MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

CYBER SECURITY OUTLOOK IN SOUTH EAST ASIAN REGION FROM CYBERSECURITY MALAYSIA'S PERSPECTIVE

CONTENTS

INTRODUCTION

Since its establishment in 1967, the Association of Southeast Asian Nations (ASEAN) has progress tremendously and it is regarded as the world's fastest-developing economic region. The establishment of the ASEAN Economic Community (AEC) formed in 2015, is a major milestone in the regional economic integration agenda offering opportunities in the form of huge market of US$2.8 trillion and over 655 million people. Base on a report from usasean.org, it is the third fastest-growing major Indo-Pacific economy in the past decade, after China and India. As a critical hub for global trade, over $3.4 trillion in global trade transits through the ASEAN region yearly.

Today, the centre of ASEAN connectivity is digital technology which is recognized as a key driver in the region's economic and social transformation. It is expected that ASEAN will further leverage its digital technology in many more years to come to enable an innovative, inclusive, and integrated ASEAN.

Digital Age has provided unprecedented opportunities for ASEAN member states to utilise telecommunication infrastructure, computers, and applications to progress and prosper. Southeast Asian markets account for approximately 18 percent of the Asia Pacific internet population. ASEAN region is becoming the most important political, economic, strategic, and socially diverse and dynamic region in the world. The major factor driving this change is the opportunities offered by digital technology and the ability of the states to exploit them to their advantages at both national and regional levels. The widespread use of digital technology, however, has introduced new cyber security challenges.

ASEAN has already witnessed the rapidly changing world of cyber threats and how they are encroaching in every sphere of human activities. Increasing dependency on cyber space by states has exposed the region to a significant risk. Hence, ensuring secure, resilient, and trusted regional cyber environment is essential to sustain ASEAN's progress and prosperity. Although, most states have already put in place their respective domestic cyber security, ASEAN should also enhance the collective measures of cyber security cooperation to the mutual benefit of the regional community.

ASEAN was established on August 8, 1967 in Bangkok by the five founding member states of Indonesia, Malaysia, the Philippines, Singapore, and Thailand. Brunei became a member in 1984, Vietnam in 1995, Laos and Myanmar in 1997 and the last member to join was Cambodia in 1999. The idea to set up the regional bloc was to ensure a comprehensive, cooperative and neutrality in an era of global conflict amidst the Cold War setting in the Southeast Asia region.

The main aims behind the establishment of ASEAN were to promote economic growth, regional peace and stability, active collaboration, and mutual assistance on matters of common interest to all the members. ASEAN also seeks to maintain close and beneficial cooperation with existing regional and international organizations that share common aims and objectives. ASEAN operates under six fundamental principles, two of which are mutual respect for independence, sovereignty, and territorial integrity, and non-interference in member state's internal affairs.

Association of South East Asian Nations (ASEAN) Map

ASEAN Logo

ASEAN'S JOURNEY TOWARDS DIGITALIZATION

As the world is moving towards digitalization, ASEAN too need to keep pace with the transformation to ensure that the region is at par with other developed regions in the march towards digitalization. The adoption of digitalization in all sectors will create an environment that could spur the economic growth and social well-being of a nation. The digital technologies can drive innovation, increase efficiency, managing data and information and create job opportunities.

ASEAN is the fastest growing Internet market in the world. With 125,000 new users coming onto the Internet every day, the ASEAN digital economy is projected to grow significantly, adding an estimated USD1 trillion to regional GDP over the next 10 years. However, with a significant number of issues standing in the way of realizing this potential, ASEAN has laid out important policy measures and frameworks, including the ASEAN Economic Cooperation (AEC) Blueprint 2025, Masterplan on ASEAN Connectivity 2025, and the e-ASEAN Framework Agreement to address these roadblocks. However, these ambitious goals will demand detailed research, visionary policy-making, and substantial buy-in from regional stakeholders.

The digitalization process will be incorporated in almost all sectors: government, defence, healthcare, education, finance and banking, transportation, etc. The growth in the development of digital environment and infrastructure is very much evident as ASEAN member states are striving towards enhancing their digital capabilities. ASEAN's digital economy, a collective term for all economic transactions that occur online, is progressing and expected to expand 6.4 times from USD31 billion in 2015 to USD197 billion by 2025 according to the Economic Research Institute for ASEAN and East Asia (ERIA).

Economic growth relied very much on the implementation of digital infrastructure to ensure businesses can offer their products and services on a timely basis and of high quality. Implementation of digital solutions in their businesses and services enable organizations to reach a broader range of customers throughout the globe. For government entities, the digitalization era promotes better services to the public, organized functions and operations, improved and enhanced connectivity among agencies throughout the country.

