NDCP POLICY BRIEF

A PUBLICATION SERIES ON SECURITY ISSUES AND CONCERNS BY THE NATIONAL DEFENSE COLLEGE OF THE PHILIPPINES

12 July 2013
No. 11

Trends and Threats in Cyberspace: Are We Secure? *

Introduction

The rapid growth and advancement of Information and Communications Technology (ICT) has ushered in the boom of information age and the social media in the 21st century. No doubt, the ICT has significantly transformed the pace of living and way of thinking of wired people in the postmodern global village.

Southeast Asia is considered as one of the promising techno hubs for students, professionals, and electronic-oriented consumers in the world. With a growing economy and over half a billion population of techno savvy people, this region has tremendous participation and contribution to the social media dynamics.

However, there are also dangers lurking behind the phenomenal success of social networks in the region's cybersecurity infrastructure. As the trends in ICT continue to invade and pervade human life, threats to cybersecurity likewise become invasive and pervasive. Taking advantage of these realities, cybercriminals and cyberterrorists have learned to use sophisticated technology and exploit this as a new weapon of destruction. This is what makes cybercrime and cyberterrorism as human-induced disasters in the crisis management discourse.

That hackers and terrorists would employ ICT as efficient and effective media of cyber crime is a policy issue that must not be undermined. While ICT is being used as vital element that links and educates people, it can also be employed as a weapon to disrupt and destroy critical cyber infrastructure. The devastation of the cyberspace can cause damages to privacies and properties, as well as endanger human and state security.

While ICT is being used as a vital element that links and educates people, it can also be employed as a weapon to disrupt and destroy critical cyber infrastructure.

Given the foregoing scenario, this policy paper delves on emerging concerns on cybersecurity in the region. What are the trends and threats in the cyberspace? Are there laws to secure the rights of cyber-users? What are the issues in social media governance that must be addressed?

Trends in Cyber Technology

Social Media is defined as a new kind of online media that has the characteristic elements of [1] participation; [2] multiple conversations; [3] openness to feedback; [4] formation of communities; and, [5] connectedness.[1]

In a 2008 study by McCann Universal, Filipinos ranked first in social networking, sharing photos, and viewing videos. They were second to South Korea in reading blogs, second to Brazil in sharing videos, fourth in writing blogs and downloading podcasts, and sixth in using rich site summary or RSS feeds. Email, instant messaging, and web search were reported to be the most common online activities of Filipino internet users.[2] In an investment analysis of Wall Street in 2011, the Philippines was proclaimed as the "Social Networking Capital of the World."

In another study, Nielsen in 2012 reported that social media received high trust rating among consumers in Southeast Asia, particularly in Vietnam, Thailand, Philippines, and Indonesia. Although

* This policy brief was prepared by Chester B Cabalza, with Ananda Devi Domingo-Almase, DPA as Editor.

Produced by the Research and Special Studies Division, National Defense College of the Philippines
For inquiries, please call Tel/Fax. (63-2) 912-9125 * Trunkline: 911-6001 local 4591/4558 * www.ndcp.edu.ph

television remains the most popular form of media, online use has grown rapidly in reach and influence in the last decade.[3]

According to cyber business practitioners, the benefits of social media in marketing include the following: [1] promotion of business and products; [2] improvement of web traffic; [3] opportunity to build new partnerships; and, [4] generation of qualified leads.

In the sphere of social media, Twitter--a popular microblogging service launched in 2006--has topped all other social networking services in terms of user base in the world today. In a 2012 report by Semiocast, a social media monitor, Indonesia and the Philippines ranked 5th and 10th in "Twiterverse," respectively. The two countries were said to be hooked to Twitter's ever growing 517 million users worldwide.[4] Initially, it was Facebook that had held the most popular spot among the social networking sites around the world.

With the expanding influence of the worldwide social media, governments have learned to harness the power of these networking sites in engaging its citizens and encouraging them to participate in policy-making. Through social media, writers with sense and sensibilities on policy issues managed to establish wide readership and following. They set the agenda for social discourse within the political blogosphere to influence policy actors and decision-makers in governance.

On the lighter side, common people become popular through their blogs and other web posts which would not be possible if there were only traditional media of the past. Driven by group identity, blogs draw individuals and facilitate the creation of networks of like-minded individuals.[5]

Threats in the Cyberspace

Cyberspace has become a platform of the best and worst things that people can come up with when they are online. While it can be considered as a hotbed for game-changing ideas and artistic expressions, cyberspace has also turned into a breeding ground for trolls, felons, and cyberthugs.

