SULTAN HAJI HASSANAL BOLKIAH INSTITUTE OF DEFENCE AND STRATEGIC STUDIES

Defence & Strategic Analyses

2018

Defence & Strategic Analyses

2018

SULTAN HAJI HASSANAL BOLKIAH
INSTITUTE OF DEFENCE AND STRATEGIC STUDIES

Perpustakaan Dewan Bahasa dan Pustaka Brunei
Pengkatalogan data-dalam-Penerbitan (Cataloguing-in-Publication)

DEFENCE & strategic analyses 2018 [edited] by Sultan Haji Hassanal Bolkiah
Institute of Defence and Strategic Studies. – Bandar Seri Begawan : Sultan Haji
Hassanal Bolkiah Institute of Defence and Strategic Studies, Ministry of Defence, 2020.

p. cm.
ISBN 978-99917-36-76-1 (paperback)
ISBN 978-99917-36-78-5 (e-book)
1. Military policy 2. National Security

355.0335 DEF (DDC23)

First published**: 2020**
ISBN: 978-99917-36-76-1 (pbk)
ISBN: 978-99917-36-78-5 (e-book)

Printed and bound in Brunei Darussalam by: **Brunei Press Sdn. Bhd.,**

All correspondence should be addressed to:

Research Division
Sultan Haji Hassanal Bolkiah
Institute of Defence and Strategic Studies
Ministry of Defence
Bolkiah Garrison
Bandar Seri Begawan BB3510
Negara Brunei Darussalam

Tel: +673 2386987 / 2386986
Fax: +673 2381424
Email: shhb.idss@mindef.gov.bn

SHHBIDSS

Defence Strategic and Analyses (DSA)

The mission of the Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (SHHBIDSS), as the Ministry of Defence's policy research institute, is to study and discuss defence, security and strategic issues relevant to Brunei Darussalam and its surrounding environment.

The Defence Strategic and Analyses (DSA) is a publication of SHHBIDSS covering aspects of defence, security and strategic issues. It aims to share perspectives and promote awareness related to but not limited to issues under its Research Programmes in the Defence Management Studies, Defence and Military Studies and Regional Strategic and Security Studies.

DSA 2018 is based on the commentaries by SHHBDSS researchers in Track 2 engagements in the region including The Track 2 Network of Defence and Security Institutions (NADI) and their own papers that reviews and assess the various regional security developments and challenges.

Contents

1. Perspectives on the New Emerging Non-Traditional Security Issues[1]

Selina Farahiyah Teo

Certainly the list of benefits technology brings is endless, but they also present governments with potential national security challenges and ill elements along with the opportunities. On top of what we see today, emerging technologies – Artificial Intelligence (AI) and the Internet of Things (IoTs) among others – are proving to be key disruptive drivers of the future which will inevitably harbour new risks. The digitalisation of the economy provides wider opportunities and challenges for the region. However, the growth of technology has always been heavily focused on efficiency, cost and user-convenience instead of security. As the region embraces digitalisation, the cybersecurity gap represents a big challenge especially as the higher level of reliance on technology will only lead to increasing severity and damage caused by cyberattacks. The prevailing lack of recognition and understanding on cybersecurity urgency and fragmented cybersecurity efforts are two stumbling blocks that ASEAN needs to get around in order to jointly respond together effectively to cybersecurity threats and the impending impacts of new emerging technologies.

1.1. Overview

The threats and challenges posed by Non-Traditional Security (NTS) issues are not new and have gained global and regional attention due to their transboundary nature. The threats are also not as visible and directly linked compared to the challenges posed by traditional security (TS) issues. The repercussions of NTS threats are also likely to be more diverse as they are (a) affecting economic development and social stability; (b) cannot be contained by traditional national military capabilities / law enforcement agencies / economic sanctions and (c) are caused by non-state actors. These consequences and the continuously shifting nature of the threats and other destabilising forces are changing Southeast Asia's security architecture.

[1] This commentary was prepared for the 11th NADI Annual Meeting on New Emerging Non-Traditional Security from 2 to 5 April 2018, taking place in Marina Mandarin Hotel, Singapore.

In recent years, cybersecurity has received increasing attention. Indeed, from just merely the threats of spam and malware, cyberattacks are growing in prevalence and have increased in sophistication and in its destructiveness. The defining moment in the birth of cyberattacks as an NTS issue was the advent of the Internet in the early 1970s, which was at that time, an emerging information and telecommunications technology.

In assessing the new emerging NTS issues in the region, this paper will focus on the advent of new technologies and the associated risks that comes with it, particularly those that have and potentially be used by ill elements and opportunists alike as convenient tools to execute their agendas in further exploiting the interconnected and global nature of the cyber domain.

As global events continue to demonstrate, terrorists, criminals and other cyber threats actors have become increasingly creative in the exploitation of the cyber domain.

1. Hacker Attacks		
a.	Information Theft / Breach of privacy	*Hacking of UK Lender Company, Wonga, Apr 2017*. Hackers stole personal data of around 245,000 customers including bank account, sort codes, home addresses and email details.
		Hacking of US CloudPets Smart Toys, Feb 2017. The hacking exposed 2 million voice recordings of children and parents, email addresses and password from more than 800,000 accounts.
		Hacking of Singapore MINDEF I-Net System, Feb 2017. Hackers stole the NRIC numbers, telephone numbers and birth dates of 854 personnel.
		Hacking of UK Telecom Giant, TalkTalk Website. Breach of privacy of 150,000 customers including sensitive financial data from more than 15,000 people costing the firm £42m revenue loss.
b.	Extortion	*WannaCry Ransomware Attacks, May 2017*. The attacks affected more than 230,000 computers in more than 150 countries, as it locked up all the computers and uses asymmetric encryption to prevent recovery of the key needed to decrypt the ransomed file. The UK's National Health Service (NHS), Spanish phone company Telefónica and German state railways were among the organisations infected by the ransomware.
		Petya Ransomware Attacks, Jul 2017. The attacks affected around 2000 users in Russia, Ukraine, Poland, France, Italy, the UK, Germany and the US. The Ransomware also infected banks and electricity grid and has also attacked one of the world's largest container ship and supply vessel operator, Maersk, resulted in $300 million lost in revenue. The infected computers also displayed a message demanding a Bitcoin ransom worth $300.

