ASEAN Cyber Situation Awareness: Foresights and Perspectives

CONTEXT

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

   a. Cyber technology is a double-edged sword and the increasing dependency on cyberspace is imminent as the world is undergoing the fourth industrial revolution.

   b. 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.

   c. Cyberspace is a highly complex phenomenon due to the borderless and anonymous nature of threats in the cyber realm involving diverse range of stakeholders.

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

OVERVIEW

2. 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.

3. 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?

4. 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.

5. 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.

DEFINING PERIOD FOR CYBERSECURITY

6. 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.

7. 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.

8. Evidently, the past ten years have been the **defining period** where the attention to cybersecurity as a national security issue has surged.

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

i. *The World Economic Forum's Annual Global Risk Report*. In **2012**, Cyberthreat 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.

b. 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 Cyber Security, 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.

TIPPING POINTS IN CYBERSECURITY URGENCY

9. 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 cyberdefence 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

a. ***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.

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

c. ***The alleged interference in the 2016 US Presidential Elections*** demonstrated how the cyberspace can 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.

d. ***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.

10. 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.

11. Looking ahead, as the digital future is fast approaching our doorstep - Digitalisation, The Internet of Things, Artificial Intelligence and Smart Cities - all stakeholders must become aware of the increasing cyber risks that this future will unleash.

RECOMMENDATIONS

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

a. Devise a comprehensive regional delivery chain to establish clearer accountabilities (roles and responsibilities for responses and building resilience to cyber incidents).

b. Set up regional clusters and champions for incidents that may / will require responses at the regional level.

c. Utilise existing Programmes and upcoming Centres as the hub of cybersecurity cooperation.

d. Create joint research/assessment reports to review progress of ASEAN Cybersecurity Cooperation in "Readiness, Response and Recovery" areas such as:

i. *Policy/Governance aspects.*
ii. *Human & Technical competencies.*
iii. *Presence of overarching guidelines/frameworks (vision, strategies, current state of delivery, past &present performances, delivery chains, etc).*
iv. *Existing reporting or cross-sectoral coordination mechanisms & any proposed changes*
v. *Platforms (if any) to bridge policy and technical gaps.*
vi. *Areas of prioritisation via a two or three year work plan.*

vii. *Legal-Related Requirements.*

e. Set potential targets, timelines, routines and expected outcomes.

--- oo ---