A Small State Perspective on the Evolving Nature of Cyber Conflict

Lessons from Singapore

By Eugene E.G. Tan

Cyber conflicts among states are still largely driven by geopolitical and political considerations and should not be seen as separate from other kinds of conflict or political objectives. Brandon Valeriano, Benjamin Jensen, and Ryan Maness observe that modern cyber strategies are neither new nor revolutionary and that actions in cyberspace fall into "a domain of limited coercive actions designed to alter the balance of information as well as manage escalation risks in long-term competitive interactions." Cyber operations may offer new ways to test the robustness of networks, control messaging, or degrade a network, but they do not fundamentally change great power competition or the hierarchy of states in the international system.[1]

Small states are particularly vulnerable to the effects of cyber conflict, with larger states seeming to prefer cyber means as a way of affecting policies of the target state because of the possibility of the effects of an attack being reversed once the preferred policy of the hostile state is selected. A good example of how this happens can be seen in the 2007 Estonian cyberattack, where Russian actors sought to influence Estonian policy of moving Soviet-era statues from the city center.

Eugene E.G. Tan is an Associate Research Fellow at the Centre of Excellence for National Security of the S. Rajaratnam School of International Studies, Nanyang Technological University.

This culminated in the degradation of Estonian networks over a four-day period. While the cyberattack did not produce a change of Estonian policy, it highlighted the lengths to which states would go to affect other states' policies.

That said, the Estonian cyberattack did not cross the armed attack threshold, making an international response to the cyberattack both difficult and unprecedented.[2] To this day, states are still finding ways to address cyber conflict and are no closer to finding an acceptable mechanism to govern state behavior in cyberspace.

For the purposes of this article, the parties involved in cyber conflict are states (or state-sponsored actors) and not individuals or private corporations. That said, individuals and private corporations may still play a part in causing or exacerbating conflict by cyber means domestically and regionally or be the victims of state-led compellence measures. It is also of note that state-sponsored cyberattacks often serve a purpose and target rather than causing disparate and collateral damage to different targets, as did NotPetya.[3]

Using Singapore as the main example, this article aims to show how cyber conflict affects small states. While the means of cyber conflict may be evolving, it is still subject largely to the push and pull of geopolitical forces.

Intent to Compel

Carl von Clausewitz noted that "two different motives make men fight one another: hostile feelings and hostile intentions. Our definition is based on the latter, since it is the universal element. Even the most savage, almost instinctive, passion of hatred cannot be conceived as existing without hostile intent; but hostile intentions are often unaccompanied by any sort of hostile feelings-at least by none that predominate."[4] Using Clausewitz to understand cyber conflict may presuppose that conflict in cyberspace is in fact an act of war, but on the contrary, understanding Clausewitz well may help us understand why conflict in cyberspace will not result in cyberwar.[5] Clausewitz notes three main characteristics of war: its violent nature, its instrumental character, and its political nature.[6] Clausewitz's dictum that war is a continuation of policy by other means and the continuation of political intercourse to reach a definite goal is especially salient to the discussion on regional cyber conflict.[7] Thomas Rid's instructive piece debunking cyber war further argues that all politically motivated cyberattacks are merely sophisticated versions of sabotage, espionage and subversion.[8] Cyber conflict lacks war's violent nature but may address how it fulfills an instrumental and political purpose. Cyber conflict should therefore be understood as just one way of achieving policy goals short of war.

Internationally, in a competitive and rational situation, it is conceivable that any state will seek to use any tool, including cyber, to achieve an absolute advantage over its adversaries through a mix of deterrence and compellence. According to Thomas Schelling, there are important distinctions between deterrence and compellence as components of a coercion strategy. The main differences are in the timing and the initiative. In a compellence situation, the attacker already has accomplished the offending action, and the defender must take the initiative to respond, not just sit and wait. In other words, "The threat that compels rather than deters often requires that the punishment be administered until the other acts, rather than if he acts." In a deterrence situation, the defensive picture has already been painted. The adversary need not know the specific features of the painting, as long as no offensive act is committed. In fact, ambiguity may support deterrence. In a compellence situation, the picture must be painted for that specific situation, and it must be clear to the offender what must be done, and by when, for the victim's coercive response actions to cease.[9]

State-sponsored cyberattacks should therefore be seen in the same vein as other attacks or policy levers rather than as standalone incidents. Although the coercive effects of cyber incidents are seen as limited, the use of cyber tools is observed to complement, not replace, traditional statecraft, serving as an additive foreign policy tool.[10] The potential for regional cyber conflict should therefore not be seen as separate from other analyses of regional geopolitics.

