Technology and security: Adapting to changing cyber security threats in South East Asia

Benjamin Ang

Senior Fellow, Cyber and Homeland Defence /

Deputy Head, Centre of Excellence for National Security (CENS)

S Rajaratnam School of International Studies (RSIS)

Nanyang Technological University Singapore

Twitter @benjaminang

RSiS

Cyber threats in South East Asia

1. Comparative analysis of cyber threats and their evolution in South East Asia

2. Digitization of critical infrastructure and growing security risks

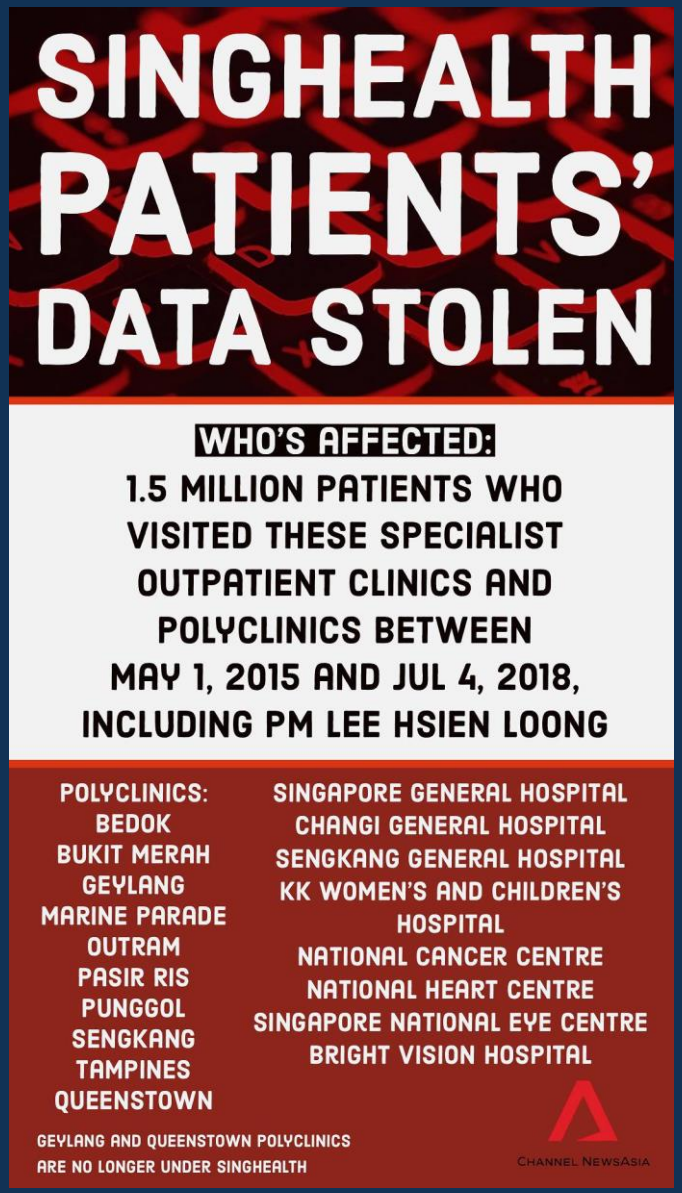
3. Conceiving of and preparing for cyber warfare

CYBER THREATS AND THEIR EVOLUTION IN SOUTH EAST ASIA

RSiS

SingHealth breach

- 1.5 million patients' non-medical personal data stolen, incl PM
- “This was a deliberate, targeted and well-planned cyberattack. It was not the work of casual hackers or criminal gangs … we are not able to reveal more because of operational security reasons.”
- Symantec attributed to APT



Incidents in ASEAN 2018-2019

- Singapore
  - 2,400 MINDEF/ SAF personnel, by phishing a 3rd party vendor
- Singapore
  - 14,200 people diagnosed with HIV, taken by ex-lover of a doctor with access
- Thailand and Vietnam
  - Toyota customer data, no details given
- Philippines
  - 82,150 customers of Wendy's
- Philippines
  - 900,000 customers of pawnshop Cebuana
- Thailand
  - 45,000 customers of True Corp mobile
- Malaysia
  - 46 million mobile subscribers' data

