-sector response to mitigate widespread cyber attacks. A CII Protection Programme will be implemented to put in place robust and systematic cyber risk management processes. With a cyber-resilient infrastructure in place, it will provide peace of mind to Singaporeans as well as reinforce confidence in Singapore as a resilient and trusted global centre of trade and commerce.[[54]](#footnote-55)

Singapore has also developed a national cyber security response plan which allows for timely response and ground initiative at the local level, complemented with effective coordination and strategic support at the sectoral and national level. The plan envisages three tiers of response – Tier 1 for cyber campaigns that threaten national security, Tier 2 for cyber-attacks on a sector, and Tier 3 for cyber-attacks on a specific operator. The plan requires CSA to work closely with CII operators and the cyber security community to ensure an effective response. The national response to a cyber attack at the national level will be led by an inter-agency Cybersecurity Crisis Management Group, or CMG (Cyber). It is led by the Permanent Secretary of the Ministry of Communications & Information, supported by CSA, and comprises senior policy decision makers from government agencies overseeing the different critical sectors. CMG (Cyber) serves dual functions: (a) it is responsible for the development of cyber security policies and standards, and oversees the implementation of cyber security protection measures in the critical sectors; and (b) in a cyber crisis, it mobilises the necessary resources and directs the operational responses to provide a coordinated response to the threat.

Regular multi-sector cyber security exercises will also be conducted to enhance the readiness and responsiveness to significant cyber attacks at the national level. This will ensure a high level of preparedness to mount a robust response and implement reliable recovery plans, which is likely to require co-ordinations and support at the sectoral and national level, when under a cyber attack.

Other efforts include strengthening the cyber security governance and legislative framework, as well as making the government systems more secure. In this regard, a new Cyber Security Act was introduced in 2018. The Act augments existing cyber security policies to include a framework to ensure CII owners and operators take responsibility for securing their systems and networks, and also comply with promulgated cyber policies and standards,. The Act also empowers CSA and sector regulators with the authority for regulated sharing of cyber security information from affected parties so as to expeditiously resolve cyber security incidents and recover from disruptions.[[55]](#footnote-56) Government systems are among the prime targets for cyber-attackers as it contains sensitive data, including those about their citizens. These systems are also used to support a wide range of public services including the maintenance of national security and sustaining the economy. As such, investments in technologies such as analytics, automation, artificial intelligence, and other state-of-the-art security technologies will be made to further safeguard these government systems and networks.

**3.1.2 Pillar #2: Creating a Safer Cyberspace**

Digital connectivity has both empowered and endangered businesses and individuals.[[56]](#footnote-57) On one hand, it opens new social and commercial opportunities. On the other, it also exposes citizens to cyber crimes operated by criminal syndicates across the world. The second pillar on Creating a Safer Cyberspace seeks to keep cyberspace safe by embodying a collective responsibility towards cyber security, involving also businesses, individuals and the community besides the Government. Efforts were made to mobilise businesses and the community to play their part to make cyberspace safer, by fostering their understanding of cyber security issues through outreach programmes such as the Collaborative Social Programme (CoSP), where the police works with schools and Non-Governmental Organisations (NGOs) to raise cybercrime prevention awareness among vulnerable groups.[[57]](#footnote-58) Another effort undertaken to help keep the cyberspace safe is through the Public Cyber-Outreach & Resilience Programme (PCORP), where it promoted the adoption of good practices such as taking preventive measures to secure their computer systems and digital devices, particularly to prevent malicious actors from hijacking their systems and devices to cause harm to others.[[58]](#footnote-59)

**3.1.3 Pillar #3: Developing a Vibrant Cyber Security Ecosystem**

The threat posed by rising sophistication in cyber attacks is exacerbated by the current shortage of cyber security practitioners with deep expertise in Singapore. Therefore, the third pillar on Developing a Vibrant Cyber Security Ecosystem focuses on developing highly skilled cyber security professionals, growing companies with deep cyber security capabilities, and promoting strong research collaborations between the government, academia and industry in the cyber field. Among the many initiatives launched to develop and grow its professional cyber security workforce, one of which was to leverage on its National Service conscription system to start training soldiers on relevant cyber security skills to serve in cyber roles to defend the Singapore Armed Forces’ networks and information systems.[[59]](#footnote-60) This can help quickly increase the pool of skilled cyber expertise when these servicemen continue to develop their professional knowledge in the digital and cyber domains. Other efforts include working with institutes of Higher Learning to incorporate cyber security into their curriculum or creating specialised cyber track in the current degree programmes.

The development of R&D expertise and capabilities in cyber security for Singapore is done through its National Cyber Security R&D Programme (NCR). Launched in 2013, $180 million have since been allocated to support R&D development in cyber security to improve cyber infrastructure with an emphasis on security, reliability, resiliency and usability.[[60]](#footnote-61)

**3.1.4 Pillar #4: Strengthening International Partnerships**

Cyber security is a global issue. Cyber threats do not respect sovereign boundaries. Cyber attacks disrupting one country can have serious spill-over effects on other countries given the increased inter-dependencies through trade and global financial market. Under the fourth pillar of Strengthening International Partnerships, Singapore continues to engage other countries and contribute to global efforts in combating cyber threats through international forms and platforms such as the annual ASEAN CERT Incident Drill (ACID), ASEAN Network Security Action Council (ANSAC), ASEAN Regional Forum (ARF) Mechanisms as well as ASEAN cybersecurity and cybercrime workshops.[[61]](#footnote-62)