In recent years, several ASEAN members states such as Singapore, Thailand and Indonesia have increasingly embarked on digital transformation to improve their societies' way of life and accelerated the economic development, potential, and opportunities. Since the outbreak of COVID-19 pandemic, digitalization effort has been multiplied and resulting in greater reliance on the digital realm and eventually influence on how we live, work, and interact. As our dependency on digital tools and online space grows, we have inevitably also become more vulnerable to malicious cyber activities and largely exposed to greater cybercrime and cybersecurity risks. Incidences such as espionage, data theft, and attempts to disrupt our day-to-day services and activities have also increasingly gone digital.

The ASEAN leaders are unanimous and ambitious in making the region to become the world's fourth largest economy by 2030. This lofty aim can be achieved by harnessing the potential of the younger generation and it is a transition that will be championed by an increasingly tech-savvy younger population which is rapidly rising the socio-economic ladder.

Based on a report from ASEAN-USAID (United States Agency for International Development) in August 2020, Southeast Asia has the potential to become one of the world's top five digital economies. Its digital market has expanded threefold in the past three years and represents seven percent of ASEAN's US $2.8 trillion GDP. Through ASEAN-USAID IGNITE (Inclusive Growth in ASEAN through Innovation, Trade and E-Commerce), USAID supports ASEAN's efforts to enhance internet connectivity and accessibility while adopting approaches that could strengthen cybersecurity and digital finance.

Even though the overall ASEAN's businesses, government and population are moving towards digitalization, many are still lacking the required infrastructure and quite slow in making the progression in adopting digital environment. Many are still wary and concern about regulatory issues and lack of trust in electronic transactions. Micro, small, and medium-sized enterprises (MSMEs) accounted for at least 95 percent of all business establishments and more than half of the total employment in ASEAN. Despite their pervasiveness, ERIA estimates that MSMEs only contribute 30 to 53 percent of ASEAN's gross domestic product (GDP) and 10 to 30 percent of its imports.

A report by Kearney (previously known as A.T. Kearney), a global management consulting firm, suggested that ASEAN should spend nearly $171 billion on cybersecurity by 2025 to safeguard the bloc's digital economy environment. The report which was published to elaborate on the opportunities of ASEAN in becoming a digital economy gave an insight into some important cybersecurity aspects. It also advises that the bloc needs to create a unified agency to prevent cybercrimes.

In its comparative analysis with the European Union (EU), the consulting firm pointed out that on the grounds of consumer protection, primarily for data privacy and cybersecurity, EU has a common privacy initiative for data protection and cybersecurity, making it an important part of regional priority which ASEAN is still lacking.

Another statement from the firm suggested that the region's cybersecurity industry faces a shortage of home-grown capabilities and expertise, fragmented products and solutions and few comprehensive solution providers. Engaging multiple vendors and product deployments are creating operational complexity and increased vulnerability in some cases.

CYBER SECURITY THREAT IN THE ASEAN REGION

As a developing region, ASEAN has faced numerous traditional crime and security challenges. The traditional acts of crime such as human trafficking, contraband smuggling, fraudulent, various type of cyber theft etc., has long become a concern in the ASEAN region. Other issues like territorial dispute, geopolitical conflict, ethnic conflicts, laws and regulation, religion and race issues etc., increased the proportion of conflict in the ASEAN region. With the implementation of digitalization, these traditional issues have moved towards digitalization and created various kinds of threat in the cyber realm.

Cyber Threat Is the Highest Concern In ASEAN

The growth of digital adaptation in economic activities has also contributed to the region's vulnerabilities to cyber-threat. With large amount of money invested in digital development projects, the ASEAN region has become potential for cyber-attack for various motives. The region has already witnessed the rise of incidents related to cyber-crime, hacktivism, data breach and cyber espionage. The borderless nature and the anonymity of attackers has made the criminals opted for cyber-attack and difficult for the authority to track the culprit. The attack can be of various cyber offensive action ranging from web defacement, system intrusion, cyber espionage, malicious software including ransomware to high-scale state sponsored cyber-attacks with diverse political, economic and military motives.

Due to the important strategic of ASEAN and its geopolitical circumstances, the region is facing the threat in the form of Advanced Persistent Threat (APT). Cyber-attacks today are becoming more complex and damaging. It is alarming to note that APT actors are one of the biggest challenges for the region. In simple terms, APT is sophisticated, covert and continuously conduct cyber-attack based on well-coordinate plans and strategies committed to achieve both business and political motives. As increasing investments and diversifying economies spur development in the region, this growth simultaneously becomes even more attractive to APT groups. They are mainly geared towards targeting critical services that will result in high impact on national and public security. Critical services encompass among others, telecommunication, banking and finance, transport, energy etc.

