ASIA CENTRE
centreasia.eu

DGRIS

note

OBSERVATOIRE ASIE DU SUD-EST 2017/2018

Cybersecurity in Southeast Asia

Note d'introduction à la table ronde du 22 mai 2018

*par **Dr Michael Raska**, Assistant Professor in the Military Transformations Programme at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore and **Benjamin Ang,** Senior Fellow and Head of Cyber and Homeland Defence Programme at the Centre of Excellence for National Security, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore*

Note de présentation n°5/8 de l'Observatoire Asie du Sud-Est, cycle 2018-2019
Mai 2018

The digital economy of Southeast Asia is growing rapidly. This brings great benefits to countries in the region but also increases their exposure to cybersecurity threats. Southeast Asian countries face many challenges in improving their cybersecurity, including lack of governance and skilled capacity. Lack of attribution capability also leads to the risk of escalating cyber incidents or cyber-enabled information conflicts within the region. Southeast Asian nations need to develop cyber norms of behaviour to preserve regional stability. In particular, ASEAN member states strongly support the development of cyber norms for ASEAN. Singapore has committed substantial resources to this effort under its own national Cybersecurity Strategy, building capacity and to facilitate norms building in ASEAN. Other Southeast Asian nations have also announced national Cybersecurity Strategies. However, challenges remain for the region.

Maison de la Recherche de l'Inalco
2 rue de Lille
75007 Paris - France
Tél. : +33 1 75 43 63 20
Fax. : +33 1 75 43 63 23
ww.centreasia.eu
contact@centreasia.eu
siret 484236641.00037

The Digital Economy of Southeast Asia

Southeast Asia's digital economy, including e-commerce and ride-hailing services, is projected to reach US $200 billion by 2025. (CNBC, 2017) In particular, Southeast Asian states who are members of the Association of Southeast Asian Nations (ASEAN) have the potential to add US$1 trillion to GDP over the next 10 years. (Dobberstein, 2018) This is no surprise because ASEAN countries like Singapore, Malaysia, Indonesia, and Thailand, invest heavily in digital infrastructure, and in modernizing their economies. (Baka, 2016)

Cybersecurity Issues facing Southeast Asia

This increase in internet use makes Southeast Asian nations more prone to cyberattacks resulting in a data breach or system failure. (Baka, 2016) Philippines, Singapore, Vietnam and Indonesia, are particularly at risk. Singapore (along with Australia, Japan, New Zealand, and South Korea) is one of the "Cyber Five" countries that are disproportionately vulnerable to cyberattacks because of their reliance on technology. (Baka, 2016)

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). Some notable incidents include:

- In July 2016, Vietnam was cyberattacked by Chinese hacking group '1937CN' that hijacked the flight information screens and sound systems in Noi Bai and Tan Son Nhat airports, resulting in loss of local control, and broadcasting anti-Vietnamese and Philippines propaganda.

- Hacking group APT32, also known as OceanLotus, which was previously linked to the Vietnamese government, is reported to have broken into the computers of ASEAN before the summit of regional leaders in the Philippines capital Manila. They also compromised websites of ministries or government agencies in Laos, Cambodia and the Philippines, so they would load malicious code onto the computers of targeted victims. The targets included Cambodia's ministries of foreign affairs, the environment, the civil service and social affairs, and national police; Philippines' armed forces websites and the office of the president; the websites of dozens of Vietnamese non-government groups, individuals and media; and websites belonging to several Chinese oil companies. (Reuters, 2017)

- Indonesia experiences more than 50,000 cyberattacks daily and is the second most targeted country for cyberattacks, following Vietnam. The public and private sectors suffered 3.9 million cyberattacks from the 2010-2013. Indonesia overtook China as the number one source of cyber-attacks in the second quarter of 2013. (Kelleher, 2017)

These cyber risks could impede trust in the digital economy and prevent the region from realizing its full digital potential. (Dobberstein, 2018)

Challenges for Cybersecurity in Southeast Asia

There are many challenges for improving cybersecurity in Southeast Asia.

- Many Southeast Asian countries lack a strategic mind-set, policy preparedness, and institutional oversight over cybersecurity. (Dobberstein, 2018). Responsibility may be split between national police (for cybercrime), interior ministry (for critical infrastructure), telecommunications ministry (for breaches), and military (for cyber conflicts), with little or no coordination. The absence of a unifying framework often results in significant underinvestment.

