RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

RSIS WORKING PAPER

***The RSIS Working Paper series** presents papers in a preliminary form and serves to stimulate comment and discussion. The views expressed in this publication are entirely those of the author(s), and do not represent the official position of RSIS. This publication may be reproduced electronically or in print with prior written permission obtained from RSIS and due credit given to the author(s) and RSIS. Please email RSISPublications@ntu.edu.sg for further editorial queries.*

NO. 309

CYBER DETERRENCE IN SINGAPORE

FRAMEWORK & RECOMMENDATIONS

EUGENE EG TAN

**S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
SINGAPORE**

2 APRIL 2018

About the S. Rajaratnam School of International Studies

The S. Rajaratnam School of International Studies (RSIS) was officially inaugurated on 1 January 2007. Prior to this, it was known as the Institute of Defence and Strategic Studies (IDSS), which was established 10 years earlier, on 30 July 1996, by Dr Tony Tan Keng Yam, then Deputy Prime Minister and Minister for Defence. Dr Tony Tan later became the elected seventh President of the Republic of Singapore. Like its predecessor, RSIS was established as an autonomous entity within Nanyang Technological University (NTU). RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. To accomplish this mission, it will:

- Provide a rigorous professional graduate education with a strong practical emphasis
- Conduct policy-relevant research in defence, national security, international relations, strategic studies and diplomacy
- Foster a global network of like-minded professional schools

Graduate Programmes

RSIS offers a challenging graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The Master of Science degree programmes in Strategic Studies, International Relations, Asian Studies, and International Political Economy are distinguished by their focus on the Asia Pacific, the professional practice of international affairs, and the cultivation of academic depth. Thus far, students from 66 countries have successfully completed one of these programmes. In 2010, a Double Masters Programme with Warwick University was also launched, with students required to spend the first year at Warwick and the second year at RSIS.

A select Doctor of Philosophy programme caters to advanced students who are supervised by senior faculty members with matching interests.

Research

Research takes place within RSIS' five components: the Institute of Defence and Strategic Studies (IDSS, 1996), the International Centre for Political Violence and Terrorism Research (ICPVTR, 2004), the Centre of Excellence for National Security (CENS, 2006), the Centre for Non-Traditional Security Studies (NTS Centre, 2008); and the Centre for Multilateralism Studies (CMS, 2011). Research is also conducted in the Studies in Inter-Religious Relations in Plural Societies (SRP, 2014) Programme, the National Security Studies Programme (NSSP, 2016), and the Science and Technology Studies Programme (STSP, 2017). Additionally, within the Office of the Executive Deputy Chairman, the Policy Studies group identifies new emerging trends of concern in the broad national security domain that may then be gradually incubated to form new policy-relevant RSIS research programmes. The focus of research in RSIS is on issues relating to the security and stability of the Asia Pacific region and their implications for Singapore and other countries in the region.

The School has four endowed professorships that bring distinguished scholars and practitioners to teach and to conduct research at the school. They are the S. Rajaratnam Professorship in Strategic Studies; the Ngee Ann Kongsi Professorship in International Relations; the NTUC Professorship in International Economic Relations; and the Peter Lim Professorship in Peace Studies.

International Collaboration

Collaboration with other professional schools of international affairs to form a global network of excellence is a RSIS priority. RSIS maintains links with other like-minded schools so as to enrich its research and teaching activities as well as learn from the best practices of successful schools.

Abstract

As a small state, Singapore’s ability to create deterrence against cyberattacks is very limited. There is limited value in pursuing classic deterrence through denial and punishment because: (i) technology is relatively cheap and widely available; (ii) there is difficulty in accurately attributing blame; and (iii) there is difficulty in identifying and punishing attackers. If there is no detection or ability to punish, Singapore’s credibility suffers.

The report suggests six ways that Singapore can improve its cyberattack deterrence:

1. Develop a response mechanism to guide deterrence
2. Create resilient systems
3. Share collective responsibility in cybersecurity
4. Increase capabilities through the improvement of penetration detection
5. Create norms with enforcement capabilities
6. Strengthen international law enforcement, cooperation, and legislation

It is also not feasible to measure deterrence in cyberspace the same way as nuclear deterrence, where a no-attack scenario denotes that deterrence is successful. Rather, deterrence should be seen as a mitigating effort that leads potential attackers to believe it is not in their best interest to attack. These efforts at deterrence can be further enhanced by improving the accuracy of attribution, the detection of cyber incidents regardless of size, and ensuring that timely action is taken against cyberattackers.

****

Eugene EG Tan is an Associate Research Fellow specialising in cyberspace security issues, Singapore’s foreign policy, and aviation issues. He previously taught various international relations and comparative politics modules, including International Politics of Southeast Asia, European Politics, South Asia Politics and Singapore’s Foreign Policy, at the National University of Singapore, Department of Political Science. Eugene reserves a keen interest in aviation issues and state behaviour in international affairs, stemming from his research done for his Masters and PGDipArts theses done at the University of Otago, New Zealand. Currently, Eugene is working on research projects covering cybersecurity and state behaviour in cyberspace.

Introduction

As the frequency and intensity of cyberattacks increase, states and businesses are increasingly looking for ways to reduce the volume and lessen the impact of cyber incidents. According to Symantec's "Internet Security Threat Report", there were 431 million new malware variants added in 2015 – a 36 per cent increase from the previous year. Ransomware incidents, mobile phone vulnerabilities, web attacks, and zero-day vulnerabilities also increased year-on-year at an alarming rate.[1]

The constant attacks and probing by hackers and malware developers increase the stress and strain on states. States and companies need a broad strategy to prevent cyberattacks on their systems. Increasingly, they are looking to deterrence as a means of curbing the number of low-level attacks on critical systems, allowing the cyber defence capacity and capabilities that have been established be used against major attacks.

Deterrence is traditionally a cold war doctrine employed by military strategists to prevent the proliferation of nuclear arms among states.[2] The cyber realm is organised differently; other than bringing concerns to both military and civilian populations, it is accessed by many users on different platforms, and most importantly, there is the presence of non-state actors. Cyberspace deterrence is thus not limited to relationships between states, but has expanded to incorporate the malicious activity of non-state actors as well. With the proliferation of computers and computing knowledge, cyberattacks can be undertaken by almost anyone or any group, with or without state affiliation.

Cyberspace is multidimensional, and involves both public and private entities. The infrastructure in cyberspace is partially owned by private interests, meaning that governments do not have the same level of control as they have in the physical space.[3]

There is therefore a need to look at the objectives of state and non-state actors in committing cyberattacks. State-sponsored objectives could include espionage and military conflict,[4] industrial and economic espionage, intelligence, information operations, and disruptive operations on other states.

[1] Symantec, "Internet Security Threat Report, Symantec, Volume 21," 2016.

[2] The definition of deterrence refers to the development of defensive and offensive capabilities that will discourage a state's enemies from attacking it. Classical military theory maintains that deterrence is created when one side intimidates the other to the point that it avoids reverting to armed force, realizing that the likely costs of this move would far exceed its anticipated gains.
Gil Baram, "Israeli Defense in the Age of Cyber War", *Middle East Quarterly,* Winter 2017 http://www.meforum.org/6399/israeli-defense-in-the-age-of-cyber-war#.WFensTExXws.gmail ; Austin Long, *Deterrence: From Cold War to Long War: Lessons from Six Decades of RAND Deterrence research,* Santa Monica, CA: RAND, 2008

[3] Jessica R. Gross, "Hack and Be Hacked: a framework for the United States to respond to non-state actors in cyberspace," in *California Western International Law Journal*, Vol 46, No 2, 2016.

[4] David J. Lonsdale, "Britain's Emerging Cyber-Strategy," in *The RUSI Journal*, Vol 161, No 4, 2016.; Brantly, Aaron F."Aesop's wolves: the deceptive appearance of espionage and attacks in cyberspace," in *Intelligence and National Security*, 31:5, 2016.

Currently, normative behaviour among states has yet to be fully defined even after years of negotiations at the United Nations and other forums.

Non-state objectives can include hobby hacking, general mischief, financial gain through fraud or theft (cybercrime), and vigilante justice (hacktivism). The need for harsher and more active law enforcement in cyberspace is required to curb the actions of these non-state actors and will be discussed further in the report.

The efforts needed to deter these different groups in cyberspace are manifestly different from those prescribed in nuclear deterrence. The use of the same framework as nuclear deterrence is insufficient and a new form of deterrence encompassing denial, punishment, norms and capacity building, and international cooperation needs to be envisioned. Normative understanding of deterrence deals largely with state actors and how they can be dissuaded from pursing actions that are detrimental to another state’s security. Thus, the means to deter non-state and state actors are also very different, and the concept of cyber deterrence needs to expand beyond the current understanding. Nevertheless, the study of classic deterrence theory still provides a framework to understand and explore the new field of cyber deterrence.

This report seeks to explain the nuances of deterrence theory and how the theory can be evolved into a model operational for cyberspace, and calls for a calibrated approach towards the development of deterrence strategy in cyberspace. Case studies will be used to illustrate how deterrence can take place, unwittingly or otherwise. Further, this report will explore the feasibility of Singapore adopting deterrence as part of its cyberspace strategy, and provide recommendations to develop deterrence in cyberspace. A strategic framework for Singapore’s cyber policy can then be fleshed out to incorporate elements of deterrence.

Classic Approach to Deterrence in Cyberspace

Deterrence as a concept is not new, and its roots can be traced back to Thucydides and the Peloponnesian War.[5] In the modern era, deterrence has been applied with varying levels of success in many fields including nuclear, space, ballistic missiles, conventional build-up of military means, and even contemporary security issues like terrorism.[6] With the increasing incidence and magnitude of cyberattacks, there is a growing interest by both academics and policymakers in applying the concept of deterrence to cyberspace.