Evolving Nature of Cyber Conflict

There are also different understandings of what cyber conflict actually entails. For decades, Western governments, practitioners, and scholars have understood cyber conflict to include protection of critical infrastructure and computer networks from hacking, or breaches of confidentiality, integrity, and availability. This understanding has been the basis of international discussions on the applicability of international law to cyber conflict, cyber norms of behavior, and deterrence of cyberattacks. The focus has been on the technology—networks, hardware, and software—instead of on the information carried by the technology.

An alternate view, led by Russia and China, has traditionally seen information as an inalienable part of cyber conflict. Russia introduced a draft resolution on information security in the First Committee of the United Nations (UN) General Assembly in 1998 and has continued to press for information security to be part of the international conversation on cyber conflict, including submitting a letter in January 2015 (together with China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan) to the UN calling for an international code of conduct for information security.[11]

While the letter was noted by the 2015 UN Group of Governmental Experts (UNGGE), the recommendations proposed by the group squarely focused on the protection of critical information and communications technology infrastructure, which was reflected in the norms proposed in the consensus report.

One reason for this focus on technology rather than information has been the philosophy of many Western democracies that any controls over the flow of information would infringe on the fundamental right to freedom of expression. Incidentally, respect for the freedom of expression, right to privacy, and other human rights was one of the norms proposed by the 2015 UNGGE.

This position appears to have shifted since the alleged Russian interference in the U.S. presidential elections in 2016. At various international conferences in 2018, including the landmark Conference on Cyber Conflict (CyCon) organized by the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, keynote speeches addressed how the use of information operations through cyber means is now an important part of cyber conflict.

Keynote speeches at CyCon 2018 by Alex Stamos (then chief security officer of Facebook) and Camille Francoise (principal researcher at Google Jigsaw) highlighted how social media is used in state-sponsored information operations, citing numerous examples of how states have used tools to influence elections and promote questionable content to destabilize incumbent governments.[12] They also called for cooperation and a common approach to misinformation and manipulation of social media. This leads to the conclusion that social media platforms need protection as much as critical infrastructure like power plants and airports.

However, including information operations in the discussion of cyber conflict is not straightforward, because the threats faced by social media platforms are different from those faced by traditional cyber targets. First, in information operations, the networks of social media platforms are not being breached but are being used for their built purpose:

spreading information. The challenge is to curb the spread of misinformation without hindering freedom of expression.

Second, information operations are designed to exploit vulnerabilities not in the technology but in the society being targeted. Tackling them requires expertise in socio-political issues, psychology, communications, and other humanities.

Third, states can build resilience to cyberattacks by constructing strong technical defenses and conducting exercises and drills. But resilience to information operations is built through institutional trust-building, media literacy education, independent fact-checking, and transparency in communication.

Fourth, while the international community has already found it difficult to develop international norms of behavior in cyber operations, where those norms only considered technology, it will be even more complex if information is included in the discussion because of states' differing philosophies on the control of information versus freedom of expression.

It can thus be said that cyber conflicts transcend the cyber domain. Potential conflicts in cyberspace may be found embedded in the broader context of information conflicts. These conflicts may take on political, economic, information, technological, media, and ideological forms in competing for influence. Targets in cyber conflict can range from key government services and institutions, internet service providers, collected personal data, or even electoral systems or media. It is therefore prudent to look for political motives to how and why cyber conflict happens to small states, how these states can choose to react to these cyber incidents, and what their limitations are.

Small States and Cyber Conflict

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 options for carrying out punitive action against a hostile state, with punishments being ineffective due either to scale or to the possibility of cutting off potential markets in the case of sanctions. The evolving nature of cyber conflict also means that the potential threat to small states from cyberspace no longer resides in just the physical protection of infrastructure, but also in the psychological aspects of conflict.