**3.2 DIGITAL DEFENCE AS PART OF SINGAPORE’S TOTAL DEFENCE STRATEGY**

As Singapore works towards being a Smart Nation, digital technology will pervade all aspects in the way Singaporeans live, work, and play. The digital revolution has presented opportunities for Singapore to build a Digital Economy, Digital Government and Digital Society. But with these digital transformation initiatives, it has also make Singapore more vulnerable to threats from the digital domain. Not only will cyber attacks disrupt the way of life of its citizens, it can also undermine its social cohesion and strike at the confidence and psychological resilience of its people. Hence, Singapore must be able to both respond to cyber attacks that target its networks and infrastructure, and also handle well threats that can be perpetrated through the digital domain such as fake news and deliberate online falsehoods. To do so, it will need to build robust cyber defences and have effective cyber recovery plans to remain resilient even when things go wrong. Therefore, Singapore has included Digital Defence as the sixth pillar in its Total Defence strategy.[[62]](#footnote-63)

Digital Defence is a whole-of-nation effort to protect and defend the nation and secure its citizens online. It requires Singaporeans to practice good cyber security habits, guard against fake news and disinformation, and consider the impact of actions performed online on the wider community.[[63]](#footnote-64) Singapore has also strengthened its legislation over disinformation online, with the promulgation of the Protection of Online Falsehoods and Manipulation Act (POFMA) in May 2019.[[64]](#footnote-65) This purpose of this law is to guard against potential misuse of the internet for information conflict by other states. POFMA seeks to prevent the electronic communication of falsehoods (i.e. false statements of fact or misleading information), as well as to safeguard against the use of online platforms for the communication of such falsehoods. POFMA also puts in place various measures to counteract the effects of such communication and to prevent the misuse of online accounts and bots (i.e. computer programmes that run automated tasks).[[65]](#footnote-66)

**3.3 THE ISRAELI NATIONAL CYBER SECURITY STRATEGY**

According to the Israel National Cyber Security Strategy,[[66]](#footnote-67) the first milestone in the development of Israel’s national cyber security efforts was laid in 2002, when the Israeli government authorized the National Information Security Authority (NISA) to instruct and protect vital computerized systems of selected public and private civil organizations. The second and major milestone was the establishment of the Israel National Cyber Bureau (INCB) in Jan 2012, which reports directly to the Prime Minister’s Office. INCB was tasked with: devising the State’s national cyber policy and strategy, promoting national processes, developing national cyber capabilities and strengthening Israel’s leadership in the field. In Feb 2015, the government of Israel adopted two pioneering resolutions recommended by INCB, which were to establish a national cyber security regulatory mechanism and national regulatory body. These resolutions resulted in the establishment of the National Cyber Security Authority (NCSA), a dedicated government entity leading the operational cyber security efforts of the State of Israel. Together, the INCB and the NCSA constitute the INCD – Israel National Cyber Directorate. In 2017, the Israel National Cyber Security Strategy was published.[[67]](#footnote-68)

Israel's cyber security strategy is based on a generic concept of operations for national cyber security.[[68]](#footnote-69) The concept of operations defines three operational layers: Aggregate Cyber Robustness, Systemic Cyber Resilience and National Cyber Defence. The three-layer approach is derived from the unique nature of the cyber threat and the central role of private organizations in achieving national cyber security. The three layers differ from one another in their goals, in the role of the State and in the relations between the State and private organizations.

**3.3.1 1st Layer: Aggregate Cyber Robustness**

Under the Israel National Cyber Security Strategy, cyber robustness is seen as the ability of organizations and processes to continue operating despite a routine of cyber threats by repelling and preventing most of the attacks.[[69]](#footnote-70) Israel sees it as the very basic level of cyber security and has set a goal to raise the overall level of cyber robustness as a means of preventing high-level damage and reducing the cumulative risk. A bill (Government Resolution 2443), promulgated in Feb 2015, introduced nation-wide efforts to enhance the national robustness through the promotion of security efforts undertaken by organizations (best practice, guidance, regulations, incentives, etc.) and by regulating the cyber security market.

**3.3.2 2nd Layer: Systemic Cyber Resilience**

The second layer in the concept of operations is the systematic ability to confront cyber-attacks before, during, and after incidents, prevent them from spreading and reduce their cumulative damage to the nation.[[70]](#footnote-71) While the first layer is focused on reducing attacks a priori, regardless of any specific event, this layer is event-driven by definition. Systemic resilience can be achieved through state processes encouraging information sharing, generating and disseminating valuable information, and assisting organizations during cyber incidents. This effort is led by the NCSA, with the national CERT at the forefront. The national CERT works closely with the private sector, both directly and through sector-based cyber centres which operate within the CERT. The CERT strives to engage in global and local cooperation while supporting innovation and harnessing it for its goals.

**3.3.3 3rd Layer: National Cyber Defence**

A national-level campaign is required against severe threats by determined, resource-rich attackers who pose serious danger to the nation. National defence campaigns incorporate defensive effort, to contain such attacks and their ramifications together with active efforts to confront the sources of the threats.[[71]](#footnote-72)

**CHAPTER 4**

**COMPARATIVE ANALYSIS OF SINGAPORE’S AND ISRAEL’S NATIONAL CYBER SECURITY STRATEGY**

**4.1 COMPARISON METRICS**

Taking reference from some of the comparison metrics adopted in other studies that analysed and compare different nation’s cyber security,[[72]](#footnote-73) a comparative analysis of Singapore’s and Israel’s cyber security strategy is made with the following factors, chosen so as to help gain insights on the measures adopted within the respective countries cyber security strategy that influence social and psychological resilience towards cyber threats:

1. Perception of cyber threat
2. Which are the stakeholders identified and the approach adopted
3. Incident response capabilities: i.e. existence of Cyber Early Warning systems, Threat Information Sharing approaches, Computer Emergency Response Teams (CERTS) etc
4. Capacity Building: i.e. efforts on cyber security workforce development, Research and development (R&D) etc
5. Policy and regulations: i.e. introduction of new or amendments to legislation.