- In the private sector, cyber risk is still perceived to be an information technology (IT) rather than a business problem, so regional businesses do not have a comprehensive approach to cybersecurity.

- The region's cybersecurity industry struggles to meet demand because it lacks capabilities and expertise (Dobberstein, 2018)

- Growing interconnectedness between Southeast Asian economies will intensify the systemic risk.

- Southeast Asian nations have limited sharing of threat intelligence, often because of mistrust and a lack of transparency.

- Rapid technological evolution makes threat monitoring and response more difficult, especially with more powerful encryption, cloud computing, and the widespread growth of the Internet of Things (IoT). (Dobberstein, 2018)

Cyber-Enabled Information Conflicts in East Asia

While cyberattacks on the confidentiality, integrity, and availability of data (commonly called "hacking") are worrying, what causes even greater concern is the growth of cyber-enabled information conflicts in the East Asian region, and particularly Southeast Asia.

In East Asia, cyber-enabled information conflicts are increasingly shaping the character of regional security flashpoints: the struggle for dominance by the region's two major powers (China and Japan); the future of the Korean Peninsula; intra-regional competition in territorial disputes in the East China Sea and South China Sea; and long-term regional strategic competition between China and the United States. In particular, every major security issue in East Asia reflects parallel and continuous confrontations in and out of cyber space, and varying cyber and information operations by both state and non-state actors. On one hand, these "hybrid" operations serve as asymmetric means of warfare, providing a range of options that pose relatively lower risks of escalation or without any visible military commitments. The character of asymmetric cyber-attacks, however, may also increase the propensity for offensive and unrestricted character of cyber operations given the prevailing perceptions of lesser risks of detection, the lack of accountability, and the resulting low probability of successful deterrence.

As conflicts move into the cyber and information domains, there is an ongoing debate on the magnitude and impact of cyber and information operations on East Asian security. On one hand, sceptics argue that there are serious limitations with regard the use of cyberspace for political purposes, particularly at the higher end of the conflict spectrum in East Asia. In this view, cyber-enabled information operations alone cannot strengthen capabilities for coercion or deterrence – they do not transform regional power structures, do not replace the military capabilities of the most advanced powers in the region, and ultimately, have a limited utility to achieve desired political outcomes. Consequently, they may not provide significant strategic advantages in achieving political objectives. The prevailing view, however, is that regional conflicts and potential flashpoints in Asia Pacific already transcend into the cyber and information domains and have significant political ramifications. Indeed, the confluence of varying cyber strategies and information operations capabilities in the broader context of regional power transitions shapes the direction, pace, character of military change in Asia Pacific.

In particular, cyber-enabled information operations enable and reinforce strategic ambiguity in terms of effects, sources, and motives, and therefore can be used to deny or create political outcomes without visible military commitments. Second, the deepening systemic interdependencies brought by information technologies in nearly all aspects of governance (i.e. energy systems, communications, water, transportation, finance, etc.) render traditional conceptions of deterrence and defense vulnerable to strategic surprises - asymmetric forms of information and cyberwarfare. Third, cyber-enabled information operations – defensive, offensive, and intelligence-driven increasingly serve as a key enabler and force-multiplier of kinetic operations – enabling actions, capabilities, and effects of land, sea, air, and space operations in all physical domains. Fourth, cyber operations are synonymous with information operations – in the ability to penetrate target audiences in real time. For example, crafting messaging campaigns to go "viral" to shape perceptions, narratives, and create cognitive effects in which online behavior has offline consequences and vice versa. Fifth, cyber-enabled information warfare capabilities evolve parallel with military-technological advances such as electronic miniaturization, additive manufacturing, nano-technologies, artificial intelligence, space capabilities, and unmanned systems that alter the character of future warfare. Given the varying levels of socio-economic development, defense resource allocation, and military-technological trajectories, there will also be considerable variation in the adaptation of cyber capabilities. The variance will also reflect different strategic cultures and doctrinal conceptions on the use of cyber means as instruments of warfare.

