Small States Learn Different Survival Lessons

Benjamin Ang

Every state wants to learn lessons from the multitude of cyber incidents that strike it and others, so that it can protect itself in the future. But when international cyber incidents are viewed together with geopolitical contestation, the lessons learned by small states are very different from those recognized by the global superpowers. Large states in NATO or the EU need to understand these other lessons to achieve their initiatives in the UN and elsewhere internationally. This chapter conveys five key lessons from the perspective of one small, highly connected state, and its small state neighbors in Southeast Asia. These lessons need to be recognized by the larger, globally dominant nations which seek the support of, or to support, the smaller nations in global cyber conflicts.

Lesson 1: Small states are often on their own when it comes to cyberattacks.

The 10 member states of ASEAN – the Association of South East Asian Nations – are Brunei, Cambodia, Laos, Myanmar, Vietnam, Philippines, Thailand, Malaysia, Indonesia, and Singapore. The dynamic between states is a major factor in their perception of and response to cyber incidents.

ASEAN has some similarities but is quite different from the European Union (EU) or the North Atlantic Treaty Organization (NATO). Key differences that are relevant here:

(1) ASEAN is an inter-governmental organization without pooled sovereignty (unlike the EU which is a supranational organization that has pooled sovereignty).

(2) ASEAN has no parliament but has an Inter-Parliamentary Association, and the ASEAN secretariat is not at all as powerful as the EU secretariat.

(3) ASEAN takes all decisions by unanimous consensus instead of votes. (Tommy Koh, 2017)

These differences illustrate that ASEAN member states do not have sufficient common interests, trust, and shared identity to form the collective security framework needed to establish a NATO-type security structure. (Chau Bao Nguyen, 2016) NATO has pronounced

Benjamin Ang is the Senior Fellow leading Cyber and Homeland Defence research at the Center of Excellence for National Security (CENS), a policy research think tank in the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. His team examines how laws and public policy respond to developments in cybersecurity and information and communications technology, international law and norms, technology nationalism, smart cities, artificial intelligence, disinformation and information operations, foreign interference, social media, and emerging technology.

He draws from private sector experience as a former litigation lawyer, CIO, legal counsel, law lecturer, technology consultant, and even Novell Netware Administrator back in the day. He is a trainer for the UN/Singapore Cyber Diplomacy Programme, presented at the United Nations Open-Ended Working Group on Developments in Information and Telecommunications in International Security, and testified before Singapore's Select Committee on Deliberate Online Falsehoods.

that a serious cyberattack on any of its members would trigger collective defense under Article 5. This has been criticized as lacking clarity, but ASEAN states lack even this framework for collective defense. When it comes to cyberattacks, small states are often on their own. This has implications for their response, as we will see below.

Lesson 2: Small states often lack an international response to cyberattacks.

Asia-Pacific states are increasingly vulnerable to cyber threats, with organizations 80 percent more likely than others to be targeted by hackers, but the global median dwell time (time to detection of breach) in Asia is double the global median. (Christy Un, 2020) ASEAN countries have also been used to launch attacks, either because they have unsecured infrastructure which can be exploited or they are well-connected hubs for initiating attacks. (Dobberstein, 2018).

Despite these challenges, only four ASEAN countries have clearly defined agencies responsible for cybersecurity: Singapore (Cyber Security Agency of Singapore), Malaysia (CyberSecurity Malaysia), the Philippines (Department of Information and Communications Technology), and Indonesia (Badan Siber dan Sandi Negara, the Cyber Body and National Encryption Agency). The rest split responsibilities among the ministries of defense, telecommunications, and police. Singapore, Malaysia, Thailand, and Vietnam have national cybersecurity strategies and legislation. Limited progress has been made across the rest of ASEAN. (AT Kearney, 2018 cited in Ang and Raska, 2018) Almost half of the Asia-Pacific states still do not have national cybersecurity strategies in place. (Christy Un, 2020) More details of the state of cyber maturity can be found in reports from the Australian Strategic Policy Institute (ASPI) and EU Cyber Direct.

