Hacking: A Rapidly Increasing Cybercrime

Von Matthew Alfafara
School of Computer Science and Information Technology
Asia Pacific College
Makati, Philippines
vsalfafara@student.apc.edu.ph

Jameiah Nicole Jauod
School of Computer Science and Information Technology
Asia Pacific College
Makati, Philippines
jgjauod@student.apc.edu.ph

Allen Baldovino
School of Computer Science and Information Technology
Asia Pacific College
Makati, Philippines
aabaldovino@student.apc.edu.ph

Louise Gabrielle Lazaro
School of Computer Science and Information Technology
Asia Pacific College
Makati, Philippines
ldlazaro@student.apc.edu.ph

Abstract

In recent years, the percentage of hacking activities in the Philippines is maintained or growing rapidly in relation to evolving technologies, whether the purpose is disrupting a person's reputation, stealing information, stalking, or pranking. A recently approved law called the Cybercrime Prevention Act of 2012, that targets cybersquatting, cybersex, child pornography, identity theft, illegal access to data and libel as offenses, has flared the curtailment in Freedom of Speech. Limiting access or activities online, specifically social media sites, has brought netizens to object to such restrictions, and several would involve themselves in hacking activities to further express their distaste on the unwanted law, oblivious to the proper consequences of the said law, allowing them to boost their confidence in the fight against it. The government has yet to establish a better and secure way of using the internet, allowing no heinous online undertakings to surface upon a website for the betterment and safety of netizens. Exploiting such controversial issue in such a way that the government can begin to see through it will help in lowering the percentage of hacking activities in the Philippines. This paper explores possible motives in hacking, the risks of hacking, as well as minor preventions or remedies for cybercrimes for a safer cyberspace.

II. Introduction

"*I think something will soon have to be done to protect people from hacking and blogging and lying and spreading rumors and chasing you down the street. Lives are wrecked that way.*" – Ali MacGraw [1]

Cybercrime is a fast growing crime. Why? Because it is a modern way of attacking hardware and software in relation to computers and the internet. Familiar crimes also have evolved on the development of the internet, such as child abuse, monetary crimes and even terrorism. Nowadays, a very common offense in cybercrime is hacking – the gaining of access (wanted or unwanted) to a computer and viewing, copying, or creating data without the intention of destroying data or maliciously harming the computer. People violating this offense are called hackers – a person who gains authorized/unauthorized access to a computer without the intention of causing damage. [2]

According to the Republic Act No. 10175, hacking is the act of accessing to the whole part of the computer without a right.

According to a phrase in Ali MacGraw's quote, "something will soon have to be done to protect people from hacking" and the government of the Philippines passed a law about cybercrime, which was signed by President Aquino last September 12, 2012. The purpose of the Cybercrime Prevention Act of 2012 or Republic Act No. 10175 was to address legal issues regarding online interactions. [3]

The Act recognizes the importance of giving the environment beneficial to the development, acceleration and rational application, and the manipulation of information and communications technology to attain free, easy, and clear access to the exchange or delivery of information that needs to protect and defend the whole integrity of computers, computer communications systems, networks and databases, all confidential information, availability of information and data stored therein from all forms of misuse, abuse, and hacking. [4]

Republic Act No. 10175 was the first law in the Philippines, points out the computer crimes, which prior to the passage of the law had no strong legal precedent in Philippine jurisprudence. The Act was divided into 31 sections which have eight chapters, several types of offenses: data interference, cybersquatting, hacking, device misuse, computer-related offenses such as computer fraud, content-related offenses such as spam and cybersex, and a lot more offenses.

III. Problem Statement

Since technology is rapidly growing, it has a lot of risks to take and a lot of ways on how to misuse the internet. People tend to violate the laws regarding cybercrime because they thought they could not be caught doing it. Most of the violators really don't know if what they're doing is legal or not. Researchers want to know if the Philippines have any system that could track down the people violating this Act.

Another problem that the researchers want to solve is if Cybercrime Prevention Act of 2012 can really help to control cyber crimes. Since hackers are rapidly increasing in the Philippines, they need to be aware that there are laws need to be followed. They need to know the penalties when they commit such things.

Finally, the researchers want to know if there are other laws that can be associated with hacking. This problem must be addressed in order for people violating the law, knows what law they're violating and if it is not just one law that they have violated. This information is needed so that these problems can be avoided and can help victims of such offenses to know the proper sanctions to those who committed it. [10]

IV. Results and Discussion

This study within the research proposal was designed to further discuss the possible solutions that must be implemented to address the problems.