[5] “Thucydides is the first person to frame deterrence and compellence as a strategic interaction problem and to emphasize the determining importance of motives for the strategic calculus of actors. His analysis has important implications for contemporary conflict management.” Richard Ned Lebow, “Thucydides and Deterrence”, *Security Studies,* Vol. 16 No. 2 (2007); Austin Long, *Deterrence: From Cold War to Long War: Lessons from Six Decades of RAND Deterrence research,* Santa Monica, CA: RAND, 2008.

[6] Paul K. Davis and Brian M. Jenkins, “Deterrence and Influence in Counter-Terrorism: A component in the war on al-Qaeda,” Santa Monica, CA: RAND, 2002.

Deterrence, according to Jervis, is largely a rational attempt to understand what can be seen as a psychological relationship with an adversarial state.[7] Studies have shown that the effect deterrence has on state is abstract and cannot be quantified or qualified. Thus, how states behave in a given scenario may vary according to circumstance, such as the state doing the deterring and the fundamental relationship between states.

There is a need to look at deterrence holistically rather than solely from a military perspective because one of the unique features of cyberspace today is the dual-use (military and civilian) nature of technology. The indistinguishability of offensive capabilities from the defensive nature of cyber tools used for penetration testing has become a serious problem, pushing states to reevaluate the capabilities they should employ. Military tools can also be now used by civilians and vice versa.[8]

Deterrence often implies a degree of threat from both sides, with each party in the conflict possessing adequate capability to harm the other. For it to work, there should be a credible threat from a willing attacker and the willingness of the prospective victim to retaliate against the said attacker.[9]

There is much debate by academics over what constitutes deterrence both in and outside cyberspace. Most thinkers like Geers and Glaser limit the discourse of deterrence in cyberspace to the classical interpretation of deterrence through denial and the threat of punishment.[10] Some scholars like Nye however extend the concept of deterrence to the development of norms and the creation of interdependence among states in cyberspace.[11] Recent thinking has also extended the discourse to include deterrence by futility, which is to deter would-be attackers by minimising the effects of a cyberattack.The flaw of deterrence is that it does not offer advice on how to avoid crises, or how to decide whether the national interests at stake are sufficient to warrant the use of military force. Accordingly, deterrence remains in the cognitive domain, and is essentially an influence operation shaped by the interplay of credibility, capability, and communication.

Deterrence by denial

Deterrence by denial is a strategy whereby enemies are physically prevented from obtaining technology that can threaten the existence of the state. Comparing cyber to nuclear deterrence,

[7] Robert Jervis, "Introduction: Approach and Assumptions," in *Psychology & Deterrence*, by Robert Jervis, Richard Ned Lebow, and Janice Gross Stein (eds.), Baltimore, Maryland: Johns Hopkins University Press, 1985.

[8] Management Association, Information Resources, *Violence and Society: Breakthroughs in Research and Practice*, IGI Global, 2016.

[9] Patrick M. Morgan, "Saving face for the sake of deterrence," in *Psychology & Deterrence,* by Robert Jervis, Richard Ned Lebow, and Janice Gross Stein (eds.), Baltimore, Maryland: Johns Hopkins University Press, 1985.

[10] Charles L. Glaser, "Deterrence of Cyber Attacks and U.S. National Security", *Report GW-CSPRI-2011-5,* Washington, D.C.:The George Washington University Cyber Security Policy and Research Institute, June 1, 2011; Kenneth Geers, "The Challenge of Cyber Attack Deterrence," in, Computer Law & Security Review, Vol 26, 2010.

[11] Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace", *International Security*, Vol. 41, No. 3 (Winter 2016/17)

Geers explained that successful deterrence by denial must meet three criteria: capability, credibility, and communication.**[12]**

Capability

Capability refers to the ability to procure materiel, capacity, and the means of conducting a successful attack on a given state.

There have been documented cases where states undertake military action against another state to physically destroy their nascent nuclear infrastructure.[13] The cost, time needed, and lack of political will may deter some states from rebuilding a clandestine nuclear programme. Through the active denial of capabilities acquisition, the adversary is thus deterred against pursuing nuclear power.

The cyber equivalent of deterrence by denial would be the wholesale destruction of both the state's computing hardware and software in cases where any possession of computing power by a potential adversary may be a threat. As observed above, this scenario is highly unadvisable because the technology could be used for benign operations in peacetime such as the management of health records or the streamlining of government processes. The destruction of a state's computer infrastructure for "deterrence" would exceed the mandate that deterrence by denial confers because of the potential harm to civilians.

The same technology may also be used to carry out espionage activity, because cyberspace is much more expedient as compared to the traditional trawling of information from physical filing cabinets.[14] As espionage is not prohibited in international law,[15] states seeking to use cyber tools to conduct such activities cannot be legally denied because there is no such provision against them.[16] Theoretically,

[12] Kenneth Geers, "The Challenge of Cyber Attack Deterrence," in *Computer Law & Security Review,* Vol 26, 2010.

[13] Israel carried out a pre-emptive strike on Iraq's Osirak nuclear power plant in June 1981, despite expert opinion that the production of plutonium and uranium is not viable at the plant. The reactor was also safeguarded by IAEA. There was also sabotage in France, where the nuclear fuel was supposed to be sent. See Whitney Raas and Austin Long, "Osirak Redux? Assessing Israeli Capabilities to Destroy Iranian Nuclear Facilities." In *International Security,* Vol 31, No 4, 2007.

[14] Jessica R. Gross, "Hack and Be Hacked: a framework for the United States to respond to non-state actors in cyberspace," in *California Western International Law Journal*, Vol 46, No 2, (Spring 2016).

[15] Espionage is traditionally seen to be a passive tool to support policy rather than pursue it, with no physical alteration to the status quo. Espionage largely contributes toward intelligence gathering rather than an act of war itself, and is therefore tolerated both in the cyber and non-cyber contexts. Interstate military conflict in cyberspace should hence be considered as a higher set of state activity separate from espionage. These activities can include joint operations with the arms of the military, offensive preparation of the battlespace, and offensive takedown of other states' critical infrastructures in times of peace.
The relationship between espionage and conflict is especially complex in the nebulous world of cyberspace. The difference between espionage and conflict is basically a difference in the will and intent of the attacker, which makes it difficult for states to formulate a coherent cybersecurity strategy. (Lonsdale, "Britain's Emerging Cyber-Strategy") The tools used for espionage activity can easily be used to alter the information found on the system, which can be considered an act of war. Singapore will need to think about how it will react should another state actor undertake any action against it in cyberspace, or how it can use cyberspace as a tool of espionage if the need arises.

[16] Ibid.

Singapore is free to conduct espionage on other states, which is widely seen as a globally accepted norm.

In order to deny a state the ability to procure materiel, capacity, and the means of conducting a successful attack, the defending state must be able to verify the presence of such dangerous materiel or prove the development of offensive capability. But because cyber tools are non-physical, defending states will have difficulty conducting verification on capability belonging to potential attacking states. How can a state deny capability that it does not even know exists? And even if they can see the code, how do they prove the code is malicious given that it has not been executed?

For example, no one could have seen the Stuxnet worm crawling towards Iran, or to even detect it, when it struck the systems controlling the nuclear centrifuges.[17] Effectively, the Iranians had no way of denying their attackers this capability.

This is unlike verification of nuclear weapons which can be done physically. To facilitate verification regimes also requires one state to facilitate these verification efforts by another state.[18] However, the non-physical and non-quantifiable nature of cyber tools makes verification almost impossible.

There are two more factors that will critically hinder any effort at creating a cyber verification regime. First, cyberattacks are primarily based on vulnerabilities found in computer codes. If the defending state does not know what its vulnerabilities are, it would not be able to verify if a cyber tool is dangerous or not. Second, no prospective attacker would want to disclose their cyber weapons for verification because the act of disclosure would enable the defending state to find a defence and render the weapons useless.

Credibility

Credibility is the attribute of being believed – the prospective attacking state must believe that the defending state is capable of inflicting damage, and at the same time, committed through its political will to use that capability.

No state can credibly claim they can deny all sources of cyberattacks. The widespread proliferation of computing devices would require a herculean effort by a state to eradicate all possible sources of cyberattacks. The ease and low cost of procuring computers, servers, and software on the dark net by persons of any age and nationality mean that potentially anyone with a computer can conduct a

[17] Stuxnet is a malicious computer worm that targets industrial computer systems and was responsible for causing substantial damage to Iran's nuclear program in 2010.

[18] Herbert Jr. Scoville, “Verification of Nuclear Arms Limitations: An Analysis,” in *Bulletin of the Atomic Scientists,* Vol 26, Iss 8, (Oct 1970).

cyberattack. Hackers can be armed with as little as a personal laptop, be as young as 15 years old, and be anywhere in the world.[19]

Communication

Deterrence by denial also requires that the threatened costs be communicated clearly to the prospective attacking state.[20] This can be achieved through the communication of repercussions that states or individual actors may face should they be found in contravention to what was agreed to by international treaties, laws, or mutually agreed norms.

In the case of Iran's nuclear crisis, its obligations and potential sanctions were clearly communicated in the Nuclear Non-Proliferation Treaty that it signed. This enabled sanctions to be placed on them when they failed to comply, and was only lifted when they agreed to reduce their holdings of nuclear fuel and have a verification regime set up to prevent them from reneging on their commitments.[21]

Transposing this to the cyber domain, it is beneficial to have international treaties, laws, or mutually agreed norms.