Cyber criminals are exploiting system vulnerabilities to intrude computer systems using a combination of techniques. The trends of computing such as cloud computing, big data, Internet of Things (IoT) and social media were created for convenience with limited security functions, hence posing new security challenges. Opportunities for cyber attacks have increased with the continued advancements of Internet. States and organizations are enjoying the benefits of new technologies, while criminals are also using the same innovations to facilitate their malicious activities.

Cyber Crimes

Cybercrimes today are gradually overtaking the traditional act of crime. Today, most states are facing a lot more threats posed by international organized crimes that misuse Internet to facilitate drug and human trafficking, financial fraud, scams and money laundering. With continuous advancement of digital technology, cyber crimes are on the rise making today's crimes more complex. Based on Juniper Reports, data suggested that cyber crimes had cost businesses over US$2 trillion total in 2019.

Today's cybercrimes have its own supply chain structure that reflects how all serious crime will be organized in the future. Internet underground market provides cyber criminals with a connection for the trade of goods and services using web currency creating and organized set of criminal relationships. Such situation created challenges for law enforcement especially regarding to tracing the sources of criminal activities. Not only could the experts make profit from selling their services, but also, they could make equal profit by performing the crimes themselves.

APT - Threat Actors Related to Cyber Espionage

Cyber-attacks today are becoming more highly sophisticated, complicated and damaging. These cyber-attacks are carried out by APT actors and they are causing serious damage to the information infrastructure in the region.

An APT is an attack (typically performed by state-sponsored threat actors and/or organized crime syndicates) that occurs when an unauthorized user utilizes advanced and sophisticated techniques to gain access to a system or network. APTs are more concerning than the everyday "hacker," as they are typically target high-value organizations and governments with the goal of stealing information over a long period of time. A regular hacker would gain access to a system, do what they needed, and leave quickly. However, an APT group tends to hack and use small businesses as steppingstones to reach larger organizations because the smaller organizations are not well defended. In recent years, state-sponsored attacks are far less common than cybercrime and hacktivism, but they are nonetheless a real and concerning trend.

Leading companies that performed business in critical sectors are also targeted by the APT groups. In case of financial sectors, it faced both cyber criminals attempting to steal money as well as APT actors seeking sensitive financial information. It is alarming to note that the very existence of the APT attacks highlights ASEAN's vulnerability.

Another reason why the ASEAN region is vulnerable to cyber-attacks is due to its lack of technical resources and cyber security professionals as well as ineffective cyber security policies and strategies. Although there have been several cyber security initiatives being implemented by respective ASEAN countries, they are done in isolation, hence they were not well coordinated and integrated. Despite the current threat landscape, there are a lot of opportunities to enhance ASEAN cyber security. As cyber security becomes critical to ASEAN's peace and prosperity, all member states seem to have the motivation to enhance their cyber security collaboration towards achieving their regional common interest.

China's Threat Actors and APT

One of the greatest threats to information networks is Chinese state-sponsored malicious cyber activity. These networks often undergo a full array of tactics and techniques used by the Chinese state sponsored threat actors to exploit computer networks of interest that hold sensitive intellectual property, economic, political, and military information. Since these techniques include exploitation of publicly known vulnerabilities, it is critical that network defenders prioritize patching and mitigation efforts. For example, researchers have unveiled that attacks on government sectors in South East Asia that has reportedly infected more than 200 systems were carried out by a Chinese APT Group called FunnyDream over the past two years. It has been revealed by another security firm that FunnyDream's targets were in countries like Malaysia, Taiwan, the Philippines, and while most of the perpetrators were based in Vietnam. FunnyDream Group is reportedly still on the move, and as per the security firm's investigation, they are primarily interested in cyber-espionage that aims to obtain illegally sensitive documents that focus on national security and cyber-espionage.

Another sophisticated APT group that is believed to be operating out of China has been stealthily targeting Southeast Asian governments over the past three years. The fact that some of these open-source tools are known to be of Chinese origin and the use of other resources in Chinese led the researchers to the conclusion that the group behind these attacks consists of Chinese natives. For persistence, the adversary employed digitally signed binaries that are leveraged to side-load one of the backdoors into memory. Data of interest is identified and exfiltrated using custom tools. The attacker's infrastructure appears to be active even today, despite many of the command and control (C&C) servers being inactive. Believed to be state-sponsored, the group was observed using numerous other malware families, including the Chinoxy backdoor, PCShare RAT, and the FunnyDream backdoor.