c.	Distributed Denial of Service	*Attack on Ukraine's National Postal Service, Ukrposhta's Website, Aug 2017*. Its online system that tracks parcel was affected for two days when hackers flood the website's servers with a huge amount of web traffic taking the website offline.
2. Exploitation of the Internet and Social Media Platforms		
a.	Recruitment	Not only is the social media platforms used by different marketing agencies as a job recruitment tool, terrorists and other perpetrators have also took advantage of the available platforms for recruitments. Terrorist groups, specifically ISIS, for example, have successfully recruited over 1000 Americans to join ISIS in 2016 using social media platforms.
b.	Propaganda	Terrorists also used the Internet and various social platform promote their cause. For example: 1. The publication of ISIS first magazine, Dabiq, in 2014, followed by Rumiyah magazine in 2016. 2. The use of specific hashtag on twitter to interact with ISIS influential online coach following an instruction for potential recruits to contact through Telegram, an encrypted messaging app. 3. Twitter has also been used to promote terrorism where in response; twitter has removed 935,897 accounts between 2015 and 2017.
c.	Financing	Terrorist groups have also used the internet to raise and transfer needed funds to support their activities. The advent of cryptocurrency has sparked new opportunity for terrorist financing due to its unregulated and anonymous nature. 1. In 2015, a Virginia man pleaded guilty to conspiring to provide material support to the Islamic State for attempting to teach others how to use Bitcoin to anonymously fund the terrorist group. 2. In Nov 2017, an ISIS-affiliated website Akbar al-Muslimin used the internet to seek for donations of Bitcoins. 3. In Dec 2017, an American woman was charged with fraud and conspiracy as she was accused of laundering cryptocurrencies for terrorist funding as she loaned a total of $85,000 to purchase worth of bitcoins. This is following a launched by ISIS affiliated website for bitcoins donation.
d.	Identity theft	The popular use of social media has made it an easier platform for identity thefts. Facebook, Twitter and LinkedIn are among the most popular hunting ground for theft. In the UK, a total of 148,000 were victims of identity thefts in 2015 alone.

e.	Dissemination of Fake Information	Social media and instant messaging platforms enabled by the Internet such as the WhatsApp have facilitated the fast spread of fake news and fake information and allowed them to multiply quickly. The deliberate disinformation operation can sow discord within society, undermining societal values and national unity. They can also be used to influence the outcome of important events such as elections.

1.2. Emerging and Disruptive Technologies

Technology is moving at a fast pace. Certainly, the list of benefits technology brings is endless, increasing convenience and efficiency in daily life. But they also present governments with potential national security challenges and ill elements with opportunities. On top of what we see today, emerging technologies – AI and IoTs among others – are proving to be key disruptive drivers of the future, which will inevitably harbour new risks.

1. AI		
a.	Cheaper attacks	It was highlighted that cybercriminals will increasingly use AI techniques, as it will lower the cost of cyberattacks. AI is also able to scan documents and store the information while waiting for the best time to leak it.
b.	Useful in ransomware	AI can be utilised to encrypt files in a way that cannot be discovered easily.
2. IoTs		
a.	Physical effects by cyber means	IoT poses a tremendous security threat as users and devices become increasingly connected. As more and more devices and public infrastructure become connected to the Internet, it increase the ability of attackers to create significant physical effects by cyber means. IoT-connected devices, such as smart refrigerators, webcams, and Smart TVs are more vulnerable to attacks.

1.3. Implications

The digitalisation of the economy represents wider opportunities and challenges for the region. With the amount of information and platforms available online, the number of connected devices is set to grow to 50 billion by 2020. Southeast Asia, for instance, is highly dependent on the internet and social media as a form of information, communication and entertainment. According to Hootsuite, a well-known social media management platform, Hootsuite, Southeast Asia, which has the world's fourth largest Internet population, stated that internet usage in the region has rapidly increased from 41% in 2016 to 58% as of January 2018. This growth has been credited to access to cheaper mobile phones and devices, competitive internet prices and packages as well as the expansion of technological infrastructure that supports the usage of Internet and mobile connections in the region.

However, the growth of technology has always been heavily focused on efficiency, cost and user-convenience instead of security. ASEAN member states (excluding Singapore) for example, have only spent around $1.9 billion collectively making the member states' infrastructure vulnerable to be manipulated as platforms for cybercrimes. This gap represents a big challenge for the region especially as (1) the higher level of reliance on technology will only lead to a growth in the severity and damage caused by cybercrimes and (2) it serves as opportunities for malicious users including hostile states, criminals or terrorist organisations and individuals to conduct ill-activities and feeds into a growing dark web and interconnectedness of transnational crimes. Some ASEAN member states for example, Malaysia. Indonesia and Vietnam have been identified to become 'global hotspots' for suspicious web activities.

A report published by the Marsh & McLennan Companies titled *Cyber Risk in Asia Pacific: The Case for Greater Transparency* further confirms the vulnerability of the region, as hackers are 80% more likely to attack organisations in Asia as they take 1.7 times longer, on average, to discover a breach compared to global organisations. The level of crimes committed through the cyberspace reflects the vulnerabilities and wide range of opportunities available to both minor and major cybercriminals as well as opportunists.

These cybercrimes or internet-related crimes, defined by the United Nations Office on Drugs and Crime (UNODC) include "identity theft, crime, scams facilitated through email and social networking sites, sex offenses and fraud, and can ensnare victims through social media websites and mobile phones as well as standard internet sites" are unlikely to slow down and will continue to show an increasing trend globally and regionally. For ASEAN itself, just over ten years ago, reports showed cyber threats and malicious activity among ASEAN countries were not as serious as in China, South Korea, India, Taiwan and Japan. In 2008, for example, although four ASEAN countries (Thailand, Vietnam, Singapore and the Philippines) were listed among the top ten countries for malicious activity in Asia Pacific, this only represented around 10% of the total malicious activities in the region. By 2016, however, ASEAN member states are ranked among the countries most subjected to malware threat in the Asia Pacific.

A report titled *'The ASEAN digital transformation' by A.T. Kearney Analysis*, predicted that ASEAN will be one of the world's top five digital economies by 2025 adding on around $1 trillion to its GDP. This signals an urgent need for ASEAN to secure its cyberspace as the report further suggested that ASEAN member states should spend $171 billion collectively between 2017 and 2025 on cybersecurity to cope with the transformation and impact of digitalisation on ASEAN seen in "*Figure 1*".

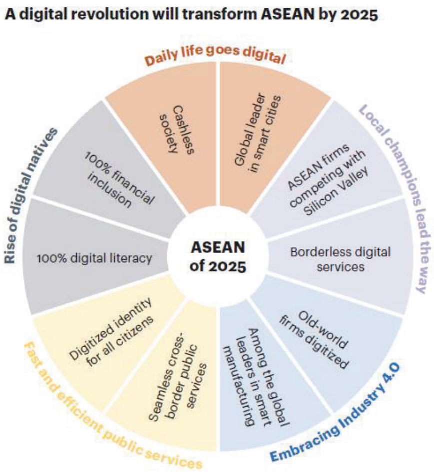

A digital revolution will transform ASEAN by 2025
Daily life goes digital
Cashless society
Global leader in smart cities
Local champions lead the way
ASEAN firms competing with Silicon Valley
Borderless digital services
Embracing Industry 4.0
Old-world firms digitized
Among the global leaders in smart manufacturing
Fast and efficient public services
Seamless cross-border public services
Digitized identity for all citizens
Rise of digital natives
100% digital literacy
100% financial inclusion
ASEAN of 2025

Figure 1

1.4. Observations

Despite the urgent call for ASEAN to promote security and stability in cyberspace, there are two important factors that regional countries need to get around in order to move forward in jointly tackling cybersecurity issues and building regional cybersecurity capabilities.