While Singapore is seen to be an exception to the notion of a small state because of its successful economy, advantageous strategic location, and outsized diplomatic voice, its small physical size nonetheless plays an influential role its strategic thought. In fact, Singapore, with its Smart Nation program and quest to become a data hub, has a larger cyber threat landscape than other small states, making it and its government systems more vulnerable to cyber threats made by other states.[13]

Vulnerability has been a constant theme in Singapore's foreign policy outlook since its independence, with Michael Leifer noting that Singapore, like most small states, suffers from an innate vulnerability arising from geopolitical circumstances.[14] Small states like Singapore do not have the wherewithal to carry out threats or be the aggressor because they lack the strategic depth to counter hostile actions by other states. However, while it is conceivable that small states may go rogue and use cyber means to attack a larger state (like the Sony attacks perpetrated by North Korea), these states do so in full knowledge that they have nothing to lose in not abiding by international law. Singapore, as a law-abiding international state that seeks a rules-based international order, does not have such illusions. It is well documented that Singapore employs a mix of deterrence and diplomacy to ensure its survival, and this is probably true in cyber conflict as well.[15]

As a small state, however, Singapore's ability to create deterrence against cyberattacks against other states is very limited. For several reasons, there is limited value in pursuing classic views of deterrence through denial and punishment: technology is relatively cheap and widely available, accurately attributing blame is difficult, and identifying and punishing attackers are complex. If there is no detection or ability to punish, the credibility of deterrence by a small state like Singapore suffers.

While all states have the possibility of reacting to a cyber incident on the whole spectrum of diplomatic, information, military, economic, financial, intelligence, and law enforcement activity, small states like Singapore have limited recourse to act in the way large states like the United States or China can.[16] Small states need to be especially careful in any response because any disproportionate response to a cyberattack, which results in escalation by the attacker, could be potentially catastrophic given the vulnerability of the nation's economy, infrastructure, and physical size.

There is also a need to think about the stability in the international system should Singapore decide to pursue a deterrent strategy. The possibility of the escalation in hostilities among states is a cause for concern should a response be deemed disproportionate or inaccurate. Responses should be made when there is a clear case, rather than being based on conjecture on the potential intent of various states. Further, solely "naming and shaming" perpetrators of cyberattacks is ineffective as a response because it does not carry a strong message or have a deterrent effect. Fergus Hanson describes the Australian experience in naming and shaming the perpetrators behind WannaCry, NotPetya, and a third incident that used compromised routers for a future attack as inadequate at best and emboldening at worse. Using arson as an example, Hanson alluded that arsonists would light more fires if there were no added costs, with some relishing the added infamy of being named.[17]

In addition, there is a good chance of cyber conflicts escalating out of control should a retaliatory cycle among states take place, which will have huge implications on stability in cyberspace. The reliability of a state's commitment to enforcing its own policy statements is a significant symbol of its political and military power. If it does not retaliate or respond proportionally when a 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 (for example, the spread of the Stuxnet or NotPetya malware). Therefore, 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 wrong actor; incorrect attribution could trigger unnecessary escalation with a third party while the real aggressor goes unpunished and undeterred.

The best way for Singapore to protect its national interest vis-à-vis cyberspace is therefore by diplomatic efforts, contributing to the formation of international norms. Most norms have been agreed at international forums such as the UNGGE, in which Singapore was not a participant in the 2016–17 round. In order for Singapore to promote in detail the norms that it would like to have discussed around the world, such as the applicability of international law in cyberspace, it can do so in forums such as the Association of Southeast Asian Nations (ASEAN) Regional Forum and its various ministers' meetings and in the Shangri-La Dialogue.

In the meantime, small states should consider bolstering their domestic resilience as part of their arsenal of responses vis-à-vis conflict in cyberspace.

World Cyber Games Finals in Singapore 2005 (Conew at Polish Wikipedia https://commons.wikimedia.org/wiki/File:World_Cyber_Games,_Singapore,_2005.jpg)

Small states should prioritize the building of robust and resilient systems, which could mitigate the effects of a cyberattack. There is also a need to inoculate society against the effects of state-sponsored cyberattacks through a mix of prompt communication, proper cyber hygiene, having up-to-date systems, and quick remediation of the cyberattack. Small states should have a clear understanding of the origins of these cyber conflicts and the objectives of the aggressor state.

