PGA Webinar Promoting Universality and Implementation of the Budapest Convention on Cybercrime and its Protocols in the Asia Pacific Region

December 8th, 2021

Florian Delsert, Programme Associate, International Peace and Security Program, PGA

Asia Pacific – a prime target for cybercrime

- *Second most targeted region in the world.*
- *A 168% increase in the number of cyberattacks between May 2020 and May 2021.*
  - *India: a 400% increase in cybercrime cases against children in 2020*
  - *Taiwan: government website under attack more than 20 million times per month*

- *To prevent cybercrime, it is important that states are equipped with comprehensive cybercrime laws aligned with international standard. While some countries are proposing a new UN standard, the Council of Europe Convention on Cybercrime (Budapest Convention) is by far the most adopted international standard.*
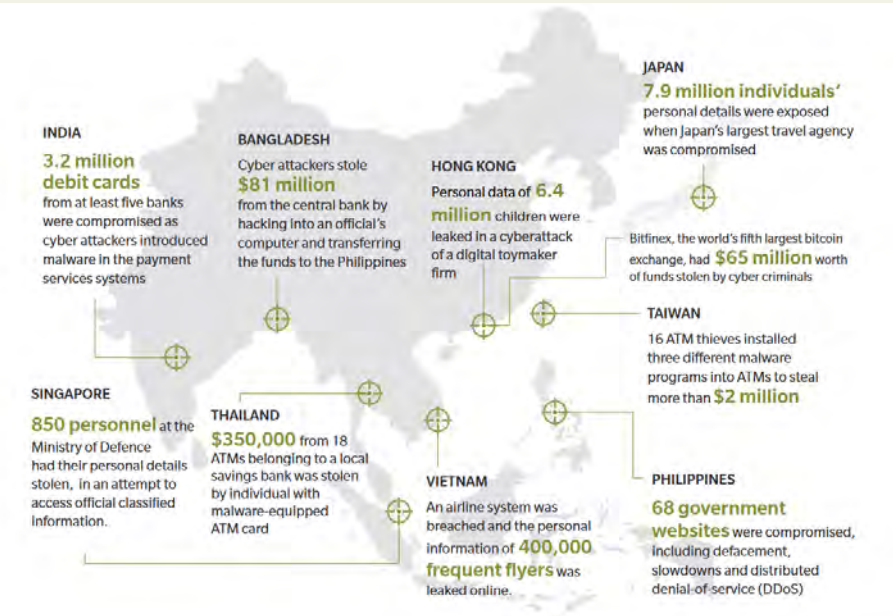
Source: Marsh & McLennan, 2021

Asia Pacific – a prime target for cybercrime

Philippines - 'Billions of requests, thousands of dollars': Inside a massive cyberattack on a PH human rights group

❖ *In July 29, the site belonging to Karapatan, a human rights organization in the Philippines, was targeted by a sophisticated, well-resourced dedicated denial of service (DDoS) attack. Traffic flooded in from botnets spread across the world, from Ukraine to Indonesia — all aimed at a single folder on Karapatan's site, which hosts the group's reports detailing extrajudicial killings in the Southeast Asian country.*

Malaysia - Cisco: 50% of M'sian businesses suffered cyberattacks last year

❖ *ABOUT 50% of small and medium businesses (SMBs) in Malaysia suffered a cyber incident in the last 12 months, according to a report titled Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defence by Cisco Systems Inc. The report revealed that 67% of Malaysian businesses also lost their customer information to the hands of malicious actors as a result of these accidents.*

Indonesia - Indonesia probes police data breach in latest cyber attack

❖ *Using a now suspended Twitter handle, a hacker who said they were from Brazil claimed to have obtained the data of 28,000 officers by infiltrating Indonesia's national police server, according to local media reports*