**4.2 Perception of Cyber Threat**

Singapore sees itself vulnerable to cyber threats such as fake news and deliberate online falsehoods from the digital domain as well as cyber attacks that target its networks and infrastructure. These cyber threats can undermine its social cohesion and strike at the confidence and psychological resilience of its people, or disrupt the way of life of its citizens. This threat perception guides the formulation of its Digital Defence pillar under its Total Defence strategy, as well as its National Cyber Security Strategy. As for Israel, the approach to its National Cyber Security Strategy is developed based on the assumption that the organisation would be the basic target of any cyber security challenge. It places the organisation as a basic frame of reference in its approach, and an elementary unit of analysis in the strategy instead of individual, group or state, given that organisations own the networks.[[73]](#footnote-74)

**4.3 Stakeholders Identified and Approach**

Singapore adopts a “Whole-of-Society” approach to cyber security. It sees cyber security as a collective responsibility where individuals, the community, businesses and the Government have a role to play in defending against the cyber threats. For Israel, it pursues a perpetrator-indifferent approach that encompasses the entire range of cyber challenges and creates a national-level holistic remedy as its National Cyber Security Strategy.[[74]](#footnote-75) It assumes that protection of the specific asset is more important than dealing with the perpetrator, and focuses on the types of possible attacks and on the specific assets whose protection is vital, regardless of the attacker. Israel focuses on critical national targets that should be protected against a diapason of threats.

**4.4 Incident Response Capabilities**

Both Singapore and Israel have in place robust frameworks and response plans to respond to cyber attacks. This includes having a central agency, such as the CSA in Singapore’s case and NCSA in Israel’s case, to lead in the handling of cyber incidents and to stop its proliferation. Both countries also have the capabilities to anticipate cyber threats and in the event of cyber attacks, respond decisively and expeditiously recover from it.

Singapore has its National Cyber Security Centre (NCSC) that monitors and analyses the cyber threat landscape to maintain cyber situational awareness and anticipate future threats. Should large-scale cyber incidents involving multiple sectors occur, NCSC will be the lead agency to coordinate with the sector regulators to provide a national level response and facilitate quick alerts to cross-sector threats. The National Cyber Incident Response Teams (NCIRT) drawn from the incident response teams from CSA, Government Technology Agency (GovTech), the Ministry of Home Affairs (MHA) and the Ministry of Defence (MINDEF), will execute the response under the national cyber response plan.

Israel’s NCSA is charged with the mission of defending cyberspace by conducting, operating and implementing all the operational defensive efforts in cyberspace at the national level, from a holistic perspective, for the purpose of providing a complete and continuous defensive response to cyber attacks, including handling cyber threats and incidents in real time, formulating an ongoing situational awareness, consolidating and analyzing intelligence, and working with the defence community. Israel’s Cyber Event Readiness Team (CERT-IL) falls under the charge of the NCSA. The CERT-IL is responsible for national cyber security incident management, intelligence sharing with trusted partners in Israel and abroad, developing cyber security best practices, promoting cyber security awareness, and ‘providing a single point of contact in Israel regarding cyber security threats and incidents for international corporations, cyber security companies and other CERTs’.[[75]](#footnote-76)

**4.5 Capacity Building**

Both countries placed emphasis on capacity building efforts to grow and sustain its national cyber capabilities, enabling it to develop innovative responses and technological solutions to make their respective network and infrastructure robust and resilient. Capacity building emphasizes less on the technical aspects of cyber defence, and more on the peripheral and holistic factors that complement it.

Singapore recognised its shortage of cyber security manpower and the Singapore Government has collaborated with industry partners, Institutes of Higher Learning to grow the cyber security workforce. It is also building up its cyber security industry by developing strong cyber security companies and nurturing local cyber security start-ups. Efforts were also invested in academia and research institutes to produce cyber security research expertise and to develop cyber security capabilities. These capabilities include engineering expertise to develop innovation solutions for security needs. Israel’s efforts to foster its national cyber ecosystem includes supporting and stimulating state-owned industry as well as private commercial R&D in the leading cyber fields, fundamental and applicative research, and cultivating scientific-technological human capital throughout all stages of education, from elementary to high school.[[76]](#footnote-77)

**4.6 Policy and Regulations**

The Cyber Security Act, promulgated in Singapore in 2018, provided CII owners with clarity on their obligations to proactively protect the CII from cyber-attacks. This builds resilience into the CII, protecting Singapore’s economy and its citizens’ way of life. With the Act, it also empowers the Commissioner of Cyber Security to investigate cyber security threats and incidents to determine the impact and prevent further harm or cyber security incidents from arising. The Act also provides a framework for CSA to request information, and for the protection and sharing of such timely and critical information, to help identify vulnerabilities and prevent cyber incidents more effectively. To strengthen its legislation over disinformation online, Singapore promulgated the Protection of Online Falsehoods and Manipulation Act (POFMA) in May 2019 to tackle growing concerns over the scourge of fake news and misinformation, communicated particularly through various online and social media platforms.

In Israel, when the draft Cyber Security Bill was discussed in the Knesset in 2018, concerns were raised by members of the public that it involves an infringement of the rights to privacy both in relation to the premises and the contents of the data found in equipment.[[77]](#footnote-78) Thos was because the law would give Israel’s National Cyber Directorate, the agency charged with protecting Israel’s civilian national cyberspace, the authority to instruct organizations on how to act if there are suspicions of a hack or data breach, monitor the internet traffic to gather information as well as enter private premises to confiscate equipment without a court order, in order to foil or deal with a cyber attack.