Cyber resilience of ASEAN states, measured as their ability to deliver the intended outcome continuously despite adverse cyber events, is hindered by lack of policy leadership in some states. Some of the

notable cyber incidents in ASEAN states of the past few years have included the following:

1. **Vietnam:** Chinese hacking group "1937CN" took over flight information screens and sound systems in two airports and used them to display propaganda supporting China's rule over the South China Sea.
2. **Philippines:** APT32, also known as OceanLotus, which has been linked to Vietnam, breached ASEAN computers in Manila and compromised government agencies in Philippines, Laos, and Cambodia.
3. **Singapore:** SingHealth, the national health care system, was breached and 1.5 million patients' non-medical personal data were stolen; 160,000 dispensed medicines records were taken, including those of the Prime Minister.
4. **Singapore:** A database of 2,400 Ministry of Defencse/Singapore Armed Forces personnel was breached, by phishing a third party vendor.
5. **Singapore:** A list of 14,200 people diagnosed with HIV was copied by the ex-lover of a doctor who had access to the Ministry of Health database.
6. **Thailand and Vietnam:** Toyota customer data were breached, with no details given.
7. **Philippines:** Personal data of 82,150 customers of Wendy's restaurant were breached.
8. **Philippines:** Personal data of 900,000 customers of pawnshop Cebuana was breached.
9. **Thailand:** Personal data of 45,000 customers of True Corp mobile was breached.
10. **Malaysia:** Personal data of 46 million mobile subscribers were breached. (Source: CSO Online)

Only the first three cyber incidents have been attributed to nation-states. The rest were classified as cybercrime. Contrast this with Kaspersky's report that at least seven APTs are carrying out cyber incidents for economic and geopolitical intelligence gathering. In none of these cases do we see public diplomacy being used, or indictments being issued, or 'name and shame' exercises being carried out, against the attackers.

Table 1: APTs carrying out cyber incidents for economic and geopolitical intelligence gathering.

APT	Target countries	Target entities
FunnyDream	Malaysia, Philippines, Thailand, Vietnam	High-level government organizations; political parties
Platinum	Indonesia, Malaysia, Vietnam	Diplomatic and government entities
Cycldek	Laos, Philippines, Thailand, Vietnam	Government, defense, and energy sectors
HoneyMyte	Myanmar, Singapore, Vietnam	Government organizations
Finspy	Indonesia, Myanmar, Vietnam	Individuals
PhantomLance	Indonesia, Malaysia, Vietnam	Entities
Zebrocy	Malaysia, Thailand	Entities (source: Kaspersky)

Lesson 3: Small states usually do not attribute cyberattacks.

In the first cyber incident listed, the media attributed the Vietnamese airport attack to 1937CN because its name was displayed prominently on the screens that had been breached, alongside propaganda supporting China's claim to the South China Sea. This was corroborated by reports from FireEye and Fortinet that there was forensic evidence of 1937CN conducting a phishing campaign targeting Vietnam Airlines. Since 1937CN had claimed responsibility for the attack prima facie, there was no need for the Vietnamese government to prove the attribution. Presumably, Vietnam has the forensic or foreign intelligence capabilities to carry out attribution of cyber incidents, but most of the other ASEAN states do not.

In a confusing twist, 1937CN publicly denied involvement in the attack, while reiterating in the same announcement that the South China Sea belongs to China. 1937CN also described itself as a patriotic hacker independent of the Chinese government. The Vietnamese government has neither pressed the issue nor taken any public steps against China.

This does not mean that Vietnam does not conduct acts against China at all. According to cybersecurity firms, the threat group APT32, also known as Ocean Lotus, which cybersecurity firms have linked to Vietnam (some call it "government-backed"), targeted Chinese government officials during the coronavirus outbreak in January 2020 and aimed to compromise the professional and personal email accounts of employees at China's Ministry of Emergency Management and the Government of Wuhan. To be clear, this is far from an official Vietnamese government action.

