

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 26-04-2018		2. REPORT TYPE Master's of Military Studies		3. DATES COVERED (From - To) SEP 2017 - APR 2018	
4. TITLE AND SUBTITLE A Minnow Among Sharks: Cyber Conflict and the Implications for Singapore				5a. CONTRACT NUMBER N/A	
				5b. GRANT NUMBER N/A	
				5c. PROGRAM ELEMENT NUMBER N/A	
6. AUTHOR(S) Chua, Edwin, Y., Major, Singapore Army				5d. PROJECT NUMBER N/A	
				5e. TASK NUMBER N/A	
				5f. WORK UNIT NUMBER N/A	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068				8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068				10. SPONSOR/MONITOR'S ACRONYM(S) Dr. Benjamin Jensen	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The cyber domain is a new arena for interaction between states. Much of the current literature focuses on cyber interactions between the major powers: The United States, Russia, and China. However, the global reach of the internet means that any developments in cyberspace will also affect all other states, big or small. In particular, small states such as Israel and Estonia have responded differently to the cyber challenge, with Israel embracing a more offensive posture, while Estonia embraces a more defensive posture. Using Israel and Estonia as examples, the paper seeks to determine which elements of their cyber strategy Singapore should adopt. The MMS paper finds that given current cyber threat, it is imperative that small states like Singapore increase their cyber capability in order to defend themselves in this new domain. In doing so, Singapore must strengthen the foundations of a proper defense through leveraging public-private partnerships, build cyber resilience, cooperate with regional and international partners, and develop cyber active defense capabilities.					
15. SUBJECT TERMS CYBER, CONFLICT, SMALL STATES, SINGAPORE					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 74	19a. NAME OF RESPONSIBLE PERSON USMC Command and Staff College
a. REPORT Unclass	b. ABSTRACT Unclass	c. THIS PAGE Unclass			19b. TELEPHONE NUMBER (include area code) (703) 784-3330 (Admin Office)

*United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068*

MASTER OF MILITARY STUDIES

TITLE:

A MINNOW AMONG SHARKS: CYBER CONFLICT AND
THE IMPLICATIONS FOR SINGAPORE

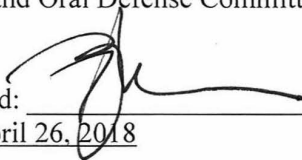
SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

MAJ EDWIN CHUA, SINGAPORE ARMY

AY 17-18

Mentor and Oral Defense Committee Member: Dr. Benjamin Jensen

Approved:  Benjamin Jensen PhD
Date: April 26, 2018

Oral Defense Committee Member: Dr. Brandon Valeriano

Approved:  Brandon Valeriano PhD
Date: April 26, 2018

Executive Summary

Title: A Minnow Among Sharks: Cyber Conflict and the Implications for Singapore

Author: MAJ Edwin Chua, Singapore Army

Thesis: Given current cyber threat, it is imperative that small states like Singapore increase their cyber capability in order to defend themselves in this new domain. In doing so, Singapore must strengthen the foundations of a proper defense through leveraging public-private partnerships, build cyber resilience, cooperate with regional and international partners, and develop cyber active defense capabilities.

Discussion: The cyber domain is a new arena for interaction between states. Much of the current literature focuses on cyber interactions between the major powers: The United States, Russia, and China. However, the global reach of the internet means that any developments in cyberspace will also affect all other states, big or small. In particular, small states such as Israel and Estonia have responded differently to the cyber challenge, with Israel embracing a more offensive posture, while Estonia embraces a more defensive posture. Using Israel and Estonia as examples, the paper seeks to determine which elements of their cyber strategy Singapore should adopt.

In order to determine if an offensive or defensive posture is most appropriate for Singapore, the potential threat of cyber operations for small states and the outcomes of cyber operations are analyzed using the Dyadic Cyber Incident Database 1.1. The analysis concludes that out of all the incidents captured in the dataset, 131 out of 192 incidents, about two thirds, involve small states. This indicates that a majority of cyber conflicts actually involve states that are not major powers. Further statistical analysis indicates that cyber operations involving non-major power states have a higher than expected incidence of disruption, when compared to cyber operations involving major powers.

Next, the reaction of a state's population to cyber operations is examined in order to determine what defensive strategy should be adopted. Surveys by Pew of the American public's reaction in the aftermath of cyber operations on the United States in recently years, as well as a survey by the Cyber Security Agency of Singapore are used. These surveys indicate that apart from tangible measures, greater public outreach is required to engage the public and build support for national cyber defense.

Contextualizing the research findings in light of recent developments in Singapore's cybersecurity landscape, the paper develops recommendations for how Singapore can better leverage public-private partnerships, increase public engagement, engage international partners for cooperative cyber defense, and develop its cyber capabilities.

Conclusion: A strong cyber defense is needed to ensure that Singapore can continue to leverage advances in technology to grow its economy and improve the lives of its people. Furthermore, Singapore's cyber defense strategy must be continuously updated to keep pace with the increasing rate of technological developments in the cyber domain.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

	Page
EXECUTIVE SUMMARY	i
DISCLAIMER	ii
LIST OF ILLUSTRATIONS	iv
LIST OF TABLES	iv
PREFACE	v
INTRODUCTION AND THESIS STATEMENT	1
LITERATURE REVIEW	4
Major Power Behavior in Cyberspace	6
The Development of Cyber Capabilities by Small States	12
The Evolving Characteristics of Cyberspace	15
Way Ahead	16
METHODOLOGY	18
DATA ANALYSIS AND FINDINGS	21
Character of Cyber Threats Facing Small States	21
Attitudes of Singaporeans Towards Cyber Threats	27
United States Population's Response to Cyber Threats	29
CURRENT STATE OF CYBERSECURITY IN SINGAPORE	32
RECOMMENDATIONS	38
Strengthening Cyber Defense	39
Building Cyber Resilience	40
Leveraging International Cooperation	45
Developing Cyber Active Defense	46
CONCLUSION	49
APPENDIX A: DCID 1.1	52
NOTES	57
BIBLIOGRAPHY	64

List of Illustrations

	Page
Figure 1. Attitudes of Singaporeans Towards Cyber Threats.....	28
Figure 2. Awareness of Singaporeans Towards Cyber Threats.....	28
Figure 3. Attitudes of Americans Towards Cyber Threats	31
Figure 4. Original Logo for Total Defence.....	43
Figure 5. Proposed Logo for Total Defence	44
Figure 6. Proposed Symbol for Cyber Defence.....	44

List of Tables

	Page
Table 1. Cyber Conflict between Major Powers and Other States	22
Table 2. IBM's Statistical Package for the Social Sciences (SPSS) Analysis of Cyber Conflict for Target Type	23
Table 3. Chi-Square Tests for SPSS Analysis of Cyber Conflict for Target Type.....	24
Table 4. IBM's SPSS Analysis of Cyber Conflict for Cyber Objective.....	25
Table 5. Chi-Square Tests for SPSS Analysis of Cyber Conflict for Cyber Objective.....	26

Preface

This MMS examines the current state of cyber competition among the major powers (the United States, Russia, and China), analyses the implications for small states like Singapore, and develops recommendations for how Singapore can manage the risks and seize opportunities in the cyber domain. This study is especially timely and relevant, as the Ministry of Defence has recently established the Defence Cyber Organisation (DCO) in March 2017. The new DCO will take the lead for cyber defense within the military and work with the civilian Cyber Security Agency to contribute to national cyber response. This study will contribute to the discussion on how the DCO can develop itself to fulfil both missions. It will also provide a small state perspective on global developments in the cyber domains.

I would like to thank Dr. Benjamin Jensen and Dr. Brandon Valeriano for their valuable guidance and incisive comments which have helped to make this thesis better. I would also like to thank Ms. Andrea Hamlen at the Leadership Communication Skills Center for her help with the draft. Most of all, I would like to thank my wife, Claire, for her unfailing support and encouragement.

INTRODUCTION

“We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations.” – Summary of the 2018 National Defense Strategy of the United States of America.

Since the 1980s, the ever-expanding network of computers and servers around the globe, also known as cyberspace, has had a significant impact on our world. The US Department of Defense defines cyberspace as “a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.”¹ Cyberspace affects how people live, work and play. It has also become a virtual domain where states pursue their national interests, similar to how states compete and cooperate in the physical world. The indictment by special counsel Robert Mueller of Russian nationals and entities for meddling in the 2016 US presidential election is the fallout from an example of how two states, in this case Russia and the United States, have interacted in cyberspace.² Cyber-interference in the US presidential elections is but one of many state-level cyber operations that have occurred in recent times; other examples of such operations include Shamoon in 2012, the Sony Hack in 2014, and the Petya attacks against Ukraine in 2017.³

The cyber operations conducted by major powers such as the United States, Russia, and China often set a precedent which is subsequently adapted or emulated by other states, given the pressures inherent in the anarchic global system. As a result, it is expected that cyber threats will proliferate given the increasing use of cyber capabilities by major powers as well as other states. Analysis of the Dyadic Cyber Incident Database compiled by Valeriano, Maness and Jensen indicates that out of all the successful cyber incidents from 2000 to 2014, 68.2%, or about two

thirds of all incidents, involve small states. Of these incidents, 58%, or more than half of the cyber incidents are between a major power and a middle or smaller power, while the remainder are cyber incidents occur between two middle or smaller powers. This indicates that despite the attention that the media and researchers have placed on cyber conflict between the major powers, a majority of cyber conflicts actually involve states that are not major powers.

This paper intends to focus on cyber operations at the state-level, i.e. where the perpetrator is state or state-sponsored, and the target of the attacks in another state, in order to determine an effective strategy for Singapore to secure its interests in cyberspace. The paper is developed in four parts. Firstly, the current literature on cyber conflict among states is reviewed. Next, data on the outcomes of state-sponsored cyber operations is analyzed. Subsequently, the paper will examine the current state of cybersecurity in Singapore. Finally, recommendations for how Singapore can strengthen its cyber defense and resilience will be developed.

The recommendations will take into account the assumptions and limitations of the research, which are that this study takes a snapshot of the current publicly-known state of cyber conflict and does not account for how future technological advances such as quantum computing and cryptography will influence cyberwarfare. The study also focuses on broad cyber campaigns that are state-centric, while acknowledging that the majority of cyber operations target private organizations and individuals, and that even a cyber campaign that targets a state can be comprised of operations that target organizations and individuals within a state. The study is also necessarily limited by the availability of open source material, given that the close relationship with espionage means that many cyber operations remain classified. Despite these limitations, the proliferation of publicly known cyber operations around the world today, including Stuxnet, the Chinese cyber espionage campaign against the United States, and the aforementioned cyber

operations against the 2016 US Presidential elections, have generated a rich dataset to inform the study and to develop robust recommendations for Singapore.

Given current cyber threats, it is imperative that small states like Singapore increase their cyber capability in order to defend themselves in this new domain. In doing so, Singapore must strengthen the foundations of a proper defense through leveraging public-private partnerships, build cyber resilience, cooperate with regional and international partners, and develop cyber active defense capabilities.

LITERATURE REVIEW

“Just like we dropped bombs, we’re dropping cyber bombs.” – US Secretary of Defense Ashton Carter, Interview with NPR Radio, February 28, 2016.

This segment reviews the literature on cyberspace cooperation and competition. It examines the dominant trends in cyberspace, based on the actions of major powers, in order to determine the dynamics of cyber conflict today. This is because the actions of the major powers often set a precedent for behavior on the global stage that other states subsequently adapt or emulate. Specifically, the review looks at how the opportunities of cyber offense have been overhyped in public perception, and conversely, how states have taken a variety of measures to defend themselves in cyberspace. It then analyzes the response of smaller states such as Israel and Estonia in meeting their cyber challenges and examines the opportunities and challenges inherent in a more offensive (Israel) versus a more defensive (Estonia) approach. It also examines the influence of non-state actors such as information technology and cybersecurity companies in the cyber domain and finds that these non-state actors can be partnered with to strengthen the cyber capability of a state. The literature review concludes that competition and conflict in the cyber domain are extensions of state behavior in the real world, and that a strong cyber defense is achievable and a necessary pre-condition to securing state interests in cyberspace. With global commerce conducted in cyberspace estimated to reach US\$2.86 Trillion in 2018, and critical information infrastructures necessary to support financial, transport, and energy networks, cybersecurity is increasingly a vital national interest.⁴ The implications on cyber competition and cooperation for small states, and how small states can respond to this challenge, are identified as areas for further research.

The public conversation about competition and conflict in cyberspace is often dire, with public figures such as former US President Barack Obama declaring that the “cyber threat is one of the most serious economic and national security challenges we face as a nation.”⁵ Former US Secretary of Defense Leon Panetta has even warned of a “cyber Pearl Harbor.”⁶ Other commentators agree that cyber is a fundamentally new weapon and also a double-edged sword. On the one hand, it can be used against a country’s adversaries and achieve effects similar to, or exceeding that, of conventional weapons. The proponents of the promise of cyber weapons look to examples such as Stuxnet against Iran and the online campaign against ISIS to prove their point that cyber provides the ability for a nation state to bypass geographical and physical boundaries. Stuxnet temporarily retarded the ability of Iran to develop its nuclear deterrent by disrupting the nuclear centrifuges used to purify uranium for a nuclear weapon.⁷ Proponents argue that these efforts, together with diplomatic and economic pressure, were successful in convincing Iran to accede to the Joint Comprehensive Point of Agreement (JCPOA), freezing the Iranian nuclear program for the next decade.⁸ The cyber campaign against ISIS was also publicized as an attack on “the ability of someone sitting in Raqqa to command and control ISIL [ISIS] forces outside of Raqqa, or to talk to Mosul, or even to talk to someone in Paris or to the United States.”⁹

Conversely, there is also significant fear about the threat of cyberattack disrupting institutions and infrastructure within a country. The US Government has had concerns about Chinese cyber espionage efforts against the United States since 2003, when the first major cyber espionage campaign, code named “Titan Rain”, was discovered.¹⁰ Over the years, other Chinese cyber operations such as “Night Dragon”, “Aurora”, and “Moonlight Maze” have been publicly attributed. Russia is widely seen to be behind the efforts to disrupt elections in the US via the

proliferation of fake news via social media sites using bot networks, the exposure of politically sensitive information from hacked email accounts, and the attacks on state voter rolls .¹¹ The compromise of the Democratic National Committee's (DNC) email servers in the run-up to the US Presidential Elections in 2016, and subsequent release of sensitive information, resulted in the resignation of the DNC Chair, CEO, CFO and Communications Director before the Democratic National Convention.¹² An investigation is also ongoing into the use of Facebook by actors associated with the Russian government to deliver targeted messages to influence US voters during the election itself, with 126 million Facebook users in the United States being exposed to these messages.¹³

However, the poorly understood nature of the internet and cyberspace lends itself to misunderstanding and fear-mongering. As Eric Schmidt, one of the founders of Google, stated: "The Internet is among the few things humans have built that they don't truly understand," and calls it: "the largest experiment involving anarchy in history."¹⁴ The reality of cyber competition between states is more mundane despite the dire reports commonly found in the media.¹⁵ A proper examination of the behavior of states in cyberspace thus far is required to better understand the character of cyber conflict.¹⁶

Major Power Behavior in Cyberspace

When examining major power behavior in cyberspace, Valeriano, Maness, and Jensen find that rival states use cyber operations as a means of influencing their adversaries.¹⁷ The activities of the major powers, the United States, Russia, and China, in cyberspace can be broadly classified as disruption, espionage and degradation.¹⁸ Cybersecurity researcher Erik Gartzke finds that while degradation is more effective at influencing the behavior of a target group, the high risk of attribution, retaliatory action, and other unintended consequences limit

these activities.¹⁹ Conversely, disruption and espionage activities are conducted frequently but usually are not useful as a means of coercion. Overall, cyber activities must be used as part of a larger campaign that combines other instruments of power (such as in the activities against the Iranian nuclear program) in order to achieve the intended effects. Cyber operations are an attractive option to major powers, as well as small states and non-state actors. Different actors exploit different characteristics of cyberspace. Rival states utilize cyber operations as a means of compellence (a term used by Thomas Schelling) while managing the risk of escalation.²⁰ This is possible due to the difficulties associated with attribution of cyber operations in a timely manner. Less powerful groups such as terrorists leverage the ubiquity and access of the internet to leapfrog borders and influence the target audience directly for recruitment and to coordinate attacks.²¹

