Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 4224- 4231
Research Article

Cybercrime In The Philippines: A Case Study Of National Security

Jia Li
International College, Krirk University,
Thanon Ram Intra, Khwaeng Anusawari, Khet Bang Khen,
Krung Thep, Maha Nakhon10220, Thailand
Email:1146043158@qq.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: Transformations in technology that have impacted the global economy have ushered in an information and communication technology-led revolution. This global shift has paved the way for what many has described as "a borderless world" that has led to new ways of doing things in both the private and public sector of a nation in today's modern times.

The concept of E-service (short for electronic service) which is the hallmark of this technology represents an application that utilizes the use of information and communication mediated technologies for the facilitation of the delivery of a varied scope of services or aptly called "electronic services". In the public sector, E-service enable public agencies who are the service providers achieve enhanced administration in delivering services for citizens or the public. This allows the flow and process of information for all stakeholders to be processed efficiently. In the private sector, applications of e-commerce are continually affecting trends and prospects for business over the internet. E-commerce in the country encourages shifts from traditional modes of doing business to electronic alternatives, thereby enhancing the processing of business transactions. Its benefits are limitless, from expanded geographic reach, easy access to information, marketing and advertising visibility and cost reduction which all bottom lines to increase revenues.

Security is the challenge that faces the implementation of e-services in a country in the country where such implementation is crucial to the delivery of basic services to the populace. Without a guarantee of privacy and security for information circulating in the internet, e-services will fail. The menace of the proliferation of cyber crime activities hampers the reach of e-government and compromises the achievement of its national goals in creating enhanced socio-economic environment for its citizens. In essence, it is tantamount to becoming a grave threat to national security.

This paper sought to present how cyber crime has impacted areas of both the public and private sector here in the Philippines that threaten national security of its citizens. It presented among others, a profile of cyber criminals including their tools and motives, the modes and manner on how different cyber crimes are being committed and the implications to specific stakeholders most vulnerable.

In view of the results, recognizing the national economic implications of cyber threats, this paper concludes that the implications of cybercrime in the Philippines are of an impending grave nature which threatens that national security of its people, its private sector and its government.

Keywords: cybercrime, national security

Introduction

Cybercrime is any crime committed with the use of a computer system, or instances in which a computer system is targeted for criminal purposes. Cyber attacks affect millions of internet users. While this damage is relatively minimal in proportion to the traffic volume of the Internet, cyber attacks are a wake-up call as to the extent of cyber crime, and the degree to which people are all vulnerable.[1]

Cyber crime is generally defined as any type of illegal activity that makes use of the internet, a private or public network, or an in-house computer system.[2] There is a grim reality that these kinds of crimes has taken an increasinly international presence as organized cyber attacks has become a menage not only to individuals and businesses but to governments as well around the world. Recent trends of cyber activities of malicious individuals

[1] Romero,A.2011,Cybercrimes pose serious threat to Phil,https://www.philstar.com/headlines/2011/07/25/709381/cybercrimes-pose-serious-threat-phl-psa,last accessed:May 3,2021

[2]Jerome,S.&Samoy,L. (2017),Industrial Security Management Reviewer,https://kupdf.net/download/industrial-security-management-reviewer_598b0205dc0d60215a300d18_pdf,last accessed:May 2,2021

set governments to view such a posing as a grave threat to their individual thriving global economies and poses a threat to the national security of any country.

Information from organizations like NATO, the FBI, the Center for Education and Research in Information Assurance and Security (CERIAS), the Serious Organized Crime Agency (SOCA), the International Institute for Counter-Terrorism, and the London School of Economics in a 40-page report has further indicated that the Internet is becoming a weapon for political, military, and economic espionage, even between countries. [3] The report has indicated that such activities are getting more sophisticated. It suggests that cyber criminals have no fear of law enforcement because there is no deterrence in the form of organization with mandated international legislation between countries as to how to prosecute these kinds of crimes and the criminals behind them(Sheman, 2005) .

The Philippine Situation

According to the Philippines National Police (PNP), cyber crimes increased sharply in 2010 and it is rising every year in this country. Criminal Investigation and Detection Group (CIDG) revealed that the Philippine police reported 4,673 cyber crimes last year while there were only 527 cyber criminal cases reported in 2006, a three-fold increase in a year. As per the police, a total of 2,624 cases were reported between 2005 and 2010. In 2004, only 37 cases were reported and they kept surging every year with 56 cases in 2004 and 161 cases in 2005. In the span of two years, from 2004 to 2006, the PNP investigated 195 computer crimes, in which cases on various subjects like credit and debt card fraud, Internet pornography, violation of copyright laws, and other computer related crimes were noticed. [4]

Symantec, a software firm already released a report that stated more and more Filipinos are falling as victims to online criminal activities and other malicious attacks every year. Filipinos have fallen to a variety of attacks, which include among others, malware invasion, online or phishing scams, and "sexual predation. [5]For individual personal users, social networking services, particularly Facebook, which so far has at least16 million users in the Philippines is an area most vulnerable to these crimes.