To do this, Singapore has proactively erected Digital Defence as the sixth pillar in its Total Defence strategy.[18] Digital Defence is a whole-of-nation effort to protect and defend the nation and secure its citizens online. It requires Singaporeans to practice good cybersecurity habits, guard against fake news and disinformation, and consider the impact of actions performed online on the wider community. Singapore has also strengthened its legislation over disinformation online, with the Protection of Online Falsehoods and Manipulation Bill being enacted by parliament to guard against potential misuse of the internet for information conflict by other states.[19]

Capability for Cyber Conflict

That said, there are not many states around the world that have the political will, capability, and disregard for international reputation to carry out cyber operations in the areas of both information manipulation and system degradation. While an increasing number of states has expressed interest in possessing offensive cyber capacity, there is little way of knowing the level of expertise of these states. Attackers can plausibly deny responsibility for the attack, claiming that it is a false-flag operation or even that their computers have been unlawfully used to conduct an attack.[20] Conversely, attributing an attack to an innocent third party would trigger unnecessary escalation while the real aggressor goes unpunished and undeterred. The true attacker may even encourage "cascading an attack in cyberspace into a much bigger conflict."[21]

It takes a combination of technical forensics, human intelligence, signals intelligence, history, and geopolitics to identify the machine used, the specific human actor, and the entity/state that is ultimately responsible for the attack.[22] If the evidence is derived from covert intelligence operations, the state may not want to reveal its sources or capabilities.[23] It was thus prudent at the press conference following the SingHealth breach for the chief executive of the Cybersecurity Agency Singapore to state that "there are only a few countries in the world who have shown this level of sophistication when it comes to cyberattacks. . . . We are not able to reveal more because of operational security reasons."[24] As a responsible state of good repute, Singapore has not used its cyber capabilities offensively.

There is therefore a pressing need, as Clausewitz noted, to look at the intentions of the offending state. Max Smeets and Herbert Lin observed that the possession of offensive cyber capabilities is not effective in deterring other states from taking adversary military action unless a state possesses a credible threat. Offensive cyber capabilities, however, are observed to play a larger role in compellence because the effects of offensive cyber capabilities are, first, reversible, and second, do not have to be disclosed. Smeets and Lin also note that there are two points to assess if coercion is taking place: first, that the attacker may not make explicit, but implicit, demands owing to the longstanding relationships among states; and second, the demands will not explicitly spell out where the threat is going to materialize.[25] Smeets and Lin thus lay out a set of questions that states that are being coerced should ask in cyber conflict:

- What are the cyber capabilities a rival state has demonstrated, or what are the cyber trends that should be tracked?
- What is the broader context of the cyber conflict?
- Has the state been subject to longstanding demands?[26]

Singapore and the Region

According to the 2017 Australian Strategic Policy Institute Cyber Maturity Report, the Asia-Pacific region has so far escaped a major state-led cyber incident more because of the peaceful macro environment than because of strong defenses and resiliency. At the individual level, more than 55 percent of people in the Asia-Pacific are still not connected to the internet. While this represents a massive growth opportunity, it also points toward large-scale early user vulnerability as this population comes online.[27]

As a small state that seeks to be a friend to all but an enemy of none, it is probable that Singapore will not employ tools of coercion to advance its interests. This is especially so for Singapore's immediate neighbourhood, where peace and stability in Southeast Asia are absolutely essential. Consequently, Singapore as a founding member of ASEAN remains a strong advocate of the association's unity and centrality.[28]

There are two main documents that have largely contributed to the peaceful regional order in Southeast Asia: the declaration of the Zone of Peace, Freedom, and Neutrality, and the Treaty of Amity and Cooperation. Relations among ASEAN member states have been generally stable, and with the exception of the Thai-Cambodian border dispute, there has been no armed conflict among the ASEAN member states.[29] There have been other minor arguments between ASEAN member states, but these have not crossed the threshold where war or direct conflict is the automatic extension of government policy.

This is not an indication that cyber conflicts will not happen in ASEAN, but merely an indication that member states have not resorted to cyber operations to influence policies. Further, it is perhaps fortunate that because ASEAN member states are not as developed in terms of cyber capabilities, conflicts among them in the physical domain have not evolved into cyber degradation exercises.