» [source: CSO Online]

APTs and their targets in Asia

APT	Target countries	Target entities
FunnyDream (C)	Malaysia, Philippines, Thailand, Vietnam	High-level government organisations; political parties
Platinum	Indonesia, Malaysia, Vietnam	Diplomatic and government entities
Cycldek (C)	Laos, Philippines, Thailand, Vietnam	Government, defence, and energy sectors
HoneyMyte	Myanmar, Singapore, Vietnam	Government organisations
Finspy	Indonesia, Myanmar, Vietnam	Individuals
PhantomLance	Indonesia, Malaysia, Vietnam	Entities
Zebrocy (R)	Malaysia, Thailand	Entities [source: Kaspersky]

Economic and Geopolitical intelligence gathering

Information Operations in ASEAN

- Facebook took down accounts from Iran, Israeli company targeting SE Asia, and Russian campaign targeting Thailand (2019)
- Facebook took down a Chinese disinformation campaign in Philippines of 155 accounts, 11 pages, 9 groups, 6 Instagram accounts with 130,000 followers

Cybercrime in ASEAN

INTERPOL ASEAN Cybercrime Operations Desk reported increase in 2019

- Botnets
- Phishing
- Business email compromise (BEC)
- Banking malware.
- Ransomware
- Cryptojacking

Vulnerability is due to

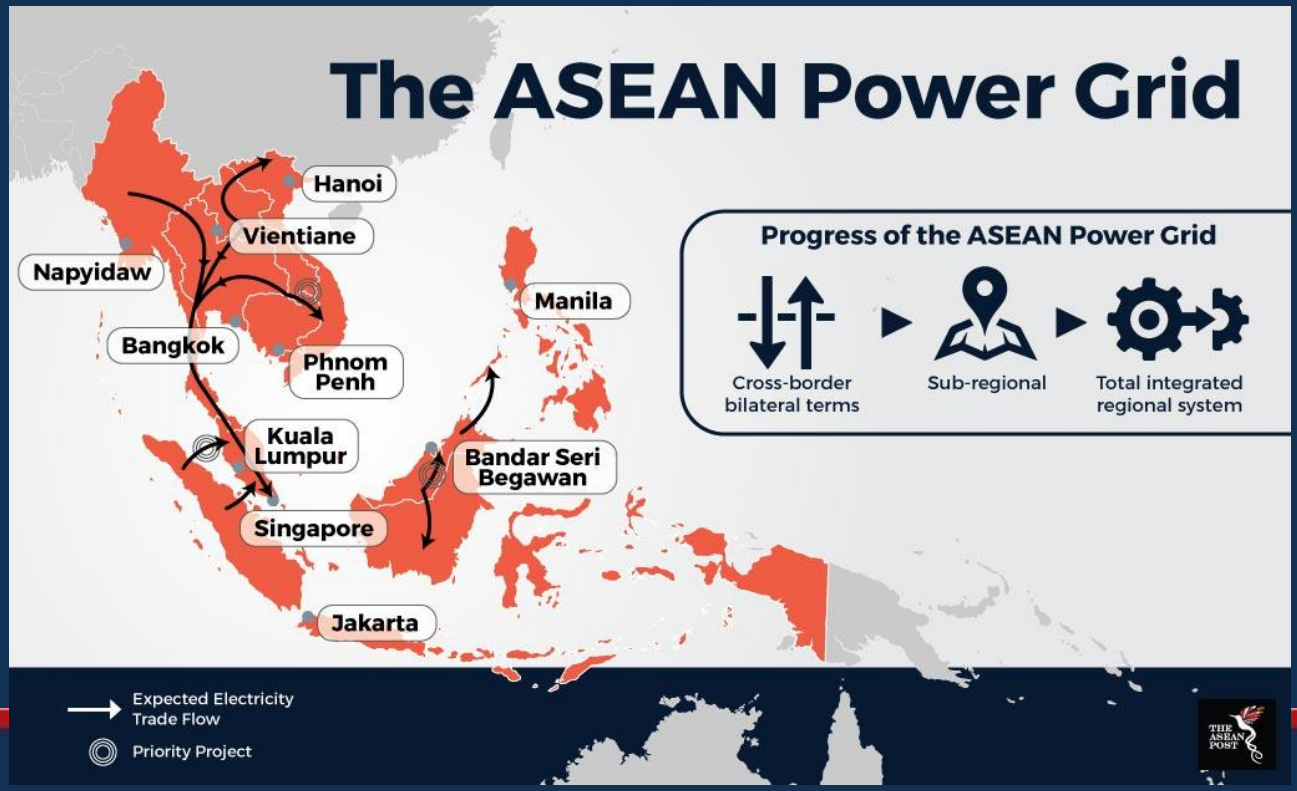
- Quicker digital transactions
- Greater internet connectivity
- Growing digital economies
- Asia becoming digital asset hub
- Lacking cybersecurity investment
- Low awareness