Deterrence by punishment

Punishment as a mode of deterrence is similarly a classic way to discourage undesirable behaviour. However, there needs to be clarification that deterrence by punishment is seen as a strategy of last resort, rather than an immediate go-to policy.

Diplomacy, information, military, economic, financial, intelligence and, law enforcement

States can theorise about reacting to cyber incidents through the Diplomacy, Information, Military, Economic, Financial, Intelligence and, Law Enforcement (DIMEFIL) model. **[22]** There is a full spectrum of punishments that can be undertaken, including economic sanctions, diplomatic protests, and show of military force.

Using law enforcement as an example, five Chinese military officers were charged *in absentia* with cyber espionage against American corporations for commercial advantage in 2014.[23] Subsequently,

[19] One of the individuals arrested in the TalkTalk cyberattacks in October 2015 was a 15 year-old boy from Co Antrim, Northern Ireland. Another was a 16 year-old boy from Norwich. See "Boy, 16, bailed over TalkTalk hacking attack", *BBC News*, November 4, 2015, http://www.bbc.com/news/uk-34717572.

[20] R.J. Harknett, "The Logic of Conventional Deterrence and the End of the Cold War," in *Security Studies*, Vol 4, No 1, 1994.

[21] "Iran Nuclear Crisis: Six key points," *BBC News*, July 14, 2015, http://www.bbc.com/news/world-middle-east-32114862.

[22] Jelle van Haaster, "Assessing Cyber Power," in *8th International Conference on Cyber Conflict: Cyber Power*, by Pissanidis, Nicolaos, et al (eds.), Tallinn, Estonia: NATO CCDCOE, 2016.

[23] Department of Justice, United States, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014,

China and the US (and later the UK) came to an agreement not to engage in economically driven espionage.[24]

Geers noted that policymakers have to decide on a response that meets both the deterrent objective and the level of proportionality to the initial attack. The decision to respond in kind to a cyberattack or to create a kinetic response through the use of conventional weapon systems must be made carefully. Geers warned that while a cyber response may seem logical, it can exceed the level of proportionality and may lack the precision of conventional weapons.[25]

Proportionality in punishment

The US has demonstrated proportionality in its response to several major cyberattacks which have been attributed to state actors. In the case of the 2014 cyber espionage, although the act was committed by military officers, the hacking activity was not seen to require state-on-state economic sanctions, and criminal charges were pressed instead.

Adequate thought to formulate a proportional response should be given because it is a delicate exercise that may lead to escalation if not handled properly. To this end, there are three variables that policymakers should consider before developing a response:

i. States must gauge the level of confidence they have in their capability to attribute a case.[26] Forensics is not perfect and if there is a lack of concrete evidence, policymakers may be hard-pressed to initiate retaliatory action even if the cybersecurity incident was serious.

ii. States must assess the damage done by the cyberattack. Damages done include the destruction of physical infrastructure, the cost to the economy, the destabilising of society, and the harm done to national interests. For example, while North Korea's cyberattack on Sony caused a loss of data and reputation, there was no physical destruction of infrastructure. Hence, no punishment was initiated at that stage.

https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[24] Matthew Dahl, "Agreements on Commercial Cyber Espionage: An Emerging Norm?" *Lawfare*, December 4, 2015.

[25] Ibid. p. 301

[26] A strategy of punishment is difficult to execute, mainly because of the anonymity that is afforded to actors in cyberspace. Anonymity can be seen as the "cornerstone of internet culture". The identity of users can often be masked though a variety of ways, such as the use of software like Tor or "spoofing" another person's IP address. This complicates efforts to track where the attacks come from in the first place, and complicates attribution efforts in both for law enforcement purposes and state-on-state activity. The difficulty in accurately ascertaining the source of the attack means that attackers could plausibly deny any responsibility for the attack, citing reasons that they could be part of a 'false-flag' operation, or even claim that their computer has been unlawfully used to conduct an attack (Geers, "The Challenge of Cyber Attack Deterrence").

iii. States must consider all the responses available. These responses do not have to be cyber in nature, and can range from a simple diplomatic rebuke to complex economic sanctions or in severe cases, military action. Policymakers should remember that these punishments, if undertaken, do have escalatory risks of their own.[27] These risks can include retaliatory sanctions, military actions, and the withdrawal from international agreements.

Former US officials reportedly said that the White House had sought to undertake covert cyber operations against Russia before, but ultimately abandoned the idea of action because these plans were not thought to be particularly effective. Scholars like Jason Healey also pointed out that retaliatory action is technically illegal under the United Nations (UN) charter and may lead to an escalation of hostilities between the US and Russia. Hence, there may be a limit to the operations the US can carry out without the risk of escalation.[28]

International law also prohibits the excessive use of force to deter future attacks. Feakin noted that some states might respond disproportionately to send a clear signal and deter future cyberattacks.[29] However international law compels states to react in a way that is necessary and proportionate to repel or defeat a cyberattack, and in a manner that the scale, scope, duration, and intensity of the retaliatory action are justifiable. Feakin also added that by acting proportionally, a state may find it easier to build coalitions to address the hostile behaviour of the offending state, as well as limiting the possible escalation of the incident.

In the context of Singapore, the state needs to be careful with its response because any disproportionate reaction to a cyberattack, resulting in escalation by the attacker, could be potentially catastrophic given the vulnerability of the nation’s economy, infrastructure, and physical size.

Redlines in cyberspace

Some academics have proposed using redlines in cyberspace to signal the response mechanisms a state may undertake should it be the target of a cyberattack. For example, attackers conducting denial-of-service attacks may face diplomatic démarche or have their behaviour exposed through the media. This sends a warning to future attackers on the consequences that they may face should they choose to act in an aggressive and hostile manner.

Governments will likely come under increasing pressure to react decisively to cyberattacks, and it is suggested that they develop a framework for response so policymakers have a point of reference. For example, US officials have suggested that punishment could include wide-ranging covert cyber

[27] Tobias Feakin, “Developing a Proportionate Response to a Cyber Incident,” Council on Foreign Relations, http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927.

[28] Ibid.

[29] Ibid.

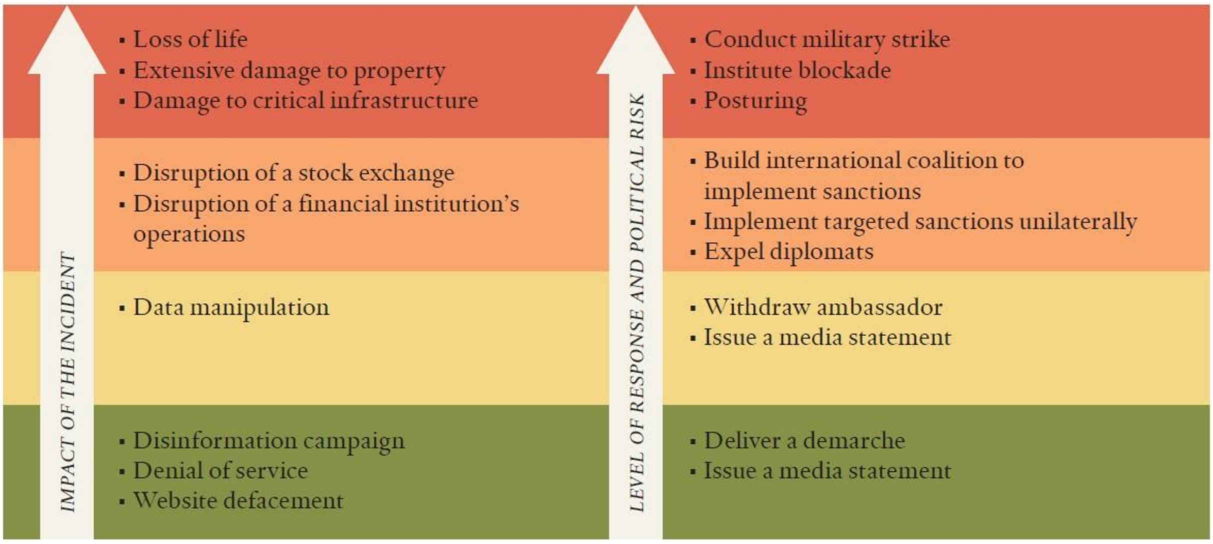
operations devised to distress and rattle the Russian leadership, or more traditional methods such as trade sanctions in response to the perceived election meddling.

In Feakin's brief to the Council on Foreign Relations,[30] he outlined a model (Fig. 1), to show the impact to society and the options available to policymakers.

The model also addresses the issue of proportionality raised earlier in the chapter. He observed that proportionality in international relations is not solely a matter of scale, but borne out of state practice. An example of this state practice can be seen in the escalatory cycle of sanctions. The US had placed sanctions on Russia for annexing Crimea. Russia, in retaliation, also placed sanctions on the former.[31] Feakin said that this logic of tit-for-tat sanctioning should also be applied to cyberspace and such outcomes should be expected when hostilities escalate.