Cybercriminals capitalize on unethical online practices by most Filipino users and by using social engineering to make it possible for internet users to believe they are in legitimate website. Such sites are embeded with malicious applications into the would-be victim's PC, giving cybercriminals free access to personal information.

In the business, as well as in the public sector, cyber crime activities compromises the benefits of stakeholders who patronize government's efforts to thrust the use of e-commerce and e-services in the country. Inappropriate use of personal information is detremental for both these sectors. E-services allow for the private and public sector a whole range of services pertinent to inter-agency processes needed by the general public. This is part of the national government's effort to shift to e-governance as a way of efficiently bringing its services to the public, hence if such is compromised, it then becomes a grave national concern.

Factors Affecting the Proliferation of Cybercrime in the Philippines

There are around seven other pending House bills addressing the problem of cybercrime in the country but up to now there is no other law on Internet activity, aside from the E-Commerce Law, has been enacted in the Philippines. Other factors that worsen the situation: measly budget earmarked for cybercrime prevention, non-

[3] Cheng ,J. (2007),Cybercrime poses threat to National Security,https://arstechnica.com/information-technology/2007/11/mcafee-cybercrime-all-grown-up-spreading-its-wings/l,ast accessed:May 2,2021

[4]*SPAMfighter.(2008).Computer Crime becoming a Headache for Philippines Police, http://www.spamfighter.com/News-9943-Computer-Crime-becoming-a-Headache-for-Philippines-Police.htm.last accessed: May 2,2021*

[5] Brenner,Suan W. (2009).Threat Morphing in Cyber Space. In Cyberthreats: Emerging Fault Lines of the Nation-State .New York: Oxford University Press .https://www.e-ir.info/2010/03/08/threat-morphing-in-cyberspace-by-susan-w-brenner/,last accessed: May 2,2021

existence of an umbrella agency mandated to address the problem, lack of cooperation and coordination between government and private sector, ill-trained law enforcers, and lack of public awareness. [6]

The situation has become a "silent epidemic," as termed by Effendy Ibrahim, Internet Safety Advocate and Consumer Business Division Head of Symantec Asia who lamented that the Filipinos lack genuine concern about escalating cybercrime issues in this country.

Theoretical Framework

Some researchers have tried to explain cyber crimes with traditional theories, such as Social Learning Theory which posits that people learn from one another, via observation, imitation, and modeling. The theory has often been called a bridge between behaviorist and cognitive learning theories because it encompasses attention, memory, and motivation and Routine Activities Theory which states that users who routinely use the medium have a propensity to use it inappropriately.[7] However, these theoretical explanations were found to be inadequate as an overall explanation for the phenomenon of cyber crimes, because cyber crimes are different from crimes of physical space.

A Space Transition Theory of Cyber Crimes (Jaishankar ,2008) was postulated to serve as explanation of criminal behaviour in the cyberspace. This theory explores the nature of the behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical space and cyberspace. Space Transition involves the movement of persons from one space to another (e.g., from physical space to cyber space and vice versa). Space Transition Theory argues that, people behave differently when they move from one space to another and having done so, acquires certain behaviors they may or may not act out in the physical space giving them a sense of heightened capability to act out their salient impulses which in some cases are deviant. This is the framework espoused by this paper.

Objective of the Study

The paper postulates that the scope of cybercrime activities int the Philippines has enabled it to become a national threat to the sovereign security of Filipinos and the country as a whole. It's objectives include the following:

- To identify the profile description and the motives of cyber criminals.
- To present the different forms of cybercrime activities documented as being committed in the country.
- To enumerate the effect of these crimes on users in both in the individual/private and public sectors.
- To analyze the impact of cybercrime on national security in the Philippines.

Methodology

The paper is qualitative in nature and made use of data gathered from various resources available in the internet documents, journal articles and books related to the topic. A subsequent documentary analysis ensued to present the discussions relevant to the postulate of the paper.

Data Findings and Discussion

The following are summary data findings that the paper have gathered in relation to its objectives.

The Profile of the Cyber Criminal

Cybercriminals are of various types and they come from all walks of life. But there are certain generic facets of the human personality that differ between criminals and non-criminals. External motivations are not sufficient to determine who is a criminal or who is not. There is a need for a deep understanding of networks and technology on alongside criminal mindset.