That said, apart from the gaps in capability, ASEAN has been doing much in cyber diplomacy to stave off cyber conflicts. In 2018, ASEAN member states sought to advance the operationalization of cyber norms in the region. The 32nd ASEAN summit in April 2018 brought on a slew of statements from leaders recognizing that norms and the rule of law are needed for cyberspace and as a basis for using technology to advance economic growth in the region.[30]

The ASEAN Leaders' Statement on Cybersecurity made at the summit called for the identification of a concrete list of voluntary, practical norms of state behavior in cyberspace that ASEAN can work toward adopting, taking reference from the 11 norms recommended by the 2015 UNGGE.[31]

The ASEAN Ministerial Conference on Cybersecurity (AMCC) held in September 2018 also agreed that there is a need for a more formalized mechanism for ASEAN cyber coordination and has tasked Singapore to propose a mechanism for the AMCC to consider. The AMCC also has agreed in principle to subscribe to the 11 voluntary, nonbinding norms recommended by the 2015 UNGGE, as well as to focus on regional capacity building in implementing these norms.[32]

Singapore and Extra-Regional Conflict

Cyber conflicts are not limited by region, as can be seen by the Stuxnet and Shamoon cyberattacks inflicted on Iran and Saudi Arabia respectively. Southeast Asia is a confluence point for great power competition, with an increasingly assertive China and a still interested United States each emphasizing its role in the region.

Flashpoints have resulted in offensive cyber capabilities being used to signal displeasure and compel and coerce some states in the region to heel. For example, it is widely speculated that China was behind a series of distributed denial of service attacks on the Philippines after the Permanent Court of Arbitration ruling dismissing China's claim of ownership of the South China Sea. The attacks began almost as soon as the verdict was released on July 12, 2016, and targeted key Philippine government agencies including the Department of Foreign Affairs, the Department of National Defense, the Central Bank, and the Presidential Management Staff. Similarly, Vietnam has been targeted by Chinese cyber units because of its South China Sea position, particularly after an incident over a Chinese oil rig in Vietnamese-claimed waters in May 2014. In this instance, Vietnamese intelligence networks were compromised by Chinese hackers, leaking sensitive information over Vietnam's diplomatic and military strategy.[33]

With the superpowers and other regional powers, Singapore's aim is to expand its relationships, both politically and economically, to remain relevant and ensure that it is in the best interests of other states that Singapore continues being successful. This delicate balancing act is easier in good and peaceful times, but obviously more difficult when superpowers and regional powers contend with one another, such as the power competition and trade war between the United States and China. Nevertheless, Singapore aims for balance and promotion of an inclusive architecture. Singapore fastidiously avoids taking sides in great power conflict, refusing to side with one side against another. While Singapore spares no effort to develop a wide network of relations, these relations must be based on mutual respect for each other's sovereignty and the equality of nation states, regardless of size. Diplomacy is not about just having "friendly" relations at all costs, but about promoting friendly relations as a way to protect and advancing Singapore's important interests.[34]

Singapore's uncompromising but principled stance when rivals make unreasonable demands that hurt or compromise its national interests may cause friction with the great powers in the region. A good example of this is the impounding of Singapore's armored personnel carriers in Hong Kong in December 2016 as one way that Beijing signaled displeasure toward Singapore for its stance on the affirmation of international law on the South China Sea issue.[35] While China has in this instance used a physical lever to pressure Singapore to change its stance, China is well capable of using its huge offensive cyber capability for similar reasons. China has also demonstrated its capability and willingness to use information warfare tactics on other states such as Taiwan.[36]

Other states with vested interests in the region have declared their offensive cyber capabilities and have shown a willingness to use these capabilities. Australia, for one, announced that it has used its offensive cyber capabilities to degrade the Islamic State's command and control networks.[37] The United Kingdom has also announced that it will set up a 250-million-pound cyber taskforce to combat Russian and terrorist aggression in the wake of the Novichok chemical attack in Salisbury.[38] The United States has announced that it has authorized the use of offensive cyber operations against adversaries to protect its interests without specifying how these will be used or what behavior it will seek to coerce.[39] The possibility of extra-regional conflict is therefore high and may inadvertently affect Singapore and the other states in the Southeast Asian region both domestically and internationally.