**4.7 Summary of Comparative Analysis**

The key findings is summarised in the table below.

|  |  |  |
| --- | --- | --- |
|  | **Singapore** | **Israel** |
| Perception of cyber threat | * Cyber attacks on critical infrastructure and digital information system * Cyber crimes * Fake news and online falsehoods that threaten social cohesion | * Cyber threats to organisation as a basic frame, and an elementary unit of analysis in the national cyber security strategy approach |
| Stakeholders Identified and how are they addressed | * Adopts a whole-of-society approach * Demands collective responsibility from business, Government and also society | * Adopts a perpetrator-indifferent approach that encompasses the entire range of cyber challenges * Focus on critical national targets that should be protected against a diapason of threats |
| Incident Response Capabilities | * CSA as central authority * Monitoring teams (CWC) and response teams (CERT) | * NCSA as central authority * IL-CERT conducts detection of threat, confine the expansion of threat infiltration, mitigate its effects, and deny its occurrence |
| Capacity Building Efforts | * Growing its cyber security workforce. Initiatives include leveraging its national service to augment build up of cyber workforce, by training its recruits in cyber roles * Building a strong cyber security industry * Promoting R&D collaborations between the Government, academia and industry | * Ecosystems to promote learning and mastering of cyber technology * Used its national service as a pipeline to supply skilled workforce to the security area, by training its recruits in cyber intelligence * Vibrant cyber security industry to sustain and grow cyber expertise |
| Policy and regulations | * Cyber Security Act, 2018 * Protection from Online Falsehoods and Manipulation Act, 2019 | * Draft Cybersecurity Law, 2018 |

**CHAPTER 5**

**RECOMMENDATIONS**

**5.1 RAISE THE LEVEL OF CYBER THREAT PERCEPTION**

|  |
| --- |
| In a study conducted, the findings suggested that individuals, when confronted with the threat of lethal and non-lethal cyber terrorism, will support strong government measures to police and regulate cyberspace and to respond forcefully to cyber attacks.[[78]](#footnote-79)  Singapore’s current cyber security strategy has rightfully placed emphasis on ‘resilience’, nonetheless, more could be done. Specifically, efforts could be directed towards building up psychological resilience – simply put, to mentally prepare residents against the possibility that Singapore might one day succumb to a major cyberattack. Singapore’s residents should be made aware that although the government would continue to work with the private sector and the community to harden cyber defences, it would not be foolproof. And, in the event of crisis, the community cannot rely solely on the government. Instead, a whole-of-society response would be required for Singapore to ‘bounce back’ quickly. On its part, the Government should avoid being too prescriptive about the actions to be taken during a crisis. Rather, it should seek to sensitise the population to the threats so as to reduce the ‘shock factor’ and encourage organisations and communities to development their own resilience plan.  To achieve this, the Government could consider releasing more information to the public on on-going cyber-intrusions against Singapore. It could also be worthwhile to embed cyber defence into the concept of Total Defence to enhance societal awareness and to promote discussions. For this purpose, cyber road shows and ‘cyber drills’ could also be carried out at various constituencies in a manner similar to Civil Defence’s ‘Community Bonding’ programme or water rationing drills. The declaration of a ‘Cyber Security Day’ or the launching of a ‘Cyber Security Campaign’ akin to the ‘Courtesy Campaign’ of the late 1970s and 1980s could also be considered to heighten nation-wide awareness.[[79]](#footnote-80) |

|  |
| --- |
| the ill-preparedness of individual citizens to defend their computers from cyber threats increases the security challenges for states attempting to reduce the risk from these types of operation.  How do they convince their citizenry that these threats are immediate and important? Our study points to some rhetorical strategies leaders could use to more effectively communicate cyber threats (and cyber-safety) to the mass public. Namely, we demonstrate that only personally relevant data breaches can shift citizens’ risk perceptions and behaviors. Interestingly, both personal and national cybersecurity threats may lead citizens to support greater state investment in cybersecurity. As such, messaging campaigns designed to increase citizens’ cyber-preparedness should emphasize citizens’ potential personal vulnerability, while also highlighting concrete steps individuals can take to better protect themselves online.  actual online behavior is more resistant to change. Together, these results suggest that policy-makers will continue to face an up-hill struggle in mobilizingthepublictoimprovestatecybersecurity. Rather,state-corporatepartnershipswith private sector stakeholders and automated security protocols that reduce individual agency online are likely to make for more effective cybersecurity strategies[[80]](#footnote-81) |

|  |
| --- |
| Education is key. It lies at the heart of social resilience, and informs the coping, adaptive and transformative capacities of individuals and community groups. However, where smart cities are concerned, education is almost exclusively centred on helping people acquire the skill-sets that will generate higher levels of individual productivity.  Education must also mean improving people’s ability to support their communities on the often difficult road to change, providing access to services, cultivate environmental awareness and fostering social cohesion and solidarity |