DIGITIZATION AND RISKS

ASEAN established the ASEAN Power Grid

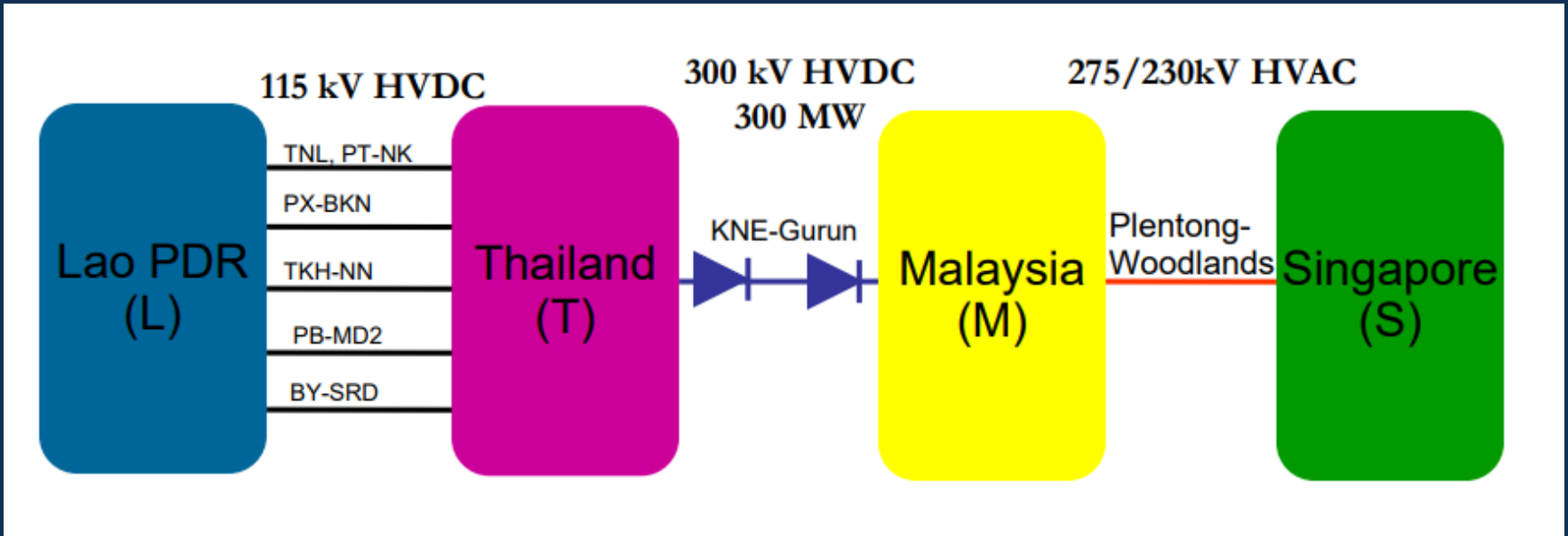
Stages

- (1) Bilateral (2) Sub-regional (3) Total integrated



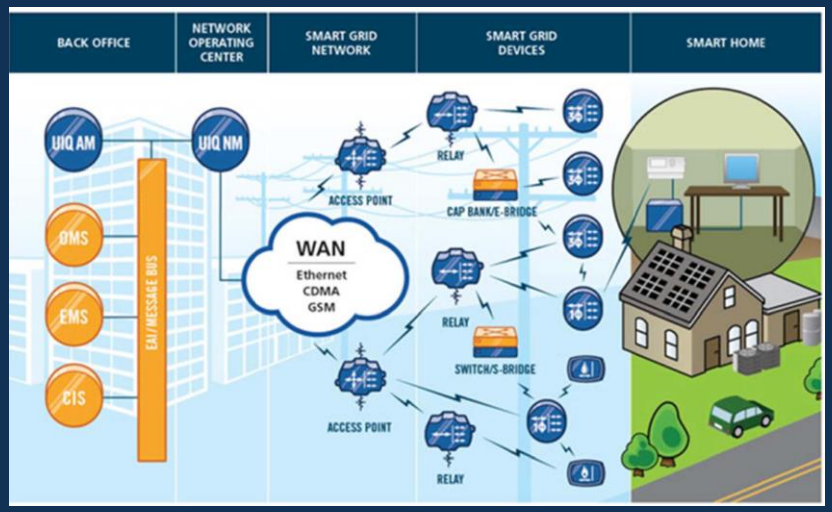
RSiS

Laos – Thailand – Malaysia project