Another example of what kind of redlines will trigger a reaction can be seen in the Sony hacks. Punishment against North Korea, the alleged perpetrator, was only implemented when threats to carry out 9/11 style attacks on movie theatres were made. This crossed a red line which was unacceptable to the US government, as it undermined its constitutional right to freedom of expression. Not defending this right would cause reputational damage to the US from both outside and within.[32]

Figure 1: Policy Responses to Escalating State-Sponsored Cyber Incidents



IMPACT OF THE INCIDENT	LEVEL OF RESPONSE AND POLITICAL RISK
▪ Loss of life ▪ Extensive damage to property ▪ Damage to critical infrastructure	▪ Conduct military strike ▪ Institute blockade ▪ Posturing
▪ Disruption of a stock exchange ▪ Disruption of a financial institution's operations	▪ Build international coalition to implement sanctions ▪ Implement targeted sanctions unilaterally ▪ Expel diplomats
▪ Data manipulation	▪ Withdraw ambassador ▪ Issue a media statement
▪ Disinformation campaign ▪ Denial of service ▪ Website defacement	▪ Deliver a demarche ▪ Issue a media statement

Source: Tobias Feakin, *Developing a Proportionate Response to a Cyber Incident*, Council on Foreign Relations Press, 2015.

[30] Ibid.

[31] "Sanctions tit-for-tat: Moscow strikes back against US officials," *Russia Today*, March 20, 2014, https://www.rt.com/news/foreign-ministry-russia-sanctions-133/.

[32] "Obama imposes new sanctions against North Korea in response to Sony hack," *The Guardian*, January 2, 2015. https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview

Feakin acknowledged that this model addresses mainly interstate activity, but commented that law enforcement responses are better for disruptive or destructive activity. He suggested that states should consider formulating policy responses for private sector incursions first, before developing one for interstate relations.

This is crucially so for the critical infrastructure not under the control of the state. A key point to consider in relation to creating a response is the criminality of a cyberattack on critical infrastructure. Will the state see the cyberattack as a criminal matter or a diplomatic/ political one? For example, Ukraine took little action when their power grids were cyberattacked in December 2015. The attack was thought to have originated from Russia. While power was eventually restored by manually staffing electrical substations,[33] there was no retaliation due to a lack of attribution which ultimately limited the response mechanisms of the Ukrainian government. This non-response may have affected the credibility of Ukraine in deterring cyberattacks. In addition, it could also have casted doubts on the ability of the Ukrainian state to provide an adequate response to a cyberattack.

There is a critical need for Singapore to think about how it would react should there be a cybersecurity breach anywhere in the system. This response should be made to help policymakers achieve the maximum possible deterrent to both state and non-state actors in any given situation. It should be updated frequently, based on changing variables of harm done to the system, the intelligence gathering mechanisms, and the tools at the state's disposal.

Credibility in punishment

If states are using the threat of punishment as a means of deterrence, they first need to ensure that this threat is credible. There has been increasing rhetoric worldwide over the possession of offensive cyber weapons, with states choosing to declare that they own such weapons as a form of deterrence. Countries like the US, the UK, and Australia have already affirmed that they will use these weapons in retaliation if cyberattacked, reacting in the same way if a physical attack was upon them.[34]

While Singapore has spoken much on promoting cybersecurity, it has so far refrained from threatening retaliation for attacks. Singapore has limitations in its credibility for punishing state-sponsored perpetrators. The reality is Singapore has physical vulnerabilities and constraints. Hypothetically, if a large state carried out a cyberattack, Singapore would be hard pressed to impose economic sanctions, or to show military or cyber might. At best, Singapore could raise diplomatic protests.

[33] Kim Zetter, "Everything We Know About Ukraine's Power Plant Hack," *Wired*, January 20, 2016. https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.

[34] US Cyber Command, Beyond the build: delivering outcomes through cyberspace, June 3, 2015; George Osborne MP, "Chancellor's speech to GCHQ on cyber security", November 17, 2015; UK Government, National Security Strategy and Strategic Defence and Security Review 2015: a secure and prosperous United Kingdom, November 23, 2015; US Department of Defense, The DoD Cyber Strategy, April 2015.

Rhetoric in cyber action may have a level of deterrence through the perceived capability of states, but there must be actualisation of this rhetoric after calling out a perpetrator in order to maintain the credibility of this deterrence. One example being how the US turned words into action when it was discovered Russia cyberattacked their Democratic National Convention servers. After former US Vice President Joe Biden confirmed that the US will be "sending a message" to Russian President Vladimir Putin at "a time of our choosing, and under the circumstances that will have the greatest impact", 35 Russian diplomats were expelled.[35]

The former US National Intelligence Officer for Cyber Issues, Sean Kanuck, commented during his visit to Singapore that the US, having officially blamed the Russians for interfering in the election, could not stand aside and do nothing.[36] According to him, this would set a bad precedent in terms of both the credibility of the threat of retaliation, and the credibility of cyber capability.[37]

The visibility of sanctions and criminal indictments may explain why the responses the US has been undertaking thus far have been in the physical rather than virtual realm. There is a need for the effects of the punishment to be made visible to the public to create third party deterrence. Punishment via cyber capabilities often lack the visibility needed to build a credible declaratory policy, which makes the declaration less credible because other states do not see the punishment being meted out.

There is a clear need to communicate to the rest of the world that the punishment has been done. Deterrence is highly dependent on both a state's ability to deliver the threatened punishment and their will to do so, so failure to do so will harm this posture.

States should also be aware that there may be a risk of escalation if cyber deterrence policy is based on a series of hard and fast redlines.[38]

Credibility-stability paradox

On the other hand, should a victim state backtrack on its threat of action, it may face a credibility-stability paradox (see Annex A) that could harm its reputation because of the given impression that the victim does not actually have the capability to react to its attacker.

[35] "Obama expels 35 Russian diplomats in retaliation for US election hacking," *The Guardian,* December 30, 2016, https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack.

[36] The former United States National Intelligence Officer for Cyber Issues, Sean Kanuck, visited Singapore at the invitation of the Centre of Excellence for National Security (CENS). Kanuck gave three seminars during his visit to Singapore: 1) "Global Information Risk: From Insecurity to Insurance"; 2) "Is Strategic Deterrence Possible in Cyberspace?; and, 3) "Technical, Legal, and Philosophical Issues in the New Digital World Order".

[37] "CIA Prepping for Possible Cyber Strike Against Russia," *NBC News*, October 14, 2016, http://www.nbcnews.com/news/us-news/cia-prepping-possible-cyber-strike-against-russia-n666636.

[38] Liam Nevill and Zoe Hawkins, "Deterrence in Cyberspace: Different domain, different rules," Canberra, Australia: Australian Strategic Policy Institute, 2016, https://www.aspi.org.au/publications/deterrence-in-cyberspace-different-domain,-different-rules/SR92_deterrence_cyberspace.pdf

Having this escalatory cycle in cyberspace would have a detrimental impact on interstate stability in the long term. The unique characteristics of cyberspace already contribute widely to the view that it is an offence-dominant domain, which naturally benefits attackers.[39] Defence is seen to be the more difficult strategy to pursue because of the perceived difficulties in detecting and addressing network vulnerabilities, compounded by the perceived strategic gain by proactively developing targeted cyber weapons that cannot be readily detected. This has generated the view that the initiation of an attack is "cheaper and easier" than to conduct robust defence on own networks.[40]

As a result, this could promote the "cult of the cyber offensive" – a cycle of unintended escalations increasing the appeal of the first-strike advantage and encouraging pre-emptive cyber offences.[41]

In saying this, it does not mean that states should not pursue offensive or even second strike capabilities. It however shows that these capabilities should not be used as a threat mechanism for fear of escalation and fermenting distrust.

Punishment for non-state actors

Cobb commented that deterring cybercrime is about making crime less appealing through reducing the benefit to the attacker, increasing the risk, and creating social disdain for such activities. Criminals can be deterred if the benefits from cybercrime are reduced. Risks can be increased through more active enforcement of the law, harsher punishments, and increasing the propensity of getting caught. A code of cyber ethics can also be introduced to promote societal rejection of cybercrime.[42] Hacktivists and casual hackers can be similarly deterred by these factors. In most jurisdictions and in Singapore specifically, any cybersecurity breaches including unauthorised access, alteration, or interruption of services, would amount to cybercrime offences.

> **Reducing the benefits of cybercrime** – When systems are more robust and difficult to penetrate, the costs of conducting a successful attack increase and the benefits of cybercrime reduce.
>
> **Increasing the risks of cybercrime** – There is a need to increase the probability of punishment to deter would-be criminals.[43] The law must be enforced in a timely fashion; cyber attackers must be detected, apprehended, and dealt with promptly. However, most attacks go unnoticed because of the difficulty of detecting malicious events. Punishment for cybercrime

[39] Ibid p. 13.

[40] Jan van Tol, Mark Gunzinger, Andrew Krepinevich, and Jim Thomas. *AirSea Battle.* Centre for Strategic and Budgetary Assessments, 2010.

[41] PW Singer and Allan Friedman, "Cult of the cyber offensive: why belief in first-strike advantage is as misguided today as it was in 1914," *Foreign Policy*, January 15, 2014.

[42] Stephen Cobb, "Cybercrime deterrence: 6 important steps," *WeLiveSecurity,* January 20, 2015, http://www.welivesecurity.com/2015/01/20/cybercrime-deterrence-6-important-steps/.

[43] S. N. Durlauf,and D. S. Nagin, "The Deterrent Effect of Imprisonment," in *Controlling Crime: Strategies and Tradeoffs,* by P. J. Cook, J. Ludwig, and J. McCrary (eds.), Chicago, IL: University of Chicago Press, 2011.

> is also not immediate enough, because it is difficult to identify and locate the attacker. It has been observed that cybercriminals find more value in launching low-intensity attacks at high frequencies, because these attacks may go unnoticed, and even if they were found, a single act may be deemed too minor for retributive punishment. These small acts can however snowball into bigger attacks in the long run.

