Newsletter

LET'S TALK: CYBER SECURITY AND CYBER DIPLOMACY

VOLUME 5 | JANUARY 2023

Cyber Crimes: A Threat to Society (Unsplash.com)

Cyber Security: Securing Our Digital Borders Through Cyber Diplomacy

By Adli Amirul Hisyam bin Mohd Yusof

Introduction

The COVID-19 outbreak has boosted the demand for remote working, e-commerce, e-learning, and a plethora of other digital services due to worldwide lockdown measures. This accelerated digital shift has prompted a stealthier outbreak in the cyber world, dubbed the 'ransomware epidemic', with the number of cyber crimes almost doubling in 2021 compared to 2020 (NCC Group, 2021). Nation-states with a vision of digital government transformation are finding cyber security a major challenge, Malaysia included.

According to the Economic Planning Unit (2021), the Malaysian government, through the MyDIGITAL initiative, aims to move 80 percent of all government documents and public services into cloud. This is an effort to lay the digital foundation for the country and signal the public sector's commitment in digitalisation. This raises the questions of: is our cyber space sufficiently resilient to host critical government operations; do we have the expertise required to defend ourselves against cyber attacks; how can our foreign policy help ensure a safe and secure cyber space?

Understanding the Risks

In his *Art of War*, Sun Tzu said: "Know your enemy and you can win a hundred battles". In our war against cyber crimes, it is thus important to identify the threats, evaluate the risks, and assess the potential impacts of cyber attacks to our assets.

The spectrum of cyber threat actors is extremely broad, from recreational hackers to big nation-states with varying levels of sophistication. Both have a similar goal: accessing sensitive information to advance financial or political motives. Corporations are constantly exposed to social engineering cyber crimes like phishing and spoofing that manipulate users into divulging personal information.

While these have wide-ranging financial impacts to the private sector, the magnitude of impact is nowhere near that of a political cyber warfare launched

A poster showing six wanted Russian military intelligence officers (Photo by AP Photo/Andrew Harnik)

The First ASEAN Digital Ministers Meeting (ADGMIN), held via video conference in January 2021
(Photo from ASEAN.org)

between nation-states. These attacks could result in the failure of a country's critical infrastructure and essential services including medical facilities, financial system, energy, water, and sanitation infrastructures.

Consider the case of Estonia – one of the world's most advanced digital governments – which became the target of Russian hackers in 2007 causing a total paralysis of Estonian government agencies, banks and media outlets. It was the first cyber assault in the world to cripple a country's digital infrastructure and has since been dubbed Cyber War I.

Malaysia has not been spared by financially and politically motivated cyber attacks. In 2020, Chinese hackers were suspected to be behind attempts to steal data on government-backed projects. According to the Malaysia Computer Emergency Response Team (2021), over 10,000 cyber incidents were recorded in 2021. Malaysia stands to suffer up to RM51 billion in economic loss due to cyber security incidents, representing over 4 percent of the national GDP (National Cyber Security Agency, 2019).

The transnational nature of cyber attacks means they can affect government networks and industrial supply chains across different nation-states. Much like the physical world, the cyber space has military and strategic dimensions that require governments to collaborate to defeat cyber opponents. Never has the realm of digital policies been so important in intergovernmental discussions, making cyber diplomacy a critical foreign policy issue to protect countries' critical infrastructures, democracies, and ultimately, citizens.

Cyber Diplomacy, the ASEAN Way

With a population of over 660 million people across 10 countries, ASEAN is the fastest growing digital market in the world. As most cyber assets are owned and operated by private entities around the region, ASEAN governments must build consensus on the regulatory principles governing cyber space to

ASEAN Digital Master Plan 2025 was adopted at the First ASEAN Digital Ministers Meeting (ADGMIN) in January 2021 (Photo by ASEAN)

ensure responsible use of ICT resources by public and private actors.

The ASEAN Cyber Security Strategy 2017-2020 was the first roadmap to coordinate regional cyber security cooperation. The ASEAN Computer Emergency Response Team (ASEAN CERT) was established as a direct outcome of this strategy, allowing member states to share expertise and resources to bolster the region's cyber security capabilities. In 2018, INTERPOL established the ASEAN Cyber Crime Operations Desk with support from the Singapore Government and the Japan-ASEAN Integration Fund with the aim to develop cyber crime intelligence, provide multi-jurisdictional cyber threat investigations, and promote good cyber hygiene to all member states.