Table 1. Profile Description of Cyber Criminals

Term Used	Profile Description/Abilities	Motives
Novice	➢ Limited computer and programming skills.	➢ Starts with perceived harmless intention. ➢ Looking for media attention.

[6] Philtechnology, We will maintain Sun's Unli Service,http://philtechnology.blogspot.com/2011_03_01_archive.html, last accessed:May 2,2021

[7] Ursolino,Elmer,(2012),Social Learning Theory,https://elmerursolino.wordpress.com/category/uncategorized/,alst accessed:May 2,2021

	➢ Rely on toolkits to conduct their attacks. ➢ Can cause extensive damage to systems since they don't understand how the attack works.	
Cyber-punks	➢ Capable of writing their own software. ➢ Have an understanding of the systems they are attacking. ➢ Many are engaged in credit card number theft and telecommunications fraud.	➢ To show capability to underscore attacks or engage in petty theft and telecommunication fraud. ➢ Have the tendency to brag about their exploits.
Internals	a)Disgruntled employees or ex-employees ➢ May be involved in technology-related jobs. ➢ Aided by privileges they have or had been assigned as part of their job function. ➢ Pose largest security problem. b) Petty thieves ➢ Include employees, contractors, consultants . ➢ Computer literate. ➢ Opportunists taking advantage of poor internal security.	➢ Disgruntled employees want to disrupt functional systems operations as a way to get even with their former employers. ➢ Petty thieves are motivated by greed or necessity to pay off other habits such as drugs and gambling debts.
Coders	➢ Act as mentors to the newbies. Write the scripts and automated tools that others use. ➢ Dangerous — have hidden agendas, use Trojan horses.	➢ Motivated by a sense of power and prestige.
Old Guard Hackers	➢ Has a strong tendency for criminal intent. ➢ Has an alarming disrespect for personal property or privacy.	➢ Motivated by the satisfaction of claiming personal intellectual capability in doing their endeavors.
Professional Criminals	➢ Specialize in corporate espionage. ➢ Guns for hire. ➢ Have access to state of the art equipment.	➢ Highly motivated, highly trained and usually contracted to accomplish their crimes.
Information Warriors/Cyber Terrorists	➢ Well funded individuals. ➢ Mix political rhetoric with criminal activity. ➢ Political activists. ➢ Engage in “hacktivism”.	➢ Motivated by political ideologies to engage in anarchical activities.

Table 1 presents the different kinds of cyber criminal categories, their profile descriptions, abilities and tools of the trade and their internal motives that have been speculated to engaged in cyber criminal activities.

The Types of Cybercrimes Documented Here in the Philippines

The growing use of computers, cyber crime is that has become more predominant in today's world have allowed the occurrence of arious types of Cyber crimes that can be encountered over the net. These computer crimes are known by lots of different names, including cybercrime, e-crime or electronic crime. All of these are crimes are where computers or networks are used or attacked. Many traditional crimes such as theft, blackmail, forgery,

embezzlement and fraud today are all conducted on the internet and encompassed in the many categories around cybercrimes.

Table 2. Type of Cybercrimes According to Description and Tools Used

Type of Cybercrime	Description	Tools Used
Assault by Threat	Threatening a person with fear for their lives or the lives of their families.	The use of computer networks such as email, videos or phones.
Child Pornography	Sexual exploitation of children.	The use of computer networks to create, distribute or access material related to the sexual exploitation of children.
Cyber Contraband	The transfer of illegally banned items such as encryption technology.	The Internet.
Cyber Theft	Theft and pilferage activities related to breaking and entering computer systems through illegal access.	The use of the computer networks and the Internet to: >Advertise and solicit prostitution. >Sell illegal and prescription drugs inappropriately. >Commit computer based fraud such as scams, unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy.
Cyber Trespass	The unauthorized entry to the network of any individual or entity with the objective to alter , disturb, misuse, or damage the data or system.	The use of a computer's or network's resources for hacking with the purpose of entering an electronic network to: >Accessing private files. > Reading email, files, or noting which programs are installed on a third-party's computer system without permission just for fun.
Cyber Vandalism	Damaging or destroying data rather than stealing or misusing them thus, depriving the computer/network owners and authorized users (website visitors, employees) of the network itself and the data or information contained on the network or causing the network to stop its operations.	Using the network to: > Alter, destroy or delete data or files. >Deliberately entering malicious code (viruses, Trojans) into a computer network to monitor, follow, disrupt, stop, or perform any other action without the permission of the owner of the network. >Prevents legitimate website visitors from accessing the network resources with the proper permissions.
Cyber Stalking	The act of expressing or implying physical threats that creates fear through computer or network activities.	The use of computer technology such as email, phones, text messages, webcams, websites or videos.
Cyber Terrorism	The premeditated, usually politically-motivated violence committed against civilians through the use of computer technology.	The use of, or with the help of, computer technology devices and/or network and internet sites.