Intellectual knowledge about the cybercrime laws and penalties must be thoroughly discussed in public in order to raise awareness for those people who tend to violate the law and what are the possible consequences or penalties that will be charged on them. This issue must be integrated into educational materials and courses provided in public education institutions. Raising public awareness of the seriousness of the cybercrime problem should be the first step in a broader education program on how to counter the

threat effectively—how to detect and react to cyber attackers, and how to report crimes and losses. [11]

Hacking is one of the most hostile and dangerous enemies of the internet. It required advanced technologies to gain unauthorized access or trespass relevant sites like government websites for example. It may even require multiple presence of hackers and brilliant minds to meet such desires. Especially in the Philippines, there are definite number of reasons why people tend to involve themselves in hacking activities. An infamous hacking group called Anonymous Philippines has had successful undertakings in hacking official government websites.

So what are these reasons? One would be to protest against a law like the Cybercrime Prevention Act of 2012 that had a strong negative impact on netizens. Hacking government sites would be the number one target of hackers with such reason. They would claim it and may be infest it with virus or use it to express their protest against the Cybercrime Law. [5]

Another reason would be slow internet connection in the Philippines. The National Telecommunications Commission's website was vandalized with Anonymous Philippines' message. A portion of the message's content says "We, Anonymous Philippines, are sympathizing with our fellow Filipino netizens whose battle cries are the 'OVER PROMISED, UNDER DELIVERED' system of our internet service providers", which is actually considered true by most Filipinos. In terms of payment, paying the same amount of money, or even higher, compared to other countries (not counting internet speed) makes Philippines one of the countries that have the poorest internet services. [6]

After the 44 members of the police's Special Action Force were killed, many Filipinos expressed their condolence to the families and colleagues of the said members, including Anonymous Philippines, who have successfully hacked 20 government sites. They were disgusted about President Benigno 'Noynoy' Aquino's absence at the burials at Villamor Air Base, failing to honor the fallen soldiers who have served under his supremacy. [7]

International issues were one of the reasons for hacking international government sites like China's to strengthen Philippines' side on the territorial dispute against China or poaching. PHCA, Anonymous Philippines, Digital Nodes, Family Pride, and Xhint Knowsz were involved in the hacking. [8]

A common cause for hacking is personal issues, leading one to hack another's account in Facebook, Twitter, etc. Ruining one's reputation by hacking is a very common purpose. Or if not any one of these reasons, it would be just plain pranking. [9]

These reasons show that the Philippines overflow with disputes that cause people to engage in digital combat.

In the case of cybercrime, the openness, ease of access and slow institutional response has made it a low-risk and high-reward risk. However, the use of new technologies that are accelerating the volume and rate of cybercrime are of great concern that is why it is important for the public to know more about this issue. Philippines have the specific laws against hacking and to those people who caught violating the law shall be penalized by fine and/or imprisonment. [12]

According to the Republic Act No. 8792 of Philippines Electronic Commerce Act of

2000 under the Part V-Final Provision – Section 33(a) [13]

"Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years." [13]

According to Republic Act No. 10175 (Cybercrime Prevention Act of 2012) section 4(a), "*Offenses against the confidentiality, integrity and availability of computer data and systems* shall be punished with imprisonment of *'prision mayor'* or a fine of at least Two Hundred Thousand Pesos (P200,000.00) up to a maximum amount commensurate to the damage incurred, or both, except with respect to number 5 herein:" [4]

One type of the offenses against confidentiality is illegal access, *"the access to the whole or any part of a computer system without right."* [4] This can be associated with hacking because violators tend to get information of a certain person, a group of people, bank accounts in banks and even small things like information from a student in a specific computer and a lot more.

Section 4(b) of the Republic Act No. 10175, "*Computer-related Offenses*, which shall be punished with imprisonment of *prision mayor*, or a fine of at least Two Hundred Thousand Pesos (P200,000.00) up to a maximum amount commensurate to the damage incurred, or both, are as follows:" [4]

Computer-related Identity Theft – *"The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right"* [4] This type of computer-related offense can be used in a lot of ways. One way is that the violator can hack or get information from the victim. Their reason of doing this could be for personal reasons, or they just want to steal some information from the victim.