To further the regional cyber security agenda, the first ASEAN Digital Ministers' Meeting (ADGMIN) was held in January 2021, chaired by Dato' Sri Saifuddin bin Abdullah, who was the Minister of Communications and Multimedia Malaysia. The meeting saw the launching of the ASEAN Digital Masterplan 2025 (ADM2025), the Implementing Guidelines for the ASEAN Data Management Framework (DMF), as well as the ASEAN Cross Border Data Flows (CBDF) Mechanism. ASEAN businesses are quickly adopting cloud computing and e-payments; therefore, these initiatives aim to boost economic integration while safeguarding customer privacy and maintaining cyber security best practices through sound data governance. This is especially important as digitalisation has been adopted as a key strategy under the ASEAN Comprehensive Recovery Framework (ACRF) post-COVID.

Beyond ASEAN

ASEAN's key dialogue partners include China, the United States, Japan, South Korea, and India. During the first ADGMIN, the group agreed to cooperate on digital development policy, pandemic prevention and control, digital security, and digital capacity building, among other things.

Malaysia, along with other ASEAN member states, actively participate in the annual UN Open-Ended Working Group (OEWG) and Group of Governmental Experts (GGE) to raise cyber security concerns such as the issue of cross-border Critical Information Infrastructure (CII). According to the United Nations (2021), during a UN General Assembly First Committee Thematic Debate held in October 2021, ASEAN representatives urged the international community to strengthen international cooperation in cyber security, prevent the cyber space from becoming an arena of conflict, and formulate cyber space rules in accordance with international law.

Overall, ASEAN continues to lead the way in global cyber diplomacy. To date, it is the first and only regional organisation

to adapt UN's 11 norms of responsible state behaviour in cyber space.

Conclusion

Digitalisation erases many lines: lines between the physical and virtual worlds, borderlines between nation-states, and even lines separating legal jurisdictions. This absence of tangible boundaries present many new economic opportunities, but also unprecedented security threats with far-reaching consequences both online and offline. While it is virtually impossible to stop cyber attacks, governments have the responsibility to build defensive capabilities to protect its critical infrastructures and minimise the impacts to citizens. Governments must also hold all ICT stakeholders (corporations and nation-states) to account through effective policymaking, starting with a common framework to establish cyber security global standards and best practices. These can only be achieved if nation-states work together towards making the global cyber space more secure and resilient.

References

Economic Planning Unit. (2021). Malaysia Digital Economy Blueprint. https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf

Malaysia Computer Emergency Response Team (MyCERT). (2021). Reported Incidents Based on General Incident Classification Statistics 2020—2021. Incident Statistics. Retrieved June 1, 2022, from https://www.mycert.org.my/portal/statistics?id=b75e037d-6ee3-4d11-8169-66677d694932

National Cyber Security Agency. (2019). Malaysia Cyber Security Strategy 2020—2024. https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyber securityStrategy2020-2024.pdf

NCC Group. (2021). Annual Threat Monitor 2021 Report. https://campaign.cyber security.nccgroup.com/annual-threat-monitor

United Nations. (2021). Delegates Propose New Programme of Action for Struggle against Threats to Cyber security, in First Committee Thematic Debate. Meetings Coverage and Press Releases. Retrieved June 1, 2022, from https://www.un.org/press/en/2021/gadis3673.doc.htm

Adli Amirul Hisyam is a participant of Diploma in Diplomacy 1/2022

Cyber Diplomacy: Malaysia's Virtual Border

By Tajul Azhar bin Mohd Tajul Ariffin

In cyber space, diplomacy is more complicated and constantly evolving than in traditional domains like land, air, and sea, where diplomacy has laid the foundation of the state's normative interaction. Despite the widely held belief that cyber space is a global common, cooperation in this area has been fragmented and *ad hoc*. Coherent multi-stakeholder diplomacy is needed to deal with cyber space intangible yet dynamic nature because it has attracted various actors with differing normative and ideological motives. Thus, cyber diplomacy emerged as a new frontier for developing cooperation and interoperability in a contested space.

Malaysia has been rapidly ushered into the digital age with the rest of the world for the past few decades due to the exponential and unprecedented advancement in Information and Communications Technology (ICT). However, we have made massive progress since the first adoption of the Internet back in 1995. Today, the Internet has become a necessity for Malaysia's businesses, services, and citizens to succeed and be relevant in the age of the Fourth Industrial Revolution (Industry 4.0). Hardly any person or thing is unconnected to cyber space. Businesses are becoming deeply reliant on democratised technologies such as mobile, social, Big Data, Internet of Things (IoT), Artificial Intelligence (AI), and hyper-scale cloud that are all dependent on this connectivity. Hence, cyber security should be made a national priority.