Punishment for cybercrime should be carried out in a visible manner to achieve a deterrent effect on cybercriminals. For example, former News of the World editor Andy Coulson was found guilty of conspiracy to hack phones in a highly publicised trial, which also led to the closure of the tabloid in 2011. Similarly, the coverage of the hackers who attacked TalkTalk, a telecommunications group in the UK, is another example of publicly showing that laws in cyberspace are continually enforced and there are consequences if caught. The attacks, arrests, and trials are all well documented by the media, potentially creating a deterrent effect on non-state actors.[44]

In Singapore, James Raj Arokiasamy (also known as "the Messiah" hacker), was convicted in an equally public trial for hacking into the webservers of Fuji Xerox, the People's Action Party Community Foundation, Ang Mo Kio Town Council, and other government agencies such as the Prime Minister's Office, prisons, and the Ministry of Communications and Information. He was sentenced to almost five years in jail and the presiding judge, Jennifer Marie, commented that the stiff sentence was meant to act as a strong deterrent to would-be hackers, and underscored the point that cyberattacks can harm the country.[45]

International cooperation

Singapore has recognised in its national cybersecurity strategy the need to strengthen the enforcement of laws against cybercrime to increase the risks for criminals, as well as to increase international cooperation to combat the dislocation caused by cyberspace. This can be best seen in the case above where Arokiasamy was arrested by the Malaysian police to face charges in Singapore.[46] International cooperation is discussed in greater detail in the next part of this report.

[44] "Boy, 17, who hacked TalkTalk also targeted Cambridge and Manchester universities as he 'showed off'", *The Telegraph,* November 15, 2016, http://www.telegraph.co.uk/news/2016/11/15/boy-17-who-hacked-talktalk-also-targeted-cambridge-and-mancheste/.

[45] "Hacker 'Messiah' James Raj Arokiasamy pleads guilty to charges of computer misuse." *The Straits Times,* January 23, 2015, http://news.asiaone.com/news/singapore/singapore-hacker-dubbed-messiah-jailed-almost-5-years.

[46] Ibid.

Norms Development and International Cooperation as Deterrence

Norms for a stable international system

The stability among states in cyberspace is under pressure because of the lack of agreed norms of behaviour. It is thought that having norms in cyberspace will offer predictability, stability, and security to the international system. Facilitating cyber norms and jurisdiction exchanges is one of the pillars of Singapore's Cybersecurity Strategy.

Current position

In the absence of universally agreed norms, the strong do what they can, and the weak suffer what they must. Attacking states can get away with little or no accountability on what they have done in cyberspace. The only factor that may be restraining the magnitude of their activities is the risk of escalation and blowback towards their own infrastructure. This still does not mean that an "electronic Pearl Harbour" will never happen; the increasingly sophisticated cyber capabilities states now have mean they can be used both offensively and defensively.[47]

Desired position

The development of internationally agreed norms is increasingly seen as a part of every state's arsenal for deterrence. Establishing normative frameworks and building confidence in the mutual benefits of complying with agreements and norms of behaviour will help reduce the risk of cybersecurity incidents entering an escalatory spiral of punishment and counter-punishment.[48]

It is through these norms that states can be ordered to behave in an internationally accepted manner. If there is non-compliance, offenders will be rightly punished based upon the principles of proportionality and credibility, in turn discouraging the pursuit of retaliation.

Development trajectory

Work to develop agreed norms for cyberspace is underway at both global and regional levels, as well as between key actors, particularly the US, China, and Russia. Different sets of behavioural norms have been created by different international groups such as the United Nations Group of Governmental Experts (UN GGE) and the Shanghai Cooperation Organisation. Some of the proposed norms overlap, while others only address the interest of one group. There have been confidence-building measures from both regional organisations and private enterprises such as the Association of

[47] Lonsdale, "Britain's Emerging Cyber-Strategy"
[48] Nevill and Hawkins, Deterrence in Cyberspace.

Southeast Asian Nations Regional Forum, Organization for Security and Co-operation in Europe (OSCE), and Microsoft.[49] There are also efforts made by think tanks such as the NATO Cooperative Cyber Defence Centre of Excellence and the Red Cross to draft international laws compatible with cyberspace.[50]

So far, four seminal events regarding the creation of norms and limitations have happened between 2015 and 2016. The first was the UN GGE report published in July 2015, in which states reaffirmed that international law applied in cyberspace, but did not elaborate how it applied. There were also a series of other norms agreed at the UN GGE, like not attacking the computer emergency response team capabilities of another state. The second of these events was the norm of not conducting economic espionage that Chinese President Xi Jinping and former US President Barack Obama agreed upon in September 2015. This was later adopted in a joint statement by the G20 in November 2015, and what started off as a bilateral process has become a broadly accepted conduct. That was the third seminal event in the period. The fourth event was the confidence-building measures report published by the OSCE in March 2016. These events reflect the collective aspirational desires of the international community to build stability in cyberspace.

Singapore has similarly called for more international dialogue and for the development of such norms within ASEAN and the wider community. In the latest iteration of its cybersecurity strategy, Singapore sees it as a necessity for ensuring cybersecurity in the region.

Challenges

Establishing norms in cyberspace is not a straightforward process as the recent shift in global power politics means that reformist actors are emboldened to challenge existing international norms. The US' unipolar moment is giving way to a multipolar world, and that has serious implications for the survival of current international norms. China and Russia are both challenging accepted norms in political, military, and economic arenas, testing the limits of the status quo. The relative "newness" of cyberspace makes it more malleable than other traditional domains that have set legal and normative frameworks.

[49] Microsoft, International Cybersecurity Norms, Microsoft, 2015

[50] The NATO CCDCOE is responsible for the he Tallinn Manual on the International Law Applicable to Cyber Warfare, written at the invitation of the Centre by an independent 'International Group of Experts. The Tallinn Manual is the result of a three-year effort to examine how extant international legal norms apply to this 'new' form of warfare.

The Tallinn Manual pays particular attention to the jus ad bellum, the international law governing the resort to force by States as an instrument of their national policy, and the jus in bello, the international law regulating the conduct of armed conflict (also labelled the law of war, the law of armed conflict, or international humanitarian law). Related bodies of international law, such as the law of State responsibility, are dealt with in the context of these topics. The Tallinn Manual is not an official document, but instead an expression of the scholarly opinions of a group of independent experts acting solely in their personal capacity.

Another manual, colloquially known as Tallinn 2.0, will deal with cyberattacks that fall below the threshold of international conflict. Tallinn 2.0 was released in February 2017.

Stevens noted that a norms-based approach to cyber deterrence might engender deterrent effects at the state level, but is unlikely to work in the case of “rogue” states or on certain non-state actors.[51] For example, the norm of not attacking critical information infrastructure in peacetime would not be observed by non-state actors like the Islamic State and cybercriminals.

This norm was recommended by the UN GGE in 2015, and is part of a set of norms that were proposed to limit the behaviour of states. They are however non-binding in nature. As a consequence, some may choose not to heed these norms, especially states that were not consulted in the GGE process.

Recommendations

While an agreement on norms in cyberspace may still be far off, Singapore should articulate its position on cyberspace and make known the behaviour that it would not tolerate. There are a few informal processes that Singapore can contribute to, like the discussion on the applicability of the *Tallinn Manual* in times of conflict, and future discussions on the responses to incidents that do not fulfil the threshold of conflict.[52] There is also a need to consider the norms put forth by other organisations like the Shanghai Cooperation Organisation for these may align closer to what Singapore needs to protect its own interests.[53]

Norms for the protection of small states

Small states are typically insecure about their survival and have long been the victims of great power intervention. Small states also have little recourse to both cyber and physical forms of punishments, with the punishments being either ineffective due to scale, or the possibility of cutting off potential markets in the case of sanctions.

To ensure that the rights of small states are protected in cyberspace, a set of binding international norms or laws needs to be globally agreed upon. These norms should include the protection of critical infrastructure from malicious attacks, the sanctity of information within borders, the non-interference in the political processes of a state, and the illegality of economic espionage.

[51] Tim Stevens, “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace,” in *Contemporary Security Policy*, Vol 33, Iss 1, 2012.

[52] Michael Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge, UK: Cambridge University Press, 2017.

[53] UN General Assembly, “*Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General,* A/69/723,” https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

Small states like Singapore should speak up whenever large states interfere in the affairs of other small states, as this helps to support the norm of non-interference. For example, if Russia was found to have carried out cyberattacks on Estonia (see Annex B), then other small states need to protest the large state's intervention in the domestic politics of the victim.

A parallel can be seen with Singapore's maritime interests and the role it played in the formulation of the United Nations Convention on the Law of the Sea (UNCLOS). While UNCLOS has proven to be unenforceable at times, like the current South China Sea dispute between China and the Philippines,[54] these norms have given Singapore and the international community a reference point for acceptable behaviour and if there are disputes, an adjudication mechanism. There is thus a need for a punishment mechanism to be present should a state choose to damage another state's infrastructure, and this bar should be set high to deter these adversarial states from pursuing a policy that may be detrimental to the global community.

International cooperation in dealing with non-state actors

Benefits

To deter non-state actors there is a need to increase the level of cooperation with other states in the enforcement of laws. The need to step up international cooperation and engagement was highlighted in Singapore's National Cybercrime Action Plan.