Disruption is the use of cyber operations as a means of information operations to interfere with the institutions of a target group. Since the early 2000s, Russia has been particularly active in using cyber operations as a means of disruption and political coercion against states in its near abroad. In response to the removal of a bronze statue of a Soviet soldier in Tallinn, Estonia, Estonia's government and commercial servers were hit by a series of massive DDoS attacks from tens of thousands of botnet computers and knocked offline.²² These attacks were routed through multiple intermediaries which prevented cyber experts from NATO from definitively proving the source of the attacks. Russian "patriotic hackers" also spread pro-Russian propaganda during its invasion of Georgia in 2008 and its annexation of Crimea in 2014.²³ In the 2008 invasion of Georgia, Russia employed DDoS attacks to isolate the Georgian population from the government and from the rest of the world. Georgia's banking system, government servers, and mobile networks were all taken offline during the invasion, effectively cutting off the nation from the

outside world. Faced with overwhelming military and cyber force, the Georgian government was forced to allow the annexation of South Ossetia and Abkhazia into Russia, and allow the deployment of Russian forces in a buffer zone.²⁴ The use of “patriotic hackers” and other actors such as the Russian Business Network, a criminal hacking gang, allows the Russian government to leverage on the capabilities non-state actors in support of its national goals. The Russian Business Network (RBN), a cybercrime organization, conducts cyberattacks at the direction of the Russian government in exchange for safe haven in Russia.²⁵ The Russian government does not need to pay for its upkeep or training, as its criminal activities fund its operations to the tune of USD 150 million a year.²⁶ Yet, when called upon, RBN hackers can use their skills, honed by cybercrime, to hack into domestic and international targets of the Russian government. Cyber operations such as Russian data breaches and disinformation campaigns represent a modern form of political warfare as described by George Kennan in 1948.²⁷ A critical analysis of significant cyber incidents in the past decade by academics Brandon Valeriano and Ryan Maness has also shown that the use of cyber operations is “part of a larger function of active foreign policy disputes between states,” used because they are “quick, easy, and can affect the rival’s populace.”²⁸

The utility of cyber operations for espionage purposes has been recognized by many states. In some ways, it can be seen as an extension of SIGINT capabilities that were developed with the proliferation in the use of radio at the turn of the 20th Century.²⁹ This is seen in the history of many organizations which are today associated with cyber operations such as the National Security Agency in the US and Government Communications HQ in the UK. However, the internet revolution has made the exfiltration and analysis of enormous volumes of data a possibility – what took months or years to obtain in the 20th century can now be lost in an instant

in the 21st century, as seen in the recent data breaches in the US resulting in the loss of sensitive information from the NSA.³⁰ Cyber espionage can be targeted at commercial entities as well. In the 1970s, Soviet agents were tasked with commercial espionage against US companies.³¹ In a similar vein, China has been active in conducting cyber commercial espionage in the 21st century, with 5 military officers being indicted by the FBI for the theft of commercial secrets.³² This commercial espionage by China has allowed their companies to improve the Chinese industrial technology base, generating economic advantages.³³ In the area of national security, the success of Chinese hackers in gathering data related to the US F-22 and F-35 stealth fighter programs has allowed them to accelerate their fielding of the J-20 and JF-31 stealth fighters.³⁴ This espionage campaign, codenamed “Titan Rain”, is directed at both the US government and defense contractors such as Raytheon, Lockheed Martin, Boeing and Northrup Grumman, and resulted in the loss of up to 20 terabytes of data.³⁵

While China has not overtly used cyber capabilities for military operations, it has progressively taken steps to build a cyber capability within the People’s Liberation Army (PLA). In response to the 1991 Gulf War, a variety of strategies were developed to enable the PLA to defeat a technologically superior opponent. *Unrestricted Warfare*, a think-piece written by two Chinese colonels, Qiao Liang and Wang Xiangsui, proposed the use of cyber means as an asymmetric capability to overcome the conventional military advantage of the United States.³⁶ Since the publication of that document in 1999, the PLA has grown its cyber capabilities in units such as Unit 61398.³⁷ Doctrines for the use of cyber capabilities have also been incorporated into the PLA textbook *The Science of Military Strategy*, whose authors state that “informationized [sic] warfare seeks to achieve strategic goals through information control and information attack, including conducting soft sabotage or hard destruction of the infrastructure, basic information

sources, or battlefield information systems.”³⁸ China’s first white paper on military strategy in 2015 publicly stated that China’s armed forces would “aim at building an informationized [sic] military and winning informationized wars.”³⁹ The establishment of the Strategic Support Force in 2016 brought together cyber espionage and information warfare units into a single service, indicating that the Chinese military has begun to revamp its force structure to realize these doctrinal developments.⁴⁰

These developments by the PLA are a synthesis of Chinese strategic thought, such as Mao’s idea of People’s War, with the emerging technologies first pioneered by the US military. Shen Weiguang, an architect of Chinese cyber policy, wrote that networks across society can be mobilized to wage information warfare on behalf of the nation.⁴¹ Shen saw that modern connectivity would increase the potential to mobilize citizens and businesses and create new attack surfaces for cyber campaigns to influence and adversary over time.⁴² This was in line with classical Chinese concepts of attacking *Shih*, the source of strength of the adversary.⁴³ Through these attacks, China would be able to “defend [its] legitimate interests without resorting to actual hostilities,” and win without fighting.⁴⁴ From this perspective, China is using its cyber capabilities as part of a broader strategy to achieve its national interests while limiting strategic escalation.

Degradation is the use of cyber means to attack physical or network infrastructure. Russia has actively used cyber operations in support of military operations in Ukraine during the annexation of Crimea.⁴⁵ Aside from Russia, the United States has also used cyber operations as a means of achieving military aims. Valeriano, Maness, and Jensen describe the United States as having established a “Cyber Reconnaissance-Strike Complex”, which relies on espionage operations, including counter-intelligence, to gather critical information that allows the United

States to develop cyber weapons that can degrade the capabilities of strategic rivals in the digital domain.⁴⁶ In 2010, Kaspersky Labs uncovered a computer virus, codenamed Stuxnet, which specifically targeted the uranium enrichment centrifuges at the Natanz nuclear site in Iran. This virus rewrote the control software to change the frequency of centrifuge speeds, causing the centrifuges to self-destruct, disrupting and delaying the Iranian nuclear program.⁴⁷ Separately, the US Department of Defense has conducted a cyber offensive against the Islamic State in Iraq and Syria (ISIS) since 2016, in conjunction with its military campaign to defeat the terrorist group. This cyber offensive aimed to disrupt ISIS's command and control by limiting their ability to communicate with each other and conduct operations. However, while these operations by the United States are narrowly targeted, they can also lead to unintended proliferation of cyber weapons. For example, the Stuxnet virus used against the Iranian nuclear centrifuges ended up spreading to 155 countries.⁴⁸ Iran was also able to learn from the Stuxnet virus used against it and develop Shamoon, a computer virus targeted against the computer network of Saudi Arabia's national oil and gas firm, Saudi Aramco, successfully infecting 30,000 of Saudi Aramco's computers.⁴⁹

The United States' development of cyber weapons in support of its "Cyber Reconnaissance-Strike Complex" can also contribute to cyber weapons proliferation in another way. In August 2016, a hacker group called the "Shadow Brokers" announced that it had successfully hacked the US National Security Agency (NSA), and released a cache of hacking tools purportedly used by the NSA.⁵⁰ This announcement was used to create publicity for an auction for another cache of cyber weapons that the Shadow Brokers had stolen from the NSA. While the auction was unsuccessful, the hacking tools in the original release included zero-day exploits for Microsoft Windows, Huawei, and Cisco.⁵¹ Some of the exploits were used by other

hacker groups to breach firewalls, switches and routers made by Cisco Systems less than a month after the Shadow Brokers released them.⁵² These examples of cyber weapons proliferation as a result of the United States' development of its cyber capability demonstrate the ease and speed at which the cyber weapons developed by the major powers can be "democratized" and made available on the open market.⁵³

The proliferation of these advanced cyber weapons from the major powers creates an impetus for all other states to increase their investment in cyber defense in order to be able to defend themselves against these weapons. This is because even if a particular state is not the original intended target of a specific cyber weapon, a malicious actor could easily acquire the cyber weapon once it has been released in the "wild" to attack the state. The 2017 WannaCry ransomware is one example of such an attack. The hacking tools stolen by the "Shadow Brokers" and posted in the public domain were used by hackers to execute a global cyber operation that spread to more than 74 countries.⁵⁴ The cyberattack severely degraded the United Kingdom's public health system, affected computers at Russia's Interior Ministry, and affected corporate computer systems in many other countries including Spain's Telefónica.⁵⁵ Continuing investment in cyber weapons by the major powers and other states will increase the risk of cyber weapons proliferation, thus increasing the impetus for all other states to invest in stronger cyber defenses.

The Development of Cyber Capabilities by Small States

Having examined the behavior of major powers in cyberspace, the literature review now examines how smaller states such as Estonia and Israel have responded to the cyber threat. Both Estonia and Israel are chosen as examples that can inform how Singapore should develop its cyber capabilities, as both countries are small and technologically advanced countries, with high

internet penetration rates and an educated populace. The similarities in country and population characteristics has led Singapore to model many of its conventional defense policies after Israel ever since Singapore's independence in 1965. Increasingly, Estonia is another model for Singapore to learn from, especially since Estonia has embraced all aspects of the internet, having implemented e-government, with all government services, including voting in national elections, being accessible online.⁵⁶ These initiatives are in line with how Singapore is developing its Smart Nation initiative, which aims to make Singapore "a nation where people live meaningful and fulfilled lives, enabled seamlessly by technology."⁵⁷ However, the convenience created by e-government in Estonia has also generated security risks, which were targeted in 2007. The removal of a Soviet-era military statue resulted in political street riots, while well-coordinated botnet attacks paralyzed government, media and financial sites and effectively cut the country off from the rest of the world.⁵⁸

In the aftermath of these attacks, Estonia has also made its e-government system more resilient by establishing a "data embassy," locating digital backups of critical government information in another country using cloud computing in order to ensure that Estonia's e-government systems remain running even if the IT infrastructure of Estonia comes under cyberattack.⁵⁹ The first such data embassy is set to open in Luxembourg in 2018.⁶⁰ Estonia has also strengthened its alliance structures in cyberspace, by establishing the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Founded with the contributions of Estonia and six other NATO countries in 2007, it has since expanded to include contributions from 19 of the 28 NATO countries, including the US.⁶¹ The NATO CCDCOE was established to accumulate, create and disseminate information about cyber operations in order to strengthen the cooperative cyber defense of NATO members and partners.⁶²

In addition to increasing cyber resilience and strengthening defensive alliances, Estonia has invested in establishing a cyber defense unit of volunteers, the *Küberkaitse Üksus*, which taps on the pool of civilian IT professionals to defend against cyber operations on the state and private telecommunications infrastructure of Estonia.⁶³ Since its formation, the cyber defense unit's role in national cyber defense has been formally recognized in Estonia's National Security Strategy, as well as its National Defence Development Plan 2013-2022.⁶⁴ The unit has also been integrated into the national defense system, which provides it with a legal framework for structure, management, membership and function as part of the EDF.

In contrast with the more defensive approach by Estonia, Israel has decided to emphasize the development of offensive cyber capability to support its national security objectives. In doing so, it has taken a route that mirrors the US, by building cyber capabilities within Unit 8200, traditionally a SIGINT unit.⁶⁵ Unit 8200 is said to comprise several thousand cyber warriors and is the equivalent of the US National Security Agency.⁶⁶ However, unlike the NSA, it is part of the Israeli military and not a civilian agency. Israel is also unique in leveraging its system of conscription in order to source for skilled cyber personnel. Under the *Talpiot*, *Gvachim*, and *Magshimim* programs, Unit 8200 works with high schools in Israel to identify students who are gifted in math and science and provide these students with enrichment classes in computer programming and cybersecurity.⁶⁷ Upon graduation, these students are put through a stringent selection process and the best are conscripted to Unit 8200. After serving their conscription, many Unit 8200 alumni are highly sought after by cybersecurity companies in Israel and are able to find lucrative jobs.⁶⁸ Because of this, entry into Unit 8200 is highly competitive, which ensures that the best and brightest of Israel's youngsters are deployed as cyber operators. The success of Israel's cyber talent pipeline can be seen in the results that Israel's cyber offensive

capability has achieved. While Israel has never officially confirmed its use of offensive cyber, it is widely thought to have contributed to the series of cyber operations against the Iranian nuclear program, as well as utilized cyber means to shut down Syria's anti-aircraft radars so that Israel's Air Force could fly undetected to destroy a suspected Syrian nuclear site in 2007.⁶⁹

The Evolving Characteristics of Cyberspace

Having examined the behavior of major powers and small states in cyberspace, the review goes on to examine the key differences between cyber power, which is virtual, and the other forms of physical military power such as land, sea, air and space. The internet is an amalgam of separate semiautonomous networks owned by private companies, known as Tier 1 Internet Service Providers (ISPs).⁷⁰ Each of these ISPs is an independent entity with its own policies, services, and customer targets. The binding element of the global internet is that networks share a common framework that allows them to connect to each other. Seen in this light, then, the internet can be understood not as a global commons, but as a domain significantly influenced by both private companies and states.⁷¹ This is unlike the domains of land, air, sea or space. In the cyber domain, states do not have a monopoly on power. Private companies have developed their own cyber capabilities for both defense and offense, a reality that has most recently been recognized by the US government's Active Cyber Defense Certainty (ACDC) Act which allows companies to take active measures to hack back against an attacker to identify them and find and destroy stolen information.⁷²

Increasingly, IT and cybersecurity companies have become significant stakeholders of the internet. They monitor much of the traffic on the internet for computer viruses and cyber operations and build their business models on providing intelligence on these attacks and defending their clients in cyberspace.⁷³ Another set of actors in cyberspace, who operate mainly

on the Darkweb, are cyber weapons dealers, third-party vendors who are able to provide baseline cyber offense capabilities that are commonly used – DDoS, phishing etc.⁷⁴ While they operate in an opaque black market, states have purchased their products for use in order to strengthen their cyber capabilities and reduce the costs and signature of investing in a significant cyber offense capability.

Because of these factors, many cyber capabilities are being developed for commercial motives, and led technologically by a global industrial pull. As a result, cyber power is accessible to all countries and can be developed in tandem with the civilian IT sector. This provides an ability to project power virtually anywhere, a capability heretofore only available to states with significant military resources. Conversely, the effects of cyberwar can be more uncertain than in the physical world. Computer viruses can inadvertently spread beyond their intended target, such as the Conficker worm in 2008, which infected millions of computers around the world and forced the French military to ground their aircraft.⁷⁵

Rather than posing a challenge, the unique characteristics of cyberspace, which include commercially-led technology development, privatized infrastructure, and powerful non-state actors, provide opportunities for small states to leverage public-private partnerships to increase its cyber capability without investing similar amounts of resources as compared to the major powers. By exploiting these opportunities, Singapore would be able to leapfrog forward in its cyber capability development and tap on global expertise in cyberspace to accelerate the growth of its own cyber talent pipeline.

Way Ahead

Having examined the literature, it is clear that all states will need to develop some form of cyber capability in order to secure their interests in an increasingly interconnected world.

Most major powers have openly disclosed their possession of offensive cyber capability, and there is increasing progress in the establishment of international laws and norms for cyberspace. However, there is limited research into how small states should build up their cyber capabilities. This is one area that is particularly pertinent for small and technologically advanced states like Singapore, which have limited resources for investment into the development of cyber capability. Estonia's approach can be broadly described as deterrence by denial, a more defensive approach that taps on strengthening the resilience of its cyber systems, increasing alliance support, and establishing cyber defense units. Conversely, Israel's approach is to build up strong offensive cyber capabilities in order to support broader national security objectives. One similarity between both countries is that they tap on the broader pool of cyber talent within society, either through a volunteer league (Estonia) or conscription (Israel) in order to maximize their ability to build their cyber capability. This is one measure that small states such as Singapore can adopt. In the development of cyber capability though, further research is required to determine if defense, offense, or a hybrid of both, would be the most appropriate for other small states. Furthermore, given the unique nature of cyberspace as being made up of semi-autonomous networks owned by private companies, and the strong incentives that commercial companies have to strengthen their cyber defenses, there is a need to explore how small states with limited resources can leverage the private sector in the cyber domain.