For the Chinese People's Liberation Army (PLA), for example, achieving "information dominance" (*zhi xinxi quan*), controlling electromagnetic spectrum, while prioritizing computer network defense represent key prerequisites for air and naval superiority as well as for establishing "space dominance" (*zhi tian quan*). (Krekel, Adams, & Bakos, 2012) In this context, the PLA is conceptualizing "integrated strategic deterrence" through a holistic representation that includes simultaneous and coordinated use of offensive and defensive electronic warfare (EW), military space and counter-space, along with "network reconnaissance" and "network attack and defense operations" in varying security conditions - peacetime, crisis, and war. (Chase & Chan, 2016) According to the 2015 *Defense White Paper*, "the development of the world revolution in military affairs is deepening" while "the form of war is accelerating its transformation to informationization." (Information Office of the State Council of the People's Republic of China, 2015) Its strategic assessments of the "form of war" have changed from "integrated operations, precision strikes to subdue the enemy," articulated in the 2004 *Defense White Paper*, to "information dominance, precision strikes on strategic points, joint operations to gain victory." (Fravel, 2015) In this context, the PLA has prioritized the development of long-range, precision, smart and unmanned weapons and equipment, and space and cyber operations.

At the same time, China's foreign policy uses economic leverage and "soft power" diplomacy as primary means of power projection, Beijing has been also actively exploiting concepts associated with strategic information operations to direct influence on the process and outcome in areas of strategic competition. In 2003, the Central Military Commission (CMC) approved the guiding conceptual umbrella for information operations for the People's Liberation Army (PLA) – the "Three Warfares" (*san zhong zhanfa*). The concept is based on three mutually-reinforcing strategies: (1) the coordinated

use of strategic psychological operations, (2) overt and covert media manipulation, and (3) legal warfare designed to manipulate strategies, defense policies, and perceptions of target audiences abroad. Historically, the primary target for China's information and political warfare campaigns has been Taiwan. Since the 1950s, for example, the Nanjing Military Region's 311 Base (also known as the Public Opinion, Psychological Operations, and Legal Warfare Base) in Fuzhou City, Fujian Province, broadcasted propaganda at Taiwan through the "Voice of the Taiwan Strait" (VTS) radio. At the same time, China's information operations attempted to exploit political, cultural, and social frictions inside Taiwan, undermining trust between varying political-military authorities, delegitimising Taiwan's international position, and gradually subverting Taiwan's public perceptions to "reunite" Taiwan on Beijing's terms.

Prior to the 2016 organizational reforms of the People's Liberation Army (PLA), the strategy of "Three Warfares" was the responsibility for the PLA's General Political Department- Liaison Department (GPD/LD). In the past, the GPD-LD supported civilian and business platforms working to "promote Chinese culture" abroad such as the China Association for Promotion of Chinese Culture (CAPCC); China Association for Friendly International Contacts (CAIFC); China-U.S. Exchange Foundation (CUSEF), The Centre for Peace and Development Studies (CPDS), External Propaganda Bureau (EPB), and China Energy Fund Committee (CEFC). In doing so, the GPD/LD has been associated with PLA's military intelligence networks, identifying select foreign political, business, and military elites and organisations abroad relevant to China's interests or potential "friendly contacts." In their research, they analyse their position toward China, career trajectories, motivations, political orientations, factional affiliations, and competencies. The resulting "cognitive maps" guide the direction and character of tailored influence operations, including conversion, exploitation, or subversion. Meanwhile, the GPD's Propaganda Department broadcasts sustained internal and external strategic perception management campaigns through mass media and cyberspace channels to promote specific themes favourable for China's image abroad – political stability, peace, ethnic harmony, and economic prosperity supporting the narrative of the "China model" (*zhongguo moshi*).

In China, the strategic competition for the research, development, and acquisition of cutting-edge military technologies, including cyber capabilities that would enable the People's Liberation Army (PLA) to fight and win "informationized local wars" is embedded in the concept of military-civil integration – MCI (*junmin ronghe*, 军民融合). According to the 2015 *China Military Strategy*, "China will work to establish uniform military and civilian standards for infrastructure, key technological areas and major industries, explore the ways and means for training military personnel in civilian educational institutions, developing weaponry and equipment by national defense industries, and outsourcing logistics support to civilian support systems." (Information Office of the State Council of the People's Republic of China, 2015) While the MCI builds upon established principles of civil-military integration (*yujun yumin*, 于军于民), which have for over two decades promoted the development of dual-use technologies and combined defense and civilian industrial bases,[1] President Xi Jingping has elevated MCI into a national-level strategy:[2] "the integration of civilian and defense development will involve multiple fields and enable economic progress to provide a 'greater material foundation' for defense construction, while the latter offers security guarantees for the former." (Xinhua News, 2016) In this context, MCI aims to further integrate state-owned defense research, development, and manufacturing enterprises, government agencies under the State Council, universities, and private sector firms in order to advance PLA's military modernization, while supporting China's economic growth. (Levesque & Stokes, 2016)