In this respect, Malaysia recognises cyber security as a national priority. This has resulted in the development of the National Cyber Security Policy (NCSP) in 2006. The NCSP was explicitly designed to address the risks to the Critical National Information Infrastructure (CNII), which is

The launching of 'Malaysia Cyber Security Strategy 2020-2024' on 12 October 2022 at Kuala Lumpur Convention Centre (Photo from mkn.gov.my)

The SolarWinds logo seen outside its headquarters in Austin, Texas (Photo by REUTERS/Sergio Flores/File Photo)

made up of 10 sectors, namely: National Defence and Security; Banking and Finance; Information and Communications; Energy; Transportation; Water; Health Services; Government; Emergency Services; and Food and Agriculture.

Later, Malaysia Cyber Security Strategy (MCSS) introduced five strategic pillars that govern all aspects of cyber security planning and implementation in Malaysia until 2024. The Strategy focuses on the three overriding success factors for interrelated and interdependent organisational change, namely, People, Process, and Technology. These pillars aim to create effective governance and management through three strategic initiatives, specifically by enhancing national cyber security governance and ecosystem, improving organisation management and business operations among the government, CNII, and business entities, as well as strengthening cyber security incident management and active cyber defense.

Cyber diplomacy became more apparent following the 2007 cyber attack on Estonia. Therefore, government's involvement in formulating and escalating a national cyber security strategy to mitigate attacks with the military-strategic dimensions is required to defeat cyber opponents. Strategically-formulated threats from cyber security attacks are more than the usual physical terrorist-type of threats. Cyber espionage takes place as a weaponised method to steal the national tactical and technical technology to win the battle in cyber space. Due to the interdisciplinarity of the subject area, cyber diplomacy is a significant area for countries' foreign policies.

In 2021, the US Department of Justice confirmed that it was affected by the SolarWinds supply-chain attack and that three percent of its employees had sensitive data stolen through unauthorised email access. The Justice Department had purchased SolarWinds Orion, which hackers used to execute an attack, affecting up to 18,000 SolarWinds customers. The US Department of Justice also revealed that a small portion of its Microsoft Office 365 email accounts were compromised on Christmas Eve that same year.

The world was shocked by the most turbulent and disruptive periods with regard to security. As governments and corporations worldwide continue to navigate the uncharted waters of a global pandemic, the so-called "new normal" still seemed distant. As businesses adopted hybrid and remote working arrangements, digital transformation efforts accelerated dramatically, but the security maturity concerns that plagued many businesses in 2020 persisted into 2021. While some of these questions remain unanswered, threat actors have wasted no time exploiting the situation.

Based on the industry report, cyber attacks were up by an average of 50 percent, with the education and research sector suffering the most significant blow, averaging 1,605 attacks weekly throughout the year. Furthermore, as predicted, the infamous SolarWinds breach appears to have sparked a trend of supply chain attacks that continued throughout 2021 and even now shows no signs of abating.

Gone are the days when ransomware operators negotiated a ransom of USD 200 for your family photos. The ransomware economy of today is a complex operation that demands millions of dollars per ransom and holds entire organisations hostage under the threat of a total system shutdown. The evolution of the ransomware business model is at the core of this phenomenon. Ransomware-as-a-Service (RaaS) introduces affiliate programs at low onboarding costs, enabling attackers to join the trend quickly. The attacker chooses one of the leading ransomware 'projects' and follows the comprehensive, easy-to-follow operations manual, which contains complete instructions for each level of attack. If the intrusion is successful, the ransomware operators and affiliates would share a percentage of the victim ransom payment. This extremely profitable scheme allows attackers to reach a broader range of victims and offers higher returns to all involved parties.

The ransomware operators provide ransomware, money laundering services, and negotiation experts. Different ransomware programmes compete for affiliates, so ransomware groups continuously make their affiliate programmes more appealing by adding new tools and services. This helps them stand out in the underground community, which is very competitive. Reputation is essential, as it can affect a group's chances of earning substantial profits or even lead to apprehension by the authorities. So, it is not surprising that cyber criminal mediate their internal disputes on tribunal forums, where losing a case can cost a group its reputation and profits.