Table 2 presents the different categories of cyber crimes being committed in the Philippines. They reveal the description of computer crimes which include activities associated with them such as electronic frauds, misuse of devices, identity theft and data as well as system interference and the tools used for their individual purposes.

Impact of Cybercrimes to Specific Stakeholders.

The following table presents how different stakeholders (users) are affected by different kinds of cybercrime and its impact to these specfic users.

Table 3 Cybercrime and Specific Stakeholders

Stakeholder	Type of Crime	Impact of Cyber Crime activities
The Public In General	>Cyber bullying through internet and cell phones.	>Serious consequences of cyber-bullying victimization includes victims have lower self-esteem, increased suicidal ideation, and

		a variety of emotional responses, retaliating, being scared, frustrated, angry, and depressed.
	>Synthetic Identity	>Synthetic identity theft primarily harms the creditors who unwittingly grant the fraudsters credit. Credit ratings of victims are affective due to confused identities.
	>Cyber fraud with intent to harm.	> Social networking sites are one of the most famous spreader of posers in the online community, giving the users freedom to place any information they want without any verification that the account is being used by the real person.
	>Cyber identity theft.	>Internet source to various identity theft problems. Identity of those people who carelessy put personal information on their profiles can easily be stolen just by simple browsing.
	>Phishing and its related activities	>Criminal hacks the sensitive personal information of a user like user names, credit card details, and passwords by pretending as a friendly and trustworthy person via e-mail.
	>Cyber fraud leading to inappropriate relations.	>Romantic involvement in cyber relations leads to dire consequences such as stalking, robbery, sexual molestation, unwanted pregnancies and even death.
	>Cyber fraud on consumer items.	>Web-based products and online services mislead the public to buy into bogus investments in products and services.
The Private Sector (companies)	>Cyber theft of financial information or funds.	>Loss of revenue caused theft of sensitive financial information, using it to withdraw funds from an organization.
	>Compromised e-commerce site.	>Valuable income is lost when it is inoperable as consumers are unable to use the site.
	>Security breach to customer information/financial records.	>Security breach assosicated with cyber crime allows customer records to be compromised and a company's reputation takes a major hit. Customers lose confidence in a business company when credit cards or other financial data become intercepted by hackers or other infiltrators.
	>Performance wastage due to security breaches.	>Negative effect on employees' productivity since due to security measures, employees must enter more passwords and perform other time-consuming acts in order to do their jobs. Every second wasted performing these tasks is a second not spent working in a productive manner.
The Public Sector	>Phishing, cyber vandalism brought about by hacking on e-service applications of government agencies.	> The illegal acquisition of confidential data, hacking, identity theft, spamming, website defacement, copyright violation, of key government institutions in the health, banking, education and economic sectors compromises government’s efforts to bring services to the general public.
		>The same can be said for transportation, telecommunication

		and even the police and military sectors. Cybercrimes assosciated with the operations of these sectors compromises the peace, safety and security of the Filipino people in general.

Table 3 presents how cybercrimes affect individual stakeholders in the Philippines. It shows how cyber crime has become an increasing problem for both citizens, the private sector representing business and public sector officials.

Analysis on the Cybercrime as a National Threat

he range of sophisticated hacking operations include multinational corporations, financial institutions and embassies. Many risk consultants have claimed that cybercrime would continue to pose a threat to business and individuals in the Philippines if lawmakers do not address it. Lack of laws on information and communication technology (ICT) could negatively affect investor confidence in the Philippines. Two of the country's key sectors, business process outsourcing (BPO) and IT (information technology), along with those in other industries like banking and investment institutions are particularly vulnerable to cybercrime, and the government's inadequate approach to protecting companies will continue to affect investment. The Philippine government's response to the problem is lethargic despite the fact that the websites of its agencies have been hacked. These agencies provide basic services needed by the populace. The impediment to its operations brought about by cybercrimes compromises public confidence in government's efforts to efficiently provide fast, accurate, safe and timely services. [8]

A more potent effect of cybercrime is its capacity to obstruct justice and compromise safety and security. Cyber crime can be used to obstruct justice in a number of traditional ways: generating false evidence or destroying electronic evidence; altering or deleting court records to erase criminal convictions or charges; threatening law enforcement officers and judges; filing false reports of crimes; and shutting down crime-reporting systems. It has the capacity as well to impersonate a law enforcement officer or public official.

