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

31 May 2020

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Ministry of Defence, Singapore, or the Singapore Armed Forces.

ABSTRACT

The advent of cyberspace as a global phenomenon has offered many new opportunities to nations, companies and individuals, and led to significant changes in our social way of life. At the same time, it has also presented challenges to national security. In recent years, Singapore has faced growing cyber attacks against government and non-government entities. Singapore's multi-culturalism and multi-racialism also offer opportunities for its potential adversaries to create social disharmony by exploiting and magnifying differences and inevitable tensions between groups through disinformation campaign. Resilience can be an effective deterrent against cyber threats. Building social and psychological resilience is therefore key to both preventing as well as responding to and recovering from a cyber attack that has caused disruptions to daily life or loss of lives.

This paper examines the adequacy of Singapore's cybersecurity efforts to strengthen social resilience against cyber threats. Singapore's current cyber security strategy has rightly placed emphasis on resilience, particularly in ensuring the critical information infrastructure are protected and a responsive cyber response system is in place to recover them when attacked. In combating disinformation, Singapore has recently incorporated digital defence as a new pillar in its concept of Total Defence. Nonetheless, more could be done, specifically in directing efforts towards strengthening social resilience. To this end, the paper recommends: (1) Raising the level of cyber threat awareness of the community, (2) Adopting a bottom-up approach from community level, (3) Placing emphasis on community preparedness, and (4) Providing clear and effective communications.

ACKNOWLEDGEMENT

The past ten months that I spent in the Israel National Defence College has been an enriching and fulfilling learning journey. I not only broadened my perspectives on issues of global significance, but also deepened my understanding on regional geopolitics regarding Israel and the Middle East. This unique experience has undoubtedly sharpened my critical thinking on these matters.

My sincere thanks to MG Itai Veruv, Commander Israel Defence Forces Military Colleges and Israel National Defence College, for his warm reception to my participation in the course, and his enthusiastic personal sharing and wisdom during the course.

My deepest thanks to Prof Daphna Canetti, my academic advisor, for the sharing of her wealth of knowledge and her guidance in my research of this final paper.

My heartfelt thanks to BG Eran Kamin and Col Amiram Jakira, my team instructors, as well as my coursemates from the 47th INDC for their friendships and the many insightful sharing on the different issues.

Last, but not least, I would also like to thank Dr Anat Stern for a fantastic summer course that she organised for the International Officers, LTC Matan Or, MAJ Gal Ballas, and the staff from the ISMO Office for their support and friendships.

TABLE OF CONTENT PAGE

Abstract 1

Acknowledgement 2

Table of Content 3

Chapter 1: Introduction

1.1 Background 5

1.2 Research Outline 8

1.3 Significance of Research 9

1.4 Methodology 9

Chapter 2: Cyber Risks and its Impact to Singapore

2.1 Evolution of the Cyber Threats 11

2.2 The Collateral Consequences from Cyber Attacks 13

2.3 The Challenge to Singapore's Multiculturalism 16

2.4 Cyber Vulnerability to Singapore as a Smart Nation 18

Chapter 3: Resilience

3.1 What is Resilience? 22

3.2 The Need for Resilience 23

3.3 Social and Psychological Resilience Defined 24

Chapter 4: Singapore's and Israel's National Cyber Defence Strategy

4.1 Singapore's Cyber Security Strategy 27

4.2 Digital Defence as part of Singapore's Total Defence Strategy 32

4.3 The Israeli National Cyber Security Strategy 34

4.4 Comparative Analysis of Singapore's and Israel's National Cyber Security Strategy 37

Chapter 5: Recommendations

5.1 Raise Level of Cyber Threat Awareness 44

5.2 Bottom-up Approach from Community Level 45

5.3 Emphasis on Community Preparedness 46

5.4 Clear and Effective Public Communications 48

Chapter 6: Conclusion 50

Bibliography 52

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. Humans are now very interconnected via their smartphones and IT gadgets. Increasingly, more smart cities are being created where city infrastructures and services are linked up using interconnected systems for monitoring, control and automation. In this regard, Singapore is leveraging significantly on the 4th Industrial Revolution, fuelled by digital technologies, to develop into a Smart Nation. Singapore's Smart Nation initiative, requiring a whole-of-nation efforts approach, aims 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 new opportunities to nations, companies and individuals, it has also at the same time presented challenges to national security. As national critical infrastructures become more interconnected and dependent on computer networks and infocomm systems 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 of national critical infrastructures, potentially crippling the country.[1] One such example is 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.[2] 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] 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 are reminders on the vulnerability of a nation in a cyber era and the challenges cyber threats pose to national security, as nations become ever more dependent on cyberspace for both its most basic and most critical functions.