One example of international cooperation can be seen in the case of the "Messiah hacker". The offender, James Raj Arokiasamy, carried out cyberattacks on Singapore servers from his apartment in Kuala Lumpur. Acting on information provided by their Singapore counterparts, the Malaysian police managed to arrest Arokiasamy in his apartment. He was then extradited to face charges in Singapore, charged, and sentenced to five years imprisonment.[55]

Another example of cooperation is the Singapore police working with foreign counterparts to crack down on cyber fraud syndicates targeting Singaporeans, such as the Alipay credit-for-sex scams. After arresting 43 people involved in the scams, the number of reported cases fell.[56]

[54] "Why is the South China Sea contentious?" *BBC News,* 12 July 2016, http://www.bbc.com/news/world-asia-pacific-13748349; "Vietnam Is Challenging China's Control Of The Disputed South China Sea," *Forbes,* November 28, 2016, http://www.forbes.com/sites/ralphjennings/2016/11/28/a-resilient-mini-me-rival-is-challenging-chinas-control-of-a-disputed-sea/#5c4040eb70f1.

[55] "Hacker 'Messiah' James Raj Arokiasamy pleads guilty to charges of computer misuse," *The Straits Times,* January 23, 2015, http://news.asiaone.com/news/singapore/singapore-hacker-dubbed-messiah-jailed-almost-5-years.

[56] "Commercial crimes, including credit-for-sex and Internet love scams, up 47% in 2015: Police," *The Straits Times*, February 12, 2016, http://www.straitstimes.com/singapore/courts-crime/overall-crime-in-singapore-up-by-4-in-2015-mainly-due-to-online-commercial.

Besides bilateral cooperation, there is deterrent value in participating in international treaties. A joint study by the Hong Kong University of Science and Technology, Yonsei University, and the Singapore Management University determined that states that have signed and ratified the Budapest Convention experienced a reduction in the number of distributed denial-of-service (DDoS) attacks in their territories.[57] This signifies that hackers that seek mischief could potentially be deterred if criminal punishment for undertaking malicious activity in or from another country is a stark possibility.

What can be done to promote deterrence is to enhance the level of cooperation with international law enforcement authorities like INTERPOL, and strengthening the laws in Singapore. By cooperating with such bodies, the likelihood of catching attackers working from outside the state is greater.

Challenges

However, developing such cooperation and international agreement is not easy. Using the Budapest Convention on Cybercrime as an example, the refusal to ratify the convention by a majority of states signals the difficulty and the slow pace at which progress is made. Seventeen years after the signing of the treaty, it currently has only 56 ratifications and a further four more signatories, which while a significant number, is still short of achieving universal consensus in the international community.[58] Russia has refused to acknowledge the Budapest Convention on grounds that it violates its sovereignty, and has led efforts to launch a new cybercrime treaty under the auspices of the UN.[59]

A set of internationally agreed laws is hard to come by, as evident by the lengthy and glacial processes needed to get states to agree to the Budapest Convention. There still are some disagreements on what constitutes criminal behaviour in some jurisdictions. For example, a state may choose to prosecute libellous speech, but another state may have provisions for freedom of speech. That said, there still is common ground for states to cooperate in law enforcement, like money laundering, identity theft, and drug dealing.

Recommendations

Effective international law enforcement against cybercrime begins with states finding common ground. While Mutual Legal Assistance Treaties still govern the level of cooperation a state can render to another, the involvement of international organisations like INTERPOL can aid in the deterrent effect on non-state matters. Resources can also be allocated to developing information sharing mechanisms and digital forensics capability, both of which can contribute to the deterrence of non-state actors.

[57] Kai-Lung Hui, Seung Hyun Kim, and Qiu-Hong Wang, “Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks,” http://ihome.ust.hk/~klhui/research/2016-MISQ forthcoming.pdf.

[58] Council of Europe, *Chart of Signatures and Ratification of Treaty 185 (Convention on Cybercrime)*, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

[59] Alex Grigsby, “Coming Soon: Another Country to Ratify the Budapest Convention,” *Council for Foreign Relations*, December 11, 2014, http://blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/.

Mitigation as Deterrence

Ordinarily, the payoffs for a successful cyberattack in the physical realm often manifest itself in either the physical destruction of infrastructure or the psychological disruption of minds which plays into the fear and anxiety of people. However, if attackers cannot realise these payoffs, then there may be less motivation for them to carry through because the level of success is low.

This does not mean that cyberattacks will stop, but by raising the bar for a successful attack, the number of actors with the capability to carry out something of that scale significantly declines, and makes detection and attribution of the attack much easier.

Table 1: Table of objectives

Actor	**Objective**	**Method**
State	Destruction	• Deletion/ alteration of information • Physical damage
	Disruption	• Interruption of access
	Espionage	• Interception of data
Non-state	Profit	• Theft of property/ intellectual property • Extortion (ransomware, DDoS) • Fraud
	Personal Satisfaction	• Hacking high security website
	Vendetta	• Defacement of websites • DDoS

The continuing need for robust defence

A soft approach towards effective deterrence is the creation of robust yet resilient systems in cyberspace. This approach focuses mainly on keeping the attacks out or aggressively targeting the viruses within the system.

Definition

While one pillar of Singapore's Cybersecurity Strategy describes the need to build "resilient infrastructure", this is more accurately classified as "robust defence" because it involves adding layers of security through: (i) improving the protection afforded to critical infrastructure; (ii) designing technology with security in mind; and (iii) making government systems more secure.

A robust defence against cyberattacks requires all systems to have adequate protection. The creation of collective responsibility in cybersecurity is also a pillar identified in the strategy. It is important to note that states are not the only targets in cyberspace and every single entity has a role to play in creating a more secure cyberspace.

Perimeter defence is a standard approach to computer security, achieved by placing firewalls at the entry points of networks to block access from external attackers. However, some attacks do not seek to breach the systems; instead they seek to deny access by flooding websites with bogus requests that cause servers to crash. These are also known as denial-of-service attacks.

Robust defence and the internet of things/ smart nation

As Singapore embarks on the Smart Nation initiative, the resulting proliferation of Internet of Things (IoT) devices increases risk because most of these devices do not have robust security due to budgetary and technical constraints.

For example in 2016, Dyn, the company that controls much of the Internet's domain name system infrastructure, came under sustained assault bringing down sites including Twitter, The Guardian, Netflix, Reddit, CNN, and many others in Europe and the US. This was caused by a DDoS attack, in which a network of IoT devices was infected with a malware. Called Mirai, the botnet was coordinated into bombarding Dyn's servers with traffic until the servers failed. Unlike other botnets which are typically made up of computers, Mirai was made up of IoT devices such as digital cameras and DVR players, and involved an unprecedented 100,000 malicious devices. As a result, many websites could not be accessed for hours.[60]

Singapore also had its own DDoS episode in October 2016 when a botnet interrupted StarHub's internet service for three consecutive days.[61] Starhub said the computers and devices of their customers were turned into a botnet that repeatedly sent queries to StarHub's server, eventually overwhelming it.

Since these devices are in the hands of the general public, the responsibility of sustaining robust cybersecurity infrastructure needs to be communicated to all. This can be as simple as not clicking on phishing emails, or regularly changing passwords to prevent hackers from stealing personal and enterprise data.

Incentives for robust defence for the private sector

To achieve this, there have been proposals to make cybersecurity more robust in private sector enterprises. One of which is to use cyber insurance as a way of incentivising private enterprises to improve their cybersecurity procedures. Kanuck suggested that companies might be encouraged to improve their own cybersecurity systems in order to pay reduced premiums, though he cautioned that there was a need to improve the actuarial data used to price these insurance plans at a level where

[60] "DDoS attack that disrupted internet was largest of its kind in history, experts say," *The Guardian,* October 26, 2016, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[61] Irene Tham, "Telcos put on alert after cyber attacks on StarHub," *The Straits Times*, October 27, 2016, http://www.straitstimes.com/tech/telcos-put-on-alert-after-cyber-attacks-on-starhub.

companies can see the benefit from having such a plan.[62] This would also serve as a reward to the companies who have the best practices. Unfortunately according to a survey done by American International Group, only nine per cent of companies in Singapore have taken up cyber insurance even though two-thirds acknowledged that cyber insurance is important.[63]

Besides insurance, businesses can use existing grants like the Productivity and Innovation Credit Scheme to fund more robust defences, while the government can consider setting up new grants to increase the uptake of cybersecurity products. It is a good sign that the Singapore government intends to spend more than S$80 million as part of the 2017 budget for programmes to help small and medium-sized enterprises go digital, and to boost Singapore's capabilities in data and cybersecurity.[64]

Improving robustness with testing

Cyberattacks are uniquely based on the exploitation of vulnerabilities. Should these vulnerabilities be detected early and penetration testing be done on a frequent basis, the attack surface for cyberattacks will become significantly smaller, which might have a deterrent effect on potential attackers.

There is a need to encourage penetration testing both in the public and private sectors to ensure that the systems are robust and protected against malicious actors. Penetration testing should be done on a regular basis to test the robustness of the system. The improvement to detection capabilities will improve the effects of deterrence through the elimination of advanced persistent threats.[65]

The legal framework should also be adapted to protect security researchers who, in the course of research, discover vulnerabilities in the systems belonging to companies or government agencies, and want to disclose them to the system owners. Current laws on computer misuse mean these researchers are subject to criminal prosecution for unauthorised access, even if they have no criminal intent.

The case for resilience

Robust systems are needed to keep malicious actors from penetrating the system, but do not solve the whole problem. The idea of resilience being part of cyber deterrence comes mainly from

[62] Sean Kanuck, “Seminar on Global Information Risk,” Centre of Excellence for National Security, October 31, 2016.

[63] Ann Williams, “Demand for cyber insurance in Singapore to grow by 50% in 2016: AIG,” *The Straits Times*, http://www.straitstimes.com/business/banking/demand-for-cyber-insurance-in-singapore-to-grow-by-50-in-2016-aig.