1.4.1. Lack of recognition and understanding of cybersecurity urgency

There is a varying degree of recognition and understanding of cybersecurity urgency across countries in the region. It is reported that despite the increasing awareness of the benefits and dangers of the cyberspace, as high as 78% of societies in the region still lack the understanding of cybersecurity. Then there is also the gap between technical and policy components in the cybersecurity dynamics, which needs to be addressed.

1.4.2. Fragmented efforts

Certainly in the past few years, discourse and dialogues on cybersecurity issues at the national, regional and international levels have significantly increased. Cybersecurity has become a more prominent theme in international security conferences. South Korea, for example, has since 2014 hosted the annual Cyber Working Group meeting at the sidelines of the Seoul Defence Dialogue. In 2016, cybersecurity has been added to the areas of ADMM-Plus practical cooperation. In Jan 2018, the ARF-ISM on ICTs Security (ARF Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies) 1st open ended Study Group (SG) on Confidence Building Measures was held in Tokyo, co-chaired by Japan, Malaysia and Singapore. More recently, in March 2018, Australia organised a Roundtable on Practical Futures for Cyber Confidence Building in the ASEAN region. These are but some of the cybersecurity related initiatives that have proliferated over the years. However, these efforts have been fragmented, which outcomes are often repeating the same rhetoric, instead of complementing each other towards building up national and regional cybersecurity capacities.

1.5. Brunei Darussalam: Realities and Related Risks from New and Emerging Technologies.

The uncertainties and surprises related to emerging technologies are certainly a cause of security anxiety. For Brunei Darussalam, a number of realities and development further contributed to the concerns.

- **Brunei Darussalam has a Muslim Majority population**. 78.8% of the population are Muslims.
- **Brunei Darussalam has a young population.** 71.8% of the population is in the productive age group (15-64 years of age).

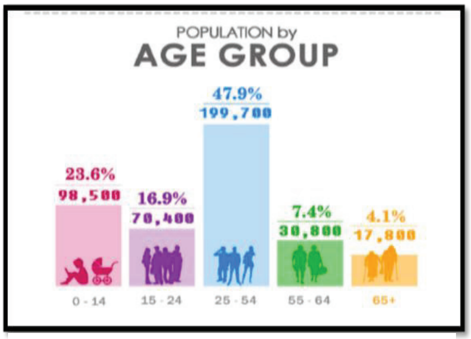


Figure 2

- **Brunei Darussalam has the highest internet penetration in the region**. 95% internet penetration.

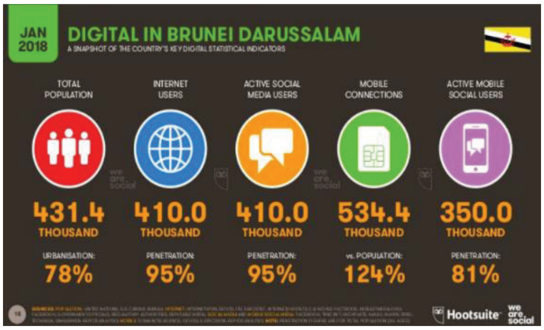


Figure 3

- **Increasing cybercrimes cases.** Cases have increased from 190 to 207 from 2016 to 2017. One of the cybercrime cases involved a student who is no older than 18 years old and was a victim of an online fraud with another man who posed as a woman. The student was later blackmailed to give his smartphone and other gadgets to the man or his compromising photos will be spread. Another case, which is Brunei's first cybercrime offence, was related to the hacking of a wireless Internet connection and using a stolen credit card for online purchases.
- **National cybersecurity capacity building needs more work.** This is according to the UN International Telecommunications Union (ITU), who in its July 2017 report indicated that, "Though the country is making some progress, a lot remains to be accomplished with regard to legal, technical and organisational institutions, educational and research capabilities, and cooperation in information-sharing networks to develop a near-perfect approach to cybersecurity.

1.6. Ways Forward

Consistent with the observations made above, recommendations in moving forward are:

- To prioritise on multi-stakeholders involvement in cybersecurity dialogues and practical initiatives, whether at the national, regional or international level with the key aim of bridging the gap between the policy and technical components in the cybersecurity ecosystem.
- To prioritise on synergising all the cooperative efforts towards the same direction that would build up and converge in producing tangible outcomes/benefits in a form of strengthened national and regional cybersecurity capabilities and resilience against cyberattacks and other surprises that new and emerging technologies may bring in the future.

2. ASEAN Cyber Situation Awareness: Foresights and Perspectives[1]

Alina binti Abang Haji Omarzuki

Although cybersecurity is not a new issue, it has, over the years, shot up to join terrorism and WMD (Weapons of Mass Destruction) proliferation as higher strategic altitude issues facing the world today. While countries are embracing the increasing attention to cybersecurity, cyber awareness and understanding are often lost in the midst of the hype. A look at the headlines-grabbing cyber-related events in the past 10 years will reveal the triggers or tipping points in cybersecurity urgency. These include the Snowden Case in 2013, the ISIS aggressive use of the internet and social media application, the alleged interference in the 2016 US Presidential Elections and the *Wannacry* Ransomware attacks in 2017. Recognizing these triggers can reconcile the different interpretations on what cybersecurity aspects are of importance to ASEAN, thus enabling a more focused cybersecurity cooperative efforts to work towards and greater clarity on the role of each stakeholder.

Context

When approaching issues relating to cyber and the cyber domain, analysis and outlook are framed in the context of the following realities:

- Cyber technology is a double-edged sword and the increasing dependency on cyberspace is imminent as the world is undergoing the fourth industrial revolution.
- Cyberspace has evolved as the latest battlefield within the overall geopolitical security situation, thus requiring a new dimension of awareness to traditional concepts of sovereignty and operations.
- Cyberspace is a highly complex domain due to the borderless and anonymous nature of threats in the cyber realm involving diverse range of stakeholders.

[1] This commentary was prepared for the NADI Workshop on ASEAN Cooperation in Cyber Capacity Building from 7 to 11 May 2018, taking place in Kameo Collection Hotel and Serviced Apartments, Ayutthaya Province, Thailand.

- There is an outstanding need to provide key stakeholders with a more practical understanding and solutions on cyber-related threats.

2.1. Overview

In recent years, cybersecurity has certainly become a hot topic, prominently discussed at major regional and international gatherings. Although cybersecurity is not a new issue, it has, over the years, shot up to join terrorism and WMD proliferation as higher strategic altitude issues facing the world today. While countries are embracing the increasing attention on cybersecurity, cyber awareness and understanding are often lost in the midst of the hype.

Cybersecurity is in fact still a grey area, an unfamiliar field to many strategic policy-makers and practitioners, who suddenly find themselves having to come up with effective cybersecurity strategies. Unlike the threats of terrorism and WMD proliferation, cyber threats are non-lethal, and so far, have not caused widespread destruction. So what is it about cybersecurity that garnered it the increasing level of urgency?

When it comes to formulating policies and responses – domestic, regional or international – there are still ambiguity and lack of common context in the scope of cybersecurity discussion, whereby cybersecurity issues are defined and framed differently depending on the experience of individual governments, businesses and users on how and to what extent cybersecurity issues have directly impacted them. This can range from cyberwarfare, to cyber espionage, cyber extortion, dissemination of fake news, and so on.