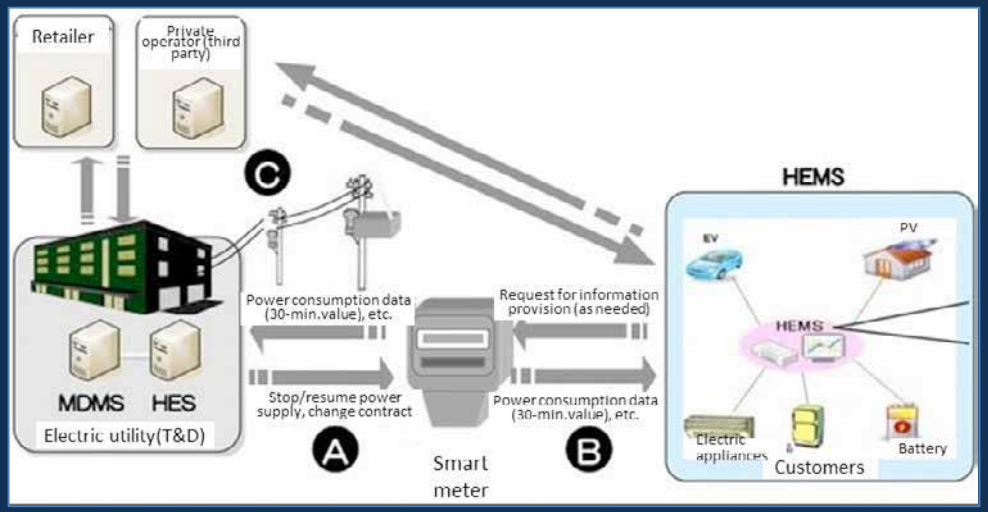


Smart Grids

- Electrical power system using ICT in generation, delivery, and consumption of electrical energy
  - Smart meters (IOT)
  - Smart generators
- Tested by Singapore, Malaysia, Indonesia, Philippines