[64] Jamie Lee, “SG Budget 2017: More than S$80m for digital, data programmes,” *Business Times*, February 20, 2017, http://www.businesstimes.com.sg/government-economy/singapore-budget-2017/sg-budget-2017-more-than-s80m-for-digital-data-programmes.

[65]An advanced persistent threat (APT) uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term,
https://www.symantec.com/theme.jsp?themeid=apt-infographic-1;
See https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html.

understanding how complex problems come to pass. Complex problems require abstract reasoning, and cannot be explained rationally. As mentioned previously, cybercrime should not be seen as a standalone problem as they negatively impact society and industries. Given that there are state-sponsored hackers seeking to create instability in other states, there is also a need to deter such actions.

“Expect to be hacked”

Most experts agree that there is no network so secure that it can never be penetrated. Eneken Tikk-Ringas opined at the 2016 Asia-Pacific Programme for Senior National Security Officers that there was a need to move away from the standard traditional understanding of deterrence, which first assumes a no-attack scenario and is based on denial and retributive methods.[66] She said that rather than only focusing on retribution, benefits from cooperation could be made clearer to actors in cyberspace as a way a deterring bad behaviour.

At the same conference, Michael Chertoff said enterprises should adopt a “human body model” for cyber defence. This model expects viruses to be in the system, and solutions to manage these viruses or malware need to be developed. He commented that the current state of cybersecurity is like an M&M candy; it has a hard shell but turns to mush once this shell is penetrated. Building on the analogy of the human body, there is a need to keep the body functioning to survive, with or without viruses. There is thus a need to create redundancies in the system to ensure continual operation with minimum disruption. The creation of systemic resilience and redundancies are common concepts in engineering, where fail-safes are built into the system with the assumption that all systems have a natural failure rate. This approach considers the societal impacts of a disruption, in addition to the cost of building the system.[67]

Build resilience through backup systems, disaster recovery, and drills

Redundancies and backups are usually built into systems for disaster recovery, making them more resilient. If a system can be rebuilt with minimal loss of data or time, this thwarts the objectives of destruction, disruption, or extortion through ransomware or DDoS.

In order to deter cyberattacks that aim to destabilise or demoralise society, Singapore needs to build resilience through public education and public drills and exercises. At the community level, cyber resilience can be built by training to respond to attacks the same way fire drills and emergency drills simulate real scenarios. At the industry level, businesses can build resilience by training to respond to breaches and by maintaining backup systems that can be called upon in times of emergency. At the

[66]“National Security Revisited Event Report,” Paper presented at the 10th Asia-Pacific Programme for Senior National Security Officers, Centre of Excellence for National Security, Singapore, 2016.

[67] Fred Cohen, “Protection and Engineering Issues in Critical Infrastructure,” in *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, by Thomas A. Johnson (ed.), Boca Raton, FL: CRC Press, 2015.

state level, the government plays the role of chief coordinator to encourage the development of resilience within society towards these new national security challenges.[68]

Detect and respond quickly

The speed at which cyberattacks or incidents are dealt with either imparts or saps confidence in the cybersecurity infrastructure. The faster threats can be detected and handled, the less attractive it becomes to attack a system.

Currently most states work on the assumption that malicious activity is meant to be kept out of the system, but given that the average time taken to discover malicious activity in the system is well over six months,[69] there is a need to radically change this mindset. The assumption is that hackers are already in the system, and more work needs to be done to mitigate the effects that these malicious actors can potentially cause. By reducing the time that malicious actors can be in the system, and by positively identifying them, these actors might be deterred against incursions into the system because the cost of undertaking such activities could be higher than the benefits gained. For example, if the StarHub DDoS incident was resolved more quickly, it could have strengthened Singapore's cyber deterrence by demonstrating the capabilities and mechanisms that Singapore has put in place.[70] Rich Barger, Chief Intelligence Officer of ThreatConnect, said:

> We can't operate with the mindset that everything has to be about keeping them out. We have to operate knowing that they are going to get inside sometimes. The question is, how do we limit their effectiveness and conduct secure business operations knowing they're watching?[71]

As a financial hub and an aspiring Smart Nation, Singapore should ensure that the systems and infrastructure are able to withstand both destructive and disruptive cyberattacks. By improving detection and penetration testing capability, there is a possibility that malicious actors would find less satisfaction in their attempts to breach the systems, and consequently be deterred for a lack of an achievable objective.

[68] Norman Vasu and Benjamin Ang, "Embracing technology to boost national security," *TODAY*, December 22, 2016, http://www.todayonline.com/technology-0/embracing-technology-boost-national-security.

[69] Phil Muncaster, "Hackers Spend 200+ Days Inside Systems Before Discovery," *Infosecurity Magazine*, February 24, 2015, http://www.infosecurity-magazine.com/news/hackers-spend-over-200-days-inside/.

[70] "DDoS attack on StarHub first of its kind on Singapore's telco infrastructure: CSA, IMDA," *Channel News Asia,* October 26, 2016, http://www.channelnewsasia.com/news/singapore/ddos-attack-on-starhub-first-of-its-kind-on-singapore-s-telco/3237478.html.

[71] Brendan Koerner, "Inside the Cyberattack That Shocked the US Government," *Wired*, October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

Conclusion

Deterrence in cyberspace is difficult to envision in the current cybersecurity landscape because primarily, there is a fundamental disconnect between classic (nuclear) deterrence and deterrence in cyberspace. It would be mistaken to assume that deterrence in cyberspace would work the same way as nuclear deterrence, where a no-attack scenario is the only measure of a successful deterrence strategy. Cyber deterrence should be seen as a reduction in attack frequency, and not absolute elimination. Even then, it will be difficult to measure how many cyber actors are deterred by these measures in place because of the anonymity afforded by cyberspace.

Therefore, absolute deterrence in cyberspace is difficult to achieve, if not impossible. This however does not mean that Singapore should stop trying to deter attacks from other states or from private entities. With the volume of malware attacks going up year-on-year, there needs to be effective measures to mitigate cyberthreats from both state and non-state actors.

The pursuit of deterrence by denying capability is not possible given the proliferation of dual-use technology on the market. The possibility of pursuing deterrence by punishment is similarly small. State actors are unlikely to be deterred if they feel their actions in cyberspace fulfil their rational self-interests.

To this end, there needs to be clear communication that such behaviour is unacceptable among states, and punishment for an event needs to be proportionate and immediate. Communication can vary among states, and states need to have ready measures to address these issues. Small states like Singapore will find it difficult to formulate a proper punishment response due the lack of strategic depth[72], the desire to be cordial with neighbours and other powerful states, and the reality of geopolitics. Attacks by state actors should be properly attributed and if the situation calls for it, made public to deter future attacks.

For non-state actors, criminal activity must be decisively and harshly dealt with to increase the cost to actors. Prosecution must be swift and decisive to deter other non-state actors from pursuing malicious action in cyberspace. The ability to detect is a powerful deterrent because it signals to actors that they are not as invisible as they would like to think. The deterrent effect would be greater if states were to cooperate on law enforcement issues. Deeper areas of cooperation among states should be worked out and if possible, enshrined in international law like the Budapest Convention.

In addition to international cooperation, Singapore should consider the pursuit of norms in cyberspace as the cornerstone of its international deterrence strategy. Technology moves at an amazing rate as

[72] Strategic depth broadly refers to the distances between the front lines or battle sectors and the combatants' industrial core areas, capital cities, heartlands, and other key centers of population or military production. Andrew I. Killgore, “Israel: No Strategic Asset,” in *Journal of Palestine Studies*, Vol 14, No 2 (Winter, 1985).

Moore’s Law would have it, but the time taken to formulate an international treaty is too long and arduous for it to be effective. Instead, academics and governments have worked on the development of norms to guide the behaviour of states. These, when developed, should be universally applied to all so as to create no impression that certain laws do not apply to the stronger powers.

Singapore is a small state with few natural defences and does not have the strategic depth to conduct deterrence by both denial and punishment on state actors. For non-state actors however, punishment can be carried out through both domestic laws and international cooperation with other states. In view of the low rate of success that deterrence may bring in preventing the tools used in a cyberattack, deterrence in the Singapore context thus needs to focus on the prevention or mitigation of the effects of what is seen to be a successful cyberattack.

The recently released Cybersecurity Strategy is thus a good framework to build deterrence in Singapore. The strategy focuses on building secure infrastructure, sharing collective responsibility, building capacity in the cybersecurity sector, and deepening international cooperation with ASEAN and the rest of the world.

From a strategic perspective, these broad goals are largely defensive in nature, and reflect accurately the number and range of tools that are afforded to a small state. While Singapore can be considered a technologically advanced state, it has to be wary of using punishments against other states in case the conflict escalates, especially in kinetic response (i.e. physical military action).

Ultimately, different actors have very different objectives, and deterrence may not work in cases where the attacker state has the will to carry out its objectives. For state-sponsored espionage, success could mean the constant surveillance of data passing through a state’s networks without detection. For hackers who are seeking to disrupt and misinform, success could mean the fragmentation of society and breakdown of communication between the public and the government. For criminals seeking to profit from hacking into systems, success is financial and potential reputation loss that a company that can incur. For hobby hackers, success may be as simple as the exploitation of an unknown vulnerability.

There is therefore a need to reduce the ability of attackers to reach their objectives. This could take the form of a state being judged by a court of international opinion should a deviation from internationally accepted norms be observed, or even a severe punishment for a cybercriminal. These tools for deterrence should be developed by the respective agencies (e.g. foreign affairs for diplomatic issues and police for criminal ones) at the national strategic level.