Malaysia, being a part of the Belt and Road Initiative (BRI) and one of the overlapping claimants in the South China Sea territorial dispute, the critical need of protecting critical information infrastructure from Chinese Threat Actors is imminent. The following key questions need to be addressed:

a. Do we identify the key infrastructure that is susceptible to cyber espionage or can it be considered as high value targets by Chinese threat actors?

b. Do we have centralized information dissemination on critical alerts?

c. Do we have risk compliance assessment for any recently critical alerts used by Chinese threat actors?

In April 2020, CyberScoop.com reported that suspected Chinese hackers were behind a phishing campaign apparently aimed at collecting data about Vietnamese government officials amid an ongoing territorial dispute between the two nations. A hacking group known as Pirate Panda, is believed to have possible ties to the Chinese government. The incident is related to one of the territorial dispute areas known as Paracel Islands. The area is one of the most hotly contested regions of the South China Sea, with Beijing claiming ownership of much of the waterway.

In August 2019, a report by TheDiplomat.com, mentioned that an article published by enSilo found that the Chinese cyber espionage group called the Advanced Persistent Threat Group 10 or APT10 deployed two malicious software variants that targeted government and private organizations in the Philippines in April 2019. According to enSilo's investigation of the malware, the tactics, techniques, procedures, and codes perpetuated by the threat actor are all unique to APT10.

USA – China trade war and effect on cybersecurity

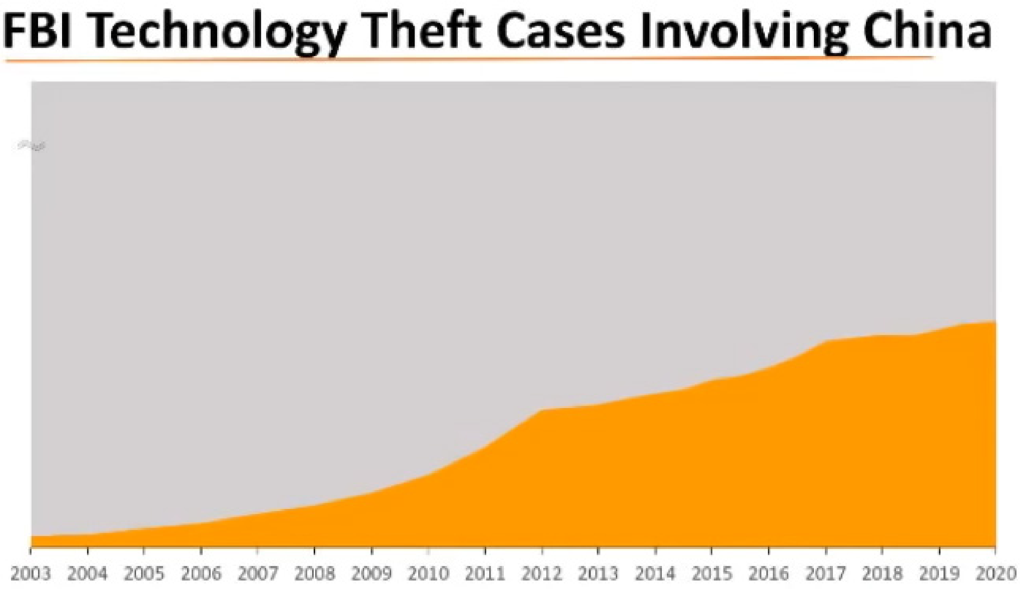
The emergence of ASEAN as a potential economic hub and nexus between the west and east has led ASEAN to be involved indirectly in the trade war between the US and China where both superpowers as well as economic titans have exerted their influence and shaping ASEAN's strategic and policy both in economic, maritime and political spheres.