Besides inflicting physical damage or disrupting the operations of national critical infrastructures, cyber terrorism can also create adverse effects on the psychological well-being of individuals.[4] Cyber attacks on information systems of essential government services and financial services can disrupt individual's daily activities, causing increased stress and anxiety in individuals and making them feel insecure.[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 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

[1] Lewis, 2002.
[2] Business Insider, 2016.
[3] BBC News, 2017.
[4] Gross, Canetti, Vashdi, 2017, pp 49-58.
[5] Ibid.

resulting from the database compromise.[6] To overcome these anxiety and sense of insecurity, it is critical for an individual to have psychological resilience as it provides one with the psychological capacity to adapt to the stress and recover from the situation.[7]

Every nation must also defend itself against the spread of disinformation on social media, another form of cyber threats, 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 conducted through disinformation could polarize this multi-cultural society, weaken social cohesion and create an adverse effect on the social fabric.

Resilience is an effective deterrent that is key to both preventing as well as responding and recovering from a cyber attack. Besides putting in place technological solutions in systems to protect it and enable it to quickly recover from cyber attacks, social resilience against cyber attacks is also important. Social resilience can play a key role as most crisis typically comprise a human element. Therefore, it is imperative that Singapore also pro-actively confronts and addresses the cyber security

[6] Goh, 2018.
[7] Hua, Chen, Luo, 2018.

challenges from the aspect of psychological and social impacts on individuals and communities, and ensure that the nation’s 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

This paper seeks to address the following questions:

a) How effective is Singapore's cyber security strategy in influencing its social resilience against cyber threats?

b) 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 national critical infrastructures and 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'. Most national cyber security strategy focus on processes and technologies to bolster the cyber resilience of its systems and physical infrastructures for business continuity and cyber disaster recovery. However, it is also important to strengthen individual and social resilience against cyber threats to mitigate chaos and terror caused by cyber attacks.

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.

Like Israel, Singapore also recognised the lurking cyber threats 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 first 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. The paper will next do a literature review on social resilience in relation to cyber threats and then examine Singapore's cyber security strategy. The paper will also make comparisons of Israel's and Singapore's cyber security approach and seek to draw out key lessons on the cyber strategy and approaches from the Israeli experience. 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 RISKS AND ITS IMPACTS 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, 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 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 MyDoom software virus, which has the capability to conduct Distributed Denial-of Service (DDoS) attacks.[8] 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.[9] 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.[10]

[8] Krepinevich, 2012, pp 38-50.

[9] Ibid.

[10] Krebs, 2007.

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.[11] 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. The ability for nation-states to launch cyber attacks in an attempt to disrupt or damage national critical infrastructure through non-kinetic means could also be seen through the recent alleged Iran’s attack on Israeli water and sewage systems in April 2020.[12]

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,[13] some with the aim to interfere in elections as well as other

[11] Herzog, 2011, pp 49-60.

[12] Haaretz, 2020.

[13] Gu, Kropotov, Yarochkin, 2017.

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.[14]

State and private actors exploit fake news to advance their agenda. Using 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

[14] Vasu, Ang, Teo, Jayakumar, Faizal, Ahuja, 2018.

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.[15] However, the effects of cyber attacks can be far reaching beyond the direct impact on the computer systems and networks.

Festering within the aftermath of massive 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.[16] 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.[17] In Jan 2017, Lloyds Banking Group suffered a DDoS cyber attack over 2 days. At the 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

[15] Lewis, 2002.
[16] Gross, Canetti, Vashdi, 2016, pp 284-291.
[17] Bada, Nurse, 2019.

improve on cyber security.[18] 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.[19]

Another related example is the outbreak of the COVID-19 virus in Jan 20, which initially caused significant global panic based on a survey results by Pharmaceutical Technology.[20] 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 initial 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.[21] Some of the social impacts that were observed in this COVID-19 episode included a growth of mistrust and racist attitudes towards Chinese people living in other countries. In the UK, there were reports of anxiety where commuters actively avoided sitting or standing near people of Chinese descent on public transport. Elsewhere, there were 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 influence adverse individual actions, which in turn have

[18] Nicholls, 2017.
[19] Dunkley, 2017.
[20] Nawrat, 2020.
[21] Ibid.

ripple effects on the community and the broader society. When news of the COVID-19 spread broke out in Singapore, online rumours 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 masks, and food supplies.[22]

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 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.[23] 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.[24]

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)*

[22] Wong, 2020.
[23] Gross, Canetti, Vashdi, 2016, 284-291.
[24] Ibid.

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[25]. 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.[26] 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".[27] 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.[28] 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

[25] Noor Aisha, 2009, pp 109-128.

[26] Yahya, 2018.

[27] Ibid.