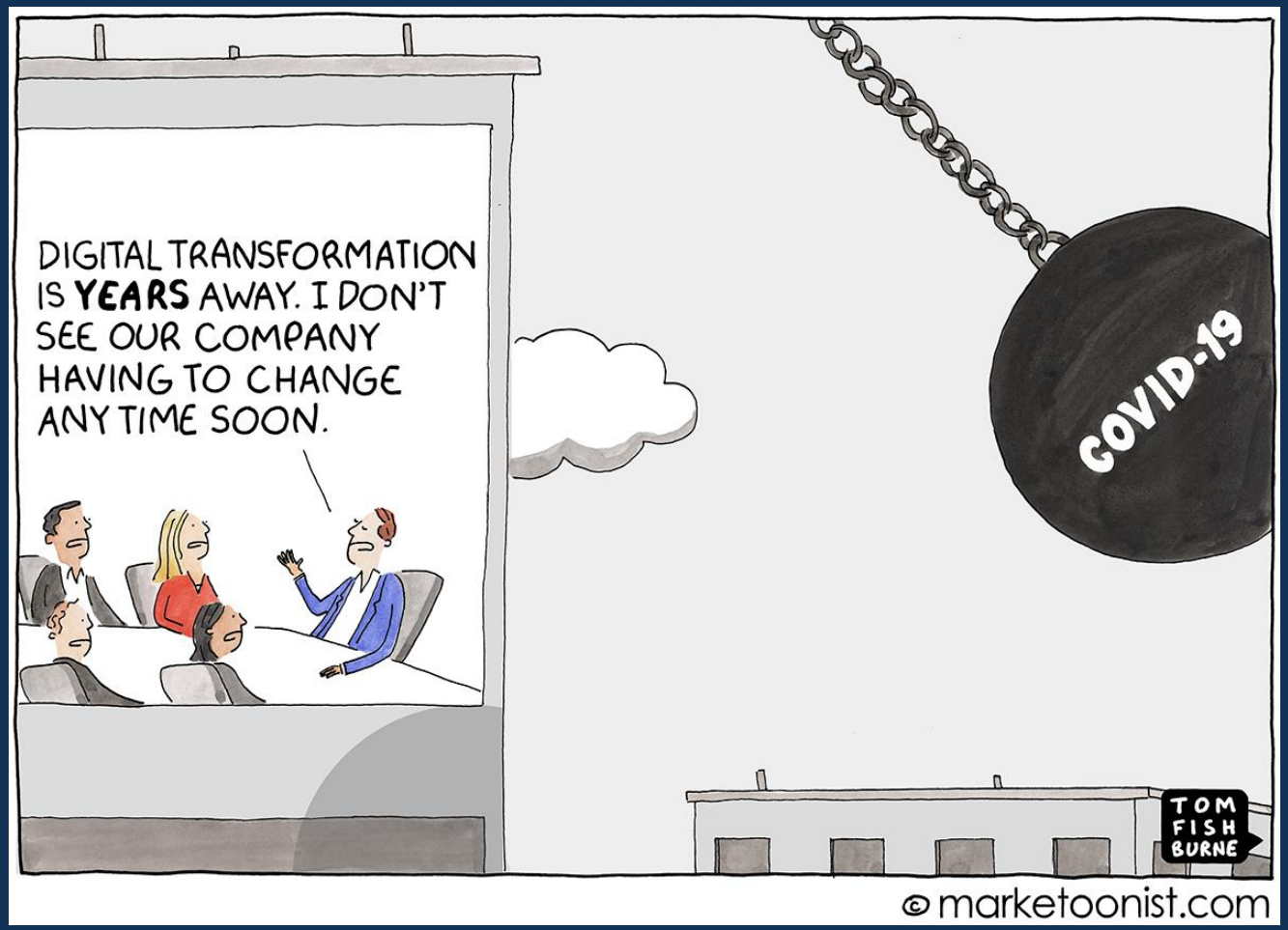


But Smart Grids are vulnerable

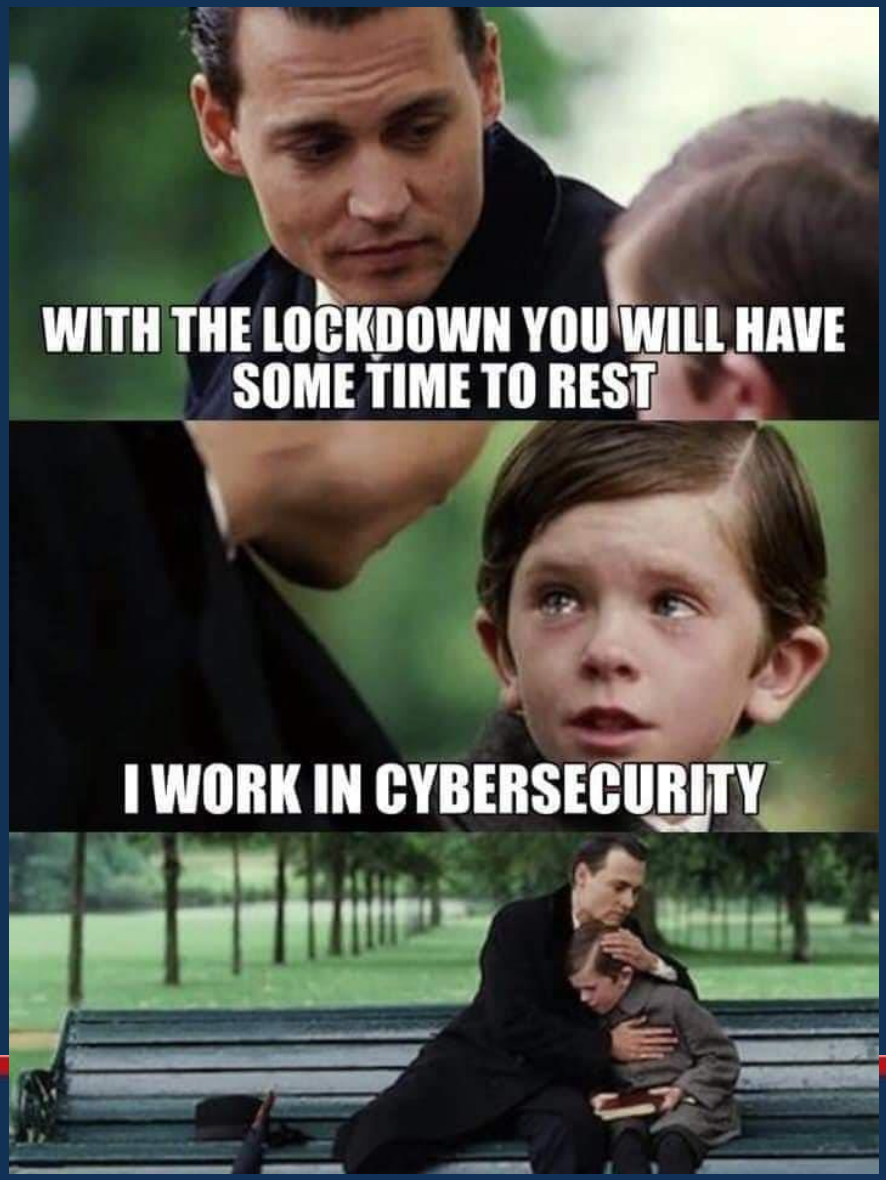


- 5G technology -> Edge Computing
- IOT enabled power plants
- Global smart grids = 440,000,000 points of attack (IEEE)

Digital transformation hits home



COVID-19 increases cyber risk



RSiS

WORKING TO AVOID CYBER WARFARE

RSiS

Strengthen international partnerships

- Singapore has bilateral MOU's with Canada, France, India, NL, USA and more
- Building capacity in ASEAN with S$10m (US$7.3m) ASEAN Cyber Capacity fund, upgraded to S$30m (US$21.9m)
- Actively participating in the UN GGE and the UN OEWG

Why build capacity in ASEAN?