The interpretations of cybersecurity will continue to be diverse as innovations in the cyberspace landscape are fast evolving and the risks and vulnerabilities associated with them continue to be unfolding. This will continue to pose challenges to operationalising cooperation and harmonisation of cybersecurity issues.

2.2. Defining Period for Cybersecurity

The advent of cyberspace and ICT, certainly inspires hope for better opportunities – politically, economically and culturally. Notwithstanding these gains, it also brings with it risks and vulnerabilities. Before the turn of the century, cybersecurity needs and concerns were largely confined to IT departments in companies and individuals at home. As the cyber technology races ahead and governments have begun to embrace all things digital (digitalisation), the nature of malicious cyber activities has also evolved correspondingly – increasing in intensity, reach and impact. This introduced vulnerabilities to the core functioning of governments, critical national infrastructures and the geopolitical sphere. Evidently, the past ten years have been the defining period where the attention to cybersecurity as a national security issue has surged.

- Firstly, in terms of cybersecurity mentions in global threat / risk assessments.

i. **The World Economic Forum's Annual Global Risk Report**
In 2012, Cyber threat began to make the top 5 list of Global Risks in Terms of Likelihood, at number four. This year, it ranked the third most likely global risk, behind Extreme Weather Events and Natural Disasters.

ii. **DNI Annual Worldwide Threat Assessment of the US Intelligence Community**
Cyber threat has made the list since 2008 and beginning 2013, cyber threat became and remained the first topic mentioned in the worldwide threat assessment annually.

- Secondly, in terms of the engagement of cybersecurity issues in strategic level conversations.

i. **ASEAN Summit**
Cybercrime has been in the ASEAN's radar since 2001 when it was added in the ASEAN definition of transnational crime, following which several initiatives have been launched including the setting up of Computer Emergency Response Teams (CERTs), SOMTC Working Group on Cybercrime, ADMM-Plus EWG on Cybersecurity, ASEAN Ministerial Conference on Cybersecurity and the on-going effort to develop an ASEAN Cyber Centre and Hub.

ii. As a sign of the increasing priority given to the issue, ASEAN Leaders, in 2017, adopted the ASEAN Declaration to Prevent and Combat Cybercrime and the ASEAN Cybersecurity Cooperation Strategy. At this year's ASEAN Summit, the urgency of the issue got added emphasis as the ASEAN Leaders issued Statement on Cybersecurity Cooperation.

iii. **Munich Security Conference (MSC)**

The issue of cyber-attacks began to get mentions at the Munich Security Conference following the 2007 cyber-attacks on Estonia. Beginning 2011, cyber issues became a permanent panel discussion topic at the Conference. A subsidiary Summit on Cybersecurity was established in 2012 and in 2017; the MSC launched the Global Commission on the Stability of Cyberspace (GCSC). At the 2018 Conference, cybersecurity took centre stage, amid the allegation of Russia's involvement in the Petya Ransomware attack in 2017 and meddling in the 2016 US Presidential election.

2.3. Tipping points in cybersecurity urgency

A look at the headlines-grabbing cyber-related events in the past 10 years will reveal the triggers or tipping points in cybersecurity urgency.

	Event	Impact	Type
Nov 2008	Breach on US military computers	- **The most significant breach of US military computers ever.** - Marked a turning point in US cyber defence strategy.	- Cyber espionage
Jan 2010	Operation Aurora attack on *Google* and dozens of other companies	- Stolen data - Loss of clients' confidence - Reputational damage	- Cyber espionage
Aug 2012	Attack against Saudi oil company Aramco	- Rendered more than 30,000 computers on Aramco's business network unusable.	- Data deletion - Network attack
Sep, Oct, Dec 2012 and Jan 2013	Distributed denial of service (DDOS) attacks on the US financial sector	- Disabled 26 US banks' retail websites.	- Denial of Service

Mar 2013	Cyber-attack against South Korea's commercial and media networks	- Damaging tens of thousands of computer workstations. - Disrupted online banking and automated teller machine services.	- Data deletion - Network attack
June 2013	Edward Snowden leaked classified information from the National Security Agency (NSA)	- Shook public trust in the government - Affecting International affairs	- Cyber Espionage - Information theft
2014	ISIS aggressive use of the internet and social media applications	- **Revolutionised modern terrorism**	- Cyber exploitation
Nov 2014	Wiper malware infected Sony Pictures systems	- Intellectual property and personal employee details being leaked online.	- Cyber espionage
Dec 2015	Attack on Ukrainian power grid	- **The first known successful cyberattack on a power grid.** - Temporary disruption of electricity supply to the end consumers affecting about 230 thousand people.	- Data deletion - Network attack
May & July 2017	*WannaCry* and Petya Ransomware attacks	- *WannaCry* affected more than **230,000 computers in more than 150 countries.** - Petya affected around 2000 users in Russia, Ukraine, Poland, France, Italy, the UK, Germany and the US.	- Cyber Extortion
2016	The hack and release of sensitive information from the US Democratic National Committee in the lead up to the 2016 US Presidential election	- Influencing public opinion - Affecting International affairs	- Information theft
2017	Fake news as emerging cyber-enabled threat	- Influencing public opinion	- Cyber exploitation

- **The Snowden case in 2013** has served to amplify the extent and depth of the exposure of everyone connected to the Internet to **cyber spying and espionage**. It was a major wakeup call and a turning point in the development of social awareness of the risks.

- **The ISIS aggressive use of the internet and social media applications** revolutionise modern terrorism, allowing it to propagate its ideology, proliferate home-grown terrorists, expand its footprint all over the world, at a pace more rapid than the world has ever seen before.

- **The alleged interference in the 2016 US Presidential Elections** demonstrated how the cyberspace could be used to **interfere with public opinion** and influence the outcome of elections for political purpose. This has also catapulted the issue of fake news, which, enabled by social media, travel faster and reach more people, thus making the exercise of malign influence over societies more effective.

- **The *Wannacry* Ransomware attacks in 2017** accentuated the surprise element and **unpredictable nature** of the threat, and demonstrated that **cyber criminals have evolved** their skills and sophistication. The attacks marked another turning point in cyber awareness particularly the importance to build cyber resilience that can no longer be ignored.

Recognising these triggers can reconcile the different interpretations on what cybersecurity aspects are of importance to ASEAN, thus enabling a more focused cybersecurity cooperative efforts to work towards and greater clarity on the role of each stakeholder.

Looking ahead, as the digital future is fast approaching our doorstep – digitalisation, the IoTs, AI and Smart Cities – all stakeholders must become aware of the increasing cyber risks that this future will unleash.