[28] Ibid.

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 can lead to a more fractious and divided society. [29] 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.[30] 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 continues to underscore significant challenges for Singapore.[31]

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

[29] Lim, 2019.

[30] Aw, 2018.

[31] Neubronner, 2017.

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 DDoS attacks on StarHub's network.[32] 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 reported an overall increase in the number of cybercrimes from 2017. [33] 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.[34] 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 could create stress and unrest in individuals and society given the scarce water resource situation in Singapore.

[32] Tham, 2016.

[33] Cyber Security Agency, 2018.

[34] Ibid.

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.[35] In this context, a Smart Nation with deep reliance on Infocomm Technology will definitely be even more vulnerable to cyber attacks. At a societal level, cyber attacks in key services sector such as energy, transportation and communications would 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

[35] Infocomm Media Development Authority, 2015.

threats made by other states.[36] These risks necessitate an immense responsibility to actively protect and make resilient the cyber infrastructure that forms the foundation of its economic activities.

[36] Cyber Security Agency Singapore, 2018.

CHAPTER 3
RESILIENCE

3.1 WHAT IS RESILIENCE?

There are many definitions on the concept of resilience. The key term to these definitions is the system's ability to adjust its functioning. Broadly, resilience can be defined as a system's capacity to persist in its current state of functioning while facing disturbance and change (coping capacities), to adapt to future challenges (adaptive capacities), and to transform in ways that enhance its functioning (transformative capacities).[37] Hollnagel[38] proposed the following four abilities necessary for resilient performance:

a) The ability to respond. Knowing what to do, or being able to respond to regular and irregular changes, disturbances, and opportunities by activating prepared actions or by adjusting current modes of functioning. It includes assessing the situation, knowing what to respond to, finding or deciding what to do, and when to do it. This is the ability to address the actual.

b) The ability to monitor. Knowing what to look for or being able to monitor that which is or could seriously affect the system's performance in the near term, positively or negatively. The monitoring must cover the system's own performance as well as what happens in the environment. This is the ability to address the critical.

[37] Keck, Sakdapolrak, 2013, pp 5-19.

[38] Hollnagel, 2010.

c) The ability to learn. Knowing what has happened, or being able to learn from experience, in particular to learn the right lessons from the right experience, successes as well as failures. This is the ability to address the factual.

d) The ability to anticipate. Knowing what to expect or being able to anticipate developments further into the future, such as potential disruptions, novel demands or constraints, new opportunities, or changing operating conditions. This is the ability to create foresight and to address the potential.

3.2 THE NEED FOR RESILIENCE

Resilience can be an effective deterrent against cyber threats. Resilience provides individuals and society with coping capacities to endure and overcome sudden disruptions reactively and rapidly. In the case of a cyber attack, this could mean the way of life of individuals that has been directly affected is maintained as a result of effective crisis management plans, and the will of the population to continue their usual routine despite fear and confusion from the ensuing attack. With resilience, society will have the adaptive capacities to perform proactive and long-term adaptation of structures, processes, or modes of behaviour to face present and future vulnerabilities, thereby reducing the potential negative impacts. For example, in face of possible cyber attacks, more emphasis could be placed on the role and responsibility of citizens in crisis management and promoting civic participation and self-help capacities at a local level. Unlike adaptive capacities, transformative capacities in the context of resilience enables society to undertake radical changes as compared to gradual changes. In facing cyber threats, this could mean adopting completely different social norms and behaviours to deal with possible consequences from cyber attack or creating new research areas to better address cyber threats.

Resilience has become a concept that has increasingly informed political and policy discussions around disaster planning and preparedness. [39] 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 comprises six key pillars - Military, Civil, Economic, Social, Digital and Psychological Defence,[40] 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.

3.3 SOCIAL AND PSYCHOLOGICAL RESILIENCE DEFINED

Disruptive events such as cyber attacks can have impacts both at the societal and individual psychological level. Building social and

[39] Walkate, McGarry, Mythen, 2014, pp 408-427.

[40] MINDEF, Total Defence.

psychological resilience is therefore key to both preventing as well as 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.[41] Resilient societies and communities demonstrate readiness to face a grand crisis, without giving up on national and strategic objectives.[42] Individual resilience pertains to the person's strength and coping behaviours that sustain individuals during stressful life events.[43] Resilient persons can continue to function normally under adverse circumstances and revert back to their original state when the stressing factors end.[44]

Research has also shown that individual resilience is integral to social and national resilience.[45] 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.[46] 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.[47] People with higher psychological resilience can more easily navigate themselves around stress and adversity, stay positive, and pursue resilient outcomes.[48]

[41] Gal, Maital, 2016.
[42] Ibid.
[43] Gal, 2014, pp. 452-475.
[44] Griffith, 2011.
[45] Hua, Chen, Luo, 2018.
[46] Bonanno, Galea, Bucciarelli, Vlahov, 2007, pp 671–682
[47] Bonanno, 2004, pp 20–28.
[48] Hua, Chen, Luo, 2018.