Criminals look for easy prey. In the dotcom era, cyberterrorists are at the threshold of using the cyberspace as a medium of pernicious crimes, such as causing massive financial and economic disruptions. Cyberterrorism is any premeditated, usually politically-motivated attack, against information, computer systems, computer programs, and data of non-combatant targets by clandestine agents of subnational groups.[6]

In the year 2000, for instance, the "lovebug" virus made by a Filipino student caused worldwide damage, amounting to approximately USD$12 billion, according to the US Federal Bureau of Investigation (FBI). Hence, this incident only showed that cyber threat to financial systems has tremendous consequences on national economy and global operations.

In 2005, the National Bureau of Investigation (NBI) in the Philippines reported handling 30 cybercrime cases in various forms. These included computer fraud, internet pornography, hacking, and violation of the E-commerce law, among others.[7]

The audio-visual, print, and the internet have emerged as the principal media to disseminate subversive ideologies in Southeast Asia. According to intelligence reports, international terrorists use the internet and state-of-the-art electronic gadgets to gather and mine intelligence targets, spread propaganda, and expand recruitment.

On a global scale, The Economist in London in 2010 reported that about nine-tenths of the 140 billion e-mails sent daily were spam, 16% of which contained money-making scams. There were also "phising" attacks that duped recipients into giving out passwords or bank details. To note, the amount of personal information now available online makes it easy to attack a computer by "spear-phising" using personalized e-mails.[8]

Cyberterrorists could apply information hiding by means of stenography through which they take one piece of information and hide it in another picture or document. This strategy could cripple cyber infrastructure, including key government sites and services, in split seconds.[9]

Computer systems could be hacked by criminals to gather information, alter data, install malicious codes and sabotage operations. Malicious codes can be installed in the forms of Trojans, worms, and viruses. Deadly Distributed Denial of Service (DdoS) attacks, which employ "zombie" machines under the control of a master server, have the ability to take down entire networks.

Government websites, especially those with weak security mechanisms, are vulnerable to espionage from cyberterrorists. Violations occur when an unauthorized user illegally accesses network computers and confidential links of public institutions, especially of defense establishments. It must be noted that at the height of conflicting territorial claims between the Philippines and China over the Scarborough Shoal in the West Philippine Sea in 2012, hactivists were reportedly engaged in a raging battle online. This rendered Philippine government sites inaccessible for some time due to alleged hacking in the cyberspace.

Vital military, commercial, and public institutions are vulnerable to cyberterrorism. They can be targeted to disrupt the free world's defense and communications systems. Computer bugs can bring down military email systems, destroy oil refineries, derail metro trains, scramble financial data, and damage electrical grid, among others.

With just a keystroke, cyberterrorists can send fatal blow from an armchair, thousands of miles away. From a mere technical nuisance, cyber disruption can become a national and regional security problem.

Responses and Challenges to Cyberthreats

Policy-makers and security practitioners in the region must be kept abreast of non-traditional cybersecurity threats in order to reduce and manage their risks to state and human security. Proper handling of information through the use of various cyber investigative techniques helps eliminate and reduce cyber threats. Institutionalizing cybersecurity programs by countries in the region will develop and improve the capacity and competency of security administrators in managing transnational cyber threats.

In the Fifth Network of the Association of Southeast Asian Nations (ASEAN) Defence and Security Institutes in 2012,[10] member states agreed to take collaborative actions to address borderless threats to cybersecurity. Some of the issues discussed in the meeting pertained to problems of jurisdiction, and lack of integrated laws on cybersecurity that will prosecute cybercriminals in Southeast Asia.

In the light of the foregoing policy concerns, the Network of the ASEAN Defence and Security Institutes (NADI) needs to build security cooperation through informal dialogue, information-sharing, and competency training, among others. For instance, re-elected American President Barack Obama and newly elected Chinese President Xi Jinping agreed in April 2013 to set up a cybersecurity technical working group after trading accusations over cyber attacks and theft. This course of action, along with enactments of appropriate laws, expedites the prosecution and extradition of transnational cybercriminals.

On the whole, the NADI must work towards the following policy objectives: [1] network building for collaborative collection and intelligence analysis of cybersecurity related information; [2] conduct of intensive research on the security of cyber structures in Southeast Asia; [3] organization of fora and informal dialogue among stakeholders (e.g. enforcers, prosecutors, and cyber users); and, [4] cooperation and international treatise between governments and cyber industries in the region. Notably, the latter objective is necessary as cybercrime and cyberterrorism are multi-jurisdictional and cut across border.[11]

Several issues and concerns on social media governance must also be addressed by policy analysts and security actors. Some of the pressing inquiries which need to be looked into by the policy community include the following: [1] What sort of risks do organizations face in terms of potential data loss, unregulated communication of confidential information, and work time? [2] How should government use the social media in its campaign for transparency and public accountability, and at the same time guard against abuse of this media for cyber security? [3] How can government formulate and adopt a cybersecurity policy that shall define roles and responsibilities, research and development, as well as monitoring and regulation for public interest?[12]

