

**Israel National Defense College**

**47th Class 2019-2020**

**Final Paper Research Proposal**

Academic Adviser: Prof. Daphna Canetti

Submitted by: Wong Khiong Seng

20 Jan 2020

**Subject of the Paper**

Social Resilience in the Cyber Era

**Background**

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

The advent of cyberspace as a global phenomenon has offered many opportunities while at the same time presented vulnerabilities to national security. In some countries, we have seen cyber attacks being conducted on its national critical infrastructure and services which caused disruptions to way of life. Cyber terrorism also has psychological effects on the well being of individuals and public confidence. We have seen how misinformation can be amplified on social media, 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 with an open economy, the relative peace and tolerance among the various religious communities that it currently enjoys is achieved by maintaining social and religious harmony. However, cyber terrorism could polarize this multi-cultural society and create an adverse effect on its social fabric. This would then weaken Singapore’s social resilience as well as degrade its capacity to contain and effectively manage major national crisis, and its abilities to ‘bounce back’ rapidly to restore normalcy. Therefore, it is imperative that Singapore pro-actively confront and address the security challenges emanating from cyber threats. It is crucial that Singapore periodically review its abilities to prevent cyber terrorism, as well as its capacity to withstand, respond, and recover from disruptions arising from cyber events. The aim is to ensure a strong national cyber system that is resilient is continuously in place.

**Main Purpose of the Paper**

The research claim that this paper deals with is that cyber technologies offer many benefits to business and social, and nation states are pursuing the adoption of this cyber technology imperative extensively. On the other hand, these same technologies can be misused by state or non-state actors, making nation states vulnerable to cyber risks. Cyber threats could challenge social resilience in the context of National Security and therefore, Singapore should continuously review and evolve its cyber defence strategy in tandem with the dynamic nature of cyber risks so as to stay ahead in this contest.

This paper seeks:

1. To analyze the effectiveness of Singapore’s national security strategy and measures against developments in the cyber space.
2. To recommend potential policy changes and/or enhancements to the cyber security efforts in Singapore in a bid to strengthen social resilience.

**Research Questions**

1. What is this cyber phenomenon and what are the associated threats and security challenges to nation states?
2. What are the psychological effects of cyber attacks on individuals and society as a whole, in particular Singapore being a small country with an open economy, and a multi-racial and multi-religious demography? How will the risks emanating from cyber threats impact social cohesion in Singapore, thereby challenging its social resilience?
3. What are the differences in approach between the State of Israel and Singapore in balancing the tension between an efficient cyber defence strategy that ensure social resilience and transforming into a digital economy?
4. Singaporeans have come a long way in fostering multicultural harmony. To what extent is Singapore’s cyber security strategy effective in future-proofing its social resilience as it progresses towards becoming a Smart Nation?
5. What are the opportunities and new/novel strategies that can be pursued to better defend against cyber threats in the context of social resilience?

**Basic Conceptual Framework of the Research (Outline):**

This paper will describe the cyber phenomenon, highlight the associated threats to nation states, and analyze Singapore's strategy and measures on cyber security. The paper will first review the phenomenon of increasing applications of cyber space in our daily lives. The paper will next analyse the associated cyber risks such as cyber attacks and disinformation, and draw the connection of its impacts to Singapore’s national security, especially in the area of societal given its unique social demography. The paper will seek to draw out key lessons on the cyber strategy and approaches from the Israeli experience and use it to make comparisons with Singapore’s digital defence approach. The paper will then conclude with a recommendation on new opportunities or framework that Singapore could adopt to better defend social resilience while enabling a digital economy/SMART nation.

The paper will comprise the following chapters:

1. Introduction and research methodology.
2. Cyberspace and Social Resilience. This chapter will highlight the duality of cyber; (a) the growing impact of cyberspace in many aspects of our lives, both individually and as a society, and (b) the rapidly rising risks emanating from cyber threats. The unique characteristics of Singapore’s society will also be described and the impacts of cyber threats on the society component of Singapore’s National Security will be discussed.
3. Critical Analysis of Singapore's Strategy. This chapter will make a comparison on the national cyber strategy currently adopted by the State of Israel and Singapore, and also critically analyse Singapore’s strategy.
4. Key Lessons Learnt and Recommendations on Cyber Security Measures for Singapore. This chapter will explore new opportunities and offer broad recommendations for policy changes that Singapore could pursue to ‘stay ahead’ of the evolving cyber threats.
5. Conclusion.

**Importance of the Paper and Potential Contributions**

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

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