MCI strategy also relies on foreign acquisition of dual-use technologies, resources, and knowledge in select priority areas identified in long-term defense science & technology plans such as the newly formulated "Defense Science and Technology Industry 2025 Plan" (国防科技工业2025) and the "Made in China 2025 Plan (中国制造2025). (Tai, et al., 2015) These plans represent a follow-on to the "2006-2020 Medium- and Long-Term Plan on the Development of Science & Technology", and "Strategic Emerging Industries Plan of 2010" (战略性新兴产业) that emphasized "Indigenous Innovation" (自主创新) or absorptive capacity to recognize, assimilate, and utilize external knowledge to accelerate the development of China's advanced technologies in both civil and military domains.[3]

According to the 2016 *US Department of Defense Annual Report to Congress*, "China continues to supplement indigenous military modernization efforts through the acquisition of targeted foreign technologies, including engines for aircraft, tanks, and naval vessels; solid state electronics and microprocessors, guidance and control systems; enabling technologies such as cutting-edge precision machine tools; advanced diagnostic and forensic equipment; and computer-assisted design, manufacturing, and engineering." (Defense, 2016) In doing so, the US sees China conducting various forms of cyber espionage, (Lindsay & Ming-Cheung,

1 - Under the principle of *Yujun Yumin* – "locating military potential in civilian capabilities," prioritized in the 2004 Defense White Paper, subsequent Five-Year Defense Plans, as well as in the 2006-2020 Medium- and Long-Term Defense Science and Technology Development Plan (MLP), China embarked on a series of defense industry reforms that would translate into qualitative technological advances for the People's Liberation Army (PLA). See: Information Office of the State Council of the People's Republic of China, *China's National Defense in 2004*, 27 December 2004, http://www.gov.cn/english/2006-02/09/content_183426.htm; Eric Hagt, 'Emerging Grand Strategy for China's Defense Industry Reform,' in Roy Kamphausen, David Lai, and Andrew Scobell (eds.) *The PLA at Home and Abroad: Assessing the Operational Capabilities of China's Military* (Carlisle, PA: U.S. Army War College, 2010), p. 481-484.

2 - "Military-civilian cooperation, as a national strategy, is crucial to national security and the bigger picture of development." Xinhua News, 'Xi Urges Greater Military-Civilian Cooperation for Strong Army', 19 October, 2016, http://news.xinhuanet.com/english/2016-10/19/c_135766754.htm.

3 - Tai Ming Cheung, 'The Chinese Defense Economy's Long March from Imitation to Innovation', *Journal of Strategic Studies*, vol.34, no. 3, 2011, p.343-344; Scott Kennedy, 'Made in China 2025', Center for Strategic & International Studies, 1 June 2015, https://www.csis.org/analysis/made-china-2025.

2015) in order to "reduce the costs and lead time" of select PLA's military modernization programs, mitigate technological risks and structural deficiencies in China's defense industries, and bypass long-standing export controls of sensitive military technologies to China. (Alexander, 2013)

The issue of cyber espionage has consistently raised tensions in the Sino-US relations. In February 2016, for example, the Director of National Intelligence, James R. Clapper, delivered his annual threat briefing to the Senate Armed Forces Committee noting that China remains engaged in malicious activities in cyberspace against the United States, despite a US-Chinese bilateral agreement to refrain from conducting or knowingly supporting commercial cyber-espionage. "China continues to have success in cyber espionage against the US government, our allies, and US companies…. Beijing also selectively uses cyberattacks against targets it believes threaten Chinese domestic stability or regime legitimacy." (Clapper, 2016) At the same time, leading US cyber experts have shared concerns over Chinese cyber penetrations of both commercial and government networks. (Lewis, 2013) These views are reflected in other influential US government reports such as the Department of Defense's *2015 Annual Report to Congress* on China. (Office of the Secretary of Defense, 2015)