2.4. Recommendations

Consistent with the observations made above, recommendations in moving forward are for ASEAN to:

- Devise a comprehensive regional delivery chain to establish clearer accountabilities (roles and responsibilities for responses and building resilience to cyber incidents).
- Set up regional clusters and champions for incidents that may / will require responses at the regional level.
- Utilise existing Programmes and upcoming Centres as the hub of cybersecurity cooperation.
- Set potential targets, timelines, routines and expected outcomes.
- Create joint research/assessment reports to review progress of ASEAN Cybersecurity Cooperation in "Readiness, Response and Recovery" areas such as:
    - Policy/Governance aspects.
    - Human & Technical competencies.
    - Presence of overarching guidelines/frameworks (vision, strategies, current state of delivery, past &present performances, delivery chains, etc.).
    - Existing reporting or cross-sectoral coordination mechanisms & any proposed changes
    - Platforms (if any) to bridge policy and technical gaps.
    - Areas of prioritisation via a two or three year work plan.
    - Legal-Related Requirements.

3. Brunei's Outreach in Countering Radicalisation[1]

Ampuan Yura Kasumawati binti DP Hj Adnan

Brunei Darussalam has not experienced direct threats from terrorist attacks, but as other countries, it remains vulnerable as transit points and terrorism financing activities. Its high internet penetration rate means that its population is also vulnerable to online radicalization. At the national level, several initiatives and measures have been in place to ensure peace and stability for the whole nation and country. In countering radicalization, Brunei Darussalam gives strong emphasis on coordination and collaboration among relevant agencies as well as cooperation with other countries through bilateral and multilateral platforms and mechanisms.

3.1. Overview

Brunei has not experienced direct terrorist attacks, but as other countries, remains vulnerable as transit points and potential terrorism financing. It is also certainly not immune from radicalisation. As a majority Muslim population 78.8% out of a total of 431,400 people in the country, the threat of radicalisation of the Muslims away from the teaching in accordance to the Ahli Sunnah Wal Jamaah is a growing concern. The recent case of a local man detained for suspected links to IS who provided financial contribution to an individual affiliated with IS and planned to move his family to Syria. Further to this, the country consists of a large young population where the highest is concentrated on ages between 25 to 54 years with the highest internet penetration in the region with a total of around 410,000 internet users. This makes it more important for Brunei to enhance awareness on extremist ideologies and better equip the community with cyber knowledge to deter away from any online crimes and ill activities.

[1] This commentary was prepared for the NADI Workshop on Counter-Terrorism, Counter Radicalisation and Cyber Security from 25 to 29 Jun 2018, taking place in Novotel on Stevens, Singapore.

3.2. Brunei's Initiatives and Measures

Brunei has taken a comprehensive whole of government and nation approach. As other countries in the region and beyond, Brunei strongly condemns terrorism in all its forms and manifestations and rejects extremism and radicalism. In this regard, Brunei also support efforts of the international community to prevent and eliminate all forms of terrorism, particularly through the various related international conventions and United Nations Security Council (UNSC) Resolutions, including Resolution 2170 (2014) calling on the international community to prevent terrorist groups from posing any threats to peace and security.

At the national level, several initiatives and measures have been in place to ensure peace and stability for the whole nation and country. Among Brunei's efforts in countering radicalisation is the importance of coordination and collaboration among relevant agencies as well as cooperation with other countries through bilateral and multilateral platforms and mechanisms.

3.2.1. Role of National Security Committee (NSC)

The committee oversees security matters at the national level. A Joint Working Group on Anti-Terrorism have been established under the Committee to look into threats relating to terrorism. Whilst countering terrorism and radicalisation lies primarily with other relevant ministries, the Ministry of Defence contributes through the various intelligence and information sharing exchanges bilaterally and multilaterally. The Royal Brunei Police Force serves at the front line to any security threats against Brunei, whereas the Royal Brunei Armed Force s play a supporting role.

Various legal instruments and frameworks are in place at domestic and international level covering all aspects to address terrorism and violent extremism. The enactment of Syariah Penal Code Order was also introduced in 2013 and enforced on 1 May 2014. Under the Syariah Law, any Muslims could be convicted should they preach or teach anything contrary to the Islamic teachings long held in Brunei and will be liable to a fine, or sentenced to imprisonment for a limited period of time. This is to ensure religion propagation (dakwah) is only carried out by qualified persons.

3.2.2. Central Authority on Religious Affairs

The Ministry of Religious Affairs, the Brunei Islamic Council and the State Mufti Department are responsible to uphold and defend the Islamic faith and teachings in accordance to *Ahli Sunnah Wal Jamaah* of Mazhab Syafi'e that is embedded in the Brunei's Constitution 1959 Chap 3 (1). Religious outreach has been in practice since 1950s to counter any elements of deviant practices that goes against *Ahli Sunnah Wal Jamaah*. The *Pusat Da'wah Islamiah* have constantly monitor religious practices and provided early interventions of deviant practices and beliefs. These are carried out through dialogues and consultations either face-to-face contacts and interviews, online and hotline. All this is important to ensure any interpretation against the Islamic faith and teachings in Brunei are addressed and extremist elements are mitigated.

Today, the challenge that poses a huge risk is the influence of online social media and Internet that supplies open information on religious practices, which may derive from invalid and uncertain sources of information and reading materials.

3.2.3. Education and Awareness

The preventive measures are centred among the youth. Through strong religious and formal education foundation and various community outreach programmes, it aims to instil values promoting a balanced way of life based on universally accepted values to ensure justice, harmony, respect of differences and help one another. *Perintah Pendidikan Ugama Wajib* or Compulsory Religious Education Order 2012 came into force in January 2013 made it mandatory for youngsters aged 7 years old and to attend religious schools in Brunei Darussalam. This is to educate and nurture the youngsters with Islamic education and knowledge.

Apart from that, scholarship awards are also given for students to study abroad to study more in depth about Islam in Egypt and Jordan, for example Islamic Jurisprudence, Syariah Law, Usuluddin and related studies. Here, scholars are exposed to various different strands of Islamic knowledge and jurisprudence for the purposes of scholarly discussions.

The *Program Khidmat Bakti Negara* (PKBN), which is a non-conscript national service programme for 16 to 21-year-olds, contributes to enhancing patriotism, building resilience and strengthening their understanding of the nation.

3.3. Recalibration of Strategies

The act of terrorism today has continuously responded to the dynamics of increasing globalisation and as such evolved in its form, key messages, motive, targets and methods of attacks. The nature of terrorism has transcended borders and boundaries, and are able to generate significantly greater influence towards both opponents and sympathisers alike.

In recent years, terrorist organisations have leveraged on technological advancements. These platforms serve as a multiplier, which enables extremists to propagate their ideologies, terrorist-linked groups to recruit home-grown terrorists thus spreading its influence globally, at a pace more rapid than before.

There is an increasing recognition and refocusing by countries on domestic counter-radicalisation strategies in the era of social media technologies. Certainly, for Brunei Darussalam, the vulnerabilities of online radicalisation including self-online radicalisation require urgent attention and pre-emptive measures including in cyberspace. Underlining all these, community plays an important proactive role to alert any suspicious activities to the authorities' attention for both preventive and enforcement measures.

4. Mapping Cybersecurity Cooperation Mechanisms[1]

Selina Farahiyah Teo

As the world grows more dependent on cyberspace and continues to pave its way into the fourth industrial revolution, cybersecurity continues to gain more traction and relevance. There are several cooperation mechanisms within ASEAN that look at cybersecurity. However, the efforts remain fragmented due to the lack of cross-sectoral collaboration. Consequently, this lack of synergy makes plans and discussions on cybersecurity often not translated into executable actions on a policy and operational level. There is thus a heightened need for ASEAN to focus more on multi-stakeholder engagement in cybersecurity dialogues and practical initiatives, on national, regional and international levels, to ensure initiatives across the various sectors are complementing each other, while avoiding duplication.