In Canetti's research, it showed that the interface between national security and resilience is rooted in individuals' perceptions and attitudes toward institutions and leadership.[49] When it comes to societal resilience, trust in institutions is also one of the central elements of functioning societies. Institutional trust indicates how people value the ability of their institutions to protect society from disruptive events and prevent future attacks.[50] 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.

There is also research that suggests that individuals exposed to cyber attacks show an increase in cyber-induced stress, which exacerbates perceptions of violent threat and personal insecurity,[51] leading to fear. Fear appeals are a proactive method for motivating people to act.[52] 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.[53]

[49] Canetti, Waismel-Manor, Cohen, Rapaport, 2013.
[50] Oksanen, Kaakinena, Minkkinen, Räsänen, Enjolrasc, Steen-Johnse, 2018.
[51] Canetti, Gross, Waismel-Manor, Levanon, Cohen, 2017.
[52] Hua, Chen, Luo, 2018.
[53] Ibid.

CHAPTER 4
SINGAPORE'S AND ISRAEL'S CYBER SECURITY STRATEGY

4.1 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 ISMP is a three-year strategic roadmap that focused on building basic cyber defence capabilities within the public sector to mitigate and respond to cyber threats.[54] This was followed by the launch of a 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. [55] The new five-year National Cyber Security Masterplan (NCSM) 2018, launched in 2013, built on the efforts of the 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.[56]

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,

[54] Infocomm Media Development Authority, 2005.

[55] Infocomm Media Development Authority, 2008.

[56] Infocomm Media Development Authority, 2013.

following the establishment of CSA, Singapore launched its Cyber Security Strategy, which encompasses 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.[57]

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, when implemented, will 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.[58]

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

[57] Cyber Security Agency, 2016.

[58] Ibid.

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.

The readiness and responsiveness to significant cyber attacks at the national level will be enhanced through the conduct of regular multi-sector cyber security exercises. 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 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.[59] 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. To further safeguard these government systems and networks, there are plans for investments in technologies such as analytics, automation, artificial intelligence, and other state-of-the-art security technologies.

Pillar #2: Creating a Safer Cyberspace

Digital connectivity has both empowered and endangered businesses and individuals.[60] 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.[61] Another effort undertaken to help keep the cyberspace safe is through the Public Cyber-Outreach &

[59] Cyber Security Agency.
[60] Cyber Security Agency, 2016.
[61] Ibid.

Resilience Programme (PCORP), where it promoted the adoption of good practices such as taking preventive measures to secure individuals computer systems and digital devices, particularly to prevent malicious actors from hijacking their systems and devices to cause harm to others.[62]

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.[63] 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 after their National Service days. 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.

[62] Bhunia, 2017.

[63] Siau, 2018.

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.[64]

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.[65]

4.2 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

[64] National Research Foundation.
[65] Cyber Security Agency, 2016.

with these digital transformation initiatives, it has also made Singapore more vulnerable to threats from the digital domain. Not only will cyber attacks disrupt the way of life of Singapore's residents, 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. Therefore, Singapore has included Digital Defence as the sixth pillar in its Total Defence strategy.[66]

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.[67] 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.[68] The 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).[69]

[66] Baharudin, 2019.

[67] Tan, 2019, pp 158-171.

[68] Tham, 2019.

[69] Singapore Legal Advice.

A series of Cyber Security Awareness Campaign has also been launched since its inception in 2017. The campaign, held in the form of roadshows at local community, aims to bring cybersecurity awareness to the community and provide an avenue for members of the public to pick up tips on good cyber security habits, and get face-to-face advice from cyber experts onsite.

4.3 THE ISRAELI NATIONAL CYBER SECURITY STRATEGY

According to the published Israel National Cyber Security Strategy,[70] the first milestone in the development of Israel's national cyber security efforts was laid in 2002, when the Israeli government authorised the National Information Security Authority (NISA) to instruct and protect vital computerised 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, 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.[71]

[70] Prime Minister's Office - National Cyber Directorate, 2017.

[71] Adamsky, 2017, pp 113-127.

Israel's cyber security strategy is based on a generic concept of operations for national cyber security.[72] The concept of operations defines three operational layers: Aggregate Cyber Robustness, Systemic Cyber Resilience and National Cyber Defence. 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 organisations. This 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 as concluded by INCD.