The second cyber incident listed has been grouped by cybersecurity firms as a campaign by the above-named APT32. All these attributions have been provided by the private sector, not states. According to this attribution, APT32 carried out attacks on three ASEAN websites, websites of dozens of Vietnamese non-government groups, individuals and media, websites of Chinese oil companies, websites of ministries or government agencies in Laos, Cambodia (ministries of foreign affairs, the environment, the civil service and social affairs, and national police) and the Philippines (the armed forces and the office of the president). (Reuters)

Despite the enormous scale of this attack, Cambodia, Thailand, Laos, and the Philippines did not choose to attribute, or in some cases even acknowledge, this cyber incident. The Philippines' foreign ministry said it would look into the report, with the spokesman asserting "Any credible information received will be investigated and addressed as necessary." Cambodian national police said it did not know who was responsible for the hacks. Officials in Thailand said they were not aware of any hacking of government or police websites. (Reuters)

One reason these governments were reluctant to attribute the attacks may be that they lacked the cyber forensic capability to gather enough evidence to substantiate attribution. This is likely to be the case for Thailand, Cambodia, and Laos, although the Philippines is believed to possess such cyber forensic capability. At the same time, FireEye, which very much has the

cyber forensic capability to substantiate its claims, very publicly and confidently attributed the attacks to APT32 and linked APT32 to Vietnam. Yet, none of the states adopted this stand.

This brings us to the third case, in which Singapore's national healthcare system SingHealth was breached. The Minister described the leak as the most serious, unprecedented breach of personal data in Singapore. A huge public inquiry was conducted through 22 hearings and resulted in a 454-page report. This has been the most public response to a cyber incident in ASEAN to date.

To understand the context, Singapore is considered a regional thought leader in cybersecurity and was ranked at the top in the International Telecommunication Union's Global Cybersecurity Index (GCI) in 2017. Singapore has published its national Cybersecurity Strategy, which outlines its vision, goals, and priorities, and a four-pillar approach to protect essential services from cyber threats and create a secure cyberspace for businesses and communities. Singapore's Cybersecurity Agency (CSA) is the government agency with a core mission to keep Singapore's cyberspace safe and secure. Singapore has even set up the ASEAN-Singapore Cyber Centre of Excellence with a substantial budget to provide cyber capacity building for its ASEAN neighbors.

Of all ASEAN states, Singapore had the capability of identifying the culprit in this cyber incident. Its response, given by the Chief Executive of the CSA, was instructive: "We have determined that this is a deliberate, targeted and well-planned cyberattack, not the work of casual hackers or criminal gangs... beyond this I apologize we are not able to reveal more because of operational security reasons."

Singapore clearly attributed the attack to a nation-state, but stopped short of identifying the nation-state, much less carrying out any cyber diplomacy response.

To understand this better, the theoretical framework of Baram and Sommers (2019) is helpful. They point out that victims of cyber incidents can either "(1) reveal the attack and attribute it to the alleged attacker, or (2) reveal only the fact that the attack had occurred, without attribution." Some victims may choose to "call out" (publicly identify) the aggressor as flouting international laws and norms, as a "naming and shaming" strategy. They may also do this for deterrence, by demonstrating their technical knowhow in identifying the attack and pointing out the entity behind it, because defensive capability can signal general technological competence and a complementary offensive know-how.

However, Baram and Sommers also acknowledge that some victims choose not to identify their attackers, to protect the safety of their intelligence sources, to prevent escalation because exposure may lead to open confrontation, or for both reasons. Singapore's restricted form of attribution appears to have been for the former reason, and we can speculate that the latter reason is also relevant.

In this respect, Singapore asserted its technical capability in identifying the attacker, which may have some deterrent value. It may also have refrained from publicly "naming and shaming" because of the danger of escalation. Singapore has neither publicly claimed nor denied any cyber offensive capability. For strategic reasons, the risks of cyber conflict to this highly connected nation are arguably too great. There is no known Singapore equivalent of APT32 that would carry out deniable operations.

Even if escalation does not go as far as cyber or armed conflict, it could adversely affect trade relationships. Trade relationships among ASEAN member states, and between ASEAN states and their trade agreement partners, are very important for their economic survival, and are described in further detail below.