Also chapter III of Republic Act No. 10175- Penalties - Section 8. [14]

"Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to a maximum amount commensurate to the damage incurred or both." [14]

Any person found guilty of the punishable act under Section 4(a)(5) shall be punished with imprisonment of *prision mayor* or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both. [14]

If punishable acts in Section 4(a) are committed against critical infrastructure, the penalty of *reclusion temporal* or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to maximum amount

commensurate to the damage incurred or both, shall be imposed. [14]

R.A 10175 (Cybercrime Prevention Act of 2012) has been implemented from different cases of cybercrime here in our country (Philippines). Based on the researches, there are several cases of cybercrime in which the law doesn't apply appropriately. The severeness of the cases must be considered wisely. If the certain case result to an extensive destruction then it is considered to be in a high severity unless the case would result to a less destructive effect then it is considered as a medium or low severity.

According to the researches, hacking of bank(s) is considered as a high severity due to the possibility outcome of having massive destruction to its customers, employees and also on the company's name. Base on article that has been given on it, there was a case of bank hacking happened at New Jersey. The hacker was an old Filipino named Peter Alexei Locsin who used to live at US and came back to live in the Philippines, Bacolod City.One of his former alleged was a former FBI Director Robert Mueller. He was at the watch list of the US FBI for bank hacking and was involved to international hacking. He was arrested inside his renting room. [15]

Child pornography is considered under the medium severity by having a limited damaged for those people who are certainly involved in this case. According to the article related to this case, a 17-year old girl has been punished by R.A 9208 otherwise known as Qualified Trafficking, R.A 10175 in relation to R.A 9775 otherwise known as the Anti-child Pornography Act of 2009. All those cases are non-bailable. The accused was arrested on August 17, 2015 in an entrapment and rescue operation by using an online decoy account pretending to be a foreigner. The accused and the foreigner decoy had an agreement to meet one of the hotels in Cebu. During their conversations, the latter, via Facebook the accused sent pornographic photos of the girls and offered him the girls, including the minor for sex. Thus, an entrapment was conducted, leading to the arrest of the minor. [16]

Internet Libel cases is considered under the low severity due to its case of having a very limited cause of damaged. Base on the related case, R.A 10175 (Cybercrime Prevention Act of 2012) there was an actress of ABS-CBN named Neri Naig and the road manager named Danilyn Nunga were charged with violations of Republic Act No. 10175 or the Cybercrime Prevention Act of 2012. In an Instragram post Danilyn posted photos of the complainants Clarence Taguiam and Donna Marie Go and accused them of being "bogus and fictitious" sellers of Go Pro Hero3 Action Camera and claimed that she had bought it for P7,500 but never received the product. Neri re-posted the post of Danilyn. Taguiam denied about selling those item and camera to Nunga. The court recommended a bail of P10,000 for the temporary liberty of both accused.[17]

V. Conclusion and Recommendation

The researchers concluded that hacking is definitely moving ahead and rapid. This research stated laws that can be related to hacking, which can help in knowing what cybercrime they've violated. The focus of this research is to know if the Republic Act No. 10175 is really effective or not. Researchers agreed to take the stand that the Cybercrime Prevention Act of 2012 is not really that effective because there were a lot of loopholes to this law. One of which is that, the law can penalize anyone violating it and people can be put to jail easily. The question will boil down to, why would you put someone to jail even if his/her case is really not that big. Does their violation affect you as an individual? Of course, not.

Cybercrime is defined, by many people, as a very serious case of illegal activity. It has a broad range of possible targets since its primary scope is the entire internet, if not other computer networks. It also has its own crime offense levels, meaning it can go to being subtle that affects next to no people and very severe that can damage possibly anyone's company, work, reputation, dignity, and others. Cybercrime Prevention Act of 2012 has any punishable acts such as the common illegal access, misuse of data, cyber-squatting, data theft, alteration or deletion, cyber-sex, etc., yet there are number of ways that these acts can be done in a very subtle way in which the person is not accountable under the law. For example, small disputes among friends. It can lead into a subtle disruption of each other's reputation, making false accusation or back-stabbing stories. This may be accountable for online libel, but it does not reach into the acceptable crime offense levels.

So just how heinous a cyber-crime must be committed before it is considered suitable and accountable under the law?

1. **Consider stalkers –** A stalker is a person who can steal information from his or her target. Only one instance of a stalker, who has hacked your phone and even the environment around you such as the CCTV camera, can be classified as libelous and can be sent to the court of justice. It is a matter of fact that this stalker can potentially disclose any confidential information about yourself that you do not want the public to know about. This instance of a cybercrime is a dangerous due to the fact that it can damage your image.

2. **Have a defense against hackers –** Hackers tend to hack by using viruses. You can put some defensive strategy so that it can easily be detected. Use anti-viruses, spywares, IDS and etc.