Domestic Implications of Cyber Conflict for Singapore

Michael Raska notes that because cyber-enabled conflicts increasingly challenge traditional boundaries between peacetime and wartime, geography and distance, state and non-state actors, and civil and military domains, Singapore's defense strategy has to correspondingly adapt to the challenges emanating from cyberspace.[40] As the international community begins to recognize information operations as part of cyber conflict, states such as Singapore will have to develop new policies and possibly even new organizations to respond to information operations alongside the more traditional cyber security challenges. This may include the development of doctrines or framing of appropriate and proportionate responses to cyber incidents.

The SingHealth cyberattacks of 2018 also show that public confidence can be easily shaken or affected by a cyberattack.[41] In order to mitigate the impact of cyberattacks that aim to destabilize or demoralize society, Singapore needs to build resilience through public education and public drills and exercises. At the community level, Singapore can build cyber resilience by training to respond to attacks, similar to fire drills and emergency drills held today. 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 state level, the government plays the key role of chief coordinator to encourage the development of resilience within society toward these new national security challenges.[42]

Information operations can also pose a threat to society and should be considered as part of cyber conflict. Some of the information fed to cyberspace is fabricated or manipulated to help hostile states achieve a certain policy objective. To better understand this phenomenon, the Parliament of Singapore convened a Select Committee on Deliberate Online Falsehoods, calling upon international experts and tech companies to testify about the effects of deliberate online falsehoods. The report of the committee has provided 22 recommendations for responding to them. These new policies and organizations will need expertise in a range of areas such as strategic communication, public education, fact checking, and international relations.[43] Cyber conflict will continue to evolve at a rapid rate, and states will need to produce timely and effective measures to prevent and combat the effects of these conflicts.

International Implications of Cyber Conflict for Singapore

Currently, because of the lack of international agreements and laws, coupled with the weak enforcement of norms regarding cyberspace, cyber conflict is largely ungoverned. The inability of the 2017 UNGGE to agree on how international law applies in cyberspace may lead states to conclude that there are few, if any, rules in cyberspace, and increase the risk of cyber conflict.

The absence of a normative regime in cyberspace at the moment allows malicious actors to operate in a grey area where there is a low-risk, high-reward scenario to the attackers. In a sense, states are bound in a no-win situation where the strong do what they want, and the weak suffer what they must in world without norms.

Establishing norms in cyberspace, however, is not a straightforward process. The recent shift in global power politics means that states with revisionist ambitions are emboldened to challenge the existing international order. The United States' unipolar moment is giving way to a multipolar world, and that has serious implications for the survival of today's 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.

Norms should preferably be applied to all states, but seeking narrow consensus with a few dialogue partners may help shape norms globally. Following the impasse at the 2017 UNGGE, China is pushing for a regional ASEAN cyber security agreement that leaves out the United States.[44] This is consistent with China's foreign policy of engaging with global institutions on its terms and mirrors what China is doing geopolitically in the region, which is to frame the United States as an outsider that should not meddle in regional matters or strategic thinking. This point of dividing ASEAN in favor of bilateral negotiations should not be taken lightly especially when a strong consensus over norms for cyberspace is needed.

One of Singapore's foreign policy principles is to promote a global world order governed by the rule of law and international norms. Norms are especially important to small states like Singapore, as norms set out the rights of states, including the protection of critical infrastructure from malicious attacks, noninterference in political processes, and the illegality of economic espionage. In a system where "might is right" or the laws of the jungle prevail, small states like Singapore have very little chance of survival. The international order is strengthened by the safeguarding of the rights and sovereignty of all states and the rule of law. Great powers will still have more influence and say, but they do not get a free pass to do as they please.

The pace at which international law is being made is slow and may at times incur headwinds that are insurmountable. For example, while the 2012–13 round of the UNGGE agreed that international law applied to cyberspace, the 2016–17 round failed to agree on how international law applies to cyberspace.[45] International law will thus take a long time to formulate, and it may be a while before states can agree on an international law regime.

But the creation of a rules-based order is one of the ten key principles underscoring the Leaders' Vision statement and calls upon ASEAN to promote the rule of law, anchored in respect for international law and norms. This will in turn help with the development of the ASEAN Smart Nation network and fulfil the leaders' pledge on cybersecurity cooperation.[46] While this may seem like a small step for most other regional organizations, the differences in the capacity and understanding of the ASEAN states is not to be and should not be conflated with the needs, interests, and wants of the individual Southeast Asian states. That is why the Leaders' Vision statement agreed at the ASEAN Summit in April 2018 is significant and should be lauded as a good piece of diplomacy.