Notably, one critical policy issue in the cybersecurity landscape in the Philippines has been the enactment of Philippine Republic Act (RA) No. 10175, otherwise known as, *The Cybercrime Prevention Act of 2013*. This covers offenses such as hacking, identity theft, cyber-squatting, cyber-bullying, illegal access, child pornography, defamation, and other internet-related crimes. The Act seeks to establish the legal framework for the investigation, apprehension, and prosecution of cyber criminals. But barely a month after the implementation of RA 10175, the Supreme Court issued a temporary restraining order initially for 120

Countries with different policies and positions must take collaborative measures of ensuring a safe and secure cyberspace through security cooperation in the region.

days, and further extended suspension for at least four months. Dubbed as a dangerous act under a regime of "digital martial law," RA 10175 was perceived by critics to contain flawed provisions that threaten fundamental rights and freedom.

Considering the imminent threats of cybercrime, security actors must respond to challenges in the cyberspace carefully and seriously. As one of the complex non-traditional security threats in Southeast Asia today, cybercrime demands that countries must undertake strategic plans and institutional arrangements to ensure comprehensive cybersecurity in the region.

Conclusion

Cyber-espionage has been the biggest ICT disaster, since the historic and brazen theft of nuclear weapons technology in the United States in 1999. Because of the occurrence of this non-traditional threat, the cyber space has become a new battlefront for defense and security in a borderless world.

Our global way of life depends on the secure and safe operations of critical systems that depend on cyberspace. It is for this reason that the government, private sector, and other concerned groups must develop the competency and technical expertise in cybersecurity.

Cyber attacks can make or break the state of normalcy in a nation and the interconnected world. Countries with different policies and positions must look beyond the traditional means of countering cyber attacks by engaging in security cooperation. This will make the region resilient to cyber threats and attacks, and ensure the promotion of cybersecurity as a common interest of all nations.

Endnotes

[1] Mayfield, Antony (2008). *What is Social Media?*. United Kingdom: icrossing. Available from: <http://www.icrossing.com/sites/default/files/what-is-social-media-uk.pdf>. [Accessed 15 April 2013].
[2] Cruz, Tonyo (2010). The Philippines' Social Media and Mobile Statistics. April 12, 2010. *politics and tech, issues and gadgets, the personal and the political, and more.* [online]. [Accessed 29 April 2013]. Available from: <http://tonyocruz.com/?p=2866>.
[3] Nielsen Holdings (2012, N/A). *The Asia Media Landscape is Turning Digital*. (N/A). $publisher New York City Available from: <http://www.nielsen.com/content/dam/corporate/au/en/reports/2012/changing-asian-media-landscape-feb2012.pdf>. Accessed: 18 April 2013.
[4] Montecillo, Paolo (2012). Philippines has 9.5M Twitter Users, Ranks 10th. *Philippine Daily Inquirer*, August 9, 2012.
[5] Pole, Antoinette (2010). *Blogging the Political*.ed. New York: Routledge.
[6] Definition presented by the Federal Bureau of Investigation (FBI), available at http://www.crime-research.org/articles/putting_cyberterrorism.
[7] The *Cybercrime Prevention Act of 2012* is now a newly enacted statute after the bicameral conference committee has approved the consolidated versions of the measure from the Senate and the House of Representatives using the senate version of the bill as its working draft (*Cybercrime Act Consolidated Versions Okayed,* Manila Bulletin, dated June 8, 2012, http://www.mb.com.ph/articles/361474/cybercrime-act-consolidated-versions-okayed).
[8] N.A. (2010). Cyberwar: War in Fifth Domain. *The Economist* [online]. Available from: <http://www.economist.com/node/16478792.>. [Accessed 23 April 2013].
[9] In reference to the examples cited from the training manual entitled, *Investigating Cyberterrorism*, US Department of State on Anti-terrorism Program.
[10] N.A. (2012). Chairman's Report of the 5th Meeting of Track II Network of ASEAN Defence and Security Institutions (NADI). *In: Enhancing Institutionalized Security Cooperation in ASEAN for a Harmonized and Secure Community*, 2-3 April 2012, Siem Reap, Cambodia.
[11] Cabalza, Chester. (2012). *New Frontiers in Cybersecurity: Its Adverse Impact in ASEAN Region,* Digest, Strategic and Special Studies, 3rd Quarter, Pressing Security Concerns, Office of Strategic and Special Studies (OSS), Armed Forces of the Philippines (AFP).
[12] Malacaman, J., (2010). *Social Media in Information Security: Lessons and Issues*, powerpoint template numbers 7-10, National Defense College of the Philippines, Quezon City.

Produced by the Research and Special Studies Division, National Defense College of the Philippines
For inquiries, please call Tel/Fax. (63-2) 912-9125 * Trunkline: 911-6001 local 4591/4558 * www.ndcp.edu.ph