References

[1] MacGraw, A. (N.d.). BrainyQuote.com. Retrieved February 24, 2016, from BrainyQuote.com Available: http://www.brainyquote.com/quotes/quotes/a/alimacgraw582972.html

[2] No Author. (2004, August). Urbandictionary.com. [Online]. Available: http://www.urbandictionary.com/define.php?term=hacking

[3] No Author. (2012, October). *What is Republic Act (RA) No. 10175 or Cybercrime*

Prevention Act of 2012. Ilonggo Tech Blog. [Online]. Available: http://www.ilonggotechblog.com/2012/10/what-is-republic-act-no-ra-10175-or.html#sthash.i7qNfZ1.dpuf

[4] De Lima, L. M., Roxas, M. & Montejo, M. G. (2015, August). *Implementing Rules and Regulations of Republic Act No. 10175*. [Online]. Available: http://www.gov.ph/2015/08/12/implementing-rules-and-regulations-of-republic-act-no-10175/

[5] No Author. (2014, February). *Cybercrime law constitutional – supreme court*. [Online]. Available: http://www.rappler.com/nation/special-coverage/cybercrime-law/51197-full-text-supreme-court-decision-cybercrime-law

[6] Adel, R. (2015, September). *Hackers deface ntc website over slow internet*. [Online]. Available: http://www.philstar.com/headlines/2015/09/21/1502366/hackers-deface-ntc-website-over-slow-internet

[7] No Author. (2014, May). Filipino hackers deface Chinese website. [Online]. Available: http://www.rappler.com/nation/58431-anonymous-ph-hacks-chinese-websites

[8] De Lazo, C. (2015, January). *Government sites hacked to protest misencounter*. [Online]. Available: http://www.philstar.com/headlines/2015/01/31/1418775/govt-sites-hacked-protest-misencounter

[9] No Author. (2015, November). *Maine Mendoza's twitter account hacked*. [Online]. Available: http://www.rappler.com/entertainment/news/111517-maine-mendoza-twitter-account-hacked-anonymous-philippines-yaya-dub-aldub

[10] Joshi, P. R. (2013). *Hacking: a critical study in emerging Cyber Crime in Nepal*. [Online]. Available: https://www.academia.edu/11292235/_Hacking_A_critical_study_in_emerging_Cyber_Crime_in_Nepal_Faculty_of_Law_For_Partial_Fulfillment_of_the_Requirement_for_the_LL.B._5_th_Year

[11] No Author. (2010). *Solution for Cybercrime, Cybersecurity and the future of the internet.* [Online]. Available: http://www.global-economic-symposium.org/knowledgebase/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet/solutions/Improve_public_education_systems_for...

[12] Blackwell, A. (2015, January). *7 ways to bring cybercrime out of the shadows*. [Online]. Available: http://www.weforum.org/agenda/2015/01/7-ways-to-bring-cybercrime-out-of-the-shadows

[13] No Author. (2002, February). *Republic Act No. 8792 of Philippines: electronic commerce act of 2000*. [Online]. Available: http://icto.dost.gov.ph/wp-content/uploads/2014/10/images_ipenforcement_RA8792-E-Commerce_Act.pdf

[14] Barua-Yap, M. B. & Lirio-Reyes, E. (2012, September). *Republic act no. 10175*. [Online]. Available: http://www.gov.ph/2012/09/12/republic-act-no-10175

[15] Dangcalan, D. (2015, June). *Pinoy hacker who targeted ex-FBI director nabbed.* [Online]. Available: http://www.philstar.com/headlines/2015/06/22/1468586/pinoy-hacker-who-targeted-ex-fbi-director-nabbed

[16] Sallan, E. P. (2016, February). *Neri Naig faces arrest of libel for re-posting Instagram post.* [Online]. Available: http://www.interaksyon.com/entertainment/neri-naig-faces-arrest-for-libel-for-re-posting-instagram-post/

[17] Manto M. P. (August, 2015). *No bail for 17-year old "pimp"*. [Online]. Available: http://www.philstar.com/cebu-news/2015/08/27/1492796/no-bail-17-year-old-pimp

[18] Linington, D. (N.d.). *Top 8 tips to prevent cybercrime.* [Online]. Available: http://www.spiceworks.com/marketing/top-8-tips-prevent-cybercrime/

[19] No Author. (2000). KeyGhost Ltd. [Online]. Available: http://www.keyghost.com

[20] Sukhai, N. B. (N.d.). *Hacking and cybercrime.* [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.3895&rep=rep1&type=pdf