SHHBIDSS Paper
11th NADI Meeting, Singapore, 2-5 April 2018

Perspectives on the New Emerging Non-Traditional Security Issues

Introduction. 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.

In recent years, cybersecurity has received increasing attention. Indeed from just merely the threats of spam and malware, cyberattacks are growing in prevalance and have increased in sophistication and destruction. 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 oppourtunists 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 cyberthreats actors have become more and more creative in the exploitation of the cyber domain.

1.	**Hacker Attacks**	
a.	Information Theft / Breach of privacy	<u>*Hacking of UK Lender Company, Wonga, Apr 2017*</u>. Hackers had stole personal data of around 245,000 customers including bank account, sort codes, home addresses and email details.
		<u>*Hacking of US CloudPets Smart Toys, Feb 2017*</u>. The hacking exposed 2 millions voice recordings of children and parents, email addresses and password from more than 800,000 accounts.
		<u>*Hacking of Singapore MINDEF I-Net System, Feb 2017*</u>. Hackers had stolen the NRIC numbers, telephone numbers and birth dates of 854 personnel.
		<u>*Hacking of UK Telecom Giant, TalkTalk Website*</u>. 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	<u>*WannaCry Ransomware Attacks, May 2017*</u>. 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.
		<u>*Petya Ransomware Attacks, Jul 2017*</u>. 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 millions 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 ecrypted 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 oppourtunity 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 victim 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.

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 – Artificial Intelligence (A.I.) and the Internet of Things among others – are proving to be key disruptive drivers of the future which will inevitably harbour new risks.

1. Artificial Intelligence		
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. The Internet of Things (IoT)		
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 increased 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.

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. Being the world's fourth largest Internet population, Hootsuite, a well-known social media management platform, further confirmed that Southeast Asia's internet usage has rapidly increased from 41% in 2016 to 58% as of January 2018. This growth has been credited to cheaper mobiles available, 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.

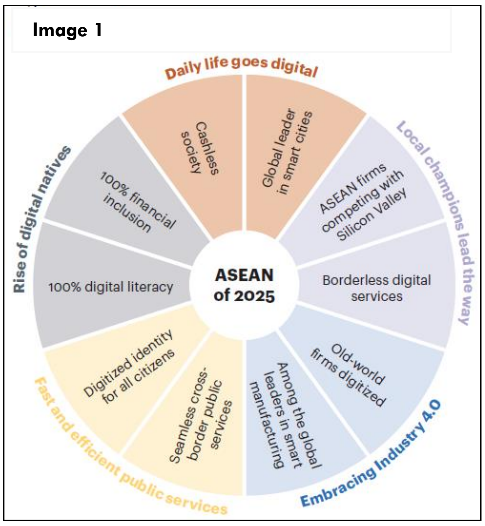
However, the growth of technology has always been heavily focused on efficiency, cost and user-convenience instead of security. ASEAN member states for example, have only spent around $1.9 billion collectively (with the exception of Singapore) making the member states' infrastructure vulnerable to be 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, regionally and globally. Among the 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 indicates the system's 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 cyberthreats 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 and strengthen 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 Image 1.

Image 1


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

Observations. Despite the urgent call for ASEAN to secure and strengthen its 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 cyber security capabilities.

a) **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.

b) **Fragmented efforts.** Certainly in the past few years, discourses 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. But these efforts have been fragmented, which outcomes are often repeting the same rhetorics, instead of complementing each other towards building up national and regional cybersecurity capacities.

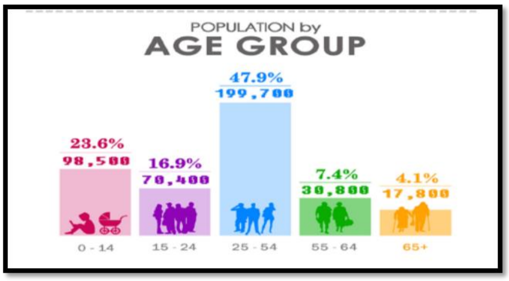
Brunei Darussalam: Realities and Related Risks from New and Emerging Technologies. The uncertainties and surprises related to emerging technologies are certainly a cause of security anxiety. For Brunei Darussalam, a number of realities and development further contributed to the concerns.

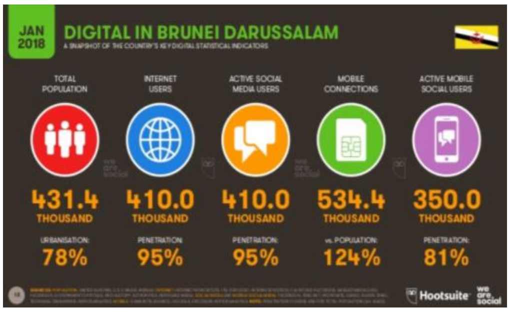
a) **Brunei Darussalam has a Muslim Majority population.** 78.8% of the population are Muslims.

b) **Brunei Darussalam has a young population.** 71.8% of the population is in the productive age group (15-64 years of age).

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

d) **Increasing cybercrimes cases.** Cases have increased from 190 to 207 from 2016 to 2017.





One of the cybercrimes cases involved a student who is no older than 18 years old and was a victim of an online scam with another man who posed as a woman. The student, was later on 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.

e) **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.

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

1. Firstly, 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.

2. Secondly, 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.