1st Layer: Aggregate Cyber Robustness

Under the Israel National Cyber Security Strategy, cyber robustness is seen as the ability of organisations and processes to continue operating despite a routine of cyber threats by repelling and preventing most of the attacks.[73] 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 organisations (best practice, guidance, regulations, incentives, etc.) and by regulating the cyber security market.

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,

[72] Prime Minister's Office - National Cyber Directorate, 2017.
[73] Ibid.

prevent them from spreading and reduce their cumulative damage to the nation.[74] 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 organisations during cyber incidents. This effort is led by the NCSA, with the national CERT (CERT-IL) at the forefront. CERT-IL works closely with the private sector, both directly and through sector-based cyber centres which operate within CERT-IL. CERT-IL strives to engage in global and local cooperation while supporting innovation and harnessing it for its goals.

3rd Layer: National Cyber Defence

A national-level campaign is required against severe threats by determined, resource-rich attackers who pose serious dangers to the nation. National defence campaigns incorporate defensive efforts to contain such attacks and their ramifications, together with active efforts to confront the sources of the threats.[75]

Capacity Building

Israel has also made it a priority to strengthen its scientific and technological cyber capabilities and innovation processes. Efforts include research, development and implementation of national level security capabilities and technologies, as well as promoting industrial innovation and supporting academic research in the cyber field.

[74] Ibid.

[75] Ibid.

4.4 COMPARATIVE ANALYSIS OF SINGAPORE'S AND ISRAEL'S NATIONAL CYBER SECURITY STRATEGY

Comparison Metrics

Taking reference from some of the comparison metrics adopted in other studies that analysed and compared different nation's cyber security,[76] a comparative analysis of Singapore's and Israel's cyber security strategy is made with the below factors. These factors were chosen to help gain insights on the level of coping, adaptive and transformative capacities that exists within the measures adopted by the respective countries in their cyber security strategy that influence social and psychological resilience towards cyber threats:

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

Characterisation of Cyber Threats

Singapore sees itself vulnerable to cyber threats such as fake news and deliberate online falsehoods from the digital domain as well as cyber

[76] Shafqat, Masood, 2016.

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.[77]

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. This helps create an overarching common goal for all entities to work together and towards it, thereby strengthening resilience against 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.[78] 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 spectrum of threats.

[77] Adamsky, 2017, pp 113-127.

[78] Ibid.

While the approach is different, the national cyber security strategy produced by both countries detailed the national vision, guiding principles, perceptions of threats and the strategic objectives. With it, it provided a comprehensive framework to holistically develop capabilities and capacities, from a cyber ecosystem perspective instead of piecemeal incremental approach, to deal with the cyber threats.

Incident Response Capabilities

Both Singapore and Israel have in place robust frameworks and response plans to serve as its coping capacities 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 analysing 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’.[79]

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

[79] Housen-Couriel, 2017.

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.[80]

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 Agency 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.

[80] Adamsky, 2017, pp 113-127.

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.[81] This 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.

Summary of Comparative Analysis

The key findings are summarised in the table below.

	Singapore	Israel
Characterisation of cyber threats	• 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

[81] Solomon, 2018.

	Singapore	Israel
		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	• Has in place 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 • Has a 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 LEVEL OF CYBER THREAT AWARENESS

Singapore's current cyber security strategy has rightly placed emphasis on resilience, particularly in ensuring the critical information infrastructure are protected and a responsive cyber response system is in place to recover them when attacked. Nonetheless, more could be done, specifically in directing more efforts towards building up psychological resilience. In other words, Singapore also needs to better mentally prepare its citizens, and not just the public and private sectors, against the possibility that Singapore might one day succumb to a major cyber attack. The government should seek to sensitise the population to the cyber threats in order to reduce the 'shock factor' and encourage organisations and communities to develop their own resilience plan. Unlike conventional terrorist attacks, cyber attacks on national critical infrastructure or disinformation often does not threaten life or cause physical harm to individual.[82] Hence, cyber threats is largely invisible to the public. How then can the level of cyber threat perception be raised?

In combating disinformation, Singapore has embedded digital defence into the concept of Total Defence to enhance societal awareness and to promote discussions. To raise awareness on the threats of cyber attacks on national critical infrastructure and its associated impacts to individuals and society, the Government could consider using cyber-doom scenarios or releasing more information to the public on on-going cyber-intrusions against Singapore. This could trigger the civilians'

[82] Gross, Canetti, Waismel-Manor, 2016.

psychological resilience by arousing a certain amount of fear and raising concerns on cyber attacks. Threat perception, not an actual attack can also unsettle individuals to the extent many terrorists desire.[83] Messaging campaigns designed to increase citizens' cyber-awareness and to involve fear appeals can be employed to raise cyber threat perception. Bruijn in his research suggested evidence-based message framing as a plausible method and some of the strategies include making it clear who the villains are in cases where it is unambiguous and non-sensitive (can also be the people causing the security lapse) or connecting the cyber security issue to other tangible and clear issues.[84] According to a research by Wayne, 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 in the cyber realm.[85] These messaging campaigns could be done in the form of Cyber road shows held at various local communities to expose residents to the issue or 'Cyber Security Campaign' to heighten nation-wide awareness. The theme of such road shows should go beyond current messaging on basic know-how of good cyber practices. Keen awareness on cyber threats by the community can encourage greater civic participation which strengthen adaptive capacities for the community to adapt their modes of behaviours to face anticipated impacts from cyber attacks.