METHODOLOGY

The literature review provides the case studies of Israel and Estonia as two other small states that have adopted distinct cyber strategies. However, the best approach for Singapore would involve integrating different elements from the Israeli and Estonian strategies into a new approach adapted for Singapore's unique circumstances. To guide the selection of useful elements, additional data from various sources are analyzed to determine the implications of increasing cyber conflict in order to inform Singapore's cyber strategy. The primary research question to be answered is: "What is an effective strategy for Singapore to secure its interests in cyberspace?" This research question can be broken down into the follow three sub-questions:

1. What is the character of the cyber threat facing small states such as Singapore?
2. What are the current cybersecurity concerns of the Singaporean population?
3. How does a population (using the United States as an example) react to cyber threats?

To answer the first sub-question, the Dyadic Cyber Incident Dataset (DCID) 1.1 from Valeriano, Maness, and Jensen, which consists of 192 publicly reported cyber incidents between rival states for the years 2000-2014, is classified into cyber operations conducted by the major powers (United States, Russia, and China) versus cyber operations conducted by other states in order to determine the amplitude of the cyber threat against small states, versus that of the major powers.⁷⁶ The success rate of these cyber operations is further analyzed to determine if such cyber operations are successful in achieving compellence, which is the ability to influence another state to act according to the wishes of the perpetrator state. Achievable compellence supports the idea that cyber operations can be used by smaller states as a means of pursuing their

national interests, whereas if compellence is not possible, a more defensive cyber strategy should be pursued in order to prevent disruption to the economy and the daily lives of the population of a state. A second-level statistical analysis is then conducted using IBM's Statistical Package for the Social Sciences (SPSS), in order to determine 1) whether there is a significant difference in the types of cyber networks targeted for small states versus the major powers; and 2) whether there is a significant difference in the objectives of cyber operations conducted against small states versus that of the major powers.

To answer the second sub-question, public surveys conducted by the Singapore Cyber Security Agency are used to help contextualize the findings from the Pew Survey to Singapore. While Singapore has thus far not encountered a large-scale cyberattack against Critical Information Infrastructure, these kinds of attacks in other countries such as the United States and Ukraine have been reported in the media. These preexisting attitudes among Singaporeans will help to determine the available "maneuver space" of the Singapore government as it works to further strengthen Singapore's cyber defenses.

To answer the third sub-question, a survey conducted by Pew into the attitudes of Americans towards cybersecurity is used to provide a snapshot of the reaction of a population towards cyber threats. This survey is useful because Singapore has not yet been the target of cyber campaigns to the extent that the United States has been. The United States was selected as a reference country because the population profile of the United States, which includes a majority of middle class, educated people, matches that of Singapore. This survey is particularly useful because incidents such as the 2014 Sony Hack, 2015 Office of Personnel Management cyber breach, as well as the 2016 cyber operations against the US presidential elections have been extensively covered by the US media, ensuring broad public awareness of the cyber

operations. The Pew Survey is further augmented by the cyber conflict survey conducted by the author, which utilizes Amazon Mechanical Turk in order to determine the attitudes of the US population towards who should be responsible for cybersecurity, public acceptance of the conduct of “hack-backs” or cyber counterattack, and what determines cyber power.

DATA ANALYSIS AND FINDINGS

Character of Cyber Threats Facing Small States

The Dyadic Cyber Incident Dataset (DCID) 1.1 from Valeriano, Maness, and Jensen compiles 192 publicly reported cyber incidents between dyadic rival states for the years 2000-2014.⁷⁷ It is focused on cyber interactions between pairs of states, including targets within each state such as national security contractors, media organizations, and other relevant corporations such as banks, technology companies (Google, Apple), and utility companies, in order to sharpen the process of data construction, since interactions with other non-state actors such as criminal organizations, hacker collectives, and individual hacktivists would require different data collection strategies and theories. All of these incidents can be seen as successful cyber operations; that is, the attackers were able to gain access to the target system in order to carry out disruption, espionage, and/or degradation. In addition to this first level of success, Valeriano, Maness, and Jensen also analyze whether the cyber operations were successful in achieving compellence, a higher-level criterion of success which is the ability to influence the target state to carry out behavior that it would otherwise not have done.

Table 1 displays an analysis of the Dyadic Cyber Incident Dataset from Valeriano, Maness, and Jensen, which classifies the set of incidents by whether they involve interactions between major cyber powers (United States, Russia, and China); between a major power and other states, which can be either middle powers (e.g. India, Japan) or small powers (e.g. Israel, Italy); and between other states. Out of all the incidents captured in the dataset, 68.2%, or about two-thirds of all incidents, involve small states. Of these incidents, 58%, or more than half of the cyber incidents are between a major power and a middle or smaller power, while the remainder are cyber incidents between two middle or smaller powers. This indicates that despite the

attention that the media and researchers have placed on cyber conflict between the major powers, a majority of cyber conflicts actually involve states that are not major powers. The cyber operations in these incidents all met the first level criteria of success, which reinforces the need for all states to strengthen their cyber defenses in order to prevent the loss of information through espionage, or face disruption and degradation to their critical information infrastructures.

Applying the second level criteria of success though, the analysis finds that while the cyber operations are successful, they rarely achieve the intent of compelling the target state. This suggests that despite the literature on the supposedly devastating effects of cyber weapons, the utility of offensive cyber capability for compellence is limited, and that states should instead focus their efforts and resources on cyber defense rather than cyber offense capabilities.

Table 1: Cyber Conflict between Major Powers and Other States

Parties Involved	Number of incidents	% of Total	Incidents of Successful compellence	% Success rate
Major Power vs Major Power	61	31.8	7	11.5
Major Power vs Other States	76	39.6	2	2.6
Other States v Other States	55	28.6	2	3.6
Total	192	100	11	5.7

Source: Analysis by author based on Dyadic Cyber Incident Database 1.1 from Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen. (Appendix A)

In order to further characterize the cyber threat facing small states, a statistical analysis of the type of target networks and cyber objectives for the different categories of cyber operations is conducted. Tables 2 and 3 show the result of the statistical analysis for target type and show that regardless of the parties involved in the cyber operation, the relative proportion of cyber

operations conducted against the different types of networks tend to be the same. Regardless of the target state, civilian, government, and military and intelligence networks will all be targeted. An implication of this finding is that any effort to improve the cyber defenses of the state must be comprehensive across the different types of networks, and that the government or military cannot just focus on defending their specific networks. At the same time, because both civilian and government networks are targeted, there would be an increased incentive for the private sector to work closely with the government through different forms of public-private partnerships in order to protect the collective interests of the private sector and the government in cyberspace.

Table 2: IBM's Statistical Package for the Social Sciences (SPSS) Analysis of Cyber Conflict for Target Type

Parties Involved	Outcomes	Target Type			Total
		Civilian Networks	Government Networks	Military and Intelligence Networks	
Major Power vs Major Power	Count	16 _a	32 _a	13 _a	61
	Expected Count	13.3	37.2	10.5	61.0
	Z-score	0.7	-0.8	0.8	
Major Power vs Other States	Count	17 _a	47 _a	12 _a	76
	Expected Count	16.6	46.3	13.1	76.0
	Z-score	0.1	0.1	-0.3	
Other States v Other States	Count	9 _a	38 _a	8 _a	55
	Expected Count	12.0	33.5	9.5	55.0
	Z-score	-0.9	0.8	-0.5	
Total	Count	42	117	33	192
	Expected Count	42.0	117.0	33.0	192.0

* Each subscript letter denotes a subset of Target Type categories whose column proportions do not differ significantly from each other at the 0.05 level.

Source: Analysis using SPSS based on Dyadic Cyber Incident Database 1.1 from Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen. (Appendix A)

Table 3: Chi-Square Tests for SPSS Analysis of Cyber Conflict for Target Type

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3.544*	4	0.471
Likelihood Ratio	3.568	4	0.468
Linear-by-Linear Association	0.065	1	0.798
N of Valid Cases	192		

*0 cells (0.0%) have expected count less than 5. The minimum expected count is 9.45.

Interaction type has no impact on target selection. The differences observed are not statistically significant.

Source: Analysis using SPSS based on Dyadic Cyber Incident Database 1.1 from Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen. (Appendix A)

Tables 4 and 5 show the result of the statistical analysis for cyber objectives across the different dyads of cyber conflict. The analysis shows that whereas cyber conflict between two major powers shows a higher than expected incidence of short-term espionage, and a lower than expected incidence of disruption, the converse is true for cyber conflict between other states, where there is an increased incidence of disruption and a lower incidence of short term espionage. Further research will be required to determine the causes of these differences, as well as whether the difference is due to the limited availability of information about espionage campaigns for the non-major powers. However, some possible implications of this finding can be drawn out. For small states, the increased incidence of disruption events rather than short term espionage could mean that public-facing networks and websites are the main target of cyber operations. The effects of these disruptions could be aimed at shaking public confidence in the state's ability to defend itself in cyberspace. Thus, any effort to enhance cyber defenses must include elements of public outreach, and not just focus on strengthening network resilience. This finding also implies that for small states, there would be fewer barriers to collaboration between

the government and the private sector for cyber defense against attacks on public-facing networks. This is because the information contained on such networks would be less sensitive. In contrast, networks which are the target of espionage usually contain more sensitive information, and a government would be more reluctant to partner with the private sector for the defense of such networks as it could unnecessarily expose sensitive information.

Table 4: IBM's SPSS Analysis of Cyber Conflict for Cyber Objective

Parties Involved	Outcomes	Cyber Objective				Total
		Disruption	Short-Term Espionage	Long-Term Espionage	Degradation	
Major Power vs Major Power	Count	10 _a	31 _b	12 _b	8 _{a,b}	61
	Expected Count	22.2	21.3	9.5	7.9	61.0
	Z-score	-2.6	2.1	0.8	0.0	
Major Power vs Other States	Count	27 _a	28 _a	10 _a	11 _a	76
	Expected Count	27.7	26.1	11.9	9.9	76.0
	Z-score	-0.1	0.3	-0.5	0.4	
Other States v Other States	Count	33 _a	8 _b	8 _{a,b}	6 _b	55
	Expected Count	20.1	19.2	8.6	7.2	55.0
	Z-score	2.9	-2.6	-0.2	-0.4	
Total	Count	70	67	30	25	192
	Expected Count	70.0	67.0	30.0	25.0	192.0

* Each subscript letter denotes a subset of Target Type categories whose column proportions do not differ significantly from each other at the 0.05 level.

Source: Analysis using SPSS based on Dyadic Cyber Incident Database 1.1 from Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen. (Appendix A)

Table 5: Chi-Square Tests for SPSS Analysis of Cyber Conflict for Cyber Objective

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	27.446*	6	0.000
Likelihood Ratio	29.104	6	0.000
Linear-by-Linear Association	7.786	1	0.005
N of Valid Cases	192		

*0 cells (0.0%) have expected count less than 5. The minimum expected count is 7.16.

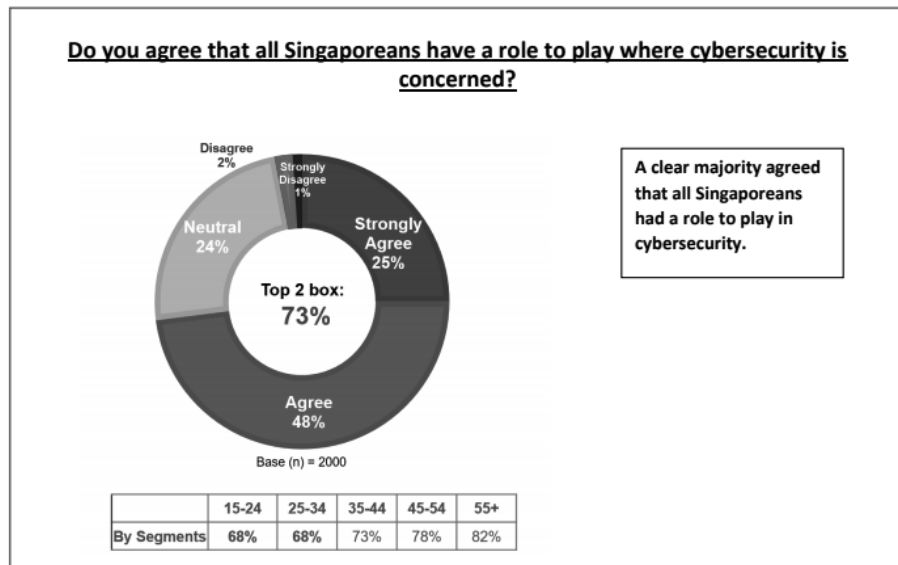
Interaction type does see significant differences across cyber objectives. Compare expected versus observed counts.

Source: Analysis using SPSS based on Dyadic Cyber Incident Database 1.1 from Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen. (Appendix A)

Singaporeans' Attitudes Towards Civilian Cyber Threats

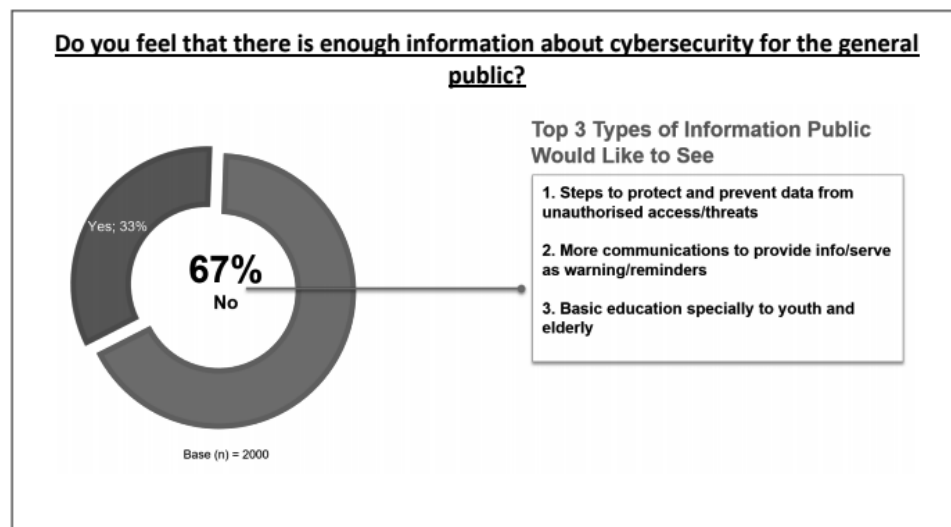
After determining the cyber threat for Singapore, this paper analyzes the survey responses of Singaporeans, who are still largely focused on non-state cyber threats. Figures 2 and 3 summarize the findings of an online survey by the Cyber Security Agency of Singapore (CSA). A total of 2,000 respondents aged 15 years and above were surveyed between July 2016 and August 2016.⁷⁸ While about 73 percent of respondents agreed that every individual has a role to play in cybersecurity (Figure 2), the majority of respondents also felt that they did not have sufficient information to protect themselves in cyberspace. However, the majority of Singaporeans were concerned with the impact of cyber operations on themselves, rather than cyber operations on public infrastructure, which could potentially have broader effects on the state. This points towards an increased need to raise public awareness about state-sponsored cyber threats among the Singaporean public. The process of creating this public awareness would also bring up a larger question about whether the Singaporean government would be responsible for protecting the digital presence of a citizen, in addition to their physical security.

Figure 1: Singaporeans' Role in Cybersecurity



Source: Cyber Security Agency of Singapore, “Cybersecurity Public Awareness Survey 2016 Key Findings,” *Cyber Security Agency Singapore*, February 15, 2017, https://www.csa.gov.sg/~media/csa/documents/key_findings/key%20findings-cybersecurity%20public%20awareness%20survey%202016.ashx?la=en.

Figure 2: Public Awareness About Cybersecurity



Source: Cyber Security Agency of Singapore, “Cybersecurity Public Awareness Survey 2016 Key Findings,” *Cyber Security Agency Singapore*, February 15, 2017, https://www.csa.gov.sg/~media/csa/documents/key_findings/key%20findings-cybersecurity%20public%20awareness%20survey%202016.ashx?la=en.