Meanwhile, China's policy makers at the highest levels have refuted these allegations, arguing that the Chinese military does not steal commercial secrets or support Chinese companies which do so. Prior to his state visit to the United States in September 2015, for example, president Xi Jinping said in a written interview with the *Wall Street Journal* that "cyber theft of commercial secrets and hacking attacks against government networks are both illegal; such acts are criminal offences and should be punished according to law and relevant international conventions. China and the United States share common concerns on cyber security." (Hutzler, 2015) Other Chinese government sources have become more direct in criticizing the US for its 'double standard' – accusing China, while conducting cyber-espionage itself. In particular, China points to the National Security Agency (NSA) cyber-activities against other countries as revealed by Edward Snowden, and views them as a threat to China. In May 2014, the Ministry of National Defense of the PRC issued a statement accusing the U.S. of hypocrisy, "from the 'WikiLeaks' to the 'Snowden' incident, the U.S. hypocrisy and double standards on the issue of network security has long been obvious."[4]

Taken together, strategic competition in East Asia is reflected in how great powers use non-military methods of thought to 'win' wars by means of intense political, economic, information, and military pressure during peacetime. These "indirect" actions include the use of information operations and political warfare, cyber-attacks, electronic warfare, paramilitary operations, and potentially, limited strikes in targeted areas without escalating to a major conflict. An important feature of new types of conflicts is in the varying struggles for influence – skilfully merging strategies of denial, deception, disruption, and subversion. They are designed to misinform and manipulate the adversary's picture of reality; to interfere with the decision-making processes of individuals, organisations, governments and societies; and to influence it in order to produce favourable conditions for promoting strategic goals without actual fighting.

In many ways, the confluence of advanced cyber and information warfare strategies creates new weapons of mass effectiveness. The weaponisation of social media, for example, provides new tools for both state and non-state actors to seed ideas, deliver "tailored" information campaigns, and in doing so, influence perceptions of events or environment in real time. As a result the effective use of social media can shape strategic outcomes of conflicts before they actually happen. Meanwhile, the continually evolving cyber-attacks coupled with the use of disinformation, concealment, and deception instigate strategic uncertainty on the magnitude and scope of potential cyberwars. At the same time, regional militaries pursue cross-domain coercion strategies. These involve deterring a military action in one domain with a threat of using force in another domain; the domains merge traditional physical environments – land, sea, air, and space; with digital and information spheres in cyberspace domain. The key aim is to manipulate the adversary's perceptions, shape its decision-making process, and strategic choices, while minimising the scale of kinetic force. Most importantly, they are waged during peacetime and wartime, simultaneously in domestic and external information spheres.

ASEAN and Cyber Norms

Both cyber-enabled information conflicts and cyberattacks on critical infrastructure run the risk of escalating into larger conflicts in Southeast Asia. Cyberattacks can be routed through any number of third party countries, but many Southeast Asian nations lack the means of accurately attributing the true source of said cyberattacks. The risk of wrong attribution is high, where country A thinks that it is retaliating to a cyberattack from country B, but is in fact starting a conflict against the innocent country B. As a result, Southeast Asian nations in general, and ASEAN member states in particular, are looking towards the development of cyber norms of behaviour and confidence building measures in order to preserve the stability of the region.

4 - Ministry of National Defense of the PRC, 'Defense Ministry spokesman Geng Yansheng's Remarks on the US Justice Department sued Chinese soldiers,' *MND Press Release* (May 20, 2014), Available at: http://news.mod.gov.cn/headlines/2014-05/20/content_4510313.htm

The Strategy of Developing Cyber Norms

Norms have a long-standing history in reducing conflict between states.[5] More recently, norms have been discussed and developed as a means of reducing conflict in cyberspace. Broad adoption of cybersecurity norms can help promote social and economic development, as well as improve stability in Southeast Asia. (Microsoft, 2017)

The international development of cyber norms was led by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), which affirmed in 2013 that international law is "applicable and essential to maintaining peace and stability and promoting an open secure, peaceful and accessible ICT environment." The UNGGE subsequently recommended eleven such norms in 2015.[6] (Microsoft, 2017)

These were agreed upon by the international community, with a view to subsequently contextualize and integrate them to national and international strategies. The UNGGE met again in 2017, to clarify how the 2015 agreement should be implemented, but the members were unable to reach a consensus. This political setback indicates that global consensus on cybersecurity norms is unlikely to materialize in the near term. But regions like OAS and ASEAN are trying to develop regional agreements on cybersecurity norms instead.