Photo from Unsplash.com

Now with global progress, democracy and peace are at stake. Various aspects are relevant in this respect: policies, politics and sociology, diplomacy, digital / cyber science, multilateralism, and world history. Despite the jargon, the solution is rather straightforward. The government will develop and implement a comprehensive National Cyber Security Capacity and Capability Plan that will determine the areas of expertise and skill sets that must be continuously improved and enhanced at national, sectoral, and organisational levels. Diplomacy has become a global security priority in an interconnected world. 'Cyber Diplomacy' is distinguished by the tools that facilitate more efficient implementation of diplomatic strategies while simultaneously generating a vast array of government-led measures that can benefit from the diplomat's standard and well-understood techniques and mindset.

Tajul Azhar bin Mohd Tajul Ariffin
is a PhD candidate in Cyber Security at Universiti Kebangsaan Malaysia

Cyber Diplomacy: Mitigating Tensions in the World of Technology

By Theventhiran Arumugam

Many states around the world are now increasingly vulnerable to the continuous evolution of cyber threats due to high usage of Information and Communication Technology (ICT) infrastructure for political, economic, and social purposes, among others. In the context of Malaysia, we too are highly dependent on such infrastructure including for defence, banking, telecommunications, and energy. We could foresee that heavy interdependency between the above mentioned infrastructures could lead to serious impact in the event of any successful cyber attacks. It is then vital for the country to formulate and develop strategies to mitigate or reduce any potential disastrous impact.

The responsibility of mitigating such impact lies on multiple actors, including diplomats. Diplomacy - defined as an effort undertaken by state actors to promote their respective nation's interests through means of negotiation[1] has expanded to include new areas such as health diplomacy, climate diplomacy, and cyber diplomacy.

In this respect, diplomats have begun to initiate communication with states and non-state actors (e.g., private entities, think tanks, and civil society organisations) to conduct studies on issues related to cyber space and approaches to secure it. However, it is becoming more apparent now that the role of diplomats in cyber diplomacy has also expanded to managing tensions between countries that are dominating the world of technology.

The launch of NTT Ltd's fifth data centre in Cyberjaya (Photo from DigitalNewsAsia.com)

Cyber Age Diplomats

Since 2001, security involving mobile telecom networks has never been a concern and is primarily limited to technical issues such as maintaining the operational functionality of the mobile networks and reduce/avoid network disruptions. The growing cyber security and hacking related issues were predominantly focused on ICT related systems and was never on mobile telecom networks due to its limited capacity to store large amount of data.

Cyber technology has without a doubt benefitted many entities by offering data storage, networking, and other online services. Even so, most ICT-related systems are still extremely vulnerable to various types of cyber-attacks, ranging from spyware to malicious attempts at disrupting the infrastructure of an entire organisation. In most cases, the attack would be launched by an individual or a group by using one or more tactics with the purpose of gaining confidential information from disrupting the victim's network.

However, cyber attacks these days are often regarded as politically motivated, rather than mere technical glitches. Such attacks are often carried out by an individual or a group of individuals, for many reasons including to tarnish a country's image - to make the country appear more vulnerable to cyber attacks, thus not secure. Additionally, a country's

The US Department of Justice announce indictments against Huawei (Photo by Joshua Roberts/Reuters))

effort in technological innovation have also been manipulated by other nations to undermine the country's efforts. This is done by turning the innovation into a political agenda which can affect the security of other nations.

One example of this is the rollout of a fifth generation (5G) network by a well-known Chinese company, Huawei. This is a perfect example of the shift from a technical issue to a political/ geopolitical one. The dynamics of mobile telecom networks changed entirely when the Wests were gearing up for the 5G network.

The United States initiated a global campaign against the Chinese telecom manufacturers, especially Huawei preventing them from penetrating into the 5G telecom market. The United States claimed that the 5G network established by Huawei contains Chinese espionage software and able to incapacitate the Westerners' critical infrastructure. As a result, charges such as defrauding banks and stealing trade secrets were filed by the US Department of Justice (DOJ) against Huawei.

To date, the United States and its allies have played a significant role in setting up international industry standards for mobile networks. However, the setting of 5G industrial standards by Huawei remains vague and raises security concerns on the possibility of creating backdoors in a 5G technology. Currently, Southeast Asia is under immense pressure, juggling the influence of Huawei with the US-China economic contestation. As such, several telco companies in the region have chosen to reduce their dependency on Chinese telco companies, especially Huawei, allowing other prominent vendors such as Nokia and Ericson into the region.