5.2 BOTTOM UP APPROACH FROM COMMUNITY LEVEL

At the national level, both Singapore and Israel have a central agency to lead in the handling of cyber incidents. These agencies will

[83] Gross, Canetti, Vashdi, 2017, pp 49–58.
[84] Bruijn, Janssen, 2017.
[85] Kostyuk, Wayne, 2019.

develop the overall response plans, mobilise the necessary resources, direct the operational cyber responses, and work closely with the affected sectors and organisations to handle the cyber threat and to expediently recover the affected critical information infrastructure. Besides top-down approach by the government, bottom up involvement of communities in cyber preparedness can also promote confidence in the public to cope with the unknowns.

In a research by Hua, the findings concluded that community support can help civilians become more resilient.[86] Community support, besides an effective crisis management plan to deal with the cyber attack on the information systems, can increase coping capacities to deal with the fallout from cyber attacks. Singapore should therefore capitalise on its existing community engagement programme (CEP) and extend its efforts to include cyber preparedness at community level. Essential procedures to follow at the community level in the event of massive cyber attacks can be developed. A core group of activists could be trained on the cyber response procedures so that they can respond quickly and decisively, and lead their local community on what to do during and after a massive cyber attack that has caused disruptions to daily activities. The aim is to keep as much as possible the functional continuity of community life and reduce fear and confusion from an ensuing cyber attack.

5.3 EMPHASIS ON COMMUNITY PREPAREDNESS

Drills and Exercises at Community Level

In the event of a massive cyber attack on Singapore's critical information infrastructure, a whole-of-society response would be required

[86] Hua, Chen, Luo, 2018.

for Singapore to ‘bounce back’ quickly. At the industry level, organisations from different sectors are already involved in rigorous cyber drills and 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. Such exercises range from industry-specific type, to national-level focused which involves a whole range of organisations from multiple CII sectors such as aviation, land transport, maritime, media, energy, government, info-comm, healthcare, water, and security & emergency. Through these drills and exercises, businesses build resilience by training to respond to breaches and by maintaining backup systems that can be called upon in times of emergency to recover from an attack. However, more needs to be done at the local community level.

Singapore’s residents should be made aware that although the government would continue to work with the private sector to harden cyber defences, it would not be foolproof. The public would also need to be able to react with resilience and unity in the event of a cyber attack, but the daily peace and security that Singaporeans are used to could make them ill-equipped to deal with degradations in public services that affects their daily activities. At the societal level, the public would then need to be acquainted on the response to cyber attacks through drills and exercises, much like the same way of practising fire drills and emergency drills simulating real scenarios. Such drills are useful for the public to be informed on who to contact in the event of a cyber attack, and where to seek help. Public involvement in drills and exercises would also reinforce the cyber security awareness campaign as such events provide training on actionable steps that the public can take. Such psychological preparation at the individual level will contribute towards cyber resilience. Research also suggested that cortisol levels rose significantly when people experienced simulated cyber attacks and people with high threat perceptions are also more willing to support strong government policies.[87] In the case of cyber security, it would mean willingness to exchange civil liberties and privacy for security and support of government surveillance.[88]

Enhancing Media Literacy

Against disinformation, efforts should also be invested to incorporate training on media literacy tools in school curriculum or community courses through government sponsored training programmes. This could help equip the public with the skills and knowledge to better discern facts and online falsehood. The public would then not only be able to avoid contributing to the spread of untruths and distorted information, as well as help to flag out online falsehood to alert others. In parallel, the government could work with private corporations and provide funding to research into using technology such as artificial intelligence and machine learning to counter online falsehoods.

5.4 CLEAR AND EFFECTIVE PUBLIC COMMUNICATIONS

In responding to a cyber attack that impacts the society at large, it is important to keep the public informed so that their anxieties are allayed, and they remain calm. There should be clear communications to the public on what the responsible agencies are doing to address the situation, what required resources have been identified or activated, and

[87] Canetti, Gross, Waismel-Manor, Levanon, Cohen, 2017.