United States Population's Response to Cyber Threats

Following the analysis of the Singaporean population's attitudes towards cybersecurity, this paper examines the effects of state-sponsored cyber operations on a target population in order to inform the recommendations about the impact of such attacks on the public. In this respect, surveys by Pew of the American public's perception of the cyber threat are a useful means of determining the public response to cyber operations, given the prevalence of media attention given to cyber operations on the United States in recently years, particularly Russian interference in the 2016 U.S. Presidential elections.

As part of ongoing studies into the attitudes of Americans towards cybersecurity, Pew conducted a national survey of 1,040 adults in Spring 2016 to examine their cybersecurity habits and attitudes.⁷⁹ Extracts of the survey as summarized in Figure 3 show that many Americans expect that the coming five years will see significant cyber operations on the country's public infrastructure and financial systems. 70% of Americans expect that the United States will experience a significant cyberattack on its public infrastructure. A similar share expects that a significant cyberattack on the country's banking and financial systems will happen over the same time frame.

Although a majority of Americans think that significant cyber operations on public infrastructure and financial systems are likely in the next five years, they express mixed opinions about the extent to which the government and private industries are prepared to face these attacks. When it comes to the U.S. government's preparedness to handle these attacks, half of the Americans surveyed feel that the government is only somewhat prepared to prevent a cyberattack on public infrastructure or on U.S. government agencies themselves. At the same time, around one-in-ten Americans feel that the government is not at all prepared to handle a

major cyberattack on public infrastructure or on government agencies. The Americans surveyed feel the same way about private businesses' ability to defend themselves in cyberspace.

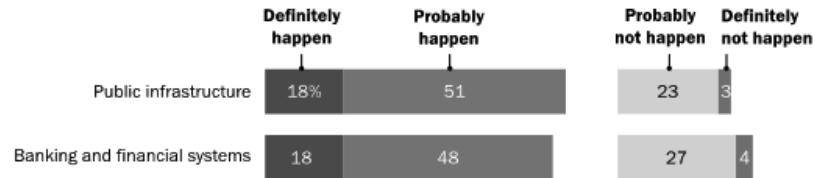
These findings show that in the aftermath of widely publicized cyber operations against America, the American people recognize the threat of cyberspace. However, more work is needed to convince the American people that the government and private business is able to defend against cyberthreats, despite the ongoing effort to strengthen US Cyber Command as well as ongoing legislation, such as the Active Cyber Defense (ACDC) Act, which will allow private businesses to hack back against cyber attackers.⁸⁰

In comparison with the survey on Singaporean attitudes towards cybersecurity, the Pew Survey finds that both Americans and Singaporeans are broadly aware of the cyber threat. However, while Americans are more exposed to the possibility of state-sponsored cyber operations, Singaporeans are still more focused on less damaging cyber operations conducted by hacktivists and hacker groups. Americans also have some confidence that the government is prepared to defend the United States against state-sponsored cyber threats, while such a concern has not yet entered the public discussion in Singapore. On the positive side, the recognition by Singaporeans that they have insufficient information about cybersecurity creates an opening for the Singapore government to provide this information through a coordinated public awareness campaign.

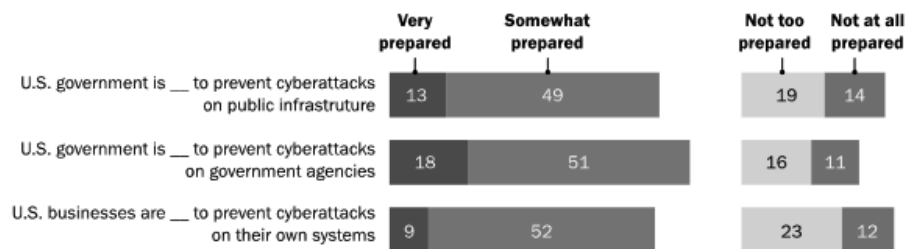
Figure 3: Attitudes of Americans towards Cyber Threats

Majority of Americans think major cyberattacks will happen in the next five years

% of U.S. adults who think a cyberattack on the following institutions will ____ in the next five years



% of U.S. adults who think the following institutions are ____ to prevent cyberattacks



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Source: Kenneth Olmstead and Aaron Smith, "Americans and Cybersecurity," *Pew Research Center*, January 26, 2017, <http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/>.

CURRENT STATE OF CYBERSECURITY IN SINGAPORE

Having reviewed the state of cyber conflict around the world today and the research findings regarding the prevalence of cyber threats for small states as well as perceptions about cybersecurity, it is timely to review the state of cybersecurity in Singapore before developing recommendations for further strengthening Singapore's position in this domain. In line with Singapore's position as a global center for trade, commerce, and finance, Singapore has always been open to new technologies and ideas from around the world. Today, Singapore is one of the most connected countries in the world, with an internet penetration rate of 82.5%.⁸¹ Going forward, Singapore will become increasingly connected as it embarks on its "Smart Nation" initiative. Launched in 2014, the initiative is meant to drive Singapore's continued social and economic development, with a vision of making Singapore "a nation where people live meaningful and fulfilled lives, enabled seamlessly by technology."⁸² Five key strategic national projects have been identified in order to achieve this vision: national digital identity, seamless e-Payments, Internet-of-Things Sensor Platform, autonomous urban mobility, and government services.⁸³ Concomitant with this initiative is an increased recognition of the vulnerabilities of cyberspace. As Singaporean Prime Minister Lee Hsien Loong said when launching the Smart Nation initiative, "[o]ne important aspect of a Smart Nation is cybersecurity. We are outing more and more functions and data into our computers, handphones, networks, and systems... It is vital that we have secure systems that we can trust."⁸⁴ These efforts at leveraging technology in Singapore parallel the experiences of Israel and Estonia. Like both countries, Singapore is building on its technological base and advanced workforce to seize new economic opportunities

in cyberspace. However, this also means that Singapore will become increasingly vulnerable to cyber threats.

In recognition of these vulnerabilities, Singapore launched its inaugural Cybersecurity Strategy in 2016 to guide its efforts to strengthen cyber defense. In launching the strategy, Prime Minister Lee Hsien Loong noted that “The Government cannot do it alone. Businesses are responsible for protecting customers’ personal data. Individuals need to practice good cyber hygiene to keep personal devices and data safe. If we each do our part to use our systems and devices responsibly, then collectively we can help to protect Singapore’s cyberspace.” Singapore’s Cybersecurity Strategy is underpinned by four pillars: building a resilient infrastructure, creating a safer cyberspace, developing a vibrant ecosystem, and strengthening international partnerships.⁸⁵ The first pillar is to strengthen the resilience of 15 Critical Information Infrastructure (CII) sectors to secure the digitally-enabled economy and society in Singapore by working with private sector operators and the cybersecurity community.⁸⁶ CII protection programs will be established to develop robust and systematic cyber risk management processes. Each CII sector will also develop response and recovery plans to cyber breaches, while cross-sector cybersecurity exercises will be conducted to test cooperation and address inter-dependent vulnerabilities. National cybersecurity resources such as the National Cyber Incident Response Team (NCIRT) and National Cyber Security Centre (NCSC) will be expanded and reinforced.⁸⁷ A Cybersecurity Bill has also been tabled in Parliament, which aims to enable the Government to better respond to cyber threats.⁸⁸

The Cyber Security Agency of Singapore (CSA) also aims to make cyberspace safer by mobilizing businesses and the community to counter cyber threats and protect personal data. The second pillar recognizes that cybersecurity is the collective responsibility of the Government,

businesses, individuals and the community. The CSA will work with global institutions, other governments, industry partners and Internet Service Providers to identify and reduce malicious traffic on the Internet, and work through business associations and the community to foster better understanding of cybersecurity issues and promote the adoption of good cybersecurity practices.

The third pillar of the cybersecurity strategy aims to develop a vibrant cybersecurity ecosystem and position Singapore as a center for cybersecurity innovation by leveraging Singapore's highly educated workforce, advanced infrastructure, technologically-advanced companies and strong global research collaborations. There is a need to grow the cybersecurity workforce and nurture local cybersecurity companies. The government has also identified opportunities for global cybersecurity companies to leverage Singapore's strengths as a financial and fintech hub.

In recognition that cybersecurity is a global issue, and cyber threats do not respect sovereign boundaries, the fourth pillar of the strategy is to strengthen international partnerships to foster collective global security. In particular, Singapore will work through international organizations such as ASEAN and the UN to address transnational cybersecurity issues. The government will also invest in cyber capacity building initiatives and facilitate exchanges on cyber norms and legislation.

Aside from the civilian cybersecurity strategy, Singapore is also investing in military cyber capabilities. The Ministry of Defence (MINDEF) established the Defence Cyber Organisation (DCO) in 2017 to oversee policies, capability development and implementation to monitor and defend MINDEF and the Singapore Armed Forces (SAF)'s networks 24/7 from cyber threats. The Minister of Defence, Dr. Ng Eng Hen, justified this additional investment during the Budget Debate in Singapore's parliament by stating that "The Next Gen SAF needs to

prepare for that environment where state-orchestrated cyber and information campaigns against another state are considered legitimate, and can be on-going all the time. The impact of that threat can have real and damaging physical consequences... The SAF must keep up with the tactics and operations of aggressors in the cyber realm, a never-ending game, as they do in conventional warfare.”⁸⁹ He went on to quote examples of recent cyber incidents such as the attack on Ukraine’s power grid and the hack on the Democratic National Committee during the run up to the US Presidential Elections.

Singapore recognizes that a passive cyber defense posture will not be sufficient to defend against all cyber threats. As such, the DCO is tasked to “proactively develop and implement solutions to protect our [defense] networks from cyber intrusions, monitor cyber defenses and networks 24/7 and coordinate response to cyber operations.”⁹⁰ The DCO is envisioned to have 2,600 personnel in the long run, including active and reserve components of the military.⁹¹ As the lead agency for cyber security operations for the defense sector, the DCO will be responsible for developing cyber strategies and policies, orchestrating capability development, and liaising with the Cyber Security Agency to support civilian authorities in the event of large-scale cyber incidents, should the need arise. Along with the establishment of the DCO, the Ministry of Defense has also created new schemes of service for national servicemen (conscripts) to serve as cyber defenders. These national servicemen will be trained to serve in three different roles: security operations center monitoring, incident response, and forensic investigation. A Memorandum of Understanding has also been signed with an education institute (Nanyang Polytechnic) and the private sector (Singapore Technologies Electronics (Info-Security) to develop a specialized, accelerated cyber security training curriculum for the training of national servicemen.⁹²

The civilian and military cybersecurity developments in Singapore parallel what has been done by Estonia and Israel thus far. In line with the governments in both countries, the Singapore government places great importance on cybersecurity, and is investing heavily in cybersecurity even as the country seeks to leverage technology for economic growth. The highly educated populace also provides a good base for the nurturing of cybersecurity talent, which can then be employed both in the civilian and military sectors.

Like Estonia, Singapore has begun to craft a “Whole-of-Nation” effort to cybersecurity which involves individuals, businesses and private organizations, and the government. The recently tabled Cybersecurity bill will also provide the CSA with greater latitude to govern cyber security in Singapore and ensure that critical sectors of the economy such as finance and transport are secured against high-end cyber threats. As the example of Estonia shows, however, encouraging voluntary cooperation of the private sector with the government should be the preferred approach to cybersecurity in these sectors, rather than relying solely on laws and regulation. Singapore has also started to engage its region in the area of collective and cooperative cyber security, and cyber capacity building and capability development. However, unlike Estonia, which can tap into the existing defense and security networks of NATO, the regional security architecture in South East Asia is not as well established. Singapore will need to explore how it can contribute to nurturing the nascent security architecture within ASEAN and promote the establishment of cooperative cybersecurity mechanisms.

In comparison with Israel, Singapore has similarly diverted some of its conscript military resource towards cybersecurity, which is a positive development. However, Israel’s cyber capability currently far outpaces Singapore’s, and Singapore must seek ways to accelerate its cyber capability development, especially because of the increasing proliferation of cyber

weapons from major powers, either through the employment of these weapons or through inadvertent loss. Singapore should also continue to seek synergies between the development of its civilian cyber industry and cyber capability development in the defense sector, just as how Israel's development of its cyber capabilities has created positive economic externalities, creating a local cybersecurity industry that generates US\$82 Billion a year and exports US\$ 6.5 Million worth of cybersecurity products.⁹³ In contrast with Israel, however, Singapore does not need a significant cyber offensive capability as it does not have to deal periodically with hostile neighboring states or non-state actors. As such, Singapore should take a more defensive cyber posture, in order to prevent the creation of a cyber arms race in the region which would work against the goals of fostering greater regional integration and cooperation in cybersecurity and other matters.

RECOMMENDATIONS

It is clear that the Singapore government is well aware of the potential threats in cyberspace and has the clear intent of strengthening its cyber defenses. Broad national goals for cybersecurity have also been set, and new organizations for cyber defense established. In answer to research sub-question 1 on the character of the cyber threat facing Singapore, analysis of the DCID 1.1 data shows that small states such as Singapore face the threat of cyberattack from both major powers as well as other states. All networks, ranging from civilian to government to military and intelligence networks, are at risk. To answer to such a threat, it would be more effective for small states to place more emphasis on defensive rather than offensive measures in cyberspace. Furthermore, the cyber threat facing Singapore is likely to have a greater emphasis on disruption of public facing networks, which enables the government to leverage public-partnerships to effectively defend Singapore's cyber networks, due to the lower sensitivity of information carried on those networks. The CSA data which was analyzed to answer research sub-question 2 on the current cybersecurity concerns of the Singaporean population shows that Singaporeans recognize the need for greater awareness about cyber threats. The Pew survey of Americans on cybersecurity was used to answer research sub-question 3, which asked how a sample population would respond to cyber threats. The analysis found that a comprehensive approach to cybersecurity that includes public outreach would be needed in order to ensure that the general public continued to support investment in cybersecurity.

The following portion of the paper proposes initiatives to achieve the cybersecurity goals and further strengthen Singapore's cyber defenses. Taking reference from the examples of Israel and Estonia, similar small states who have invested heavily in cyber, the initiatives are organized

according to the four themes of Strengthening Cyber Defense, Building Cyber Resilience, Leveraging International Cooperation, and Developing Cyber Active Defense.

Strengthening Cyber Defense

The ideas behind Estonia's establishment of the cyber defense league of volunteers can be adapted for both the civilian and military aspects of cyber defense in Singapore. On the civilian end, the CSA could establish a voluntary program to bring together cybersecurity professionals from the private sector to protect civilian CIIs. By broadening the pool of cybersecurity personnel who can be tapped on to defend CIIs during crisis, the CSA will be able to scale up its response to cyber operations when they occur, while ensuring that Singapore's limited pool of cybersecurity professionals can continue to hone their skills in the private sector, where innovation and the development of new cybersecurity techniques occurs much quicker than in the government. Networks of cyber security specialists proved to be especially effective in repelling the 2007 cyber operations against Estonia, in which information security experts from active companies and organizations worked together informally.⁹⁴ Taking into consideration the increasing risks of cyber operations, it is vital to ensure the sustainability of self-initiative and voluntary cooperation, and to establish a formal, organizational, and legal basis for the initiative. In order to attract more volunteers, while enhancing the skills of these professionals, volunteers who perform well could be sent to participate in international cybersecurity competitions and local and international training events. The volunteer program could also include an outreach and education component to engage youth in schools who have an interest in cybersecurity. Currently, many high schools and colleges in Singapore have computer science clubs, which can be an avenue to reach out to youth who may have the interest and aptitude for cybersecurity. In this way, the voluntary program will also help to grow the pool of

cybersecurity talent in the long term, which will benefit both the private sector and the government.

Within the military, the new initiative to train cyber warriors will take some time to grow the pool of cyber defenders. In order to quickly strengthen cyber defense, soldiers serving in other branches of the reserves, such as combat or combat support units, who have cybersecurity skills could be redeployed to serve within cybersecurity units in order to defend the military's networks. Tapping on military personnel for these roles will ensure that sensitive military networks are managed by personnel with the appropriate security clearances. The military should also formalize the linkages between military and civilian cybersecurity operations, given that many CII sectors, such as the energy and telecommunications grids, and transport networks, are dual-use systems which serve both civilian and military requirements. In the event of a significant crisis or attack on these CII, effective coordination between the military and CSA will be critical in managing recovery and response efforts. During daily operations, there will be a need for information sharing between the military and civilian cybersecurity agencies in order to generate a common cybersecurity situation picture and detect trends in cyber operations and intrusion attempts. This common understanding of the situation will be needed in order to determine the most appropriate means of responding to these daily attacks.