**5.2 INCREASE LEVEL OF PREPAREDNESS AND RESILIENCE THROUGH DRILLS**

|  |
| --- |
| At the industry level, businesses also build resilience by training to respond to breaches and by maintaining backup systems that can be called upon in times of emergency. More needs to be done at the community level. At the community level, cyber resilience can be built by training to respond to attacks the same way fire drills and emergency drills simulate real scenarios. By building resilience through public education and public drills and exercises involving the community, Singapore can deter cyberattacks that aim to destabilise or demoralise society. At the state level, the government can also play the role of chief coordinator to encourage the development of resilience within society towards these new national security challenge.[[81]](#footnote-82) |

|  |
| --- |
| 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. <ME6 Calvin’s article> |

|  |
| --- |
| Do more drills, exercise to raise level of threat perception, to strenbgthen resiience, to gain more support for stringent cyber policies.  This is accomplished by regularly tasking organisations from different sectors with rigorous cyber exercises, with the aim of giving them the expertise to anticipate cyber attacks by effectively reviewing and adapting incident response strategies and cooperating seamlessly across sectors. Exercises range from industry-specific such as Exercise CyberArk [6], which is focused on the finance/banking industry, to national-level such as the holistic Exercise Cyber Star, which involves a whole swathe of organisations from multiple CII sectors such as aviation, land transport, maritime, media, energy, government, info-comm, healthcare, water, and security & emergency [7]. |

|  |
| --- |
| technical glitches will occur so it will be more practical to build up the country’s resilience against these breakdowns |

**5.3 CAPITALISE ON COLLABORATION AT COMMUNITY LEVEL**

|  |
| --- |
| Collaboration is vital in fighting the growing threat of cyber-attack. Not only at the business and regulator to protect and make the systems resilient, the same concept to be apllied at the societal level. (bring in the findinds from jain hua’s paper)  facilitating public activities that bring together people from all walks of life  strengthen social cohesion as hyper-connectivity threatens to pull it apart  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. <ME6 Calvin’s article> |

**5.4 CYBER DETERRENCE**

|  |
| --- |
| One should bear in mind that the notion of resilience implies a preparedness to take the ‘first blow’ - the impact of which could be significant, maybe even catastrophic, especially if the attack is undertaken by a nation state. Depending on the severity of the attack, the ability of the victim state to ‘bounce back’ may be in question. For this reason alone, it could be worthwhile to extend deterrence to cyberspace. To be sure, not all cyberattacks can be deterred, but if the biggest and most dangerous attacks could be prevented, this alone would be an important accomplishment (Kugler, 2009, p. 309).    Cyber deterrence for Singapore should comprise both deterrence-bydenial and deterrence-by-punishment. Being a small country with clear political direction and having relatively well established whole-of-government and whole-of-society frameworks for policy implementation, Singapore is well placed to build a credible deterrence based on denial. Indeed, the impact of size on the speed of policy implementation, infrastructure development and level of complexity in co-ordination is analogous to managing greater Tel Aviv as compared to managing the whole of Israel – being small has its advantages. Singapore’s global connectivity arising from its status as a financial, air and maritime hub should also work to deter most nation-states from undertaking substantive cyberattacks against Singapore for fear of collateral damage to oneself or third parties. Only the most determined aggressors would take such risks.    A strategy of deterrence-by-denial needs to be reinforced by a strategy of deterrence-by-punishment in an offense-dominant environment like cyberspace as even the most impregnable defence would eventually succumb to a constant spate of attacks much like how a rock would eventually be eroded by raindrops. The fact of the matter is the defender has to succeed all the time, while the attacker has to succeed only once. By combining the two, the overall deterrent effect would be enhanced. |

**5.5 ESTABLISH NORMS TO PROTECT SMALL STATES**

|  |
| --- |
| Small states are typically insecure about their survival and have long been the victims of great power intervention. Small states also have little recourse to both cyber and physical forms of punishments, with the punishments being either ineffective due to scale, or the possibility of cutting off potential markets in the case of sanctions.    To ensure that the rights of small states are protected in cyberspace, a set of binding international norms or laws needs to be globally agreed upon. These norms should include the protection of critical infrastructure from malicious attacks, the sanctity of information within borders, the non-interference in the political processes of a state, and the illegality of economic espionage.[[82]](#footnote-83) |