Computer technology is widely used by the malicious minds to commit his intentions.It is extremely dangerous on a national scale when the criminal breaks into the classified systems of national defense system and extract data of top secrets and exchanges with foreign countries for benefits.More horrible,computer technology can be utilized to undermine a nation's essential infrastructures, decreases its responding capacity in case of foreign invasions and cracks its fiscal stability.

Conclusion

The issue of cybercrime has been causing more and more attentions from both academicians and government administrators in Philippines over the past ten years. The cyber threat has become rampant with the increasing number of perpetrators with various intentions, which brought to this nation an unprecedented hazard. The fast-developing cyber technology and tools exacerbated the shocking reality. To make matter worse,the country's vulnerability towards such danger is also skyrocketing as the modernization of its critical infrastructure and economic systems calls for a stronger reliance on the computer network building on national and international scales. This gives the cyber-criminals more space to attack and leaves the country's critical infrastructure and economic systems under the horrible threats of devastating consequences. All these put the national security in great danger which was unforeseeable decades ago.

The cyber threats can be in various forms, among which the most serious ones are those acts with sensitive or critical data theft. Besides, other acts like threft of intellectual property ,online juvenile sexual exploitation, cyber fraud and online trafficking have penetrated to the mass' daily life and brought great turbulence and uncertainty for the social well-being. Moreover, Cyber vandalisim that targets on key government agency websites may lead to social chaos and endanger government operation when it is committed by malicious minds that are looking for undermining the political, economic and cultural control of the central government.

Recognizing the national economic implications of cyber threats, this paper concludes that the implications of cybercrime in the Philippines are of an impending grave nature which threatens that national security of its people, its private sector and its government.

To confront such threats, this paper calls for the Philippines government install a developmental initiative to enhance its capacity of identifying and neutralizing parties that illegally access cyber operations and spread

[8] ibid

programs or apps with malicious purposes.Education programs should be put on national agenda to enhance the mass's capability in differentiating malicious operations from sound ones.An enhanced cyber monitoring system should be planned for the government to control the cyber mechanism and instantly identify the malicious minds when certain case happens.

Perpetrators with salient criminal expertise are increasingly using encryption technology to secure their communications and to exercise command and control over operations and people without fear of surveillance because there is no capacity of deterrence in this aspect. It should therefore enact the appropriate legislation investigative cyber related threats having the highest probability of threatening national security and pursue responsive sanctions for individuals and organizations who ply this trade at the expense of its dire consequences.

REFERENCES

1. Brenner,Suan W. (2009).Threat Morphing in Cyber Space. In Cyberthreats: Emerging Fault Lines of the Nation-State .New York: Oxford University Press .https://www.e-ir.info/2010/03/08/threat-morphing-in-cyberspace-by-susan-w-brenner/,last accessed:May 2,2021
2. Cheng ,J. (2007)Cybercrime poses threat to National Security,https://arstechnica.com/information-technology/2007/11/mcafee-cybercrime-all-grown-up-spreading-its-wings/l,ast accessed:May 2,2021
3. Jaishankar K., (2008). Space Transition Theory of Cyber Crimes . In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet. (pp.283-301) Upper Saddle River, NJ: Prentice Hall.http://www.sascv.org/drjaishankar/theory.html,last accessed:May 2,2021
4. Jerome,S.&Samoy,L. (2017),Industrial Security Management Reviewer,https://kupdf.net/download/industrial-security-management-reviewer_598b0205dc0d60215a300d18_pdf,last accessed:May 2,2021
5. Philtechnology，We will maintain Sun's Unli Service,http://philtechnology.blogspot.com/2011_03_01_archive.html，last accessed:May 2,2021.
6. Romero,A.2011,Cybercrimes pose serious threat to Phil,https://www.philstar.com/headlines/2011/07/25/709381/cybercrimes-pose-serious-threat-phl-psa,last accessed:May 3,2021
7. SPAMfighter,2008,Computer Crime becoming a Headache for Philippines Police, http://www.spamfighter.com/News-9943-Computer-Crime-becoming-a-Headache-for-Philippines-Police.htm.last accessed:May 2,2021
8. Studymode , Cybercrime and ethics,https://www.studymode.com/essays/Cyber-Crimes-And-Ethics-1032058.html,last accessed:May 2,2021
9. Ursolino,Elmer,(2012),Social Learning Theory,https://elmerursolino.wordpress.com/category/uncategorized/,alst accessed:May 2,2021