Building Cyber Resilience

Apart from strengthening cyber defense within Singapore to prevent attacks, there is also a need to build cyber resilience. Cyber resilience depends on two things, designing systems in a way that allows for graceful degradation during an attack being able to recover quickly once an attack has occurred. To achieve both graceful degradation and quick recovery, the government must work closely with the private sector in order to influence the design and implementation of

CII to include redundant systems. This will increase the costs of building such CII. While Singapore has had experience in building resilience into public infrastructure such as government housing and the mass-rail system, the additional costs associated with resiliency had always been borne by the government. This is not the case with some of the current CII sectors, and in new areas such as the Internet-of-Things, which will largely be built by the private sector. In ensuring CII resiliency, Government regulation alone could increase costs and render such projects non-commercially viable, which would hamper Singapore's drive to adopt more technology and become a Smart Nation. Government agencies might also not have the technical expertise to develop appropriate regulatory measures to keep up with rapidly advancing commercial technologies. As such, a strong public-private partnership would be needed in order to develop appropriate regulations, resilience measures, and cost-sharing arrangements for CII.

Rapid recovery after an attack could further be enhanced for CII by adopting Estonia's idea of establishing "data embassies". In line with ASEAN's drive to enhance regional cyber partnerships, an agreement could be reached with other ASEAN countries to co-host duplicate critical data and applications, so that in the event of an attack, the country under attack could rely on external databases from a regional partner to keep the country running. While additional security measures would be required to protect these external databases from the increased risk of espionage, the benefits of this approach could outweigh the costs, as duplicating the data would help to protect from cyber operations that aim to destroy or distort information. In order to implement this, an ASEAN e-government blockchain network could be established.⁹⁵ Using blockchain technology would provide the advantage of distributing the database in an encrypted manner, while allowing for easy verification and quick detection of any attempt to corrupt the database. Concerns about the scalability of existing blockchain algorithms are rapidly being

overcome through the development of new blockchain technologies and systems. In order to take advantage of this emerging technology, Singapore could pioneer the development of a test e-government network, in order to explore the feasibility of such a scheme. Going forward, adopting this approach to cyber resilience would improve cooperation between ASEAN countries, further supporting the goal of ASEAN integration.

Another aspect of building cyber resilience would involve public outreach and education to ensure that mass panic did not ensue in the aftermath of a cyberattack targeting public infrastructure. This is one area where Singapore's existing efforts to engage the general public in security and defense-related issues can be leveraged to create recognition and rapid adoption by the public. Singapore's Ministry of Defence has had a long-running "Total Defence" campaign which is aimed at involving every Singaporean in collective response to a crisis. Launched in 1984, Total Defence is described as containing five aspects: military defense, civil defense, economic defense, social defense, and psychological defense.⁹⁶ Military defense speaks to the need to maintain a strong Singapore Armed Forces to defend against security threats. Civil defense is about the need for all Singaporeans to be able to contribute their skills and resources should a natural disaster, such as large fires or floods, occur. Economic defense is about building up a robust economy that is resilient through economic crises or national emergencies. Social defense is about ensuring national unity. Psychological defense is about maintaining the trust that the people have in the country. These five aspects are often depicted as the five fingers on a hand, as seen in Figure 4.

Cybersecurity is an issue that cuts across all five aspects of Total Defence. For example, the Singapore Armed Forces depends heavily on citizen-soldiers for its combat power, and cyber operations on the electrical grid and transport networks could disrupt mobilization during times

of crisis. Cyber operations against financial institutions such as banks, the stock exchange, and the Monetary Authority of Singapore could degrade Singapore's economic defense. Using cyber means, information operations could be conducted to destroy the trust that Singaporeans have in each other and the government. Total Defence should be updated to better recognize the cross-cutting threat that cyber presents. One proposal would be to include Cyber Defence as the "palm" of the hand, as seen in Figure 4, in recognition that cyber defense affects all other forms of defense. A new symbol for cyber defense is also proposed in Figure 5, in order to promote public recognition of the cyber threat and to help with the branding of public outreach programs such as cyber education in schools. The computer and Wi-Fi symbol together represent the systems and the networks, while the outline of the group of people represents that end-users that are the key vulnerability, and the target audience for these outreach programs.

Figure 4: Original Logo for Total Defence.



Source: Ministry of Defence Singapore, "Total Defence Logo and Icons," *Ministry of Defence Singapore*, accessed February 17, 2018, https://www.mindef.gov.sg/oms/imindef/mindef_websites/topics/totaldefence/about_us/tdlogo_icons.html.

Figure 5: Proposed Logo for Total Defence.



Source: Created by author, adapted from Total Defence logo from MINDEF Singapore,

Figure 6: Proposed Symbol for Cyber Defence.



Source: Created by author

Leveraging International Cooperation

Singapore's efforts for cyber defense and cyber resilience should also be supported by increased cooperation at the ASEAN and international level. Within ASEAN, the establishment of a Cooperative Cyber Defense Center of Excellence (CCD COE), similar in concept to the NATO CCD COE in Estonia, would allow Singapore to better contribute to regional cyber capacity building efforts and enhance information-sharing and coordinated response. Locating the ASEAN CCD COE in Singapore would also build on the strong reputation of the country as being forward-thinking in the area of cybersecurity.⁹⁷ Similar to the NATO CCD COE, the ASEAN CCD COE would aim to be a hub of cyber defense expertise in the region, hosting technical cyber defense exercises and conferences; supporting cyber policy research, education, and training; and developing cyber doctrine for the region. Operationally, it could build up information-sharing and response protocols with individual National Cyber Incident Response Teams (NCIRTs) in order to enhance regional collective cyber defense. By tapping on cyber defense manpower from the entire region, the ASEAN CCDCOE would also be able to increase the capacity to respond to cyber operations beyond what each individual country would be capable of. The ASEAN CCD COE could also work as the regional link to the NATO CCD COE to facilitate international efforts at information sharing and establishing cyber norms.

To promote increased discussion of cybersecurity issues at the regional and international level, Singapore should also propose a Cybersecurity Forum to complement existing forums such as the ASEAN Regional Forum (ARF), East Asia Summit (EAS), and the ASEAN Defense Ministers Meeting (ADMM). The aim of this forum would be to establish a common ASEAN position and strengthen the influence of ASEAN countries on developments in cybersecurity. ASEAN member states have common interests in ensuring that cyberspace continues to support

economic growth, instead of becoming a domain for geopolitical competition. This forum would contribute to the goals of the ASEAN Political-Security Community (APSC) Blueprint, which was adopted in 2009 in order to create a robust political-security outline with ASEAN based on the principles and purposes of the ASEAN charter.⁹⁸ The ASEAN Cybersecurity Forum (ACF) would extend the aims of the APSC to the cyber domain, which include creating a rules-based community of shared values and norms; a cohesive, peaceful, stable and resilient region with a shared responsibility toward comprehensive security; and a dynamic and outward-looking region in an increasingly integrated and interdependent world.⁹⁹ The ACF would also provide a platform for ASEAN states to engage global powers, just as existing forums such as the ARF, EAS, and ADMM have done. By establishing this forum, ASEAN states would together be better able to shape the development of global cyber norms towards enhancing peace and stability in the cyber domain.

Developing Cyber Active Defense

In addition to the measures above, the Singapore government could also invest in developing cyber active defense capabilities. This would include penetration testing, threat hunting, and the ability to hack-back against cyber attackers. While these capabilities are similar to cyber offense, the aim of developing them is not to conduct cyber operations against the CII of other countries, but to broaden the options for responding to a cyberattack against Singapore. While the current research suggests that cyber offense does not contribute significantly to a state's success at compellence, the ability to hack-back would assist with the attribution of any cyber operations conducted against Singapore and support the employment of other instruments of national power, such as diplomatic, economic, or military measures, against the aggressor. Development of a cyber active defense capability would also allow Singapore to keep pace with

the latest developments in cybersecurity and support Singapore's effort to become a cybersecure Smart Nation.

Similar to building cyber resilience, any effort to build a cyber active defense capability would require close partnership between the Singapore government and the private sector. There are overlapping interests between the government and critical sectors, such as finance, in quickly attributing cyber operations and responding decisively in order to minimize the damage to investor confidence. At the same time, instead of investing in a dedicated cyber offense capability like Israel, which requires significant amount of manpower and resources, the Singapore government can leverage the capabilities developed by cybersecurity companies. Ongoing developments such as the Active Cyber Defense Certainty Act, a bipartisan bill introduced in the United States Congress, would allow private companies to hack-back against their attackers.¹⁰⁰ This bill, if passed, would incentivize greater private investment in hack-back capabilities by cybersecurity companies, a positive development which can be leveraged by Singapore. One of these companies is CrowdStrike, which has officially launched its Falcon platform.¹⁰¹ Falcon uses artificial intelligence and big data analytics in order to carry out cyber active defense operations including real-time detection of adversary activities, attribution of the threat actors, flexibility of response actions, and intelligence dissemination.¹⁰²

Apart from larger companies, companies such as Hacking Team provide more niche cyber active defense capabilities. Many countries around the world, including the United States, have purchased these niche capabilities to augment their overall approach to cyber capability development. For example, it has been reported that the FBI has spent \$775,000 on Remote Control Service eavesdropping software that can pull data from target computers.¹⁰³ Such software would be an essential part of enabling hack-back capabilities to attribute cyber

operations against Singapore back to the originators. This software was purchased from Hacking Team, an Italian company that develops offensive cyber capabilities for law enforcement and intelligence communities.¹⁰⁴ While the Hacking Team is only one of many such companies, it is the only company that has had its pricelist and capabilities publicly exposed, and this provides a reference point for the costs of such capabilities. The pricelist indicates that Hacking Team not only provides software packages, but also has a team of Field Application Engineers who can provide installation, training, assistance, and assessment services in order to ensure that their software is effectively employed. If the appropriate disclosure and security measures are taken, engaging companies such as Hacking Team could be an efficient way of quickly expanding Singapore's cyber active defense capabilities, and also training local cyber talents to take on increased roles in cyber active defense should the need arise.

CONCLUSION

Singapore's efforts to exploit the opportunities provided by cyberspace to enhance governance and develop the economy must be accompanied by increased investments in cybersecurity. Current research also indicates that 68.2%, more than two-thirds of publicly reported significant cyberattack incidents, involve small states. This provides additional impetus for Singapore to invest in cybersecurity. In defining the character of the cyber threat, analysis of the DCID 1.1 data set indicates that during a cyber operation, all networks across civilian, government, and the military will be targeted. For states other than the major powers, the goal of disruption seems to be a more significant impetus for cyber operations instead of espionage. Despite this threat, public surveys indicate that compared to the United States, the Singaporean public has limited awareness of the global cyber threat. These findings mean that any effort to strengthen cybersecurity in Singapore must involve growing public awareness of the cyber threat and enhancing the psychological resilience of the Singaporean public should attacks occur.

While there is a need to invest in cybersecurity, resources must be prioritized to maximize the effects of these investments. Research findings support the hypothesis that investing in cyber defense would have the greatest impact in securing cyberspace for Singapore, given that neither deterrence nor compellence would be achievable. As such, this paper recommends tangible initiatives under the four pillars of strengthening cyber defense, building cyber resilience, leveraging international cooperation, and developing active defense. These pillars aim to enhance the defense of CIIs, improve the resilience of networks and the people against the effects of a cyberattack, find strength in numbers by nurturing a stronger ASEAN community in cyber, and expand the ability to respond to any attacks.

The recommendations developed in this paper to strengthen Singapore's cybersecurity strategy will need to be periodically updated through further research and keeping up to date with the latest developments in the field. Currently, technological advances in cyberspace are occurring at a rapid pace, with tremendous investments by both governments and private industry into artificial intelligence and quantum computing, among other breakthrough technologies. These developments can either enhance or degrade the ability of a state to defend itself in cyberspace. For example, advances in quantum computing may render irrelevant many of the current encryption methods, while conversely, advances in quantum cryptography may allow for new ways of protecting data and infrastructure against cyber operations.

Apart from technical developments in the field, there is also a need to conduct further research into how state and non-state actors interact in cyberspace. The prevalence of stakeholders such as private companies and hacktivist groups mean that the action of any state in cyberspace will have wide-ranging effects that extend beyond the state. The response of private companies such as Sony to the hacks by North Korea, and Facebook and Twitter to the cyber operations against the 2016 US Presidential Elections, are beginning to establish norms of interaction between state and non-state actors in the cyber domain. Other developments such as the Active Cyber Defense Certainty Act currently being considered by the US Congress, which allows private companies to hack back against their attackers, will further change the dynamics of interaction.

Independent of further research, though, this study has found that focusing on enhancing Singapore's cyber defenses remains the most effective strategy to secure Singapore's national interests in the cyber domain. A strong cyber defense is needed to ensure that Singapore can continue to leverage advances in technology to grow its economy and improve the lives of its

people. Through smart investments in cyber defense, and keeping up to date with the latest developments, Singapore will be able to achieve its aim of being a secure Smart Nation.

APPENDIX 1

DYADIC CYBER INCIDENT DATASET 1.1

No.	Origin	Target	Type of Attack	Interaction Start	Interaction End	Actor 1	Actor 2	Type of Interaction			
								Major v Major	Major Other	v Other	v
1	US	Russia	Reign malware campaign	2/1/2008	3/1/2011	1	1	1	0	0	
2	US	Russia	QWERTY keystroke log	2/1/2008	3/11/2011	1	1	1	0	0	
3	US	Russia	Duke Series	4/8/2008	9/17/2015	1	1	1	0	0	
4	US	Russia	US govt employee in Georgia hacked	8/6/2008	8/12/2008	1	1	1	0	0	
5	US	Russia	CENTCOM\DOD (linked to APT 28)	10/1/2008	10/15/2008	1	1	1	0	0	
6	US	Russia	Buckshot Yankee	11/26/2008	11/28/2008	1	1	1	0	0	
7	US	Russia	Sandworm	1/1/2009	10/14/2014	1	1	1	0	0	
8	US	Russia	Power grid hacked, traced to Russia	8/24/2009	8/24/2009	1	1	1	0	0	
9	US	Russia	Energetic Bear/Dragonfly/Crouching Yeti	1/1/2011	7/1/2014	1	1	1	0	0	
10	US	Russia	Operation Pawn Storm	9/30/2013	10/22/2014	1	1	1	0	0	
11	US	Russia	CyberBerkut NATO Websites	3/15/2014	3/26/2014	1	1	1	0	0	
12	US	Russia	Operation Pawn Storm: military networks (fake OWA)	6/2/2014	2/1/2015	1	1	1	0	0	
13	US	Russia	Operation Pawn Storm: Nuclear power plants, newspapers	6/3/2014	12/1/2014	1	1	1	0	0	
14	US	Russia	US Banks hacked	6/4/2014	7/8/2014	1	1	1	0	0	
15	US	Russia	White House hack	10/26/2014	10/28/2014	1	1	1	0	0	
16	US	Russia	State Dept hack	11/15/2014	11/17/2014	1	1	1	0	0	
17	US	Iran	Stuxnet .5	11/1/2007	6/1/2010	1	0	0	1	0	
18	US	Iran	Snowglobe	4/2/2008	12/1/2011	1	0	0	1	0	
19	US	Iran	Stuxnet	6/1/2009	10/1/2010	1	0	0	1	0	
20	US	Iran	Flame	6/1/2009	12/2/2012	1	0	0	1	0	
21	US	Iran	Twitter Hack	12/18/2009	12/18/2009	1	0	0	1	0	
22	US	Iran	Iran network infiltration	3/14/2010	3/14/2010	1	0	0	1	0	
23	US	Iran	Comodo Hack	3/25/2011	3/27/2011	1	0	0	1	0	
24	US	Iran	Operation Newscaster	4/15/2011	5/26/2013	1	0	0	1	0	
25	US	Iran	Duqu	9/11/2011	12/1/2011	1	0	0	1	0	
26	US	Iran	Operation Ababil	12/28/2012	1/2/2013	1	0	0	1	0	
27	US	Iran	NMCI hack	9/23/2013	9/25/2013	1	0	0	1	0	
28	US	Iran	Saffron Rose	10/23/2013	3/15/2014	1	0	0	1	0	
29	US	Syria	Hama visit	7/9/2011	7/9/2011	1	0	0	1	0	
30	US	China	Hainan Island Incident	4/29/2001	5/1/2001	1	1	1	0	0	
31	US	China	Titan Rain	9/1/2003	4/1/2006	1	1	1	0	0	
32	US	China	Cisco Raider	2/28/2006	5/6/2010	1	1	1	0	0	
33	US	China	State Dept theft	5/28/2006	7/7/2006	1	1	1	0	0	