5 - International norms have been developed in areas such as nuclear nonproliferation and human rights with great success in generation global consensus around key issues. Norms are different from binding international law or domestic regulation, in that deviation from them isn't unlawful, but may lead to censure by other actors. Norms can promote responsible behavior by actors in an international environment, thereby ensuring predictability and reinforcing stability. While only one of several tools for promoting international stability, they are generally easier to agree to than a treaty, and easier to change, making them adaptive to an ever-evolving international stage.

6 - 1. Limiting Norms
a. States should not knowingly allow their territory to be used for wrongful acts using ICT.
b. States should not support or conduct cyber-attacks that damage critical infrastructure.
c. States should seek supply chain security and avoid proliferation of harmful tools and techniques into the market.
d. States should consider all relevant information, when attributing cybersecurity incidents;
e. States should avoid attacking Computer Emergency Response Teams (CERTs) and should not use CERTs for cyber-attacks.
f. States should respect human rights online.
2. Positive Duties Of States
a. States should improve information sharing, in particular on terrorist and criminal use of ICTs.
b. States should cooperate and respond to requests for assistance related to protecting their critical infrastructure.
c. States should protect their critical infrastructure.
d. States should engage in responsible reporting of ICT vulnerabilities.
e. States should cooperate in developing and applying measures to increase stability and security in the use of ICTs.

ASEAN Progress on Cybersecurity

ASEAN's statement to the United Nations in 2017 expresses support for promoting international voluntary cyber norms of responsible State behavior and the development of a rules-based cyberspace. The Plan of Action to implement the Joint Declaration on Comprehensive Partnership between ASEAN and the UN (2016-2020) highlights the need for closer cooperation between ASEAN and the UN in cyber. (Teo, 2017)
Areas of cooperation in ASEAN include

- The ASEAN Regional Forum (ARF) – established to foster constructive dialogue and consultation on political and security issues of common interest and concern, and to make significant contributions towards confidence building and preventive diplomacy in the Asia-Pacific region.

- The ASEAN Network Security Action Council (ANSAC) - set up to promote CERT cooperation and sharing of expertise.

- The ASEAN Cybersecurity Cooperation Strategy - a roadmap towards a more coordinated approach to building capacity in incident response

- The Inter-Sessional Meeting on Security of and in the use of ICTs under the ASEAN Regional Forum (ARF) platform – set up to discuss confidence building measures;

- Annual Cyber SEA Games - to develop cybersecurity talent and expertise.

- ASEAN Leaders and Ministers affirming, at the 31st ASEAN Summit and the second ASEAN Ministerial Conference on Cybersecurity, the need for closer coordination of cybersecurity efforts and adoption of basic cyber norms (based on the UNGGE 2015 report).

- Asia Pacific Computer Emergency Response Team (APCERT), which conducts capacity building and information sharing for CERTS from more than 20 countries in the region, also coordinates with other regional CERTS (e.g. Organization of Islamic Cooperation).

- Regional cybersecurity capacity building activities like the annual ASEAN CERT Incident Drills (ACID) (Microsoft, 2017)

- Council for Security Cooperation in the Asia Pacific (CSCAP) hosted a workshop on cybersecurity in Semarang, Indonesia, in 2017, the day before the ARF Inter-Sessional Meeting on Counter-Terrorism and Transnational Crime, for 30 officials and experts from 15 countries (CSCAP, 2017).

Importance of multi-stakeholder approach

The private sector is also important, because in most Southeast Asian countries, the majority of critical infrastructure is held by private companies and/or uses private sector software, hardware, and services. Technology companies like Microsoft have published papers to highlight their interest in partnering with governments in the development of cybersecurity standards, norms, and policies. (Microsoft, 2017)

Some countries also build information-sharing relationships with governments and industry stakeholder groups from outside the region, such as the Monetary Authority of Singapore's information-sharing relationship with the global Financial Services Information Sharing and Analysis Center (FS-ISAC). (Microsoft, 2017)

Case Study: Singapore's Strategy for Cybersecurity

Singapore's Cyber Threat Landscape

Singapore has a high level of Internet connectivity, and is particularly susceptible to cyberattacks. The victims include Small and Medium Enterprises (SMEs), individuals and Critical Information Infrastructure (CIIs), including the Government, Healthcare, and Banking & Finance sectors. (CSA, 2017) Threat actors range from script kiddies (beginners) to Advanced Persistent Threats (APTs) (state-sponsored attackers) and organized crime. The Singapore Police Force reported that the proportion of cybercrimes to overall crime cases increased from 7.9 per cent in 2014 to 13.7 per cent in 2016, while cases reported under the Computer Misuse and Cybersecurity Act (CMCA) more than doubled year-on-year to 2016. (CSA, 2017)
Prevalent cyber threats observed in Singapore's cyberspace in 2016 were

1. **Website defacements**[7] - 1,750 website defacements were reported. Most belonged to SMEs from a range of businesses, including interior design, logistics, manufacturing and construction.