An agreed set of norms will benefit and affect all states in the international system, even those that have chosen not to adhere to the norms regime. States may be deterred from flagrantly ignoring the regime because of the risk of reputational loss. Singapore strives to be part of this conversation and is a participant in the Open-ended Working Group and the UN Group of Governmental Experts. These two groups will meet in the upcoming months, and it is imperative that Singapore, through its representation at the UNGGE, represents how small states need to be protected by international law and norms.[47]

Finally, since cyber conflict does not respect borders, there is an urgent need for states to formulate rules or laws to govern international relations in cyberspace. All small states like Singapore should be proactive in participating in norms discussions globally to create a rules-based order for cyberspace and seek to prevent cyber conflict globally lest larger states run roughshod over the interests of smaller states in cyberspace. PRISM

Notes

[1] Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018), 5.

[2] "How a Cyber Attack Transformed Estonia," BBC News, April 27, 2017, available at <www.bbc.com/news/39655415>.

[3] "Petya: Is It Ransomware or Cyberwarfare?" CSO Online, June 29, 2017, available at <www.csoonline.com/article/3204508/petya-is-it-ransomware-or-cyberwarfare.html>.

[4] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 75–77.

[5] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

[6] Clausewitz, *On War.*

[7] Ibid.

[8] Rid, "Cyber War Will Not Take Place."

[9] Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

[10] Valeriano, Jensen and Maness, *Cyber Strategy*, 3.

[11] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, July 22, 2015.

[12] "CyCon 2018 Video: Current and Former Presidents, NATO and Facebook Experts," *ERR News*, May 31, 2018, available at <https://news.err.ee/836012/cycon-2018-video-current-and-former-presidents-nato-and-facebook-experts>.

[13] Cyber Security Agency Singapore, *Singapore Cyber Landscape 2018* (Singapore: Cyber Security Agency

Singapore, 2019).

[14] Michael Leifer, *Singapore's Foreign Policy: Coping with Vulnerability* (New York: Routledge, 2000, 10.

[15] "Singapore's Poison-shrimp Defence," *South China Morning Post*, February 6, 2004, available at <www.scmp.com/article/443461/singapores-poison-shrimp-defence>.

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

[17] Fergus Hanson, "Naming and Shaming the Unshamable," *The Strategist*, April 16, 2018, available at <www.aspistrategist.org.au/naming-shaming-unshameable/>.

[18] The other five pillars of Total Defence are military, civil, economic, social, and psychological defense. Ministry of Defence Singapore, "Fact Sheet: Digital Defence," available at <www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2019/February/15feb19_fs>.

[19] Government of Singapore, *Protection from Online Falsehoods and Manipulation Bill*, Bill No. 10/2019, available at <https://sso.agc.gov.sg/Bills-Supp/10-2019/Published/20190401?DocDate=20190401>.

[20] Kenneth Geers, "The Challenge of Cyber Attack Deterrence," *Computer Law and Security Review* 26, no. 3 (2010): 301.

[21] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2013), 137.

[22] Herbert Lin, "Attribution of Malicious Cyber Incidents," *National Security, Technology, and Law*, 2016, available at <www.hoover.org/sites/default/files/research/docs/lin_webready.pdf>; also, Sean Kanuck, former U.S. National Intelligence Officer, in closed-door roundtable with CENS/RSIS in September 2018

[23] Delbert Tran, "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack," *Yale Journal of Law and Technology* 20, 376.

[24] Aqil Haziq Mahmud, "SingHealth Cyberattack: What You Need to Know," *Channel News Asia*, July 20, 2018, available at <www.channelnewsasia.com/news/singapore/singhealth-cyberattack-what-you-need-to-know-10549096>.

[25] Max Smeets and Herbert S. Lin, "Offensive Cyber Capabilities: To What Ends?" in *2018 10th International Conference on Cyber Conflict Cycon X: Maximising Effects*, ed. T. Minarik, R. Jakschis, and L. Lindstrom (Tallinn, Estonia: CCDCOE, 2018), 55–88.

[26] Ibid.