**CHAPTER 6**

**CONCLUSION**

<to be included>

**BIBLIOGPAPHY**

<to be included>

1. James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, Dec 2002. [↑](#footnote-ref-2)
2. Business Insider, Hackers Caused A Major Blackout For The First Time, 5 Jan 2016, <https://www.businessinsider.com/cyberattack-blackout-ukraine-2016-1>, Accessed on 1 Mar 2020. [↑](#footnote-ref-3)
3. BBC News, Ukraine Power Cut 'Was Cyber-Attack', 11 Jan 2017, <https://www.bbc.com/news/technology-38573074>, Accessed on 25 Feb 2020. [↑](#footnote-ref-4)
4. Michael Gross, Daphna Canetti, Dana Vashdi, Cyberterrorism: Its Effects On Psychological Well-Being, Public Confidence And Political Attitudes, Journal of Cybersecurity 3(1), 2017, 49-58. [↑](#footnote-ref-5)
5. Benjamin Goh, Commentary: Singhealth Data Breach Should Give Us Pause To Think What Else Might Be Vulnerable, Channel News Asia, 2 Aug 2018, <https://www.channelnewsasia.com/news/commentary/smart-nation-vulnerable-areas-to-hackers-10579890>, Accessed on 25 Feb 2020. [↑](#footnote-ref-6)
6. Andrew F. Krepinevich, Cyber Warfare A “Nuclear Option”?, Center For Strategic And Budgetary Assessments, 2012, Pp 38-50. [↑](#footnote-ref-7)
7. Ibid. [↑](#footnote-ref-8)
8. Brian Krebs, Shadowy Russian Firm Seen as Conduit for Cybercrime, The Washington Post, 13 Oct 2007, <https://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html>, Accessed on 28 Feb 2020. [↑](#footnote-ref-9)
9. Stephen Herzog, “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses”, Journal of Strategic Security, Vol 4, No.2, Summer 2011, pp49-60. [↑](#footnote-ref-10)
10. Andrew F. Krepinevich, Cyber Warfare A “Nuclear Option”?, Center For Strategic And Budgetary Assessments, 2012, Pp 133-137. [↑](#footnote-ref-11)
11. L. Gu, V. Kropotov, and F. Yarochkin, The Fake News Machine: How Propagandists Abuse The Internet And Manipulate The Public, Trendlabs research paper, Trend Macro, 2017, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media>, Accessed on 28 Feb 2020. [↑](#footnote-ref-12)
12. Norman Vasu, Benjamin Ang, Terri-Anne-Teo, Shashi Jayakumar, Muhammad Faizal, and Juhi Ahuja, Fake News: National Security In The Post-Truth Era, RSiS, Policy Report 19 Jan 2018. [↑](#footnote-ref-13)
13. James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, Dec 2002. [↑](#footnote-ref-14)
14. Gross, M. L., Canetti, D., & Vashdi, D.R, The Psychological Effects Of Cyber Terrorism, Bulletin of the Atomic Scientists, 2016, 72(5), 284-291. [↑](#footnote-ref-15)
15. Maria Bada, Jason Nurse, The Social and Psychological Impact of Cyber-Attacks, Published in Oct 2019. [↑](#footnote-ref-16)
16. Peter Nicholls, Lloyds A Victim Of Cyber Attack That Hit Banking Services, Reuters Technology News, 23 Jan 2017, <https://uk.reuters.com/article/us-lloyds-cyber/lloyds-a-victim-of-cyber-attack-that-hit-banking-services-idUKKBN1571C8>, Accessed on 28 Feb 2020. [↑](#footnote-ref-17)
17. Emma Dunkley, A Tale Of Two Cyber Bank Heists That Reveals Their Vulnerability, Financial Times, 13 Mar 2017, <https://www.ft.com/content/2bc83132-ee18-11e6-ba01-119a44939bb6>, accessed on 28 Feb 2020. [↑](#footnote-ref-18)
18. Allie Nawrat, COVID-19 Outbreak: How Misinformation Could Fuel Global Panic, Pharmaceutical Technology, 26 Feb 2020, <https://www.pharmaceutical-technology.com/features/covid-19-outbreak-how-misinformation-could-spark-global-panic/>, Accessed on 28 Feb 2020. [↑](#footnote-ref-19)
19. Ibid. [↑](#footnote-ref-20)
20. Catherine Wong, Commentary: Outbreaks Of Diseases Make Us Exaggerate Or Under-Estimate Risks. The COVID-19 Shows That, Channel News Asia, 20 Feb 2020, <https://www.channelnewsasia.com/news/commentary/public-reaction-to-wuhan-virus-coronavirus-12444060>, Accessed on 28 Feb 2020. [↑](#footnote-ref-21)
21. Gross, M. L., Canetti, D., & Vashdi, D.R, The Psychological Effects Of Cyber Terrorism, Bulletin of the Atomic Scientists, 2016, 72(5), 284-291. [↑](#footnote-ref-22)
22. Ibid. [↑](#footnote-ref-23)
23. Noor Aisha Abdul Rahman, The Dominant Perspective on Terrorism and Its Implication for Social Cohesion: The Case of Singapore, The Copenhagen Journal of Asian Studies, 2009, 27(2), pp 109-128. [↑](#footnote-ref-24)
24. Yasmine Yahya, Select Committee On Fake News: Singapore A Target Of Hostile Info Campaigns, The Straits Times, 21 Sep 2018, <https://www.straitstimes.com/politics/spore-a-target-of-hostile-info-campaigns>, Accessed on 1 Mar 2020. [↑](#footnote-ref-25)
25. Ibid. [↑](#footnote-ref-26)
26. Ibid. [↑](#footnote-ref-27)
27. Adrian Lim, How Singapore Is Battling Three Key Security Challenges: Vivian Balakrishnan, The Straits Times, 8 Apr 2019, <https://www.straitstimes.com/politics/how-singapore-is-battling-three-key-security-challenges-vivian-balakrishnan>, Accessed on 1 Mar 2020. [↑](#footnote-ref-28)
28. Aw Cheng Wei, Total Defence Efforts This Year To Focus On Strengthening Unity, The Straits Times, 15 Feb 2018, <https://www.straitstimes.com/singapore/drive-to-build-up-social-psychological-defences>, Accessed on 1 Mar 20. [↑](#footnote-ref-29)
29. Stephanie Neubronner, Social Media and “Fake News”: Impact on Social Cohesion in Singapore, RSIS No.043, 14 Mar 2017. [↑](#footnote-ref-30)
