ISSN 2423-2912 (Print), ISSN 2423-2920 (Online)

CENTER FOR INTERNATIONAL RELATIONS & STRATEGIC STUDIES

CIRSS COMMENTARIES

VOL. IV, NO. 3 | FEBRUARY 2017

ADDRESSING CYBERSPACE VULNERABILITY: THE ASEAN AND THE PHILIPPINES

by RJ Marco Lorenzo C. Parcon

As early as the 1990s, the increasing risk and vulnerability of cyberspace was highlighted when a group of hackers known as *L0pht* issued a warning that computers' software and hardware and the connection that link computers together were not safe to use and were vulnerable to hacks. The group also stated that these problems would persist if governments and tech corporations do nothing to minimize and protect citizens from being exploited in cyberspace. More than ten years after L0pht's warning, internet security remains to be a problem.

The advent of the worldwide web has not only eased social connectivity, but has also lowered transaction costs in various ways. The internet has fostered globalization, with 40.7 per 100 people in 2014 having access to the internet worldwide.[1] The continued increase in internet usage, however, also increased the social and political vulnerabilities of people and the state, a serious problem that transcends borders.

The extent of vulnerabilities

Symantec, a cybersecurity company, stated in its 2016 Internet Security Report that it discovered more than 430 million new unique pieces of malware.[2] This is an increase of 36 percent from the 2014 data.[3] Moreover, there were a total of 318 network breaches in 2015 and the average identities exposed per breach increased to 1.3 million from 1.1 million in 2014.[4] More alarmingly, terror and non-state organizations' hacking of government and private websites have also increased. Allegedly, even states deviously utilize cyberspace for their own personal gain.

Crimes committed in cyberspace against women are also increasing worldwide. A report cited by UN Women in its 2015 publication on cyber-violence against women and girls stated that 73 percent of women worldwide have already been exposed or have experienced some form of online violence.[5]

The international community cannot stand idly by while the cyberspace continues to teem with vulnerabilities. The United Nations Office of Drugs and Crime (UNODC) Cybercrime study reminded the international community that *"In the future hyper-connected society, it is hard to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity."*[6]

The ASEAN Response

The Association of Southeast Asian Nations (ASEAN) echoed the same as the ASEAN Blueprint for the Political-Security Community 2025 called for the strengthening of cooperation between member states in combating cybercrimes, and developing and improving relevant laws and capabilities to address cybercrime issues and enhance cybersecurity. An important component of the Blueprint is the creation of a secure and connected information infrastructure to sustain regional economic growth and competitiveness. A key goal of the ASEAN Economic Community (AEC), in particular, is to develop electronic transactions through e-ASEAN to further facilitate ICT trade and services between member states.[7]

Issues related to cybersecurity have also been embedded in various ASEAN institutional meetings. The Senior Officials Meeting on Transnational Crimes (SOMTC), for example, focuses on eight types of transnational crimes, one being the

commission of cybercrimes. At the 7th SOMTC in Vientiane, senior officials adopted a common framework for ASEAN cybercrime capacity-building to further enhance the cybersecurity capabilities of the Member States. Last May 2016, during the ASEAN Defense Ministers Meeting–Plus (ADMM-Plus) in Vientiane, the defense ministers adopted the proposal of then-Philippine Defense Minister Voltaire Gazmin to create a cybersecurity working group that could facilitate the sharing of knowledge and expertise, and would also foster practical cooperation among all parties in addressing cybersecurity issues.

The Philippine response

While recognizing the important role played by the internet and the world wide web, especially with regard to the overall social and economic development plan of the country, the Philippines has also recognized the importance of instituting mechanisms aimed at providing an environment conducive to the development of its people in the field of ICT. The Philippines cannot take cyber-threats lightly as 37 percent of Filipinos use the internet and more than 102 million have mobile cellular subscriptions as of 2013. Thus, in 2012, the Philippines instituted Republic Act 10175, otherwise known as the Cybercrime Prevention Act, with the aim of preventing cybercrimes from being committed, protecting and safeguarding computers and other communication systems and networks from being exploited, abused and illegally accessed.