4.1. Overview

As the world grows more dependent on cyberspace and continues to pave its way into the fourth industrial revolution, cybersecurity continues to gain more traction and relevance in the minds of countries' decision makers especially as the growing dependence comes with great benefits and risks. The region also witnessed the proliferation of regional cooperation in cybersecurity with an aim to reduce its associated risks on national security and manage its challenges effectively together regionally.

4.2. Realities of Cyberspace

Cyberspace is a unique domain where on one hand, its borderless nature allows information to be created, stored and transmitted seamlessly regardless of one's geographical location; and on the other hand, it attracts malicious activities including cyberterrorism, cyber fraud and identity theft.

[1] This commentary was prepared for the NADI Workshop on Counter-Terrorism, Counter Radicalisation and Cyber Security from 25 to 29 Jun 2018, taking place in Novotel on Stevens, Singapore.

Cyberspace as a medium and target where as a medium, non-state actors such as terrorists and its affiliated groups exploit the current platform to recruit followers, spread propaganda and finance their activities. As a target, attacks in cyberspace disrupt functions of critical national infrastructures by disabling technology-reliant industries and services such as banking, health, water and electrical supplies. The same goes for the military where cyberspace has been widely regarded as the fifth domain of warfare.

4.3. Mapping cybersecurity cooperation frameworks

Given the ability of cyberattacks to inflict considerable damage due to its unique and pervasive nature, there are several cooperation mechanisms within ASEAN that looks at cybersecurity including the ASEAN Ministerial Meeting on Transnational Crimes (AMMTC), ASEAN Telecommunications and IT Ministers (TELMIN), ASEAN Ministers Responsible for Information (AMRI) and ASEAN Regional Forum (ARF). These cooperation mechanisms continues to multiply in the region where from 2016 to 2017, during which at least three mechanisms were established namely (i) ADMM-Plus EWG on Cybersecurity, (ii) ARF-ISM on Security of and in the Use of Information and Communication Technologies and (iii) ASEAN Ministerial Conference on Cybersecurity. The following matrix are few selected cooperation seen within the region.

ASEAN			
MECHANISMS		**PRIORITY AREAS**	**INITIATIVES / CBMs / PROJECTS**
1	ADMM-Plus EWG on Cybersecurity	▪ Defence and Military Practical Cooperation	▪ Shared Information on National Cybersecurity Strategies. ▪ Established POC for ADMM-Plus countries. ▪ Military Exercises – TTX and FTX. ▪ Cyber Glossary of Terms.
2	ARF-ISM on Security and the Use of Information and Communication Technologies (ARF-ISM on ICTs Security)	▪ Awareness Building and Exchange of Best Practices ▪ CERT-CERT Cooperation Frameworks ▪ Combating Criminal and Terrorist Use of ICTs	▪ Establishment of ARF POC. ▪ Info sharing on National Laws, Policies, Best Practices and Strategies. ▪ ARF Workshop on National Cybersecurity Strategy Building.
3	ASEAN Ministerial Conference on Cybersecurity	▪ Promoting Cyber Norms among AMS ▪ Cyber Capacity Building	▪ ASEAN Cyber Capacity Program, amounting to 10 million for the period of 5 years beginning 2016. ▪ Encourage ASEAN to begin its own dialogue on cyber norms.

4	ASEAN Ministers Responsible for Information (AMRI)	▪ Countering Fake News ▪ Communicating the right information	▪ Shared experiences in countering fake news including legislation to regulate and manage online space and fake accounts. ▪ Implementing programs to enhance media literacy, especially among the youths.
TRACK 1.5 and 2			
5	Australian Strategic Policy Institute (ASPI)	▪ Raise awareness on cyber-related issues for broader strategic policy ▪ Facilitating cross-sectoral conversations on cyber issues.	▪ Publication of an annual report on Cyber Maturity in the Asia-Pacific region
		▪ Strengthening existing CBMs on Cybersecurity	▪ Draft of Sydney Document
6	Council for Security Cooperation in the Asia Pacific Working Group (CSCAP WG)	▪ Focused on cyber threat scenarios in Asia Pacific ▪ To proposed cybersecurity strategy for ARF's consideration	▪ Cybersecurity Study Group ▪ Preparation of a draft CSCAP Memorandum on Cyber

4.4. Observations

Despite all these initiatives, there remains to be apparent gaps between various cooperation mechanisms within and across different tracks.

a) **Lack of cross-cutting discussion in cybersecurity**

Among the various cybersecurity cooperation mechanisms, the ASEAN Ministerial Conference on Cybersecurity is the only Track I mechanism that discusses on cross-cutting cybersecurity issues. Last September, Ministers, among others, reaffirmed the need for ASEAN to take a holistic and more coordinated approach to regional cybersecurity cooperation and capacity building. Others such as AMMTC, TELMIN and ARF looks into different aspects of cybersecurity and cybercrime. However, the ministerial mechanism does not have strong linkages with other Track 1 platforms.

b) **Lack of cross-sectoral collaboration between cybersecurity cooperation mechanisms** ***(Figure 4)***

In the last five years, the focus on cybersecurity issues have significantly increased at the national, regional and international level. For example, since 2014, South Korea has hosted the annual Cyber WG meeting at the sideliners of the Seoul Defence Dialogue and in 2016; cybersecurity has been added to the areas of ADMM-Plus practical cooperation. This year, in January, the ARF-ISM on ICTs Security has its first open-ended Study Group (SG) on CBM co-chaired by Japan, Malaysia and Singapore in Tokyo; and Australia organised a Roundtable on Practical Futures for Cyber Confidence Building in the ASEAN region back in March.

However, these initiatives remains fragmented due to the lack of cross-sectoral collaboration between the mechanisms. Consequently, these lack of synergy makes (1) plans and discussions on cybersecurity often not translated into executable actions on a policy and operational level; (2) the risk of overlapping and duplication of efforts higher rather than complementing each other towards building up national and regional cybersecurity capacities as seen between the ADMM and ARF; and (3) disconnect between the policy and technical components of cybersecurity.