2. **Phishing**[8]- 2,512 phishing URLs with a Singapore-link were found. 30 per cent were Banking and financial services websites, followed by government organisations (Ministry of Manpower (MOM) and Immigration & Checkpoints Authority (ICA), and online payment service provider PayPal.

3. **Ransomware**[9] - Trend Micro detected about 550 ransomware-related threats in Singapore each day.

4. **Command & Control (C&C) Servers**[10] (CSA, 2017) - More than 60 C&C servers, which can be used to launch denial of service attacks, were observed within Singapore's cyberspace in 2016.

Singapore's strategy for Cybersecurity in ASEAN

Singapore's launched its Cyber Security Strategy in 2016 with four pillars: (CSA, 2016)

1. Strengthen the resilience of our Critical Information Infrastructure.

2. Mobilise businesses and the community to make cyberspace safer, by countering cyber threats, combating cybercrime and protecting personal data.

3. Develop a vibrant cybersecurity ecosystem comprising a skilled workforce, technologically-advanced companies and strong research collaborations, so that it can support Singapore's cybersecurity needs and be a source of new economic growth.

4. Step up efforts to forge strong international partnerships, given that cyber threats do not respect sovereign boundaries.
   - Forge international and ASEAN cooperation to counter cyber threats and cybercrime.
   - Champion international and ASEAN cyber capacity building initiatives in operational, technical, legislative, cyber policy and diplomatic areas.
   - Facilitate exchanges on cyber norms and legislation. (CSA, 2016)

To complement existing ASEAN efforts, Singapore launched a S$10 million (US$7.3 million) ASEAN Cyber

7 - Hackers change the visual appearance of a single webpage or an entire website by gaining unauthorised access to the web hosting server. Defaced websites may also contain malicious code to infect visitors to the affected site. The motivation is to promote political or religious agendas through "hacktivism", achieve online fame in hacker communities, and/or distract victims from the "real" cyber-attack such as a data breach.

8 - Websites that are compromised or created by hackers to trick Internet users into believing they are accessing a legitimate, trusted website. Motivation: Obtain personal information, which can be used for future cyber-attacks, and/or financial gain

9 - A type of malware that encrypts files on a victim's device, rendering them unusable until a ransom is paid, usually in the form of Bitcoin. It is spread through e-mail or malicious advertisements that appear when users access unsafe websites.

10 - A C&C server is a machine operated by hackers to communicate with devices that have been infected with malware. Instructions are communicated to the group of infected devices, collectively known as a botnet, to perform malicious activities such as DDoS attacks. A DDoS attack occurs when a system is bombarded with large volumes of data or specially-crafted malicious traffic sent from a botnet, affecting the system's ability to respond to legitimate users in a timely manner. Motivation: Conduct malicious activities such as data theft, e-mail spam campaigns and DDoS attacks. DDoS attacks create disruptions to victim's business operations, and/ or distract victim from the "real" cyber-attack such as a data breach.

Capacity Programme (ACCP) to help fund efforts to deepen cyber capacities across ASEAN Member States. This has been used to fund resources, expertise and training, technical training and incident response training, discussion and consultancy work, formulating cybersecurity strategies, and advice on legislation. Examples included capacity building workshops for ASEAN member states, conducted in Singapore in conjunction with US State Department, UNIDIR, Australia, and The Netherlands.