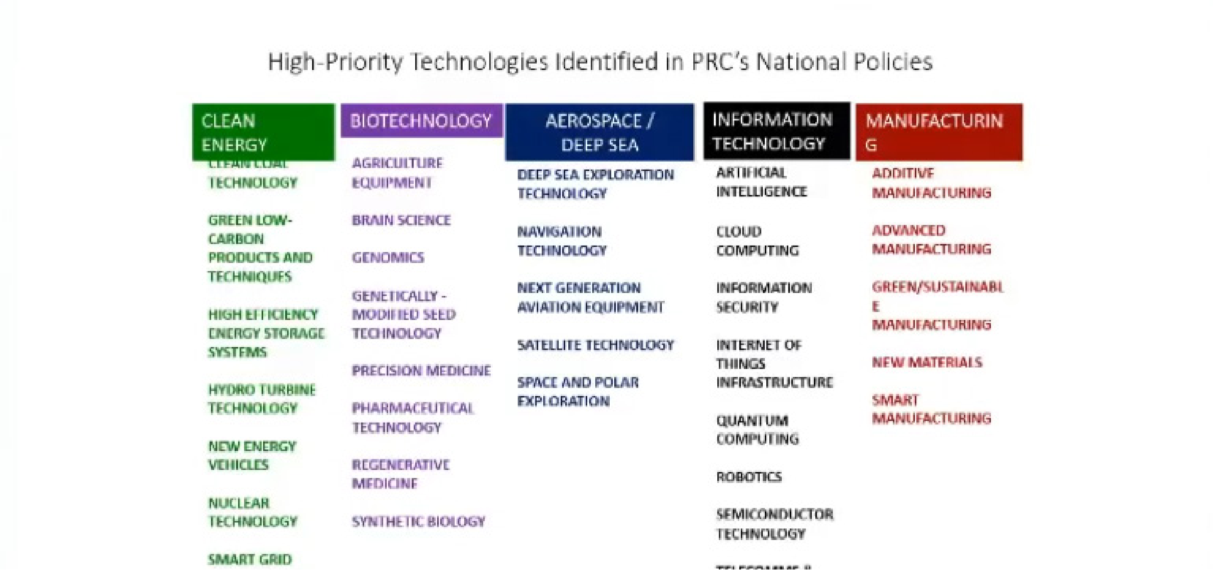
The digitalization of ASEAN's economy and other infrastructures have created an environment where related information is stored and can be access via digital devices. This includes sensitive information like personal data, confidential and strategic information and documents, financial information and other sensitive information that can be manipulated and used against one's adversary.

The US-China trade war has greatly affected industries from manufacturing to farming to information technology, which could be disastrous for the local economies. Tensions between technology sectors including products used for robotics, computing, communication technology, and aerospace have increased, and experts are warning that these related industries are vulnerable to unprecedented state sponsored cyber-attacks. Due to this, new privacy regulations have been imposed which require companies to manage their data with much more care and protection, taking cybersecurity requirements to higher demands in the market.

Another issue that has been of concern to the US is pertaining to intellectual property rights theft and the forced transfer of technology to China and believing that the country practices unfair trade with the U.S. These allegations have led to retaliatory policies where both sides have incrementally imposed tariffs and strict qualitative measures targeting the other, affecting the negotiation process.

In a February 2020 report by ZDNET, the US government held a conference to inform the private sectors, academic and research community to assist in the investigation related to IP theft from China entities. The US considered these incidents as a threat to its information, IP and economic vitality. The primary purpose of the conference was to get US companies and the academic sector up to date with all the techniques the Chinese government is using to get their data on the latest US technology. China has been using various methods and techniques from cyber intrusion, espionage to corrupting internal personnel in their zealous effort to get more information on evolving technologies.