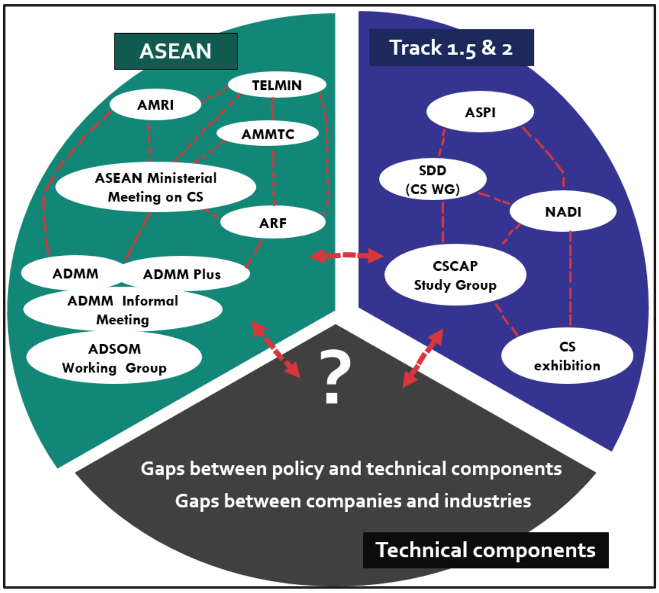


Figure 4 Cybersecurity Cooperation across different mechanisms

4.5. Managing Cybersecurity in Brunei Darussalam

Brunei Darussalam has one of the highest internet penetration among the ASEAN member states at 95%. In the last fifteen years, Brunei has continuously developed strategies to manage its increasing dependence on the cyberspace and gaps in addressing its IT and cyber challenges. Among some of its national initiatives can be seen below:

- Establishment of the National Security Committee with a host of local security agencies to manage and address cybersecurity threats.

- E-government Strategic Plan 2009 – 2014 with an aim to develop integrated e-services and deliver better public services and assist the public to better adapt to the advancement of ICT.

- The Digital Government Strategy 2015-2020 driven by the *Wawasan 2035* aiming to support the goals envisioned. (Goals: highly skilled and well-education citizens, high quality of life, and a dynamic and sustainable economy)

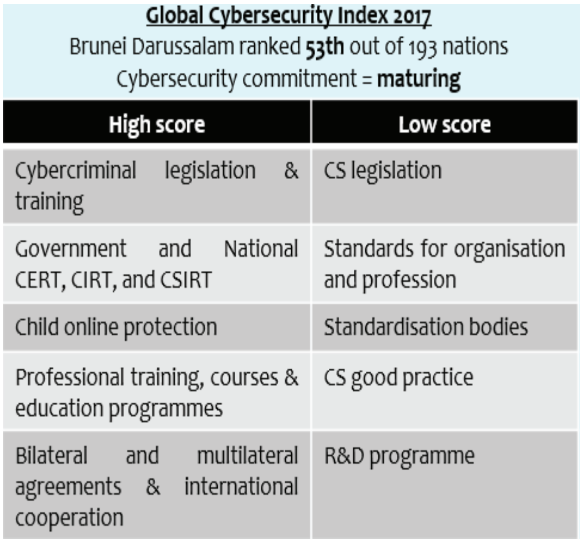
- Establishment of numerous agencies responsible for the different areas related to IT and CS including:
    - The Authority for Info-communications Technology Industry (AiTi) established in 2003 is a statutory body where one of the area it is responsible for is the country's ICT industry development.

    - IT Protective Security Services Sdn Bhd (ITPSS) established in 2003 looks into information security solutions, providing various specialised information security and physical security services including penetration testing, digital forensics, secure event management and IT security training.

    - Brunei National Computer Emergency Response Team (BruCERT) formed in 2004 is the nation's first trusted referral agency dealing with online threats and computer security incidents in the country. It is a platform for ITPSS to test its Incident Response and serves as a monitoring mechanism that addresses any computer-related and internet-related incidents through issuing early warning, early response and post-mortem of such incidents.

Currently, Brunei is focused on strengthening existing cooperation and ensuring an integrated whole-of-nation approach in dealing with cyber threats. These include (1) promoting cyber awareness especially among the society, (2) drafting of the National Cybersecurity Framework to identify laws and measures needed to protect the public and define the roles of relevant agencies, and (3) strengthening its cyber early warning system.

In recognising the global efforts in addressing cybersecurity and its challenges, a report published in July 2017 by the UN International Telecommunications Union (ITU) ranked Brunei's cybersecurity efforts at 53th out of 193 nations in the Global Cybersecurity Index 2017 and is perceived to be in the maturing stage in terms of its commitment as seen in Figure 2. The figure also highlights areas where Brunei did well and gaps that needed more work to achieve an ideal approach to cybersecurity. This is further supported by the findings in another report by ASPI on Cyber Maturity in the Asia Pacific 2017, which highlighted the country's effort in dealing with cybersecurity and at the same time highlighted its slow progress where gaps remains overlooked.



Global Cybersecurity Index 2017
Brunei Darussalam ranked **53th** out of 193 nations
Cybersecurity commitment = **maturing**

High score	Low score
Cybercriminal legislation & training	CS legislation
Government and National CERT, CIRT, and CSIRT	Standards for organisation and profession
Child online protection	Standardisation bodies
Professional training, courses & education programmes	CS good practice
Bilateral and multilateral agreements & international cooperation	R&D programme

Figure 5 Global CS Index 2017

4.6. Recommendations

The borderless nature of cyberspace and the increasing risks makes threats and challenges more complex in nature and in ensuring cooperation mechanisms are able to tackle threats more effectively, there is a need for ASEAN to:

- Firstly, engage various stakeholders in cybersecurity dialogues and practical initiatives, on a national, regional and international level to ensure initiatives across the various sectors are complementing each other, and avoiding duplication. There is also a need to bridge the gap between the policy and technical components in the cybersecurity ecosystem as current approaches to cybersecurity challenges are done separately in policy and technical platforms.

- Secondly, in view of the different priorities and inconsistent focus on cybersecurity depending on the rotation of the ASEAN Chairmanship, there is a need to devise a comprehensive regional plan to ensure continuity of cybersecurity cooperation is maintained and momentum is not lost after the end of championing chairmanships.

- Thirdly, to stocktake of existing cybersecurity cooperation and future plans across the various sectors and tracks. This will allow all stakeholders to synergise cybersecurity initiatives and produce more concrete outcomes needed to strengthen national and regional cybersecurity capabilities and resilience against cyber challenges. Here, Track II can support Track I by raising awareness on all the work that has been done across the various sectors through international cooperation and discussion. Track II can achieve this by:

    - Mapping out laws and regulations, policies, doctrines in the ASEAN region track
    - Tracking and reporting ongoing unclassified cyber activities such as exercises, workshops, conferences
    - Providing support to the ASEAN Secretariat in their cybersecurity agenda throughout succeeding chairmanships.

5. Elevating the Contribution of Regional Defence Cooperation in Tackling Transnational Security Issues Particularly Organised Crimes[1]

Haji Muhammad Abdul Aziz bin Haji Yaakub

Transnational crimes have been occupying the attention of national and regional security practitioners for quite some time now, stretching back even earlier than the advent of globalisation. Transnational criminals will continue to resort to violence in order to successfully execute their activities, affecting public safety and the welfare of the citizens, bringing significant impact on the political, economic and socio-cultural stability and security of the affected nations and the region. Regional efforts to respond to transnational crimes are spearheaded by the AMMTC (ASEAN Ministerial Meeting on Transnational Crime) and its subordinate SOMTC (Senior Officials' Meeting on Transnational Crime) and Working Groups. For its part, regional defence cooperation in tackling transnational security issues began to solidify with the establishment of the ADMM and the ensuing ADMM-Plus, particularly when issue-specific ADMM-Plus Experts Working Groups were created. Granted that transnational crimes are largely under the purview of law enforcement institutions and criminal justice, the increasingly strategic nature of the threat called for efforts to prevent and mitigate transnational crimes to cut across multiple stakeholders, both at the national and regional levels.