Other Southeast Asian responses

Other Southeast Asian nations have varying degrees of cybersecurity maturity. 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). Singapore, Malaysia, Thailand, and Vietnam drafted cyber-security bills in 2017. Limited progress has been made across the rest of ASEAN. (AT Kearney, 2018)

Malaysia

Malaysia has been hailed as one of the most progressive ASEAN nations in terms of cybersecurity strategy, because of the establishment of a national agency to consolidate and coordinate cybersecurity agenda, drafting a cybersecurity bill and a comprehensive plan to develop cybersecurity professionals to meet growing demand. (AT Kearney, 2018)

Indonesia

The Indonesian Government created the National Cyber Security Agency (BCN) in 2017, mainly to prevent and respond to cyberattacks. The agency will also work to increase public awareness about the cyber security landscape. (Kelleher, 2017) Experts recommend that the next step would be for officials to set an agenda and outline a robust national cyber security strategy, and to define the roles and responsibilities within the newly introduced national cyber security agency. (Watada, 2018)

Philippines

Philippines' Department of Information and Communications Technology (DICT) released the National Cybersecurity Plan 2022 (NCSP) in May 2017. The NCSP is intended to shape the policy of the government on cybersecurity and the crafting of guidelines, and to provide a coherent set of implementation plans, programmes, and activities to be shared with all stakeholders. The primary goals of NCSP 2022 include: (1) assuring the continuous operation of the Philippines' critical infostructure (CII), and public and military networks; (2) implementing cyber resiliency measures to enhance ability to respond to threats before, during, and after attacks; (3) effective coordination with law enforcement agencies; and (4) a cybersecurity-educated society. (Bhunia, 2017)

Vietnam

Vietnam has formulated a cyber security strategy to detect and prevent cyberattacks, focusing on national key networks such as transport, banking, aviation, and ministries. Pursuant to this strategy, a law on cyber-information security (LCIS) was passed November 2015, to ensure the safety and security of information and protect personally sensitive information. (Baka, 2016)

On the military side, Vietnam announced the establishment of a Cyber Command, under Ministry of National Defence, in early 2018, to protect military and defence information systems, as well as the nation's important information/ data. Its roles include safeguarding the national sovereignty in cyberspace and information technology. Vietnam also revealed that it has a 10,000-strong military cyber warfare unit to counter "wrong" views on the Internet, (Bhunia P. , 2018) illustrating the concerns that many Southeast Asian countries have about cyber-enabled information warfare.

Thailand

The Thai Defense Minister announced in 2015 that Thailand would establish a military group to counter growing cyber threats. Royal Thai Armed Forces (RTAF) said that the new unit would comprise all three armed forces as well as the Royal Thai Police. (Parameswaran, 2015)

In 2018, Thailand's Digital Economy and Society (DE) Ministry announced plans to set up a cybersecurity agency and hacker training centre to serve Thailand's digital economy. (Apisitniran, 2018)

China's impact on Southeast Asian Cybersecurity

As the largest cyber power in Asia, China's actions have great impact on Southeast Asian cybersecurity. The Chinese Cyber Security Law (CSL) came in effect in June 2017, and increased Beijing's control over information flows to build a 'secure and controllable' domestic infrastructure. This affects Southeast Asian businesses with interests in China, as they face operational challenges in sharing information with their counterparts overseas, have to keep China-generated data locally, and any information transfers will have to undergo a local security audit to gain government approval. (Sidek, 2017)

China also has views on cyber norms that differ from the UNGGE, and can influence the development of cyber norms in ASEAN, through ASEAN Members states that are close to China. Former Malaysian Prime Minister Najib Razak signed nine agreements with China for proposed investments worth $7.2 billion. Indonesia's President Joko Widodo signed a $5 billion loan facility for the country's Jakarta-Bandung high-speed rail link. Vietnam's president, Tran Dai Quang, used his first state visit to seek a boost in Chinese imports of Vietnamese farm produce, and signed five agreements on economic and technological cooperation. (Bloomberg, May 2017)

Conclusion

As ASEAN chairman in 2018, Singapore has announced that it seeks to connect ASEAN's people and economies seamlessly in a network of smart cities, as well as to boost cyber security, with priority towards developing "norms that will guard cyber security" (speech by Singapore Foreign Minister Vivian Balakrishnan, 2018). In support of this, Singapore CSCAP is in the process of proposing a study group on cyber norms which can inform the next ARF Inter-Sessional Meeting.

The authors suggest that the greatest challenges at this time are:

(1) ASEAN member states have different stages of cybersecurity policy development. They need to establish government agencies that are officially responsible for developing cybersecurity policy, to drive the development of cyber norms from within their states.

(2) There is a need to develop capacity in Track 2, for ASEAN academics in the field of cybersecurity policy, as well as civil society in ASEAN member states, to discuss cooperation and the development of cyber norms, in order to support the efforts at governmental level.