Singapore notably did not declare that the incident was in breach of international laws and norms. This is significant because Singapore has been one of the key drivers in ASEAN for adoption of international law and norms for cyber operations, and actively involved in the United Nations Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (UN OEWG) and United Nations Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UN GGE) processes. This may be because Singapore determined that the SingHealth breach was an act of espionage, and there is no general prohibitive rule against espionage under international law.

More recently, in Singapore's public statements about the SolarWinds breach, it also refrained from framing it as a breach of international law and norms. This is possibly for the same reason that it determined the act was espionage. (Eugene Tan, 2021)

Lesson 4: Small states' survival is more dependent on trade than cyber.

ASEAN's growth has come on the back of various free trade agreements (FTAs), some of which are the world largest. The ASEAN-Australia-New Zealand Free Trade Area (AANZFTA) covers 90 percent of goods traded among ASEAN, Australia, and New Zealand, for a population of 653 million and over US$4.3 trillion. Under the ASEAN-China Free Trade Area (ACFTA), China has been consistently ranked as ASEAN's largest investor for a decade, with total trade of over US$731 billion in 2020. The ASEAN-India Free Trade Area (AIFTA) is the world's largest free trade area market, creating opportunities for over 1.9 billion people in ASEAN and India with a combined GDP of US$4.8 trillion, and exports from India to ASEAN were US$31 billion for the 2019-2020 period while Indian imports from ASEAN were US$55 billion. Most recently, ASEAN signed the Regional Comprehensive Economic Partnership (RCEP) agreement on November 15, 2020, with Australia, China, Japan, New Zealand, and South Korea. The RCEP is the largest FTA in history and could add US$186 billion to the global economy as well as 0.2 percent to the combined GDP of its members. (Dezan Shira, 2020)

According to the United Nations COMTRADE database on international trade, Philippines exports to Vietnam were US$1.27 billion in 2019, Vietnam exports to Philippines were US$3.46 billion in 2018, Thailand exports to Vietnam were US$11.61 billion and Thailand imports from Vietnam were US$5.01 billion in 2019. Cambodia-Vietnam trade volume reached US$4.8 billion in 2019, an increase of 14% over the same period last year (https://comtrade.un.org/).

All these statistics point to the importance of trade for the small states in ASEAN. The major cyber incidents have been difficult to attribute definitively and appear to be espionage or propaganda, neither of which is prohibited under international law. Weighed against the risk of damaging trade relations, states may decide that it is better to refrain from escalating matters.

Even if calls are met for an independent, global organization to be set up for investigating and publicly attributing major cyberattacks, it is unlikely that ASEAN states will make use of such attribution in public diplomacy. They could use independent attribution in private back-channel discussions, but we will never know.

Lesson 5: Small states cannot defend forward.

With all the limitations and constraints facing small states in ASEAN, most have their hands full with cyber defense, and the idea of defending forward is beyond them. Unlike the US, most small states have no cyber capacity to seize and maintain the initiative across the competition continuum. The consequences for a small state, if it is discovered inside the network of one of the major cyber powers (US, China, Russia), would be disastrous. The adverse effect on trade if a small state is discovered inside the network of one of its trading partners would also be considerable.

It may also be risky to participate in defend forward or "hunt forward" operations initiated by the US. An ASEAN state (country A) is well within rights if it invites the US (country B) into A's networks to take the initiative against adversaries there. However, if country B uses country A's networks to seize the initiative in the networks of a large adversary (country C), there could be blowback from country C against country A. If country C is a major cyber power and/or a major trading partner of country A, this will not end well for country A.

Unlearned Lessons

The overarching lesson that we can learn is that international cyber incidents, viewed together with geopolitical contestation, have a very different impact on small states as compared to that on the global superpowers, and the calculus for response is very different. This must surely influence the positions of the many small states that populate the United Nations, and their interactions with the UN OEWG and UN GGE processes regarding international law and norms for cyber operations. More research is needed. In the meantime, it would be in the interests of the global superpowers to pay heed to the lessons learned by small states.