34	US	China	Shady RAT	8/1/2006	1/1/2010	1	1	1	0	0
35	US	China	Fred Wolf espionage	8/1/2006	8/1/2006	1	1	1	0	0
36	US	China	Commerce disable	10/1/2006	10/07/2006	1	1	1	0	0
37	US	China	Naval War College disable	12/1/2006	12/07/2006	1	1	1	0	0
38	US	China	750,000 American zombies	3/1/2007	9/23/2010	1	1	1	0	0
39	US	China	GhostNet	5/27/2007	8/1/2009	1	1	1	0	0
40	US	China	Arrow Eclipse	5/27/2007	6/13/2013	1	1	1	0	0
41	US	China	Commerce Sec hack	12/1/2007	12/5/2007	1	1	1	0	0
42	US	China	Boxing Rumble	1/1/2008	7/19/2010	1	1	1	0	0
43	US	China	2008 Campaign hack	8/1/2008	8/04/2008	1	1	1	0	0
44	US	China	Hikit	9/1/2008	10/27/2014	1	1	1	0	0
45	US	China	Byzantine series	10/30/2008	6/30/2011	1	1	1	0	0
46	US	China	FAA hack	2/4/2009	2/10/2009	1	1	1	0	0
47	US	China	Seantor Nelson theft	3/1/2009	3/1/2009	1	1	1	0	0
48	US	China	Lockheed F-35 plans stolen	3/29/2009	4/1/2009	1	1	1	0	0
49	US	China	Aurora	6/1/2009	1/1/2010	1	1	1	0	0
50	US	China	NSA Fourth Party collection	7/1/2009	6/13/2013	1	1	1	0	0
51	US	China	Night Dragon	11/1/2009	2/11/2011	1	1	1	0	0
52	US	China	Commerce theft	11/1/2009	11/5/2009	1	1	1	0	0
53	US	China	Htran	1/1/2010	2/1/2010	1	1	1	0	0
54	US	China	Shotgiant	3/10/2010	6/13/2013	1	1	1	0	0
55	US	China	U.S. Top National Security Email Hacks	4/1/2010	8/10/2015	1	1	1	0	0
56	US	China	FDIC Hack	10/1/2010	2/2/2012	1	1	1	0	0
57	US	China	Energy Dept hack	2/1/2011	1/1/2014	1	1	1	0	0
58	US	China	Penatgon Raid	3/1/2011	3/10/2011	1	1	1	0	0
59	US	China	Operation Beebus	4/12/2011	2/7/2013	1	1	1	0	0
60	US	China	White House theft	11/7/2011	11/8/2011	1	1	1	0	0
61	US	China	Ocean Lotus	4/1/2012	5/1/2014	1	1	1	0	0
62	US	China	Penn State Engineering breach	9/1/2012	5/15/2015	1	1	1	0	0
63	US	China	Wen Jiabao Retaliation	10/26/2012	12/31/2012	1	1	1	0	0
64	US	China	Iron Tiger	1/15/2013	9/16/2015	1	1	1	0	0
65	US	China	Black Coffee	4/1/2013	5/12/2015	1	1	1	0	0
66	US	China	UConn Engineering Hack	9/24/2013	3/9/2015	1	1	1	0	0
67	US	China	Operation SnowMan	2/1/2014	2/12/2014	1	1	1	0	0
68	US	China	Regsiter.com breach	3/1/2014	3/18/2015	1	1	1	0	0
69	US	China	OPM Hack	3/15/2014	3/17/2015	1	1	1	0	0
70	US	China	Premera Blue Cross Breach	5/5/2014	1/29/2015	1	1	1	0	0
71	US	China	UCLA Health system breach	9/1/2014	7/25/2015	1	1	1	0	0
72	US	China	DHS employee hack	11/6/2014	11/7/2014	1	1	1	0	0
73	US	China	USPS breach	11/8/2014	11/10/2014	1	1	1	0	0
74	US	China	Anthem Breach	12/10/2014	1/27/2015	1	1	1	0	0

75	US	N Korea	Boxing Rumble	1/1/2008	7/19/2010	1	0	0	1	0
76	US	N Korea	Fourth of July	7/4/2009	7/7/2009	1	0	0	1	0
77	US	N Korea	NK Stuxnet	3/1/2010	4/30/2010	1	0	0	1	0
78	US	N Korea	March defacement	3/1/2011	3/4/2011	1	0	0	1	0
79	US	N Korea	December defacement	12/7/2011	12/7/2011	1	0	0	1	0
80	US	N Korea	Sony Hack	11/24/2014	11/25/2014	1	0	0	1	0
81	Canada	Russia	Energetic Bear/Dragonfly/Crouching Yeti	1/1/2011	7/1/2014	0	1	0	1	0
82	Canada	Russia	CyberBerkut NATO Websites	3/15/2014	3/27/2014	0	1	0	1	0
83	UK	Russia	Energetic Bear/Dragonfly/Crouching Yeti	1/1/2011	7/1/2014	0	1	0	1	0
84	UK	Russia	CyberBerkut NATO Websites	3/15/2014	3/25/2014	0	1	0	1	0
85	Poland	Russia	Sandworm	1/1/2009	10/14/2014	0	1	0	1	0
86	Poland	Russia	Operation Pawn Storm	6/1/2014	6/30/2014	0	1	0	1	0
87	Poland	Russia	CyberBerkut Polish Stock Exchange	10/23/2014	10/24/2014	0	1	0	1	0
88	Russia	Estonia	Defacement of govt websites	4/27/2007	5/10/2007	1	0	0	1	0
89	Russia	Estonia	Defacement of private websites	4/27/2007	5/10/2007	1	0	0	1	0
90	Russia	Estonia	DDoS of govt websites	4/27/2007	5/10/2007	1	0	0	1	0
91	Russia	Estonia	DDoS of private websites	4/27/2007	5/10/2007	1	0	0	1	0
92	Russia	Lithuania	Snake	1/1/2005	5/8/2014	1	0	0	1	0
93	Russia	Lithuania	Lithuanian Parliament	6/28/2008	7/2/2008	1	0	0	1	0
94	Russia	Lithuania	Lithuanian Parliament	6/28/2008	7/2/2008	1	0	0	1	0
95	Russia	Ukraine	Snake	1/1/2005	5/8/2014	1	0	0	1	0
96	Russia	Ukraine	Sandworm	1/1/2009	10/14/2014	1	0	0	1	0
97	Russia	Ukraine	Duke Series	2/1/2013	9/17/2015	1	0	0	1	0
98	Russia	Ukraine	CyberBerkut UKR Gov Site Hack	1/1/2014	12/31/2014	1	0	0	1	0
99	Russia	Ukraine	CyberBerkut Telecom disruption	3/1/2014	3/15/2014	1	0	0	1	0
100	Russia	Ukraine	CyberBerkut Ukraine Election Intrusion	5/22/2014	5/26/2014	1	0	0	1	0
101	Russia	Ukraine	Operation Pawn Storm	6/1/2014	2/1/2015	1	0	0	1	0
102	Russia	Ukraine	CyberBerkut UKR MOD DDoS	10/1/2014	10/30/2014	1	0	0	1	0
103	Russia	Ukraine	Fancy Bear (also APT 28 linked)	10/6/2014	7/15/2016	1	0	0	1	0
104	Russia	Ukraine	CyberBerkut Billboard Hack	11/20/2014	11/21/2014	1	0	0	1	0
105	Russia	Georgia	APT28/Sofacy Group/Sednit Group/Tsar Team/Fancy Bear	1/1/2007	7/15/2016	1	0	0	1	0
106	Russia	Georgia	Duke Series	4/8/2008	9/17/2015	1	0	0	1	0
107	Russia	Georgia	Before the gunfire	4/20/2008	8/6/2008	1	0	0	1	0
108	Russia	Georgia	Osinform	8/4/2008	8/4/2008	1	0	0	1	0
109	Russia	Georgia	VoiP	8/4/2008	8/8/2008	1	0	0	1	0
110	Russia	Georgia	Russo-Georgia Cyber Actions	8/5/2008	8/5/2016	1	0	0	1	0
111	Russia	Georgia	Russo-Georgia Cyber Actions	8/5/2008	8/5/2016	1	0	0	1	0
112	Russia	Georgia	Russo-Georgia Cyber Actions	8/5/2008	8/5/2016	1	0	0	1	0
113	Russia	Georgia	US-Georgia Government defacements	8/7/2008	8/16/2008	1	0	0	1	0

114	Iran	Israel	Electronic jihad	9/1/2000	9/1/2000	0	0	0	0	1
115	Iran	Israel	Cyber jihad	8/1/2001	8/1/2001	0	0	0	0	1
116	Iran	Israel	Ant-semitic response	2/7/2006	2/7/2006	0	0	0	0	1
117	Iran	Israel	Lebanese action propaganda	10/27/2006	10/27/2006	0	0	0	0	1
118	Iran	Israel	Stuxnet .5	11/1/2007	6/1/2010	0	0	0	0	1
119	Iran	Israel	Cast Lead Retaliation	12/27/2008	12/27/2008	0	0	0	0	1
120	Iran	Israel	Stuxnet	6/1/2009	10/1/2010	0	0	0	0	1
121	Iran	Israel	Flame	6/1/2009	12/2/2012	0	0	0	0	1
122	Iran	Israel	Nuclear Facilities Virus	7/7/2009	1/1/2010	0	0	0	0	1
123	Iran	Israel	Duqu	9/11/2011	12/1/2011	0	0	0	0	1
124	Iran	Israel	Israel Infrastructure Hack	3/2/2013	6/8/2013	0	0	0	0	1
125	Iran	Israel	Duqu 2.0	6/1/2014	6/30/2015	0	0	0	0	1
126	Iran	Israel	Iranian multiple espionage	7/1/2014	6/14/2015	0	0	0	0	1
127	Iran	Saudi Arabia	Shamoon	8/15/2012	8/16/2012	0	0	0	0	1
128	Iran	Saudi Arabia	RasGas Attack	8/20/2012	8/21/2012	0	0	0	0	1
129	Iran	Saudi Arabia	Iranian multiple espionage	7/1/2014	6/14/2015	0	0	0	0	1
130	Iraq	Kuwait	Iraq hack	12/13/2002	12/13/2002	0	0	0	0	1
131	Syria	Israel	Mossad Trojan leads to Operation Orchard	12/10/2006	12/11/2006	0	0	0	0	1
132	Lebanon	Israel	Cyber-jihad on Israel	7/15/2001	8/1/2001	0	0	0	0	1
133	Lebanon	Israel	Gauss	9/1/2011	8/8/2012	0	0	0	0	1
134	China	Taiwan	DPP hack	3/1/2001	3/3/2001	1	0	0	1	0
135	China	Taiwan	Prosecuter hack	11/17/2001	11/18/2001	1	0	0	1	0
136	China	Taiwan	GhostNet	5/27/2007	8/1/2009	1	0	0	1	0
137	China	Taiwan	Shady RAT	9/1/2007	1/1/2010	1	0	0	1	0
138	China	Taiwan	Hikit	9/1/2008	10/27/2014	1	0	0	1	0
139	China	Taiwan	Election hack	8/4/2011	8/6/2011	1	0	0	1	0
140	China	Taiwan	TooHash	9/1/2013	11/3/2014	1	0	0	1	0
141	China	Japan	Htran	1/1/2001	2/1/2001	1	0	0	1	0
142	China	Japan	WWII Memorial	1/6/2005	5/15/2005	1	0	0	1	0
143	China	Japan	Hack and extort	12/27/2007	6/1/2008	1	0	0	1	0
144	China	Japan	Hikit	9/1/2008	10/27/2014	1	0	0	1	0
145	China	Japan	Earthquake hack	3/11/2010	3/14/2010	1	0	0	1	0
146	China	Japan	East China Sea Dispute	09/14/2010	9/17/2010	1	0	0	1	0
147	China	Japan	Mitsubishi Hack	09/01/2011	11/4/2011	1	0	0	1	0
148	China	Japan	Icefog	9/1/2011	9/23/2013	1	0	0	1	0
149	China	Japan	Parliament Hack	10/25/2011	11/2/2011	1	0	0	1	0
150	China	India	GhostNet	5/27/2007	8/1/2009	1	0	0	1	0
151	China	India	Shady RAT	7/1/2007	1/1/2010	1	0	0	1	0
152	China	India	Prime Minster's office hacked and info stolen	12/15/2009	12/15/2009	1	0	0	1	0
153	China	India	Indian military stolen	4/2/2010	4/7/2010	1	0	0	1	0

154	China	Vietnam	Shady RAT	3/1/2007	1/1/2010	1	0	0	1	0
155	China	Vietnam	Vietnam Hack	7/3/2011	7/6/2011	1	0	0	1	0
156	China	Philippines	Philippines hack	3/28/2009	3/30/2009	1	0	0	1	0
157	China	Philippines	Dark Hotel	1/1/2008	11/9/2014	1	0	0	1	0
158	N Korea	S Korea	Un retaliate	6/1/2008	9/2/2008	0	0	0	0	1
159	N Korea	S Korea	Government theft	9/8/2008	9/8/2008	0	0	0	0	1
160	N Korea	S Korea	Government shut down	7/6/2009	7/9/2009	0	0	0	0	1
161	N Korea	S Korea	Web portal defacement	6/1/2010	6/2/2010	0	0	0	0	1
162	N Korea	S Korea	Anti-Kim	1/4/2011	1/10/2011	0	0	0	0	1
163	N Korea	S Korea	NK retaliation	1/4/2011	1/10/2011	0	0	0	0	1
164	N Korea	S Korea	March DDoS	3/7/2011	3/8/2011	0	0	0	0	1
165	N Korea	S Korea	Bank shut down	4/3/2011	4/3/2011	0	0	0	0	1
166	N Korea	S Korea	June DDoS	6/7/2011	6/7/2011	0	0	0	0	1
167	N Korea	S Korea	December defacement	12/7/2011	12/7/2011	0	0	0	0	1
168	N Korea	S Korea	Telecom shut down	12/20/2011	12/20/2011	0	0	0	0	1
169	N Korea	S Korea	South Korea nuclear facility hack	12/9/2014	12/12/2014	0	0	0	0	1
170	N Korea	Japan	Fourth of July	7/4/2009	7/7/2009	0	0	0	0	1
171	S Korea	Japan	Textbook hack	4/1/2001	4/1/2001	0	0	0	0	1
172	S Korea	Japan	South Korea Patriotic	1/7/2004	1/14/2004	0	0	0	0	1
173	S Korea	Japan	Japan Patriotic	1/7/2004	1/14/2004	0	0	0	0	1
174	S Korea	Japan	Island Dispute	3/20/2005	3/20/2005	0	0	0	0	1
175	S Korea	Japan	Dark Hotel	1/1/2008	11/9/2014	0	0	0	0	1
176	S Korea	Japan	SK hack	3/1/2010	3/1/2010	0	0	0	0	1
177	S Korea	Japan	Japan retaliation	3/1/2010	3/1/2010	0	0	0	0	1
178	S Korea	Japan	Earthquake hack	3/11/2011	3/14/2011	0	0	0	0	1
179	India	Pakistan	October 2001 defacements	10/22/2001	10/24/2001	0	0	0	0	1
180	India	Pakistan	Worm infiltrates Pakistan govt	3/1/2003	3/13/2003	0	0	0	0	1
181	India	Pakistan	July 2003 defacements	7/12/2003	7/13/2003	0	0	0	0	1
182	India	Pakistan	November 2008 defacements	11/15/2008	11/27/2008	0	0	0	0	1
183	India	Pakistan	November 2008 defacements	11/15/2008	11/27/2008	0	0	0	0	1
184	India	Pakistan	Transportation defacements	12/24/2008	12/25/2008	0	0	0	0	1
185	India	Pakistan	September 2010 defacements	9/2/2010	9/12/2010	0	0	0	0	1
186	India	Pakistan	September 2010 defacements	9/2/2010	9/12/2010	0	0	0	0	1
187	India	Pakistan	PCA defacements	12/1/2010	12/3/2010	0	0	0	0	1
188	India	Pakistan	PCA retaliation	12/1/2010	12/3/2010	0	0	0	0	1
189	India	Pakistan	ICID defacement	10/1/2011	10/1/2011	0	0	0	0	1
190	India	Pakistan	Tranchulas incident	2/1/2013	7/2/2013	0	0	0	0	1
191	India	Pakistan	Telenor Pakistan incident	3/17/2013	3/17/2013	0	0	0	0	1
192	India	Bangladesh	Terrorist Warning	3/19/2010	3/20/2010	0	0	0	0	1
Total								61	76	55

Notes

¹ US Department of Defense, *Dictionary of Military and Associated Terms*, JP1-02 (Washington, DC: US Department of Defense, February 15, 2016), 58. https://fas.org/irp/doddir/dod/jp1_02.pdf.

