Problem Lab: Cyber Security and Emerging Crimes in Asia Pacific

Overview:

In the span of years, the Internet, mobile devices and other revolutionary technologies have shaped the way we connect, carry out transactions, analyse information and run organizations. Many countries within the Southeast Asia have increasingly embraced ICT to bring a substantial socio-economic development with the region. Such dependency on technologies has given power to the governments to proposer the wellbeing of their citizens. The development has also emerged into new opportunities for cybercriminals to exploit, launch a destabilizing threat, capitalize and disrupt services associated with critical infrastructure of a nation. The risk associated with the misuse of cyber is borderless, cannot be seen and needs to be addressed with diplomacy. Report from various sources suggests that Southeast Asian companies regularly attract the interest of cybercriminals where Advanced Persistent Threats actors are now one of the biggest challenges for the region. Vietnam seems to be one of the top 10 countries where attacks originate, Malaysia providing a lot of ammunition for botnets and Indonesia for malware infections. Singapore is ranked first within the Southeast Asia and Pacific region when it comes to meeting the legal, technical, organisational, capacity building and cooperation for a resilient cyberspace followed by Malaysia, Thailand, Philippines, Brunei Darussalam, Indonesia, Lao PDR, Cambodia, Myanmar and Viet Nam.

Critical Issues

The cyber threat landscape is transforming rapidly particularly in the Southeast Asia region. Many challenges are being faced by member nations in the region especially low level of security investments within the criminal justice system. More and more **Critical infrastructures** are being connected to the Internet exposing it to the new dangers of the new cyber attacks. Hackers are constantly trying to **access and steal data** related to regional political, economic and military issues with the design of sophisticated malware. A resilient legal and technical cyber protection framework is lacking within the region in case of an unforeseen attack. Most of the nations have a very weak regulatory climate and no reporting obligation for cyber incidents.

Piracy is one of the most considerable threats to the regional cybersecurity as it software's lacks security mechanism and is vulnerable to malware that leads to other APT. The evolution of **malware** has contributed significantly in the development of attack landscape. Network based ransomware cryptoworms is on the rise eliminating the human element in the launch of ransomware campaigns. More criminals have shifted to using **anonymous technologies including encryption** web traffic services to evade detection from law enforcement agencies. Rise in the use of **unmonitored and unpatched IoT devices** have made the companies more susceptible to botnet attacks. **Malicious Email scam, business email compromise and phishing** is still prominent in the region and remains one of the vital tools for criminals to disseminate malware along with social engineering techniques. Criminals tend to use **Sandbox evasion techniques** to evade detection. With the rise of IoT devices being used within the government and private infrastructures, **Distributed Denial of Service (DDoS)** attacks has increased its severity and scope. **Romance scam** is prominent method of **fraud** using social media whereby victim is tricked into involving into romantic intentions, gaining affections and finally committing fraud sometimes leading to blackmail.

Cybercriminals have moreover started to use **anonymous technology** such as TOR and shifted their modality of buying and selling illegal pharmaceuticals, drugs, weapons, child online abuse materials, forged documents and passports within the Darknet making it very difficult for law enforcement to trace the activities. Due to a weak regulatory regime on **Cryptocurrencies** are used by malicious actors, transnational organized crime groups and terrorist organizations to conduct pseudonymous financial transactions outside of day-to-day banking channels. More noxious use of cryptocurrencies includes money laundering, buying and selling of illicit goods within the Darknet and fraudulent investments.

Digital literacy and awareness seems to be one of the major issues. Government officials and general public lack awareness among regarding the type of cybercrime and the ways to maintain safe cyber hygiene. **Addressing the human resource** is faced by numerous nations, which requires fostering the new generation of cybersecurity professionals. The law enforcement community has very **limited technical expertise** to detect the crime, awareness, understanding knowledge, technical capability in carrying out online investigations, undercover investigation and **digital forensics** which has been limiting the capacity of the investigators to preserve, collect, analyse, transport the evidence in a secure manner thus making evidence inadmissible in the court of law leading to unsuccessful prosecution. **Lack of proper regulatory framework/policy regarding cybercrime** (online child sexual exploitation, cryptocurrencies, digital evidence) is another challenge. Government policies, legal structures should be explored to address the concerns related to cyber security along with proper mechanism for information sharing across government institutions. **Cross-jurisdictional issues** for sharing of information and request of electronic evidence from other countries are one of the major issues faced by the law enforcement community. Countries within the ASEAN region should collaborate internally and within the international community to advance regional and global security.

Reference Reading Materials:

International Telecommunication Union. 2018. *ITU*. [ONLINE] Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf. [Accessed 18 December 2018].

The Asia Foundation. 2018. *Why ASEAN Needs to Invest More in Cybersecurity*. [ONLINE] Available at: https://asiafoundation.org/2018/05/09/why-asean-needs-to-invest-more-in-cybersecurity/. [Accessed 18 December 2018].

The Diplomat. 2018. *ASEAN Takes a Bold Cybersecurity Step*. [ONLINE] Available at: https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/. [Accessed 18 December 2018].

ATKEARNY. 2018. *Cybersecurity in ASEAN: An Urgent Call to Action*. [ONLINE] Available at: http://www.southeast-asia.atkearney.com/documents/766402/15958324/Cybersecurity+in+ASEAN%E2%80%94An+Urgent+Call+to+Action.pdf/ffd3e1ef-d44a-ac3a-9729-22afbec39364. [Accessed 18 December 2018].