30. Tham Irene, Starhub Outage: Experts Sound Alarm On Attacks By ‘Smart’ Devices, The Straits Times, 27 October 2016, <http://www.straitstimes.com/tech/experts-soundalarm-on-attacks-by-smart-devices>, Accessed on 1 Mar 2020. [↑](#footnote-ref-31)
31. Cyber Security Agency, Cyber Threats in Singapore Grew in 2017, Mirroring Global Trends, Press Release on 19 Jun 18. [↑](#footnote-ref-32)
32. Ibid. [↑](#footnote-ref-33)
33. Infocomm Media Development Authority, Innovation - Driven Initiatives Pave the way for Singapore’s Smart Nation Vision, Press release on 22 Apr 2015, <https://www.imda.gov.sg/news-and-events/Media%20Room/archived/ida/Media%20Releases/2015/innovation-driven-initiatives-pave-the-way-for-singapore-smart-nation-vision>, Accessed on 1 Mar 2020. [↑](#footnote-ref-34)
34. Cyber Security Agency Singapore, Singapore Cyber Landscape 2018. [↑](#footnote-ref-35)
35. Reuven Gal, Shlomo Maital, Strengthening Social Resilience, Building Social Capital: Perspectives from Israel and China, Samuel Neaman Institute for National Policy Research, Proceedings of a Workshop held on 11 April 2016. [↑](#footnote-ref-36)
36. Reuven Gal, Shlomo Maital, Strengthening Social Resilience, Building Social Capital: Perspectives from Israel and China, Samuel Neaman Institute for National Policy Research, Proceedings of a Workshop held on 11 April 2016. [↑](#footnote-ref-37)
37. Reuven Gal, Social Resilience in Times of Protracted Crises: An Israeli Case Study, Armed Forces & Society, 2014, Vol. 40(3) 452-475. [↑](#footnote-ref-38)
38. J. Griffith, Resilience as a Multi-Level Concept: A Need for More Deliberated Thought, Paper presented at the Inter-University Seminar on Armed Forces and Society (IUSAFS) Biennial International Conference, 21 October 2011. [↑](#footnote-ref-39)
39. Jian Hua, Yan Chen, Xin (Robert) Luo, Are We Ready For Cyberterrorist Attacks?—Examining The Role Of Individual Resilience, Information & Management, Apr 2018. [↑](#footnote-ref-40)
40. George A. Bonanno, Sandro Galea, Angela Bucciarelli, David Vlahov, What Predicts Psychological Resilience after Disaster? The Role of Demographics, Resources, and Life Stress, Journal of Consulting and Clinical Psychology, 2007, Vol. 75, No. 5, 671–682 [↑](#footnote-ref-41)
41. George A. Bonanno, Loss, Trauma, and Human Resilience: Have We Underestimated the Human Capacity to Thrive after Extremely Aversive Events?, American Psychologist 59, no. 1 (2004): 20–28 [↑](#footnote-ref-42)
42. Jian Hua, Yan Chen, Xin (Robert) Luo, Are We Ready For Cyberterrorist Attacks?—Examining The Role Of Individual Resilience, Information & Management, Apr 2018. [↑](#footnote-ref-43)
43. S.Walkate, R. McGarry,G.Mythen, Searching for Resilience: A Conceptual Excavation, Armed Forces & Society, 2014, Vol 40(3). Pp. 408-427. [↑](#footnote-ref-44)
44. MINDEF, Total Defence, [https://www.mindef.gov.sg/oms/imindef/mindef\_websites/topics/totaldefence/index.html#](https://www.mindef.gov.sg/oms/imindef/mindef_websites/topics/totaldefence/index.html), Accessed on 2 Mar 2020. [↑](#footnote-ref-45)
45. Daphna Canetti, Israel Waismel-Manor, Naor Cohen and Carmit Rapaport, What Does National Resilience Mean in a Democracy? Evidence from the United States and Israel, Armed Forces & Society, 26 Mar 2013. [↑](#footnote-ref-46)
46. Daphna Canetti, Michael Gross, Israel Waismel-Manor, Asaf Levanon, Hagit Cohen, How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks, Cyberpsychology,Behavior, And Social Networking, 2017, Volume 20, Number 2. [↑](#footnote-ref-47)
47. Jian Hua, Yan Chen, Xin (Robert) Luo, Are We Ready For Cyberterrorist Attacks?—Examining The Role Of Individual Resilience, Information & Management, Apr 2018. [↑](#footnote-ref-48)
48. Jian Hua, Yan Chen, Xin (Robert) Luo, Are We Ready For Cyberterrorist Attacks?—Examining The Role Of Individual Resilience, Information & Management, Apr 2018. [↑](#footnote-ref-49)
49. Atte Oksanen a, Markus Kaakinena, Jaana Minkkinen a, Pekka Räsänen b, Bernard Enjolrasc and Kari Steen-Johnse, Perceived Societal Fear and Cyberhate after the November 2015 Paris Terrorist Attacks, Terrorism And Political Violence, 9 Apr 2018. [↑](#footnote-ref-50)
50. Infocomm Media Development Authority, Launch Of The Infocomm Security Masterplan, Opening Address by Dr Tony Tan Keng Yam, 22 Feb 2005. [↑](#footnote-ref-51)
51. Infocomm Media Development Authority, New S$70m Masterplan To Boost Singapore's Infocomm Security Competency And Resilience, Press Release, 17 Apr 2008. [↑](#footnote-ref-52)
52. Infocomm Media Development Authority, Singapore Continues to Enhance Cyber Security with a Five-Year National Cyber Security Masterplan 2018, Press Release, 24 Jul 2013. [↑](#footnote-ref-53)
53. Cyber Security Agency, Singapore's Cybersecurity Strategy, 10 Oct 2016, <https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy>, Accessed on 4 Mar 2020. [↑](#footnote-ref-54)
54. Ibid. [↑](#footnote-ref-55)
55. Cyber Security Agency, Cybersecurity Act, <https://www.csa.gov.sg/legislation/cybersecurity-act>, Accessed on 4 Mar 2020. [↑](#footnote-ref-56)
56. Cyber Security Agency, Singapore's Cybersecurity Strategy, 10 Oct 2016, <https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy>, Accessed on 4 Mar 20. [↑](#footnote-ref-57)
57. Cyber Security Agency, Singapore's Cybersecurity Strategy, 10 Oct 2016, <https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy>, Accessed on 4 Mar 20. [↑](#footnote-ref-58)
