Taiwan is crucial to the global fight against cybercrime

November 20, 2020

Reposted at RIEAS web site (www.rieas.gr) on 21/11/2020

Taiwan's national antipandemic and cybersecurity teams

Since emerging in late 2019, COVID-19 has evolved into a global pandemic. According to World Health Organization statistics, as of September 30, 2020, there were more than 33.2 million confirmed COVID-19 cases and more than 1 million related deaths worldwide. Having experienced and fought the SARS epidemic in 2003, Taiwan made advance preparations in the face of COVID-19, conducting early onboard screening of inbound travelers, taking stock of antipandemic supply inventories, and forming a national mask production team. The government's swift response and the Taiwanese people's cooperation helped effectively contain the spread of the disease.

The international community has been putting its resources into fighting COVID-19 in the physical world, yet the cyberworld has also been under attack, and faces major challenges. The *Cyber Attack Trends: 2020 Mid-Year Report* published in August 2020 by Check Point Software Technologies Ltd., a well-known IT security company, pointed out that COVID-19 related phishing and malware attacks increased dramatically from below 5,000 per week in February to over 200,000 in late April.

At the same time as COVID-19 has seriously affected people's lives and safety, cybercrime is undermining national security, business operations, and the security of personal information and property, causing significant damage and losses. Taiwan's success in containing COVID-19 has won worldwide acclaim. Faced with cyberthreats and related challenges, Taiwan has actively promoted policies built around the concept that information security is national security. It has bolstered efforts to train IT security specialists and develop the IT security industry and innovative technologies. Taiwan's national teams are ever present when it comes to disease or cybercrime prevention. Cybercrime has increased significantly since the outbreak of the COVID-19 pandemic. (Image: INTERPOL)

Cybercrime knows no borders; Taiwan seeks cross-border cooperation

Nations around the globe are fighting the widely condemned dissemination of child pornography, infringements on intellectual property rights, and the theft of trade secrets. Business email fraud and ransomware have also generated heavy financial losses among enterprises, while cryptocurrencies have become an avenue for criminal transactions and money laundering. Since anyone with online access can connect to any internet-enabled device in the world, crime syndicates are exploiting the anonymity and freedom this provides to conceal their identities and engage in illegal activities.

The Taiwanese police force has a special unit for investigating technology crimes comprising professional cybercrime investigators. It has also established a digital forensics laboratory meeting ISO 17025 requirements. Cybercrime knows no borders, so Taiwan hopes to work with the rest of the world in jointly fighting the problem.

With state-sponsored hacking rampant, intelligence sharing is essential to Taiwan.

In August 2020, the US Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense released the *Malware Analysis Report*, identifying a state-sponsored hacking organization that has recently been using a 2008 malware variant known as TAIDOOR to launch attacks. Numerous Taiwanese government agencies and businesses have previously been subject to such attacks. In a 2012 report on this malware, Trend Micro Inc. observed that all of the victims were from Taiwan, and that the majority were government organizations. Every month, Taiwan's public sector experiences an extremely high number of cyberattacks from beyond Taiwan's borders—between 20 and 40 million instances. Being the priority target of state-sponsored attacks, Taiwan has been able to track their sources and methods and the malware used. By sharing intelligence, Taiwan could help other countries avert potential threats and facilitate the establishment of a joint security mechanism to counter state cyberthreat actors. Additionally, given that hackers often use command-and-control servers to set breakpoints and thus evade investigation, international cooperation is essential for piecing together a comprehensive picture of chains of attack.

In the fight against cybercrime, Taiwan can help.

In July 2016, an unprecedented hacking infringement occurred in Taiwan when NT$83.27 million was illegally withdrawn from First Commercial Bank ATMs. Within a week, the police had recovered NT$77.48 million of the stolen funds and arrested three members of a hacking syndicate—Andrejs Peregudovs, a Latvian; Mihail Colibaba, a Romanian; and Niklae Penkov, a Moldovan—that had until then remained untouched by the law. The incident drew international attention. In September that same year, a similar ATM heist occurred in Romania. A suspect Babii was believed to be involved in both cases, leading investigators to conclude that the thefts had been committed by the same syndicate. At the invitation of the European Union Agency for Law Enforcement Cooperation (Europol), Taiwan's Criminal Investigation Bureau (CIB) visited its office three times to exchange intelligence and evidence. Subsequently, the two entities established Operation TAIEX. Under this plan, the CIB provided key evidence retrieved from suspects' mobile phones to Europol, which sieved through the evidence and identified the suspected mastermind, known as Dennys, who was then based in Spain. This led to his arrest by Europol and the Spanish police, putting an end to the hacking syndicate. To crack down on hacking syndicates, Europol invited Taiwan's CIB to jointly form Operation TAIEX.

The fight against cybercrime requires international cooperation, and Taiwan must work together with other countries. Taiwan can help these other countries, and is willing to share its experiences so as to make cyberspace safer and realize a truly borderless internet. I ask that you support Taiwan's participation in the annual INTERPOL General Assembly as an Observer, as well as INTERPOL meetings, mechanisms, and training activities. By voicing your backing for Taiwan in international forums, you can play a critical role in advancing Taiwan's objective of taking part in international organizations in a pragmatic and meaningful manner. In the fight against cybercrime, Taiwan can help!

Huang Ming-chao

Commissioner

Criminal Investigation Bureau

Ministry of the Interior

Republic of China (Taiwan)