- ASEAN needs Cyberspace, because Digital Transformation can bring economic progress for all Member States

- BUT Member States have different levels of cyber maturity – see the ASPI and EU Cyber Direct reports on Cyber Maturity in Asia Pacific region

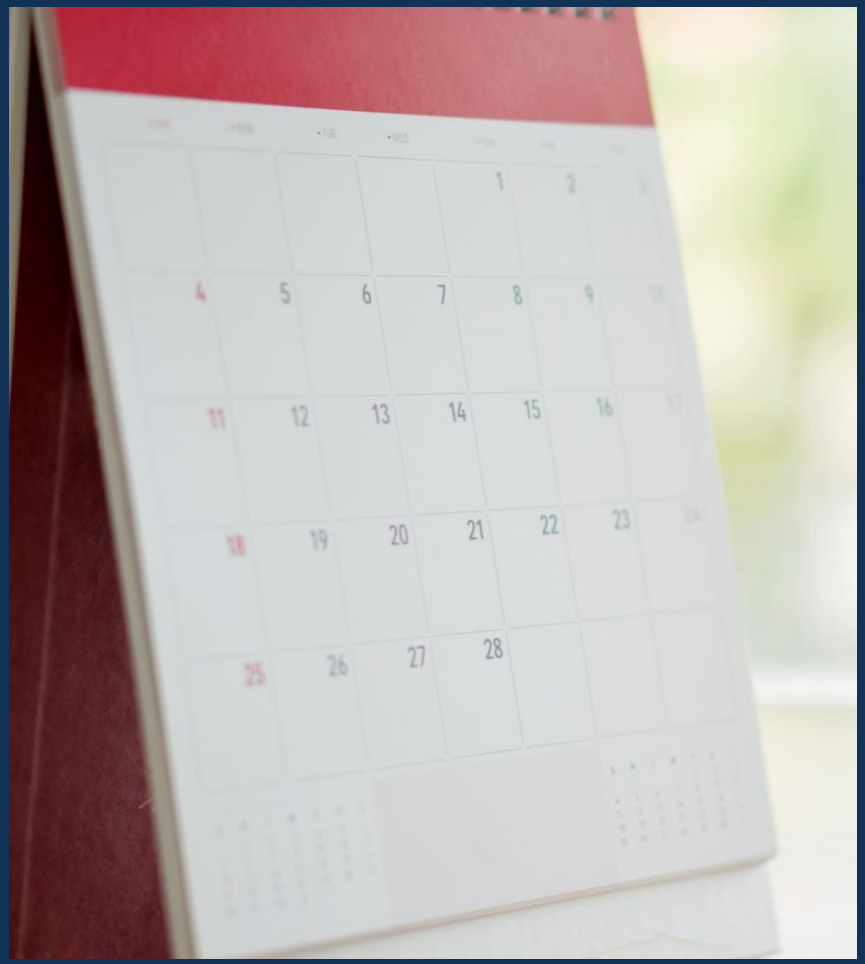
- AND cyber attackers will attack ASEAN through the weakest Member States e.g. through the ASEAN Smart City Network

ASEAN Ministers Cybersecurity Conference (AMCC) agreed …

- 2016: Agreed on value of practical cybersecurity norms of behaviour in ASEAN
- 2017: Supported development of basic, operational and voluntary norms (from UNGGE)
- 2018: Singapore would propose a mechanism to enhance ASEAN cyber coordination
- 2019: Agreed to move forward on a formal cybersecurity coordination mechanism

2020 AMCC announced:

- Singapore + United Nations will draw up a checklist of steps to implement cyber norms
- e.g. legal frameworks and sharing networks
- ASEAN will share its experience and knowledge with the UN



What next for ASEAN?

Capacity Building Programmes

- ASEAN-Singapore Cyber Centre of Excellence
- ASEAN-Japan Cybersecurity Capacity Building Centre in Thailand
- US-Singapore TCTP (Third Country Training Program) for ASEAN
- UN-Singapore Cyber Diplomacy Training

Confidence Building Measures

- Joint training between Member States to improve communication
- Sharing cyber threat information (between CERTS)
- Contact list

Technology and security: Adapting to changing cyber security threats in South East Asia

Benjamin Ang

Senior Fellow, Cyber and Homeland Defence /

Deputy Head, Centre of Excellence for National Security (CENS)

S Rajaratnam School of International Studies (RSIS)

Nanyang Technological University Singapore

Twitter @benjaminang

RSiS