However, even with RA10175 and other relevant laws in place, the 2016 Symantec Internet Threat Report still ranked the Philippines 6th in the world when it comes to web attack origins. This is even a notch higher than the 2014 ranking that placed the country in 7th place. According to the Philippine National Police Anti-Cybercrime Group (PNP-ACG), the Philippines experienced a total of 1,809 cybercrimes in 2015, around 800 more than the previous year. Just last year, around US$ 81 million were stolen from a Bangladesh bank and were funneled to a Philippine bank by cybercriminals.

"The Philippines must ensure the full implementation of cybercrime laws and continue to mainstream the cybersecurity discussion in its National Security Agenda. It must also include cybersecurity management mechanisms in the discussions. Moreover, effective communication between concerned agencies is imperative."

The Philippines must ensure the full implementation of cybercrime laws and continue to mainstream the cybersecurity discussion in its National Security Agenda. It must also include cybersecurity management mechanisms in the discussions. Moreover, effective communication between concerned agencies is imperative.

But a critical issue is human resources: the need for Information Technology Security (ITS) professionals that can further boost the country's cybersecurity. According to a press report, the Philippines has only a total of 84 Certified Information Systems Security Professionals. This pales in comparison with other countries' certified professionals, with Singapore having more than 1,000, Indonesia with 107, Thailand with 189, and Malaysia with 275.[8] The government, in partnership with the private sector, must advocate the development and certification of the IT human resource in the country. In this regard, opportunities must be given to both qualified men and women. Women's participation in the field of ICT and ITS in the Philippines and around the world must also be expanded and enhanced. This is due to the fact that although there is a huge demand for ITS professionals, women's representation is disturbingly low worldwide.

A more secure cyberspace benefits everyone

When technological discoveries are made on a daily basis, threats also abound. Where there is a chance to gain confidential information, money and other items of interest through the internet, there is also a huge chance that hackers and other cyber-threats will try to undermine cybersecurity and gain confidential information. In 2015, Kaspersky Lab alone blocked almost two billion attempts to steal money using online banking.[9]

A more secure cyberspace is beneficial not just for the government, but for the whole country. A more secure cyberspace will also mean a better economy; investors will not hesitate to pour investments into the country because the IT infrastructure is more secure. An unsecure cyberspace will leave the people to be more vulnerable than before as more malwares are being developed every day. ⚜

Endnotes

[1] "Internet Users (per 100 peple) ." *World Bank.* 2016. Accessed November 15, 2016. http://data.worldbank.org/indicator/IT.NET.USER.P2

[2] "2016 Internet Security Report" Symantec Corporation. April 2016. Accessed November 16, 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[3] Ibid.

[4] Ibid.

[5] "Cyber Violence Against Women and Girls: A World-wide Wake-Up Call." UNWomen. 2015. http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf

[6] "The use of Internet for terrorist purposes." UNODC (September 2012). Accessed November 17 2016. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[7] "e-ASEAN FRAMEWORK AGREEMENT" *November 24, 2000. Accessed, January 2017. http://asean.org/?static_post=e-asean-framework-agreement*

[8] Ted P. Torres. "Lack of IT security professionals makes Philippines prone to cyber crime." April 11 2016. Accessed November 17 2016. http://beta.philstar.com/business/banking/2016/04/11/1571843/lack-it-security-professionals-makes-philippines-prone-cyber-crime

[9] "Kaspersky Lab Security Bulletin for 2015 shows mobile banking threats among the leading malicious financial programs for the first time" Kasperky Lab. December 15, 2015. Accessed November 18, 2016. http://usa.kaspersky.com/about-us/press-center/press-releases/2015/kaspersky-lab-security-bulletin-2015-shows-mobile-banking-threa

RJ Marco Lorenzo C. Parcon is a Foreign Affairs Research Specialist with the Center for International Relations and Strategic Studies of the Foreign Service Institute.

Mr. Parcon can be reached at rjcparcon@fsi.gov.ph

CIRSS Commentaries is a regular short publication of the Center for International Relations and Strategic Studies (CIRSS) of the Foreign Service Institute (FSI) focusing on the latest regional and global developments and issues.

The Center for International Relations and Strategic Studies (CIRSS) of the Foreign Service Institute (FSI) undertakes studies in support of the formulation, review, and dissemination of Philippine foreign policy. It also organizes conferences, roundtable discussions (RTD), lectures, and forums as channels for interaction, cooperation, and integration of the efforts of local and foreign experts from government, private and academic sectors on foreign policy issues and their domestic implications.