High-Priority Technologies Identified in PRC's National Policies

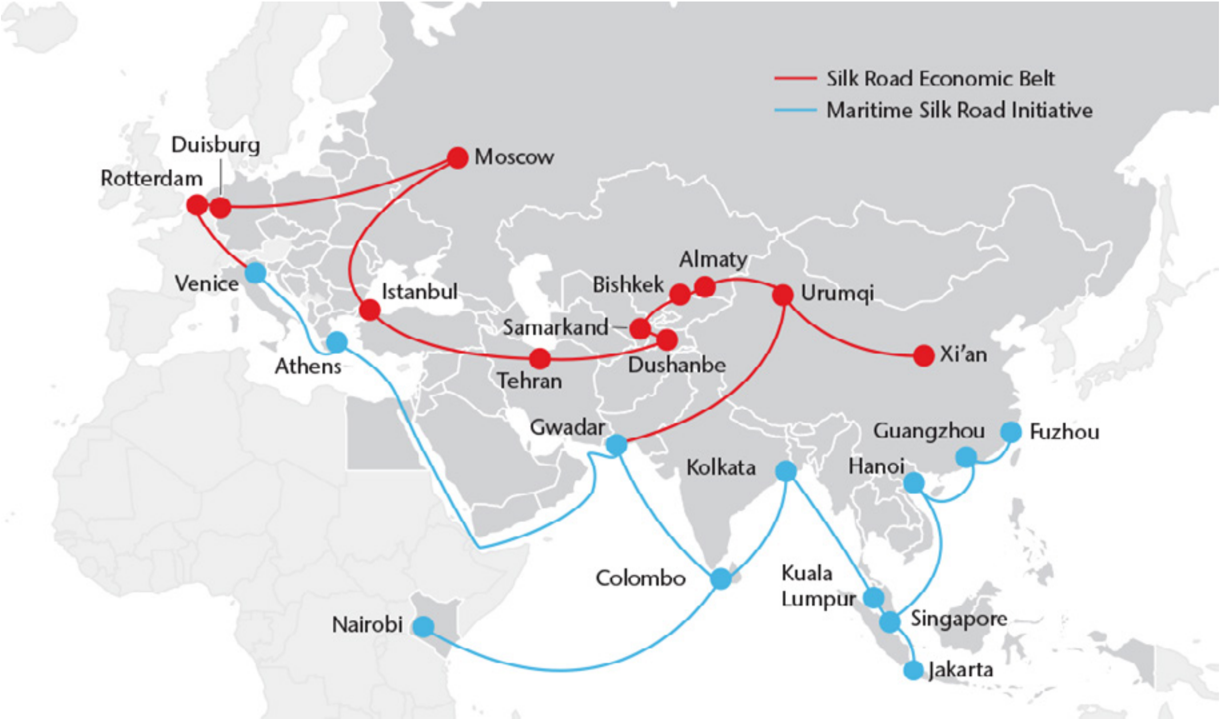
CLEAN ENERGY	BIOTECHNOLOGY	AEROSPACE / DEEP SEA	INFORMATION TECHNOLOGY	MANUFACTURIN G
CLEAN COAL TECHNOLOGY	AGRICULTURE EQUIPMENT	DEEP SEA EXPLORATION TECHNOLOGY	ARTIFICIAL INTELLIGENCE	ADDITIVE MANUFACTURING
GREEN LOW-CARBON PRODUCTS AND TECHNIQUES	BRAIN SCIENCE	NAVIGATION TECHNOLOGY	CLOUD COMPUTING	ADVANCED MANUFACTURING
HIGH EFFICIENCY ENERGY STORAGE SYSTEMS	GENOMICS	NEXT GENERATION AVIATION EQUIPMENT	INFORMATION SECURITY	GREEN/SUSTAINABL E MANUFACTURING
HYDRO TURBINE TECHNOLOGY	GENETICALLY - MODIFIED SEED TECHNOLOGY	SATELLITE TECHNOLOGY	INTERNET OF THINGS INFRASTRUCTURE	NEW MATERIALS
NEW ENERGY VEHICLES	PRECISION MEDICINE	SPACE AND POLAR EXPLORATION	QUANTUM COMPUTING	SMART MANUFACTURING
NUCLEAR TECHNOLOGY	PHARMACEUTICAL TECHNOLOGY		ROBOTICS	
SMART GRID	REGENERATIVE MEDICINE		SEMICONDUCTOR TECHNOLOGY	
	SYNTHETIC BIOLOGY		TELECOMMS &	

China's One Belt One Road Initiative

China has embarked on one of the most ambitious and expensive infrastructure projects ever undertaken. First announced in 2013, the One Belt One Road initiative, also referred to as the Belt Road Initiative (BRI), represents a resurrection of the ancient trade routes known as the Silk Road, which connected China with the economies of nearly 70 other countries across several continents.

The project is made possible by updating and improving the infrastructure along ancient trade routes both on land and at sea. In fact, the "belt" refers to the physical road, which travels from Asia through Europe and into Scandinavia, whereas "road" refers to the maritime shipping lanes, reaching as far as Venice.

One of the main arguments for the BRI is that increased global trade can lead to global growth. Nonetheless, the challenges of the project should not be underestimated. From political risk to simple economics, such cross-border trade can easily become very complex.



Apart from the BRI expansion, which the US believes for the benefit and advantage of China rather than the other way round, another irritant to the US was about China's overlapping claims in the South China Sea. On top of that, the trade war has also attracted the US interest in the region which also included the geopolitical interest particularly about controlling the shipping lane and strategic territorial dispute in the South China Sea. The US has long established its military bases in the Philippines, Thailand and Singapore for logistical purposes, communication and intelligence support. Basically, the US's aim was to show their presence in the highly sensitive and contested South China Sea against China's expansionism strategies.

As reported from Aseantoday.com, hackers from China have been spying on governments and businesses in Southeast Asia for more than a decade. According to a report from internet security company FireEye, China's cyber espionage operations dated back to 2005 or earlier and focused on targets of government and commercial personnel who hold key political, economic and military information about the region. Based on the criteria of the attack, it is believed that this activity is a state-sponsored, most likely from the Chinese government.

In 2011, McAfee researchers reported that a campaign with links to China named Shady Rat attacked Asian governments, including the ASEAN Secretariat. According to another report, China has been running at least six different cyber espionage campaigns in the Southeast Asian region since 2013. Indonesia, Myanmar, Taiwan and Vietnam are reportedly the main targets of these operations. Chinese hackers have also been targeting universities in both the US and Southeast Asia to gain access to maritime military secrets. Beijing may be spying on Southeast Asian governments to steal documents and planning related to activity in the South China Sea.