² United States of America v. Internet Research Agency LLC, Concord Management and Consulting LLC, Concord Catering, et al, 18 U.S.C. §§ 2, 371, 1349, 1028A (2018). <https://www.justice.gov/file/1035477/download>.

³ Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017), 171.

Kello, *The Virtual Weapon*, 155.

Ellen Nakashima, "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes," *Washington Post*, January 12, 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.5515ac0d57a0.

⁴ In 2018, global ecommerce at an estimated value of US\$2.86 Trillion will make up 11.5% of total global commerce. eMarketer, "Worldwide Retail Ecommerce Sales will reach \$1.915 Trillion This Year," *eMarketer.com*, August 22, 2016, <https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369>.

⁵ Barack Obama, "Remarks at the National Cybersecurity Communications Integration Center," (speech, National Cybersecurity Communications Integration Center, Arlington, VA, January 13, 2015). <https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent>.

⁶ Leon E. Panetta, "Remarks on Cybersecurity to the Business Executives for National Security," (speech, New York, October 11, 2012). <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.

⁷ Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies Vol.22* (2013), 366.

⁸ George Perkovich, "Implications of the Joint Comprehensive Plan of Action", in *American Institute of Physics Conference Proceedings Vol. 1898, Issue 1*, ed. Pierce Corden, Tony Fainberg, David Hafemeister, and Allison Macfarlane (Washington, DC: American Institute of Physics, 2017), <http://aip.scitation.org/doi/pdf/10.1063/1.5009224>.

⁹ Ashton Carter, "In Fight Against ISIS, U.S. Adds Cyber Tools," interview by Rachel Martin, *npr.org*, February 28, 2016, <https://www.npr.org/templates/transcript/transcript.php?storyId=468446138>.

¹⁰ Nigel Inkster, *China's Cyber Power* (Oxon, UK: Routledge, 2016), 68.

¹¹ Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, "Cyberwarfare has taken a new turn. Yes, it's time to worry." *Washingtonpost.com*, July 13, 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/07/13/cyber-warfare-has-taken-a-new-turn-yes-its-time-to-worry/?utm_term=.474c4314fa45.

Michael Riley and Jordan Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known," *Bloomberg.com*, June 13, 2017, <https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections>.

¹² CNN, *2016 Presidential Campaign Hacking Fast Facts*, CNN.com, October 31, 2017, <http://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html>.

¹³ Nitasha Tiku, "How Russia Pushed Our Buttons With Fake Online Ads," *Wired.com*, November 3, 2017, <https://www.wired.com/story/how-russia-pushed-our-buttons-with-fake-online-ads/>.

Mike Issac and Daisuke Wakabayashi, "Russian Influence Reached 126 Million Through Facebook Alone," *Nytimes.com*, October 30, 2017, <https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html>.

¹⁴ Eric Schmidt and Jared Cohen, *The New Digital Age: Transforming Nations, Businesses, and Our Lives*, (New York: Random House, 2013), 4.

¹⁵ Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, *Cyber Strategy: The Evolving Character of Power and Coercion* (forthcoming).

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ Ibid.

¹⁹ Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security Vol. 38 No. 2* (Fall 2013), 43, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136.

²⁰ Thomas C. Schelling, *Arms and Influence* (Hartford, CT: Yale University Press, 1995), 174.

²¹ Imran Awan, "Cyber-Extremism: Isis and the Power of Social Media," *Social Science and Public Policy Vol 54* (2017), 138. <https://link.springer.com/content/pdf/10.1007%2Fs12115-017-0114-0.pdf>.

²² Nate Anderson, "Massive DDoS Attacks Target Estonia; Russia Accused," *Arstechnica.com*, May 14, 2007, <https://arstechnica.com/information-technology/2007/05/massive-ddos-attacks-target-estonia-russia-accused/>.

²³ Paul J. Springer, *Cyber Warfare: A Reference Handbook* (Santa Barbara, CA: ABC-CLIO, LLC, 2015), 37.

²⁴ Springer, *Cyber Warfare*, 37.

²⁵ Andreas Hagen, "The Russo-Georgian War 2008," in *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, ed. Jason Healey (Arlington VA: Cyber Conflict Studies Association, 2013), 202.

²⁶ Naveen Thakur, "Russian Business Network (RBN): The Dark Hackers," *Whitecode*, accessed February 26, 2018, <http://www.whitecode.com/russian-business-network-rbn-the-dark-hackers/>.

²⁷ George Kennan, "Review of Current Trends, U.S. Foreign Policy, Policy Planning Staff, PPS No. 23," in *U.S. Department of State, Foreign Relations of the United States, Vol. 1 Part 2* (Washington, DC: Government Printing Office, 1976), 509-529.

²⁸ Brandon Valeriano and Ryan Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, (New York: Oxford University Press, 2015), 9.

²⁹ Jon R. Lindsay, "Cyber Espionage," in *The Oxford Handbook of Cyber Security*, ed. P. Cornish (Oxford University Press, Forthcoming).

³⁰ Andy Greenberg, "The NSA Officially Has A Rogue Contractor Problem," *Wired.com*, October 5, 2017, <https://www.wired.com/story/nsa-contractors-hacking-tools/>.

³¹ Springer, *Cyber Warfare*, 84.

³² Scott W. Harold, Martin C. Libicki, Astrid S. Cevallos, *Getting to Yes with China in Cyberspace*, (Santa Monica, CA: RAND Corporation, 2016), 12.

Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* (Fort Leavenworth, KS: Foreign Military Studies Office, 2012), <https://community.apan.org/cfs->

file/_key/telligent-evolution-components-attachments/13-14904-00-00-00-19-56-10/2012a-Three-Faces-of-the-Cyber-Dragon-_2D00_-Cyber-Peace-

Activist_2D00_Spook_2D00_Attacker-_2800_Thomas_2900_.pdf?forcedownload=true.

Hearing on Chinese Hacking: Impact on Human Rights and Commercial Rule of Law: Testimony before the Congressional-Executive Commission on China, 113rd Cong., (2013) (testimony of James C. Mulvenon, Ph. D, Vice-President, Defense Group, Inc. Intelligence Division; Director, Center for Intelligence Research and Analysis),

<https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg81855/pdf/CHRG-113hhrg81855.pdf>.

³³ Scott W. Harold, “The U.S.-China Cyber Agreement: A Good First Step,” *Rand.org*, August 1, 2016, <https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>.

³⁴ Ryan O’Hare, “China Proudly Debuts Its New Stealth Jet It Built by Hacking into US Computers and Stealing Plans,” *DailyMail.co.uk*, November 1, 2016, <http://www.dailymail.co.uk/sciencetech/article-3893126/Chinese-J-20-stealth-jet-based-military-plans-stolen-hackers-makes-public-debut.html>.

³⁵ Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O’Reilly Media, 2012), 4.

³⁶ Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, trans. CIA Foreign Broadcast Information Service (Rosslyn, VA: CIA Foreign Broadcast Information Service, 1999), <http://www.cryptome.org/cuw.htm>.

³⁷ Inkster, *China’s Cyber Power*, 71.

³⁸ Peng Guangqian and Yao Youzhi, *The Science of Military Strategy* (Beijing, China: Department of Strategic Research, Military Science Press, 2001), 21.

³⁹ Ministry of National Defense, The People’s Republic of China, *China’s Military Strategy* (Beijing, China: Ministry of National Defense, 2015), http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.

⁴⁰ Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND Corporation, 2017), 22, https://www.rand.org/pubs/research_reports/RR2058.html.

⁴¹ Timothy Thomas, *China’s Cyber Incursions: A Theoretical Look at What They See and Why They Do It Based on a Different Strategic Method of Thought* (Fort Leavenworth, KS: US Army Command and General Staff College, March 2013), <http://indianstrategicknowledgeonline.com/web/Chinas-Cyber-Incursions.pdf>.

⁴² Valeriano, Maness, and Jensen, *Cyber Strategy* (forthcoming).

⁴³ Derek M.C. Yuen, *Deciphering Sun Tzu: How to Read the Art of War* (New York: Oxford University Press, 2014), 46.

⁴⁴ Keith Pollpeter, “Chinese Writings on Cyberwarfare and Coercion,” in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 147.

⁴⁵ Kello, *The Virtual Weapon*, 213.

⁴⁶ Valeriano, Maness, and Jensen, *Cyber Strategy* (forthcoming).

⁴⁷ Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve* (Arlington, VA: The Langner Group, 2013), 8, <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>.

⁴⁸ Nicholas Faliere, Liam O Murchu, and Eric Chen, “W32.Stuxnet Dossier,” *Symantec*, February 2011, accessed February 26 2018,

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_s_tuxnet_dossier.pdf.

⁴⁹ Kello, *The Virtual Weapon*, 63.

Kim Zetter, “The NSA Acknowledges What We All Feared: Iran Learns from US Cyberattacks,” *Wired.com*, October 2, 2015, <https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/>.

⁵⁰ Lorenzo Franceschi-Bicchierai, “The Latest Dump of Alleged NSA Tools is ‘The Worst Thing Since Snowden,’” *Motherboard*, April 14, 2017, https://motherboard.vice.com/en_us/article/vvaepb/the-latest-shadow-brokers-dump-of-alleged-nsa-tools-is-awful-news-for-the-internet.

⁵¹ Joseph Cox, “A Brief Interview with The Shadow Brokers, The Hackers Selling NSA Exploits,” *Motherboard*, December 15, 2016, https://motherboard.vice.com/en_us/article/4xa59g/a-brief-interview-with-the-shadow-brokers-the-hackers-selling-nsa-exploits.

⁵² Lorenzo Franceschi-Bicchierai, “Hackers Hit ‘Some’ Cisco Customers with Leaked NSA Hacking Tools,” *Motherboard*, September 19, 2016, https://motherboard.vice.com/en_us/article/3dajyn/hackers-hit-cisco-customers-leaked-nsa-hacking-tools-shadow-brokers.

⁵³ John Hudson, “Here’s How the Stuxnet Virus Could Be Used Against the U.S.” *The Atlantic*, June 1, 2012, <https://www.theatlantic.com/technology/archive/2012/06/heres-how-stuxnet-virus-could-be-used-against-us/327389/>.

⁵⁴ Nicole Perlroth and David E. Sanger, “Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool,” *Washingtonpost.com*, May 12, 2017, <https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html>.

⁵⁵ Ibid.

⁵⁶ Toshio Obi and Naoko Iwasaki, *A Decade of World e-Government Rankings* (Fairfax VA: IOS Press, Inc., 2015), 59.

⁵⁷ Lee Hsien Loong, “Speech at Smart Nation Launch,” (speech, Smart Nation Launch, Singapore, Singapore, November 24, 2014), <https://www.smartnation.sg/happenings/speeches/smart-nation-launch>.

⁵⁸ Bruce Schneier, “Cyber Conflicts and National Security,” in *UN Chronicle Vol. 50, Issue 2* (New York: Outreach Division, United Nations Department of Public Information, 2013), 13.

⁵⁹ Ministry of Economic Affairs and Communications, Estonia, *Implementation of the Virtual Data Embassy Solution*, (Tallinn, Estonia: 2015), 5, https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf.

⁶⁰ Lawrence Schaack, “The World’s First Data Embassy in Luxembourg,” *Delano.lu*, August 30, 2017, <http://delano.lu/d/detail/news/worlds-first-data-embassy-lux/154026>.

⁶¹ NATO Cooperative Cyber Defence Centre of Excellence, *History*, CCDCOE.org, accessed October 20, 2017, <https://ccdcoe.org/history.html>.

⁶² NATO Cooperative Cyber Defence Centre of Excellence, *History*, CCDCOE.org, accessed October 20, 2017, <https://ccdcoe.org/history.html>.

⁶³ Monica M. Ruiz, “Is Estonia’s Approach to Cyber Defense Feasible in the United States?” *Warontherocks.com*, January 9, 2018, <https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/>.

⁶⁴ Kadri Kaska, Anna-Maria Osula, LTC Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 5.

-
- ⁶⁵ John Reed, "Unit 8200: Israel's Cyber Spy Agency," *Ft.com*, July 10, 2015, <https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c>.
- ⁶⁶ Richard Behar, "Inside Israel's Secret Startup Machine," *Forbes.com*, May 11, 2016, <https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#64d5c3141a51>.
- ⁶⁷ Josephine Wolff, "Making A New Pipeline: How Israel is Training Teenagers from Underrepresented Groups to Work on Cybersecurity," *Slate.com*, July 6, 2016, http://www.slate.com/articles/technology/future_tense/2016/07/israel_s_magshimim_program_trains_teenagers_to_work_on_cybersecurity.html.
- ⁶⁸ John Reed, "Unit 8200: Israel's cyber spy agency," *Financial Times*, July 10, 2015, <https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c>.
- ⁶⁹ Carr, *Inside Cyber Warfare*, 251.
- ⁷⁰ Mark Winther, *Tier 1 ISPs: What They Are And Why They Are Important* (Framingham, MA: International Data Corporation, 2006), 4.
- ⁷¹ Mark Raymond, "Puncturing the Myth of the Internet as a Commons," in *Georgetown Journal of International Affairs Vol. 14 Issue 2* (Washington, D.C.: Georgetown University Press, 2013), 185-191, <https://pdfs.semanticscholar.org/ce38/269bbbed316e8e46aaaf2ca52181e3ab72bfe.pdf>.
- ⁷² House of Representatives, US Congress, *H.R.4036: Active Cyber Defense Certainty Act*, 115th Cong., 2017, 3, <https://www.congress.gov/115/bills/hr4036/BILLS-115hr4036ih.pdf>.
- ⁷³ Jocelyn Aspa, "10 Top Cybersecurity Companies," *Investingnews.com*, December 5, 2017, <https://investingnews.com/daily/tech-investing/cybersecurity-investing/top-cyber-security-companies/>.
- ⁷⁴ Kim Zetter, "Hacking Team Leak Shows How Secretive Zero Day Exploit Sales Work," *Wired.com*, July 24, 2015, <https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/>.
- ⁷⁵ Daniel Ventre, "French Perspectives on Cyber-conflict," in *Cyber Conflict: Competing National Perspectives*, ed. Daniel Ventre (Hoboken, NJ: John Wiley & Sons, Inc, 2012), 89.
- ⁷⁶ Valeriano, Maness, and Jensen, *Cyber Strategy* (Forthcoming).
- ⁷⁷ Ibid.
- ⁷⁸ Cyber Security Agency of Singapore, "Cybersecurity Public Awareness Survey 2016 Key Findings," Cyber Security Agency Singapore, February 15, 2017, https://www.csa.gov.sg/~media/csa/documents/key_findings/key%20findings-cybersecurity%20public%20awareness%20survey%202016.ashx?la=en.
- ⁷⁹ Kenneth Olmstead and Aaron Smith, "Americans and Cybersecurity," Pew Research Center, January 26, 2017, <http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/>.
- ⁸⁰ Mark Pomerleau, "DoD quietly reorganizes Cyber Command," *Fifthdomain.com*, January 9, 2018, <https://www.fifthdomain.com/dod/cybercom/2018/01/09/dod-quietly-reorganizes-cyber-command-to-shepherd-command-through-elevation/>.
- Jim Garamone and Lisa Ferdinando, "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command," *Department of Defense*, August 18, 2017, <https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/>.
- House of Representatives, US Congress, *H.R.4036: Active Cyber Defense Certainty Act*, 115th Cong., 2017, 3, <https://www.congress.gov/115/bills/hr4036/BILLS-115hr4036ih.pdf>.