5.1. Overview

When approaching issues relating to transnational crimes, analyses and outlook are framed in the context of the following:

- Transnational crimes have been occupying the attention of national and regional security practitioners for quite some time now, stretching back even earlier than the advent of globalisation.

[1] This commentary was prepared for the NADI Workshop on Strengthening ASEAN Defence Cooperation in order to Control Transnational Crimes in Southeast Asia from 27 to 30 August 2018, taking place in Hotel Salak the Heritage, Bogor, Indonesia.

- Interconnectedness and the technological revolution allowed transnational criminals to thrive and prosper – to diversify their activities and become more sophisticated and organised, as well as avoid detection.

- Transnational crimes have throughout history and over the years manifested in numerous forms, ranging from:
    - Traditional transnational crimes that came to prominence in the 1970s, such as drug trafficking and arms smuggling;
    - The more contemporary types joining the foray in the 1990s, such as money laundering and piracy;
    - The new and emerging breeds of transnational crimes, such as cybercrime, environmental crime and organ trafficking.

- Transnational criminals will continue to resort to violence in order to successfully execute their activities, affecting public safety and the welfare of the citizens, bringing significant impact on the political, economic and socio-cultural stability and security of the affected nations and the region.

5.2. National Approaches to Transnational Crimes

Like any other country, Brunei Darussalam is equally vulnerable to various forms of transnational crimes. Recognising this, Brunei Darussalam is committed to work with regional partners bilaterally and multilaterally, particularly with fellow ASEAN member states to strengthen international cooperation in the fight against transnational crimes.

Brunei Darussalam is a small country both in its size and population, thus diminishing some of the pull factors for transnational criminal activities. Data for the past five years recorded minimal cases of transnational crimes.

With regard to the three areas of focus for this workshop, the national approaches in tackling them include:

Type	Legal Framework	Institutional Mechanism [Specialised Unit / Lead Agency / Working Group]	Bilateral and Multilateral Arrangements
People Smuggling	Trafficking and Smuggling of Persons Order 2014	Royal Customs and Excise Department	Capacity building assistance initiatives such as technical trainings and legislative advise Information / intelligence sharing initiatives – bilateral and through membership in Interpol and other regional and international information sharing platforms.
Money Laundering	Criminal Asset Recovery Order 2012	Financial Intelligence Unit (FIU), MOF	
Cyber Crimes	Computer Misuse Act 2007	Criminal Investigation Department (CID), Royal Brunei Police Force Brunei Computer Emergency Response Team (Bru-CERT led by PMO) Cybercrime Focus Group – Chaired by the Attorney General Chambers (AGC) National Cybersecurity Working Committee	

5.3. National Approaches: The Role of Defence

Ensuring security in Brunei Darussalam, including against the threat of transnational crimes, is addressed using the Whole-of-Government approach, to gain a multiplier effect from the diverse resources and capabilities of the various security agencies in the country.

Under the purview of the National Security Committee (NSC) and its subordinate working committees, the Ministry of Defence and the Royal Brunei Armed Forces are actively contributing to the national security strategy. These include:

- Border control management through joint patrol operations, and
- Membership in the national-level working committees on Cybersecurity, Law Enforcement, Maritime Security as well as Technical and Intelligence working committees.

5.4. Regional Frameworks in Preventing and Combating Transnational Crimes

Regional efforts to respond to transnational crimes are spearheaded by the AMMTC (ASEAN Ministerial Meeting on Transnational Crime) and its subordinate SOMTC (Senior Officials' Meeting on Transnational Crime) and Working Groups. In 1997, in its inaugural meeting, the AMMTC adopted the ASEAN Declaration on Transnational Crime, which listed out seven transnational crimes:

- Terrorism
- Drug Trafficking
- Arms Smuggling
- Money Laundering
- Trafficking in Persons
- Piracy
- International Economic Crimes.

Cybercrime was later included to the list in 2001; and in 2015, people smuggling and illicit trafficking of wildlife and timber were added.

Under the AMMTC process, plan of actions in combating transnational crime has been formulated in strengthening regional collaboration, commitment and capacity to combat the threat, which manifested in several initiatives such as the 2015 ASEAN Convention against Trafficking in Person (ACTIP). Investigative and enforcement instruments, particularly the Interpol and ASEANAPOL have also played a significant role in bolstering regional efforts against transnational crimes. Concurrently, regional working groups, for example the ARF Inter-sessional Meetings (ISMs) and the ADMM-Plus Experts Working Groups (EWGs) provided significant platforms of information / intelligence sharing and sharing of best practices, and germination of effective regional strategies in tackling transnational crimes.

5.5. Regional Approaches: Contribution of Defence

Under the ADMM-Plus Process, transnational security issues are widely discussed, and EWGs on Counter-Terrorism, Maritime Security and Cybersecurity were formed to facilitate information / intelligence sharing and formulation of issue-specific work plans for regional defence cooperation in the areas.

5.6. Observations

Moving ahead, several important observations can be made:

- The incentives particularly that of financial benefits, for committing transnational crimes will continue to remain high. At the same time, money laundering will continue to facilitate transnational crimes by fuelling the activities of organised criminals.

- Adverse impacts and the need to address transnational crimes are clear and countries have taken various concerted efforts to combat them, including efforts under international and regional frameworks.

- Nevertheless, the advent of cybercrime added complexities to prevention and enforcement efforts whereby transnational crime activities spill over from the physical world to the cyber world.

- Additionally, the growing transnational criminal-terrorist nexus – for example the increasing link between cyber extortion and money laundering to terrorist financing; as well as arms smuggling to terrorist attacks – makes effective counter transnational crime strategies ever more urgent.

- Granted that transnational crimes are largely under the purview of law enforcement institutions and criminal justice, the increasingly strategic nature of the threat called for efforts to prevent and mitigate transnational crimes to cut across multiple stakeholders, both in national and regional settings.

- The impacts of regional efforts depend on the enforcement capabilities of individual countries. Different countries have different institutional capacities to combat transnational crimes, thus improvements in the effectiveness of regional strategies must go hand-in-hand with capacity building efforts at the national level.

5.7. Recommendations

Consistent with the observations made, some operational recommendations in moving forward in strengthening ASEAN defence cooperation in order to manage transnational crimes in Southeast Asia include:

- Optimising the benefits from the multitude of available platforms of conversations, information / intelligence and best practices sharing by delivering effective recommendations for national and regional counter transnational crime strategies.

- Synergising the work of various regional working groups that look at transnational crimes towards producing tangible outcomes/benefits in the form of effective strategies and strengthened national and regional capacities against transnational crime.

- Boosting capacity building initiatives to strengthen national capacity to prevent and combat transnational crimes, in particular, technical assistance and training in detection / investigative and enforcement areas.

SHHB
IDSS

SULTAN HAJI HASSANAL BOLKIAH
INSTITUTE OF DEFENCE AND STRATEGIC STUDIES