Table 2: Possible objectives and deterrents

Actor	Objective	Deterrent
State	Destruction	• Threat of retaliation (DIMEFIL) • Criticism from international community
	Disruption	• Systemic resilience • Threat of retaliation (DIMEFIL) • Criticism from international community
	Espionage	• Criminal prosecution • Criticism from international community
Non-state	Profit	• Increased chances of getting caught and convicted (punishment) • International cooperation in prosecution • Increased difficulty of targets
	Personal Satisfaction/ Vendetta	• Punishment • International cooperation in prosecution

In addition to developing a response mechanism, this national strategy needs to incorporate the values of robustness and resilience in the responses by the state. Singapore still needs robust perimeter defence to deter malicious actors from penetrating into the system in spite of its shortcomings, and when these malicious actors do get in, how to get them out in the most efficient manner. To do this, cyber threat information (CTI) and incidents need to be shared as soon as possible so that the infection of the system is rooted out quickly. By resolving breaches effectively and efficiently, enterprises and the society at large can build resilience when dealing with major outages or cyberattacks.

For private enterprises, there needs to be an understanding that there will be occasional intrusions into their systems, and that anyone can be a target. There is a need to maintain a rigorous cybersecurity regime to detect attacks, and to reduce the malware detection time.[73] There is also a need for enterprises to share CTI and incidents, so as to create awareness on the vulnerability among all enterprises.

In conclusion, deterrence in cyberspace should be seen as a broad-based yet targeted approach to deal with the different malicious actors and possible objectives. There is a need for renewed emphasis on how everyone plays a part in ensuring there is a strong deterrence mechanism present through the capabilities.

[73] The time taken to detect malware is currently 520 days. Symantec, *Internet Security Threat Report,* Symantec, Volume 21, 2016

Annex A: Credibility-Stability Paradox

The reliability of the state's commitment to enforcing its own deterrence policy statements is a significant symbol of its political and military power. If it doesn't back up a threat when the red line is crossed, it directly reduces its credibility in the eyes of the international community, undermining its ability to both intimidate and negotiate in the future. Conversely, making good on a threat in cyberspace can have drastic impacts on international stability. The full impact of an action taken in cyberspace is difficult to control or predict. Therefore, the retaliation may spiral beyond the intended punishment, inflicting damage over and above what would be considered a proportionate response to the breach of a threshold. This risks a minor incident triggering a tit-for-tat escalation and cascading an attack in cyberspace into a much bigger conflict. This danger is exacerbated by the risk of inadvertently punishing the incorrect actor. Incorrect attribution could trigger unnecessary escalation with a third party while the real aggressor goes unpunished and undeterred. Thus, once such a cyber deterrence framework's constructed, a state faces the strategic dilemma of being forced to choose between maintaining its credibility and the risks of collateral damage.

Source: P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know,* Oxford University Press, 2013

Annex B: Case Study of Capability-based Deterrence: Estonia

Without the capability to adequately and swiftly rebound from a cyberattack, a state is still at the mercy of another should the offending state choose to undertake a non-kinetic attack leaving them helpless. A kinetic attack requires the movement of manpower and armaments, but a cyberattack requires no such thing. Estonia is a good example of how a highly interconnected state backed by robust and resilient infrastructure can use its capabilities for deterrence.

Much of this thinking was solidified during the Estonian cyberattacks in 2007. Estonia suffered what was then one of the most debilitating cyberattacks on a state when a massive denial-of-service attack on its networks left citizens without internet, and consequently, access to government services for three days. Estonia is one of the most connected states today and relies heavily on the internet for government service provision to its people. The basis and principles behind the Estonian digital foundation is that it is decentralised, seamlessly interconnected with other systems, has a flexible and open infrastructure system, and was developed as an open platform to be used by any institution.

While this is widely seen to be a service provision platform created by the Estonian government, the underlying architecture and rationale for the programme is aimed at preserving the existence of an Estonian state even after the physical state no longer exists. Estonians are acutely aware of the need to be prepared for state survival, having been annexed into the Soviet Union in 1940, and being left to their own devices after the fall of the Soviet Union in 1991. In recent years, Russia has also become increasingly assertive in the region, moving to annex Crimea from Ukrainian control in 2014.[74]

Russia was suspected to have carried out the 2007 attack, although there has been no conclusive proof of Russian involvement. Most of the evidence of the attack was considered circumstantial due to Russia’s refusal to cooperate with Estonia even when mutual assistance was sought.[75]

This experience has led Estonia to develop unique tools to continue operations regardless of what happens to the state physically. In its Cyber Security Strategy for 2014-2017, Estonia envisioned a set of “data embassies” to ensure that the state continues to survive. The data that is stored overseas also acts as a backup system should the data in the system be compromised or rendered inaccessible.[76]

[74] Molly McCluskey, “Estonia redefines national security in a digital age,” *Al Jazeera*, March 20, 2015, http://www.aljazeera.com/indepth/features/2015/03/estonia-redefines-national-security-digital-age-150318065430514.html.

[75] Gregg Keizer, “Estonia blamed Russia for backing 2007 cyberattacks, says leaked cable,” *Computerworld*, December 9, 2010, http://www.computerworld.com/article/2511704/vertical-it/estonia-blamed-russia-for-backing-2007-cyberattacks--says-leaked-cable.html.

[76] “Estonia Cyber Security Strategy 2014-2017,” *Government of Estonia*, Tallinn, Estonia: Ministry of Economic Affairs and Communication, 2014, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

Estonia also adheres to a “no legacy” principle for software. This means that the public sector cannot use ICT solutions that are more than 13 years old due to the belief that newer programmes cost less and are less encumbered by years of patching and customising by programmers. This is a forward thinking strategy that factors the fast moving nature of technology into public service provision.[77]

The credibility of the e-Estonia programme to deter state and non-state actors comes from the robust level of security, the resilience of the system, and the fact that how its concerns about the state’s physical survival are priced into the security calculus.

Estonia and the role of NATO CCDCOE

Estonia places much emphasis on its cyber defence, and is home to the NATO Cooperative Cyber Defence Center of Excellence (NATO CCDCOE). The centre’s mission is to enhance capability, cooperation, and information sharing between NATO, allies, and cyber defence partners.

One of the most important events that NATO CCDCOE organises is Locked Shields, a red-teaming exercise involving many states. Locked Shields is an advanced international live-fire cyber defence exercise held annually, and uses scenario-based real-time network defence exercise to train the security experts who protect national information technology systems on a daily basis. The 2016 edition was attended by 550 people from 26 states, and featured realistic and cutting-edge attacks, networks, and technologies.[78] This exercise enables Estonia and its allies to test their capabilities in a hostile environment where they have to react in real time, and know the tools at their disposal should a real world situation develop. With this level of preparedness, the aggregated capability, and the identification of allies, Estonia has created its deterrence based on first, its robust security, second, knowing who can help you in times of need, and most importantly, narrowing the field to who has the hostile capability and the will to harm Estonia, of which attribution of an attack would be much easier.

The emphasis on capability development is not to say that Estonia does not practice the normal forms of deterrence of denial, punishment, and norms building observed in the previous chapter. Rather, as a small state, its options to pursue denial and punishment strategies are highly limited by its relative size to its neighbours, and the escalatory risks that can happen should offensive capability be used. Instead, the Estonian model is a model of deterrence built on extreme resilience and capacity to withstand external attacks.

[77] “*e-Estonia: The future is now*,” Government of Estonia, *e-Estonia*,
[78] “Locked Shields 2016,” NATO CCDCOE, https://ccdcoe.org/locked-shields-2016.html.

RSIS Working Paper Series

(from 2016 onwards)

309 Cyber Deterrence in Singapore: Frameworks and Recommendations (2018)
Eugene EG Tan

308 Trade Policy Options for ASEAN Countries and Their Regional Dialogue Partners: "Preference Ordering" Using CGE Analysis (2018)
Xianbai Ji, Pradumna B. Rana, Wai-Mun Chia, and Chang Tai Li

307 The South China Sea: Beijing's Challenge to ASEAN and UNCLOS and the Necessity of a New Multi-tiered Approach (2017)
Christopher Roberts

306 China's Belt and Road Initiative: The Evolution of Chinese Private Security Companies (2017)
Alessandro Arduino

305 Engaging Religion with Pragmatism: The Singapore State's Management of Social Issues and Religious Tensions in the 1980s (2017)
Mohammad Alami Musa

304 Incident Prevention and Mitigation in the Asia Pacific Littorals: Framing, Expanding, and Adding to CUES (2017)
Graham Ong-Webb, Collin Koh, Bernard Miranda

303 A Political Economy Analysis of the Southeast Asian Haze and Some Solutions (2017)
Prakash Chander

302 Waiting for Disruption?! Undersea Autonomy and the Challenging Nature of Naval Innovation (2017)
Heiko Borchert, Tim Kraemer and Daniel Mahon

301 The French Counter-radicalisation Strategy (2016)
Romain Quivooij

300 Analysing Transformative Leadership in Indonesia (2016)
Alexander R. Arifianto

299 Economic and Strategic Dimensions of Mega-Ftas: A Perception Survey of Asian Opinion Leaders (2016)
Xianbai Ji, Pradumna B. Rana, Wai-Mun Chia and Changtai Li

298 Orienting ASEAN Towards Its People: Enabling Engagement with Local NGOs (2016)
Serina Rahman

297 Russia's Asia Pivot: Engaging the Russian Far East, China and Southeast Asia (2016)
Bhavna Dave

Visit the RSIS website at www.rsis.edu.sg/?p=48639

to access the full list of past RSIS Working Papers.