⁸¹ Statista, “Internet Penetration Rate in Singapore from 2005 to 2016,” *Statista*, accessed February 5, 2018, <https://www.statista.com/statistics/765544/internet-penetration-rate-singapore/>.

⁸² Lee Hsien Loong, “Speech at Smart Nation Launch,” (speech, Smart Nation Launch, Singapore, Singapore, November 24, 2014), <https://www.smartnation.sg/happenings/speeches/smart-nation-launch>.

⁸³ Smart Nation and Digital Government Office, “Why Smart Nation: Strategic National Projects,” *Smart Nation and Digital Government Office*, accessed February 17, 2018, <https://www.smartnation.sg/about/Smart-Nation>.

⁸⁴ Lee Hsien Loong, “Speech at Smart Nation Launch,” (speech, Smart Nation Launch, Singapore, Singapore, November 24, 2014), <https://www.smartnation.sg/happenings/speeches/smart-nation-launch>.

⁸⁵ Cyber Security Agency of Singapore, *Singapore’s Cyber Security Strategy* (Singapore: Cyber Security Agency of Singapore, 2016), 4.

⁸⁶ The 11 Critical Information Infrastructure (CII) Sectors are: government, info communications, energy, aviation, maritime, land transport, healthcare, banking and finance, water, security and emergency, and media.

Loh Chuan Junn, “11 Critical Information Infrastructure Sectors tested for first time in national cybersecurity exercise,” *ChannelNewsAsia.com*, July 18, 2017, <https://www.channelnewsasia.com/news/singapore/11-critical-information-infrastructure-sectors-tested-for-first-9040914>.

⁸⁷ Cyber Security Agency of Singapore, *Singapore’s Cyber Security Strategy* (Singapore: Cyber Security Agency of Singapore, 2016), 4.

⁸⁸ Ministry of Communications and Information, *Cybersecurity Act 2017*, 13th Parliament of Singapore, 2018, https://www.csa.gov.sg/~media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en.

Jalelah Abu Baker, “Cybersecurity Bill passed in Parliament; MPs raise questions on privacy, cost,” *Channelnewsasia.com*, February 5, 2018, <https://www.channelnewsasia.com/news/singapore/cybersecurity-bill-passed-in-parliament-mps-raise-questions-on-9929208>.

⁸⁹ Ng Eng Hen, “Speech at the Committee of Supply Debate 2017,” (speech, Singapore Parliament, Singapore, March 3, 2017), <https://www.gov.sg/microsites/budget2017/press-room/news/content/speech-by-minister-for-defence-dr-ng-eng-hen-at-the-committee-of-supply-debate-2017>.

⁹⁰ Ng Eng Hen, “Speech at the Committee of Supply Debate 2017.”

⁹¹ ChannelNewsAsia, “Singapore to set up new Defence Cyber Organisation,” *Channelnewsasia.com*, March 3, 2017, <https://www.channelnewsasia.com/news/singapore/singapore-to-set-up-new-defence-cyber-organisation-8775266>.

⁹² Adrian Lim, “Parliament: MINDEF sets up new cyber command to beef up defense against cyber-attacks,” *Straitstimes.com*, March 3, 2017, <http://www.straitstimes.com/singapore/parliament-mindef-sets-up-new-cyber-command-to-beef-up-defence-against-cyber-attacks>.

⁹³ Gil Press, “6 Reasons Israel Became a Cybersecurity Powerhouse Leading the \$82 Billion Industry,” *Forbes.com*, July 18, 2017, <https://www.forbes.com/sites/gilpress/2017/07/18/6->

reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#48851885420a.

⁹⁴ Andreas Schmidt, “The Estonian Cyber Operations,” in *The Fierce Domain – Conflicts in Cyberspace 1986-2012*, ed. Jason Healey (Arlington VA: Cyber Conflict Studies Association, 2013), 178.

⁹⁵ Blockchain is a software technology that enables encrypted peer-to-peer electronic transactions and interactions, using cryptographic proof that is distributed throughout the network instead of a central trust institution.

Wiliam Mougaya, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology* (Hoboken, NJ: John Wiley & Sons, Inc., 2016), 2.

⁹⁶ Ministry of Defence Singapore, “The 5 Pillars of Total Defence,” *Ministry of Defence Singapore*, accessed February 17, 2018, https://www.mindef.gov.sg/oms/imindef/mindef_websites/topics/totaldefence/about_us/5_Pillars.html.

⁹⁷ International Telecommunication Union, *Global Cybersecurity Index 2017* (Geneva, Switzerland: International Telecommunication Union, 2017), 17.

⁹⁸ ASEAN Secretariat, *ASEAN Political-Security Community Blueprint 2025* (Jakarta, Indonesia: ASEAN Secretariat, March 2016), 1.

⁹⁹ Ibid, 2.

¹⁰⁰ House of Representatives, US Congress, *H.R.4036: Active Cyber Defense Certainty Act*, 115th Cong., 2017, 3, <https://www.congress.gov/115/bills/hr4036/BILLS-115hr4036ih.pdf>.

¹⁰¹ Infosec Institute, “The Offensive Approach to Cybersecurity in Government and Private Industry,” *Infosec Institute*, accessed February 17, 2018, <http://resources.infosecinstitute.com/the-offensive-approach-to-cyber-security-in-government-and-private-industry/#gref>.

¹⁰² CrowdStrike, “CrowdStrike Falcon for the Public Sector,” *CrowdStrike*, accessed February 17, 2018, https://www.crowdstrike.com/wp-content/brochures/datasheets/CS_FalconPublicSector_DataSheet.pdf.

CrowdStrike, “CrowdStrike Falcon Overwatch Managed Threat Hunting: Stop Incidents Before They Turn Into Breaches,” *CrowdStrike*, accessed February 17, 2018, https://www.crowdstrike.com/wp-content/brochures/OverWatch_Overview_v3.pdf.

¹⁰³ Patrick Tucker, “Someone Just Leaked the Price List for Cyberwar,” *DefenseOne.com*, July 6, 2015, <http://www.defenseone.com/technology/2015/07/someone-just-leaked-price-list-cyberwar/117043/>.

¹⁰⁴ Hacking Team, “The Hacking Suite for Governmental Interception,” accessed February 17, 2018, <http://www.hackingteam.it/>.

Bibliography

ASEAN Secretariat. *ASEAN Political-Security Community Blueprint 2025*. Jakarta, Indonesia: ASEAN Secretariat, March 2016.

Awan, Imran. "Cyber-Extremism: Isis and the Power of Social Media." *Social Science and Public Policy Vol 54* (2017), 138 – 149.
<https://link.springer.com/content/pdf/10.1007%2Fs12115-017-0114-0.pdf>.

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media, 2012.

Cyber Security Agency of Singapore. "Cybersecurity Public Awareness Survey 2016 Key Findings." *Cyber Security Agency Singapore*, February 15, 2017.
https://www.csa.gov.sg/~media/csa/documents/key_findings/key%20findings-cybersecurity%20public%20awareness%20survey%202016.ashx?la=en.

Cyber Security Agency of Singapore, *Singapore's Cyber Security Strategy*. Singapore: Cyber Security Agency of Singapore, 2016.

Faliere, Nicholas, Liam O Murchu, and Eric Chen. "W32.Stuxnet Dossier." *Symantec*, February 2011, accessed February 26 2018.
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security Volume. 38 No. 2* (Fall 2013), 41 – 73,
https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136.

Hagen, Andreas. "The Russo-Georgian War 2008." in *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, edited by Jason Healey, 194 - 204. Arlington VA: Cyber Conflict Studies Association, 2013.

Harold, Scott W., Martin C. Libicki, Astrid S. Cevallos. *Getting to Yes with China in Cyberspace*. Santa Monica, CA: RAND Corporation, 2016.

Harold, Scott W. "The U.S.-China Cyber Agreement: A Good First Step." *Rand.org*, August 1, 2016. <https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>.

Hearing on Chinese Hacking: Impact on Human Rights and Commercial Rule of Law: Testimony before the Congressional-Executive Commission on China, 113rd Cong., (2013) (testimony of James C. Mulvenon, Ph. D, Vice-President, Defense Group, Inc. Intelligence Division; Director, Center for Intelligence Research and Analysis), <https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg81855/pdf/CHRG-113hhrg81855.pdf>.

Inkster, Nigel. *China's Cyber Power*. Oxon, UK: Routledge, 2016.

- International Telecommunication Union, *Global Cybersecurity Index 2017*. Geneva, Switzerland: International Telecommunication Union, 2017.
- Kaska, Kadri, Anna-Maria Osula, LTC Jan Stinissen. *The Cyber Defence Unit of the Estonian Defence League*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013.
- Kello, Lucas. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press, 2017.
- Kennan, George. "Review of Current Trends, U.S. Foreign Policy, Policy Planning Staff, PPS No. 23." In *U.S. Department of State, Foreign Relations of the United States, Vol. 1 Part 2*, 509-529. Washington, DC: Government Printing Office, 1976.
- Langner, Ralph. *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Arlington, VA: The Langner Group, 2013. <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>.
- Lee, Hsien Loong. "Speech at Smart Nation Launch." Speech, Smart Nation Launch, Singapore, Singapore, November 24, 2014. <https://www.smartnation.sg/happenings/speeches/smart-nation-launch>.
- Lemieux, Frederic. "Trends in Cyber Operations: An Introduction." In *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, edited by Frederic Lemieux, 1 – 17. New York: Palgrave Macmillan, 2015.
- Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare," *Security Studies Vol.22* (2013), 365-404.
- Lindsay, Jon R. "Cyber Espionage," in *The Oxford Handbook of Cyber Security*. Edited by P. Cornish. Oxford University Press, Forthcoming.
- Ministry of Communications and Information, *Cybersecurity Act 2017*, 13th Parliament of Singapore, 2018, https://www.csa.gov.sg/~media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en.
- Ministry of Economic Affairs and Communications, Estonia. *Implementation of the Virtual Data Embassy Solution*. Tallinn, Estonia: 2015. https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf.
- Ministry of National Defense, The People's Republic of China, *China's Military Strategy* (Beijing, China: Ministry of National Defense, 2015), http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.

- Mougaya, William. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Hoboken, NJ: John Wiley & Sons, Inc., 2016.
- Ng, Eng Hen. "Speech at the Committee of Supply Debate 2017." Speech. Singapore Parliament, Singapore, March 3, 2017. <https://www.gov.sg/microsites/budget2017/press-room/news/content/speech-by-minister-for-defence-dr-ng-eng-hen-at-the-committee-of-supply-debate-2017>.
- Obama, Barack. "Remarks at the National Cybersecurity Communications Integration Center." Speech, National Cybersecurity Communications Integration Center, Arlington, VA, January 13, 2015. <https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent>.
- Obi Toshio and Naoko Iwasaki. *A Decade of World e-Government Rankings*. Fairfax VA: IOS Press, Inc., 2015.
- Olmstead, Kenneth and Aaron Smith. "Americans and Cybersecurity." *Pew Research Center*, January 26, 2017. <http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity>.
- Panetta, Leon E. "Remarks on Cybersecurity to the Business Executives for National Security." Speech, New York, October 11, 2012. <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136>.
- Peng, Guangqian and Yao Youzhi, *The Science of Military Strategy*. Beijing, China: Department of Strategic Research, Military Science Press, 2001.
- People's Republic of China. Ministry of National Defense. *China's Military Strategy*. Beijing, China: Ministry of National Defense, 2015. http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.
- Perkovich, George. "Implications of the Joint Comprehensive Plan of Action." In *American Institute of Physics Conference Proceedings Vol. 1898, Issue 1*, edited by Pierce Corden, Tony Fainberg, David Hafemeister, and Allison Macfarlane. Washington, DC: American Institute of Physics, 2017. <http://aip.scitation.org/doi/pdf/10.1063/1.5009224>.
- Pollpeter, Keith. "Chinese Writings on Cyberwarfare and Coercion." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 138 – 162. New York: Oxford University Press, 2015.
- Pollpeter, Kevin L., Michael S. Chase, and Eric Heginbotham. *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR2058.html.

- Qiao, Liang and Wang Xiangsui. *Unrestricted Warfare*. Translated by CIA Foreign Broadcast Information Service. Rosslyn, VA: CIA Foreign Broadcast Information Service, 1999. <http://www.cryptome.org/cuw.htm>.
- Raymond, Mark. "Puncturing the Myth of the Internet as a Commons." In *Georgetown Journal of International Affairs Vol. 14 Issue 2*, 185-191. Washington, D.C.: Georgetown University Press, 2013. <https://pdfs.semanticscholar.org/ce38/269bbbed316e8e46aaaf2ca52181e3ab72bfe.pdf>.
- Schelling, Thomas C. *Arms and Influence*. Hartford, CT: Yale University Press, 1995.
- Schmidt, Andreas. "The Estonian Cyber Operations." In *The Fierce Domain – Conflicts in Cyberspace 1986-2012*, edited by Jason Healey, 174 – 193. Arlington VA: Cyber Conflict Studies Association, 2013.
- Schmidt, Eric and Jared Cohen. *The New Digital Age: Transforming Nations, Businesses, and Our Lives*. New York: Random House, 2013.
- Schneier, Bruce. "Cyber Conflicts and National Security." In *UN Chronicle Vol. 50, Issue 2*. New York: Outreach Division, United Nations Department of Public Information, 2013.
- Springer, Paul J. *Cyber Warfare: A Reference Handbook*. Santa Barbara, CA: ABC-CLIO, LLC, 2015.
- Thomas, Timothy L. *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* (Fort Leavenworth, KS: Foreign Military Studies Office, 2012), https://community.apan.org/cfs-file/_key/telligent-evolution-components-attachments/13-14904-00-00-00-19-56-10/2012a-Three-Faces-of-the-Cyber-Dragon-_2D00_-Cyber-Peace-Activist_2D00_Spook_2D00_Attacker-_2800_Thomas_2900_.pdf?forcedownload=true.
- Tiku, Nitasha. "How Russia Pushed Our Buttons With Fake Online Ads." *Wired.com*, November 3, 2017. <https://www.wired.com/story/how-russia-pushed-our-buttons-with-fake-online-ads/>.
- United States of America v. Internet Research Agency LLC, Concord Management and Consulting LLC, Concord Catering, et al, 18 U.S.C. §§ 2, 371, 1349, 1028A (2018). <https://www.justice.gov/file/1035477/download>.
- US Congress. House of Representatives. *H.R.4036: Active Cyber Defense Certainty Act*. 115th Cong., 2017. <https://www.congress.gov/115/bills/hr4036/BILLS-115hr4036ih.pdf>.
- US Department of Defense. *Dictionary of Military and Associated Terms*. JP1-02. Washington, DC: US Department of Defense, February 15, 2016. https://fas.org/irp/doddir/dod/jp1_02.pdf.

Valeriano, Brandon and Ryan Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press, 2015.

Valeriano, Brandon, Ryan C. Maness, and Benjamin Jensen. *Cyber Strategy*. Forthcoming.

Ventre, Daniel. "French Perspectives on Cyber-conflict." In *Cyber Conflict: Competing National Perspectives*. Edited by Daniel Ventre. Hoboken, NJ: John Wiley & Sons, Inc, 2012.

Winther, Mark. *Tier 1 ISPs: What They Are And Why They Are Important*. Framingham, MA: International Data Corporation, 2006.

Wolff, Josephine. "Making A New Pipeline: How Israel is Training Teenagers from Underrepresented Groups to Work on Cybersecurity." *Slate.com*, July 6, 2016.
http://www.slate.com/articles/technology/future_tense/2016/07/israel_s_magshimim_program_trains_teenagers_to_work_on_cybersecurity.html.

Yuen, Derek M.C. *Deciphering Sun Tzu: How to Read the Art of War*. New York: Oxford University Press, 2014.