58. Priyankar Bhunia, Public-private alliance launched by Singapore Police Cybercrime Command, Opencov, 27 Oct 2017, <https://www.opengovasia.com/public-private-alliance-launched-by-singapore-police-cybercrime-command/>, Accessed on 4 Mar 2020. [↑](#footnote-ref-59)
59. Siau Ming En, Mindef Launches NSF Scheme, Specialist Award For Cyber Defence, Today Singapore, 12 Feb 2018, <https://www.todayonline.com/singapore/mindef-launches-nsf-scheme-specialist-award-cyber-defence>, Accessed on 4 Mar 2020. [↑](#footnote-ref-60)
60. National Research Foundation, National Cybersecurity R&D Programme, <https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme>, Accessed on 4 Mar 2020. [↑](#footnote-ref-61)
61. Cyber Security Agency, Singapore's Cybersecurity Strategy, 10 Oct 2016, <https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy>, Accessed on 4 Mar 20. [↑](#footnote-ref-62)
62. Hariz Baharudin, Digital Defence To Be Sixth Pillar Of Total Defence, The Straits times, 15 Feb 2019, <https://www.straitstimes.com/singapore/digital-defence-to-be-sixth-pillar-of-total-defence>, Accessed on 4 Mar 20. [↑](#footnote-ref-63)
63. Eugene E.G. Tan, A Small State Perspective on the Evolving Nature of Cyber Conflict Lessons from Singapore, PRISM, Vol. 8, No. 3 (2019), pp. 158-171. [↑](#footnote-ref-64)
64. Tham Yuen-C, Parliament: Fake News Law Passed After 2 Days Of Debate, The Straits Times, 8 May 2019, <https://www.straitstimes.com/politics/parliament-fake-news-law-passed-after-2-days-of-debate>, Accessed on 6 Mar 2020. [↑](#footnote-ref-65)
65. Singapore Legal Advice, Singapore Fake News Laws: Guide to POFMA (Protection from Online Falsehoods and Manipulation Act), <https://singaporelegaladvice.com/law-articles/singapore-fake-news-protection-online-falsehoods-manipulation/>, Accessed on 7 Mar 2020. [↑](#footnote-ref-66)
66. Prime Minister’s Office - National Cyber Directorate, Israel National Cyber Security Strategy In Brief, Sep 2017, <http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf>, Accessed on 7 Mar 2020. [↑](#footnote-ref-67)
67. Dmitry Adamsky, The Israeli Odyssey towards its National Cyber Security Strategy, The Washington Quarterly, 40:2, 113-127, 14 Jun 2017. [↑](#footnote-ref-68)
68. Prime Minister’s Office - National Cyber Directorate, Israel National Cyber Security Strategy In Brief, Sep 2017, <http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf>, Accessed on 7 Mar 2020. [↑](#footnote-ref-69)
69. Prime Minister’s Office - National Cyber Directorate, Israel National Cyber Security Strategy In Brief, Sep 2017, <http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf>, Accessed on 7 Mar 2020. [↑](#footnote-ref-70)
70. Prime Minister’s Office - National Cyber Directorate, Israel National Cyber Security Strategy In Brief, Sep 2017, <http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf>, Accessed on 7 Mar 2020. [↑](#footnote-ref-71)
71. Prime Minister’s Office - National Cyber Directorate, Israel National Cyber Security Strategy In Brief, Sep 2017, <http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf>, Accessed on 7 Mar 2020. [↑](#footnote-ref-72)
72. Narmeen Shafqat, Ashraf Masood, Comparative Analysis of Various National Cyber Security Strategies, International Journal of Computer Science and Information Security, Vol. 14, No. 1, Jan 2016; Eric Luiijf, Kim Besseling, Patrick de Graaf, Nineteen National Cyber Security Strategies, International Journal of Critical Infrastructure Protection, Vol. 9, Nos. 1/2, 2013. [↑](#footnote-ref-73)
73. Dmitry Adamsky, The Israeli Odyssey towards its National Cyber Security Strategy, The Washington Quarterly, 40:2, 113-127, 14 Jun 2017. [↑](#footnote-ref-74)
74. Dmitry Adamsky, The Israeli Odyssey towards its National Cyber Security Strategy, The Washington Quarterly, 40:2, 113-127, 14 Jun 2017. [↑](#footnote-ref-75)
75. Deborah Housen-Couriel, National Cyber Security Organisation:Israel, NATO Cooperative Cyber Defence Centre of Excellence Tallinn 2017. [↑](#footnote-ref-76)
76. Dmitry Adamsky, The Israeli Odyssey towards its National Cyber Security Strategy, The Washington Quarterly, 40:2, 113-127, 14 Jun 2017. [↑](#footnote-ref-77)
77. [Shoshanna Solomon](https://www.timesofisrael.com/writers/shoshanna-solomon/), Why Is Israel’s New Proposed Cybersecurity Law Raising Hackles?, The Times of Israel, 25 Jun 2018, <https://www.timesofisrael.com/why-is-israels-new-proposed-cybersecurity-law-raising-hackles/>, Accessed on 7 Mar 2020. [↑](#footnote-ref-78)
78. Michael L. Gross\*, Daphna Canetti and Dana R. Vashdi, “Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes”, Journal of Cybersecurity, 3(1), 2017, 49–58, 15 Feb 17. [↑](#footnote-ref-79)
79. Harold’s paper [↑](#footnote-ref-80)
80. Nadiya Kostyuk & Carly Wayne, “Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats”, June 13, 2019. [↑](#footnote-ref-81)
81. Norman Vasu and Benjamin Ang, “Embracing Technology to Boost National Security,” TODAY, December 22, 2016, available at <www.todayonline.com/technology-0/ embracing-technology-boost-national-security [↑](#footnote-ref-82)
82. EUGENE EG TAN, CYBER DETERRENCE IN SINGAPORE, S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES, No.309 2 APRIL 2018 [↑](#footnote-ref-83)