[88] Gross, Canetti, Vashdi, 2017, pp 49–58.

what are the recommended steps that the public can take to facilitate the overall response.[89] At the same time, inaccurate reports or factual errors in information that could cause panic or impede recovery efforts should also be addressed. By providing timely, transparent and frequent communications, it can help to maintain public confidence and trust in government that the situation is under control. In the aftermath of a highly disruptive cyber attack, communicating a consistent message to the public in a crisis is also essential, as it would reduce confusion and stress from undue worrying. To facilitate this process, a central communications agency could be made responsible to collate and distil information from disparate entities, coordinate messages and deliver them to the public in a coordinated fashion.

[89] Smart, 2018.

CHAPTER 6
CONCLUSION

As Singapore undertakes digital transformation to improve its government systems, business and society, it also subjects itself to a larger cyber threat landscape. The increased use of digital domains for access to information also puts the nation at risks to online falsehoods. Disinformation can be used to exploit the diversity in Singapore's society and create polarisation in the social fabric, thereby undermining its social cohesion. The implementation of the national cyber security strategy that Singapore has developed will serve well to enhance cyber resiliency in its critical infrastructure as well as build capacity in its cyber ecosystem. Singapore has also included Digital Defence as a new pillar in its Total Defence concept to guard against threats from the digital domain. However, the challenges emanating from cyber threats will continue to evolve. Disruptive events such as cyber attacks can have impacts both at the societal and individual psychological level. Building social and psychological resilience is therefore also key to both preventing as well as responding to and recovering from a cyber attack that has caused disruptions to daily life or loss of lives. Individual and social resilience is integral to national resilience. As Singapore further develop and implement its cyber security strategy, it is important to also consider the need to develop capacity to ensure its people can cope with the collateral consequences from cyber terrorism.

To help strengthen individual and social resilience to mitigate fear, anxiety and confusion caused by cyber attacks, this paper has outlined four recommendations: (1) raising the level of cyber threat awareness among the public, (2) encouraging bottom-up initiatives from community level, (3) emphasis on preparedness at community level, and (4) clear and effective communications to sustain public confidence when dealing with massive cyber attack situation. This could enhance Singapore’s abilities to deter cyber threats, as well as its capacity to withstand, respond, and recover from disruptions arising from cyber events.

BIBLIOGRAPHY

1. James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, Dec 2002.

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.

3. BBC News, Ukraine Power Cut 'Was Cyber-Attack', 11 Jan 2017, https://www.bbc.com/news/technology-38573074, Accessed on 25 Feb 2020.

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, pp 49-58.

5. Ibid.

6. 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.

7. Jian Hua, Yan Chen, Xin (Robert) Luo, Are We Ready for Cyberterrorist Attacks? - Examining the Role of Individual Resilience, Information & Management, Apr 2018.Fd

8. Andrew F. Krepinevich, Cyber Warfare: A "Nuclear Option"?, Center for Strategic and Budgetary Assessments, 2012, pp 38-50.

9. Ibid.

10. 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.

11. Stephen Herzog, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, Journal of Strategic Security, Vol 4, No.2, Summer 2011, pp 49-60.

12. Haaretz, Cyberattack by Iran Targeted Israel's Water and Sewage Systems - Report Says, 7 May 2020, https://www.haaretz.com/israel-news/cyberattack-by-iran-targeted-israel-s-water-and-sewage-systems-report-says-1.8829340, Accessed on 22 May 2020.

13. Andrew F. Krepinevich, Cyber Warfare A "Nuclear Option"?, Center for Strategic and Budgetary Assessments, 2012, pp 133-137.

14. 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.

15. 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.D

16. James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, Dec 2002.

17. Gross, M. L., Canetti, D., & Vashdi, D.R, The Psychological Effects of Cyber Terrorism, Bulletin of the Atomic Scientists 72(5), 2016, pp 284-291.

18. Maria Bada, Jason Nurse, The Social and Psychological Impact of Cyber-Attacks, Published in Oct 2019.

19. 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.

20. 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.

21. 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.

22. Ibid.

23. 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.

24. Gross, M. L., Canetti, D., & Vashdi, D.R, The Psychological Effects of Cyber Terrorism, Bulletin of the Atomic Scientists 72(5), 2016, 284-291.

25. Ibid.

26. 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 27(2), 2009, pp 109-128.

27. 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.

28. Ibid.

29. Ibid.

30. 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.

31. 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.

32. Stephanie Neubronner, Social Media and "Fake News": Impact on Social Cohesion in Singapore, RSIS No.043, 14 Mar 2017.

33. 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.

34. Cyber Security Agency Cyber Threats in Singapore Grew in 2017, Mirroring Global Trends, Press Release on 19 Jun 18.

35. Ibid.

36. 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.