ASEAN COMMITMENT

ASEAN has remained resolute and steadfast in its commitment to cyber stability. It has led the way to create a rules-based multilateral order in cyberspace, through cyber norms implementation and the protection of national and cross-border critical information infrastructure supporting essential regional communications, trade, transportation, and logistics services.

Since 1994, ASEAN has initiated the ASEAN Regional Forum (ARF), with the objectives to foster constructive dialogue and consultation on political and security issues of common interest and concern; and to make significant contributions and efforts towards confidence-building and preventive diplomacy in the Asia-Pacific region. The cybersecurity area has been part of the agenda since 2012.

Since the late 1990s, ASEAN had discussed about cyber concern in the context of transnational crime and as an example of non-traditional security issues. In 2003 ASEAN structured their activities within three different communities: the Economic Community, the Political-Security Community and the Socio-Cultural Community. The Vientiane Action Programme 2004-2010 promotes progress in the different communities and in the area of the security and integrity of ASEAN Information Infrastructures. One of the action items is the establishment of national Computer Emergency Response Teams (CERTs). The importance of a secure and connected regional information infrastructure is again mentioned in the ASEAN Economic Community (AEC) Blueprint 2015 and the AEC Blueprint 2025.

The ASEAN Computer Emergency Response Team (CERT) has been conducting ASEAN Cert Incident Drill (ACID) annually since 2006 to test incident response procedures and strengthen cybersecurity preparedness and cooperation among CERTs in ASEAN Member States (AMS) and Dialogue Partners.

Cybersecurity has been a key area of focus for ASEAN. The regional body has been fostering greater regional cybersecurity cooperation and capacity building, including law enforcement training on cybersecurity and cybercrimes through efforts such as the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN), ASEAN Ministerial Conference on Cybersecurity (AMCC), ASEAN Cyber Capacity Programme, ASEAN Regional Forum (ARF) Inter-Sessional Meeting on ICT Security and the ASEAN Defence Ministers' Meeting (ADMM)-Plus Experts' Working Group Meeting on Cyber Security.

In January 2021, the ASEAN Digital Ministers Meeting (ADGMIN1) adopted the Putrajaya Declaration which promotes the ASEAN Digital Masterplan 2025 (ADM2025) at its core. The masterplan, launched by ASEAN digital Ministers, comprises eight Desired Outcomes that seek to propel the regional grouping as a leading digital community and economic bloc. The ADM2025 has identified eight desired outcomes and cybersecurity is one the agenda.

Part of the declaration emphasised the importance of harnessing ICT as a basis of progress and unity in line with the visions of ASEAN Economic Community, ASEAN Political-Security Community and ASEAN Socio-Cultural Community; and the importance of strengthening cybersecurity cooperation towards promoting an open, secure, stable, accessible, interoperable, and peaceful ICT environment in ASEAN that will support our digital economy. Further guided by the endorsement of the ASEAN Comprehensive Recovery Framework and its Implementation Plan by the 37th ASEAN Summit on 12 November 2020, which called for the acceleration of inclusive digital transformation in ASEAN including promoting e-commerce and the digital economy, enhancing digital connectivity, and strengthening data governance and cybersecurity, to emerge more resilient and stronger from the COVID-19 crisis.

WAY FORWARD

Based on a report by global management consultant, Kearney, Southeast Asian countries are still lagging in the cybersecurity area. ASEAN countries are also being targeted for cyber-attacks; with Indonesia, Malaysia, and Vietnam serving as global launchpads for malware attacks. Cybersecurity at this juncture of time is particularly necessary as internet penetration in the region is at its highest and will continue to grow. Hootsuite's report on Southeast Asia's digital usage indicates that the region has an internet penetration rate of 58 percent which means there are more than 370 million internet users currently.

ASEAN needs to enhance its development and cooperation in cybersecurity at a faster rate and with high value. The incident of cyber-attack and cyber threat has been increasing yearly and will jeopardize the intention to move towards developing the region. The effort by ASEAN in improving and progressing the economy, security, livelihood, and social standards of its citizen need to be developed together between the digitalization and cybersecurity.

However, ASEAN is still lacking and a little behind in cyber defence development as compared to Western countries. ASEAN still relies on technology especially from western countries. A lot of tools and machines are still being obtained and purchased from countries like the US and Europe including China. It needs to enhance the resources in technology skill and knowledge, together with its research in developing new in-house tools and products. This effort will help ASEAN to better protect its infrastructure where it will be able to control, secure and protect the technology from being access from external parties.