[27] Australian Strategic Policy Institute, *Cyber Maturity in the Asia-Pacific Region 2017* (Canberra, Australia: ASPI, 2017), available at <www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017>.

[28] "Full Speech: Five Core Principles of Singapore's Foreign Policy," *Straits Times*, July 17, 2017, available at <www.straitstimes.com/singapore/five-core-principles-of-singapores-foreign-policy>.

[29] "Ruling Doesn't Quell Thai-Cambodia Border Row," *Al-Jazeera*, November 13, 2013, available at <www.aljazeera.com/indepth/features/2013/11/ruling-doesn-quell-thai-cambodia-border-row-201311131220753174 7.html>.

[30] ASEAN, "ASEAN Leaders' Vision for a Resilient and Innovative ASEAN," available at <https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Vision-for-a-Resilient-and-Innovative-ASEAN.pdf>.

[31] ASEAN, "ASEAN Leaders' Statement on Cybersecurity Cooperation," available at <https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf>.

[32] Cyber Security Agency Singapore, "ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts," available at <www.csa.gov.sg/news/press-releases/amcc-2018#sthash.ZV7PZrTI.dpuf>.

[33] Anni Piiparinen, "China's Secret Weapon in the South China Sea: Cyber Attacks," *The Diplomat*, July 22, 2016, available at <https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/>.

[34] "Full Speech: Five Core Principles of Singapore's Foreign Policy."

[35] "How Singapore's Military Vehicles Became Beijing's Diplomatic Weapon," *South China Morning Post*, December 3, 2016, available at <www.scmp.com/week-asia/politics/article/2051322/how-singapores-military-vehicles-became-beijings-diplomatic>.

[36] Gulizar Haciyakupoglu and Benjamin Ang, "Civilians in the Information Operations Battlefront: China's Information Operations in the Taiwan Straits," in *DRUMS: Distortions, Rumours, Untruths, Misinformation, and Smears*, ed. Norman Vasu, Benjamin Ang, and Shashi Jayakumar (Singapore: World Scientific, 2019), 83–113.

[37] "Australian Cyber Intelligence Agents Helped Defeat IS," *9 News*, March 27, 2019, available at <www.9news.com.au/national/national-news-australian-cyber-intelligence-agents-helped-defeat-is/527d8b63-cd82-4e0e-ba8a-b2116074eeff>.

[38] "May Vows Revenge on Russia over Salisbury Novichok Poisonings," *The Times*, September 6, 2018, available at <www.thetimes.co.uk/edition/news/may-vows-revenge-on-russia-over-salisbury-novichok-poisonings-93lk85sjr?utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter#Echobox=1536215469>; "Britain Steps Up Cyber Offensive

with New £250m Unit to Take on Russia and Terrorists," *The Telegraph*, September 21, 2018, available at <www.telegraph.co.uk/news/2018/09/21/britain-steps-cyber-offensive-new-250m-unit-take-russia-terrorists/>.

[39] "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," *Washington Post*, September 20, 2018.

[40] Michael Raska, "Cyber Conflicts and Singapore's 'Total Defence' Strategy," *RSIS Commentary*, June 23, 2016.

[41] Government of Singapore, *Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018* (Singapore: Government of Singapore, January 10, 2019), available at <www.mci.gov.sg/coireport>.

[42] Norman Vasu and Benjamin Ang, "Embracing Technology to Boost National Security," TODAY, December 22, 2016, available at <www.todayonline.com/technology-0/embracing-technology-boost-national-security>.

[43] Parliament of Singapore, *Report of the Select Committee on Deliberate Online Falsehoods—Causes, Consequences, and Countermeasures* (Singapore: Government of Singapore, 2018).

[44] Valeriano, Jensen, and Maness, *Cyber Strategy*, 170.

[45] Eugene E.G. Tan, "The Challenge of Getting Responsible Behaviour in Cyberspace," *RSIS Commentary*, October 6, 2017.

[46] ASEAN, "ASEAN Leaders' Vision for a Resilient and Innovative ASEAN," and "ASEAN Leaders' Statement on Cybersecurity Cooperation."

[47] United Nations, "First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct," GA/DIS/3619, November 8, 2018, available at <www.un.org/press/en/2018/gadis3619.doc.htm>.