37. Cyber Security Agency Singapore, Singapore Cyber Landscape 2018.

38. Markus Keck and Patrick Sakdapolrak, "What is social resilience? Lessons learned and ways forward," ERDCUNDE, Vol 67, no. 1, 2013, pp 5-19.

39. Erik Hollnagel. How Resilient Is Your Organisation? An Introduction to the Resilience Analysis Grid (RAG). Sustainable Transformation: Building a Resilient Organization, May 2010, Toronto, Canada. ffhal-00613986.

40. S.Walkate, R. McGarry, G.Mythen, Searching for Resilience: A Conceptual Excavation, Armed Forces & Society Vol 40(3), 2014, pp 408-427.

41. MINDEF, Total Defence, https://www.mindef.gov.sg/oms/imindef/mindef_websites/topics/totaldefence/index.html#, Accessed on 2 Mar 2020.

42. 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.

43. Ibid.

44. Reuven Gal, Social Resilience in Times of Protracted Crises: An Israeli Case Study, Armed Forces & Society Vol. 40(3), 2014, 452-475.

45. 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.

46. Jian Hua, Yan Chen, Xin (Robert) Luo, Are We Ready for Cyberterrorist Attacks? - Examining the Role of Individual Resilience, Information & Management, Apr 2018.

47. 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, Vol. 75, No. 5, 2007, pp 671–682

48. 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, pp 20–28.

49. Jian Hua, Yan Chen, Xin (Robert) Luo, Are We Ready for Cyberterrorist Attacks? - Examining the Role of Individual Resilience, Information & Management, Apr 2018.

50. 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.

51. 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.

52. 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, Volume 20, Number 2, 2017.

53. Jian Hua, Yan Chen, Xin (Robert) Luo, Are We Ready for Cyberterrorist Attacks? – Examining the Role of Individual Resilience, Information & Management, Apr 2018.

54. Ibid.

55. Infocomm Media Development Authority, Launch Of The Infocomm Security Masterplan, Opening Address by Dr Tony Tan Keng Yam, 22 Feb 2005.

56. Infocomm Media Development Authority, New S$70m Masterplan To Boost Singapore's Infocomm Security Competency And Resilience, Press Release, 17 Apr 2008.

57. Infocomm Media Development Authority Singapore Continues to Enhance Cyber Security with a Five-Year National Cyber Security Masterplan 2018, Press Release, 24 Jul 2013.

58. 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.

59. Ibid.

60. Cyber Security Agency, Cybersecurity Act, https://www.csa.gov.sg/legislation/cybersecurity-act, Accessed on 4 Mar 2020.

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.

62. Ibid.

63. 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.

64. 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.

65. National Research Foundation, National Cybersecurity R&D Programme, https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme, Accessed on 4 Mar 2020.

66. 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.

67. 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.

68. 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.

69. 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.

70. 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.

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.

72. Dmitry Adamsky, The Israeli Odyssey towards its National Cyber Security Strategy, The Washington Quarterly, 40:2, 14 Jun 2017, pp 113-127.

73. 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.

74. Ibid.

75. Ibid.

76. Ibid.

77. 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.

78. Dmitry Adamsky, The Israeli Odyssey towards its National Cyber Security Strategy, The Washington Quarterly, 40:2, 14 Jun 2017, pp 113-127.

79. Ibid.

80. Deborah Housen-Couriel, National Cyber Security Organisation: Israel, NATO Cooperative Cyber Defence Centre of Excellence Tallinn 2017.

81. Dmitry Adamsky, The Israeli Odyssey towards its National Cyber Security Strategy, The Washington Quarterly, 40:2, 14 Jun 2017, pp 113-127.

82. 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.

83. Michael L. Gross, Daphna Canetti & Israel Waismel-Manor, Immune From Cyber-Fire: The Psychological & Physiological Effects of Cyberwar, In Binary Bullets: The Ethics of Cyberwarfare, Oxford University Press, 2016.

84. 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, pp 49–58.

85. Hans de Bruijn, Marijn Janssen, Building cybersecurity awareness: The need for evidence-based framing strategies, Government Information Quarterly 34 (2017) 1–7.

86. Nadiya Kostyuk & Carly Wayne, Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats, June 13, 2019.

87. Jian Hua, Yan Chen, Xin (Robert) Luo, Are We Ready for Cyberterrorist Attacks? - Examining the Role of Individual Resilience, Information & Management, Apr 2018.

88. 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, Volume 20, Number 2, 2017.

89. 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, pp 49–58.

90. William Smart, Lessons learned review of the WannaCry Ransomware Cyber Attack, Department of Health and Social Care England, 1 Feb 2018, https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf. Accessed on 15 Mar 20.