Another reason behind this is that it will reduce the cost of purchasing and maintaining the products and tools. A very important example is the encryption technology. By using in-house developed encryption, the country will be able to hide the data transferred and protected from being de-crypted and read by unauthorized parties. The development of encryption algorithm and encryption keys will be controlled by locals and need to be ensured its safety. The usage of this type of technology will help to reduce the incident of data theft and leakage.

The technology such as machine learning, and Big Data has been manipulated and taken advantage by cyber threat actors to enhance their attack strategically. Due to this development, these selected ASEAN countries also need to enhance its capability. These types of technology can be used to do prediction and detection of possible attack such as cyber espionage and data theft.

Since ASEAN geographical location is in the middle of superpower tussle between the west and east, ASEAN will be trapped in the middle of the economic and technological race. Cyber espionage is already occurring in most of ASEAN countries and some of them do not even realized of the incident until it is too late.

To ensure organizations whether they are from the private or public sector to implement and adopt with best practices and globally accepted standards, audit and monitoring needs to be implemented and empowered by using the legislation and rules. This enforcement will allow the government and industry players to ensure organizations and agencies adhere to the rules and guidelines and reduce the gap and vulnerability of existing system and new digital system being implemented. Legislation also needs to be improved and another area to be included is cross-border jurisdiction and how countries in this region can work together to ensure the perpetrators could be charged with the crime committed.

Cooperation among countries in the region is another matter that needs to be continuously enhanced and conducted rigorously. Forums, seminars, programs and such, need to be conducted to ensure the experience, knowledge and skill can be shared among member states. This will benefit the whole region in detecting and respond to any incidents of cyber-attack.

The effort and task to enhance cybersecurity and to keep the digital environment to be a safe working environment will not be a one-time effort. The cybersecurity area will keep changing with new and emerging technologies that keep improving rapidly and required continuous effort from all parties, industrial, government and the public to reduce the vulnerability and keep the region and organization to be resilience. Ability to continue the operation and function as normal is a must to ensure sustainability, security and expediency in order to survive any cyber-attack.

CONCLUSION

The idea to set up a regional bloc that would enhance its member states in terms of socio-economic, improve livelihood and enhanced security was a noble idea set up by the forefathers of ASEAN. The cooperation worked for ASEAN for the past 60 plus years but now ASEAN has arrived at a critical juncture whereby it has to prepare the way forward in terms of providing a holistic cyber security parameter in line with the digitalization efforts.

Cyber threat is growing in sophistication in parallel with technology evolution. Today, cyber threats have been identified among the major security challenges facing ASEAN states as the region is moving towards digital economy. The governments continue to invest heavily to protect the critical infrastructures and the demand for cyber defence capabilities also grow. The rise of hacktivism, cyber espionage, cyber crimes and cyber terrorism would remain as both national and regional security concerns in years to come. It is noted that any major cyber-attack on the network linking critical sectors would have grave implications leading towards destabilisation of the effected country and the region.

True to its foundation, ASEAN must work and cooperate together not only in terms of the socioeconomics, socio-politics and community pillars but also in the cyber security aspect as well. With the emergence of new technology and the convergence of all the new technologies it is high time for the regional bloc to assess the situation and come up with some digital deterrence and proactive measures for the regional survivability and resilience in the future digital landscape.

Reference:

[1] https://asean.usmission.gov/wp-content/uploads/sites/77/IGNITE-Digital-Economy-fact-sheet-Aug2020.pdf

[2] https://cisomag.eccouncil.org/asean-not-spending-enough-cybersecurity-t-kearney/

[3] https://datasearchconsulting.com/how-the-us-and-china-trade-war-caused-cybersecurity-boom/

[4] https://www.natlawreview.com/article/department-justice-s-national-security-division-chief-addresses-china-s-campaign-to

[5] https://www.zdnet.com/article/fbi-is-investigating-more-than-1000-cases-of-chinese-theft-of-us-technology/

[6] https://thediplomat.com/2020/08/aseans-challenges-and-the-way-forward/

[7] https://www.cyberscoop.com/south-china-sea-maritime-hacking-vietnam/

[8] https://opengovasia.com/asean-leaders-issue-statement-on-cybersecurity-cooperation/

[9] https://www.usasean.org/why-asean/asean-economy

[10] https://www.aseantoday.com/2020/09/are-southeast-asias-cyber-defenses-vulnerable-to-chinese-attacks/

Corporate Office:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

Tel: +603 8800 7999
Fax: +603 8008 7000
Email: info@cybersecurity.my
www.cybersecurity.my

@cybersecuritymy
CyberSecurityMalaysia
cybersecurity_malaysia
CyberSecurityMy

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

Best Brand
Internet Security
2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : ISMS 00114

ACB ISMS 02
SAMM 456

Status Company

Best Child Online
Protection Website