Vietnam hit by 2,900 cyber attacks in first half of 2021

❖ *Hanoi (VNA) – Vietnam recorded 2,915 cyber attacks in the first six months of 2021, an increase of 898 compared with the same period last year. According to the Vietnam National Cyber Security Centre (NCSC), 718 cyber attacks were reported in June alone. Experts attributed the rise in the incidents to the COVID-19 pandemic which has become more complicated. Criminals take advantage of the society's attention to the pandemic to increase cyber attacks, spread malicious codes and scams to destroy and steal information of users as well as organisations and businesses, they said.*

Asia Pacific – a prime target for cybercrime

Bangladesh - The story of how North Korea hackers stole $81 million from Bangladesh Bank

❖ *The BBC has published an investigative report detailing how in 2016, North Korean hackers planned a $1 billion raid on Bangladesh's national bank and almost succeeded. Here's how it happened.*

Pakistan needs national data security strategy to meet cyber-attack challenges: Arif Alvi

❖ *Pakistani President Arif Alvi has said that new cyber security challenges require a strategy to effectively counter threats and secure national data, the President House said in a statement. Cyber data has become the most valuable commodity worldwide, he added, and stressed that Pakistan direly needed to produce a huge number of graduates in the field of cyber security. The IT infrastructure of Pakistan's National Bank came under cyber-attack on October 29, but the bank did not observe any data breach or financial loss, the country's State Bank said in a statement.*

Sri Lanka - Cyberattack on several government websites;

❖ *COLOMBO (News 1st); A Cyberattack was carried out on several Sri Lankan government websites on Tuesday (18) said the Sri Lanka Computer Emergency Readiness Team. The websites of the Health Ministry, Sri Lankan Embassy in China, Energy Ministry and the Rajarata University came under a cyber attack, it said.*

Examples of cyberattacks affecting parliaments

❖ According to Finnish intelligence services (Supo), a cyberattack took place on the Parliament of Finland, as mentioned in a news article from March 2021.

❖ In September 2020 and again in March 2021, cyberattacks were launched on the Parliament of Norway.

❖ Parliaments are a key source of political information and are therefore frequently targeted by hacking campaigns. Last June, Australia announced that it was the target of a cyberattack campaign.

❖ Also In 2021, a cyberattack also targeted several institutions in Belgium, including the Parliament.

Possible Action Points
for Parliamentarians

• *Raise the matter of Ratification of the Budapest Convention on Cybercrime, with relevant Government Ministries - encourage ratification of these treaties.*

• *Raise this same matter within your respective Parliaments, also in relevant Committees, in order to generate greater/broader awareness and political will in terms of moving forward with treaty ratification, once your Governments transmit the international instrument to your Parliaments*

• *Consider writing an article in a suitable media outlet on this subject matter, also to raise awareness on the urgency and importance of this issue among the wider public*

• *Consider exploring the possibility of conducting a TV or Radio interview for the same reason.*

• *Consider mentioning this Webinar, its subject matter and your participation in any social media outlets that you may use in your day to day political activities such as Facebook or Twitter*

• *Consider outreaching to experts in your own capitals, including individuals responsible for Cybersecurity matters in relevant Government Ministries/Agencies who can also advise further on the situation within your own respective countries*

• *For further advise on effective parliamentary diplomacy/advocacy options, consider staying in contact with PGA and/or outreach also to the experts from the different relevant organizations who have presented at this Webinar today*

Examples of laws

❖ **Indonesia - Electronic Information and Transactions Law (2008)**

❖ Created largely to protect electronic transactions and computers operating in national security contexts.

❖ It contain a series of prohibited acts and are very similarly structured to the Budapest Convention itself.

❖ **Malaysia – Computer Crime Act (2011)**

❖ Many offenses listed in the Budapest Convention are not covered by Malaysia's Computer Crime Act.

❖ **The Philippines - Cybercrime Prevention Act (2012)**

❖ Strongly influenced by the Budapest Convention and covers many of the offenses listed in the Budapest Convention.

We welcome your questions and comments.

THANK YOU

PGA Webinar Promoting Universality and Implementation of the Budapest Convention on Cybercrime and its Protocol/s in the Asia Pacific Region