We could anticipate that the competition between technology titans would be inevitable in the future, triggering political and geopolitical tensions over cyber security. Therefore, realising the ongoing political and geopolitical debates, diplomats would undoubtedly play a

Malaysia is set to be one of the first countries to deploy the 5G technology in Asia (Photo by Reuters)

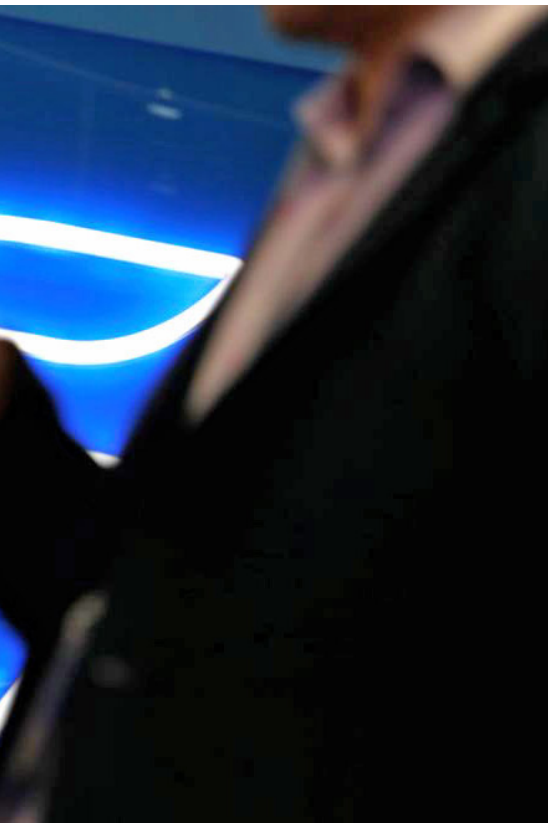
vital role in handling the issue tactfully between state actors and non-state actors in the future.

Firstly, a diplomat should not be entangled into the political game of undermining innovation of other countries. Subsequently, they need to equip themselves with the basic technical knowledge along with the legal aspects of a mobile telecom network in order for them to negotiate effectively with other state-actors and non-state actors.

Additionally, diplomats should be encouraged to build good relationship with relevant non-state actors (e.g., private entities, academicians, and activists) to gain a better understanding and a more comprehensive view of a situation arising from geopolitical/political tension between countries.

Malaysia and 5G

The Malaysian Communications and Multimedia Commission (MCMC) established a National 5G Task Force to study comprehensively the effective strategy of implementing 5G technology in Malaysia. The Task Force has acknowledged and reported the lack in standardisation of planned capabilities and operating functions of the network since it is still developing. Should Malaysia pursue its ambition to proceed with the 5G technology, the foreign policy approach requires Malaysia to be equipped with relevant countermeasures to cyber attacks. Hence, without adopting appropriate diplomatic practices (e.g., diplomatic engagements, joint investigations, and cyber dialogues), among others, Malaysia would always be vulnerable to various cyber security threats.



Conclusion

In short, tanks and troops protecting our sovereignty and borders are meaningless if the technological infrastructures which operates it are vulnerable to cyber threats. Thus far, the world has witnessed several massive successful cyber attacks which resulted in permanent physical damage (i.e., 2007 cyber attack on Estonia and Stuxnet worm attack on Iran's nuclear programme). Realising the risks of potential cyber warfare in the future, diplomats should have strong technical knowledge and skills in order to negotiate effectively with state and non-state actors in relations to cyber security.

Reference

[1] Wight, M. (1979). Systems of states. Leicester: Leicester University Press.

[2] Malaysian Communications and Multimedia Commission. (2019). National 5G Task Force Report: Malaysia Progressing Humanity. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/The-National-5G-Task-Force-Report.pdf

[3] Ministry of Science, Technology & Innovation (MOSTI). (2021). https://airmap.my/wp-content/uploads/2022/08/AIR-Map-Playbook-final-s.pdf

Theventhiran Arumugam
is a participant in Diploma in Diplomacy 1/2022 programme at the Institute of Diplomacy and Foreign Relations (IDFR).

MInistry of Foreign Affairs
Malaysia

INSTITUTE OF DIPLOMACY AND FOREIGN RELATIONS (IDFR)
Ministry of Foreign Affairs, Malaysia
Jalan Wisma Putra, 50460 Kuala Lumpur, Malaysia.
T +603-2149 1000 **W** www.idfr.gov.my

IDFRMalaysia

Let's Talk Newsletter is a series of publications IDFR's talk show series with the same title – Let's Talk.