Shanghai Jiao Tong University

The 2022 Shanghai Jiao Tong University (SJTU) United Nations Sustainable Development Goals (SDG) July Camp

A Case Report

PJ179: Internet Law and Ethics

Presented By the

Name: TARIQUL ISLAM

Abstract

The supreme art of war is to subdue the enemy without fighting."
- Sun Tsu from "The Art of War"

Cyber-attack is a sensitive issue in the world of Internet security. Governments and business organizations around the world are providing enormous effort to secure their data. They are using various types of tools and techniques to keep the business running, while adversaries are trying to breach security and send malicious software such as botnets, viruses, trojans etc., to access valuable data. Every day the situation is getting worse because of new types of malwares emerging to attack networks. It is important to understand those attacks both before and after they happen in order to provide better security to our systems. Understanding attack models provide more insight into network vulnerability, which in turn can be used to protect the network from future attacks. In the cyber security world, it is difficult to predict a potential attack without understanding the vulnerability of the network. So, it is important to analyses the network to identify top possible vulnerability list, which will give an intuitive idea to protect the network. Also, handling an ongoing attack poses significant risk on the network and valuable data, where prompt action is necessary. Proper utilization of attack modelling techniques provides advance planning, which can be implemented rapidly during an ongoing attack event. This paper aims to analyses various types of existing attack modelling techniques to understand the vulnerability of the network, and the behavior and goals of the adversary. The ultimate goal is to handle cyber-attack in efficient manner using attack modelling techniques.

Acknowledgement

First of all, we would like to thank Organizer, SJTU this season. I would like to express our gratitude to the **Faculty, PJ179: Internet Law and Ethics** for giving scope of doing research and working in the field of our interest. Adviser may be subject to operational and information security risks resulting from breaches in cyber security. A breach in cyber security refers to both intentional and unintentional events that may cause Adviser to lose proprietary information, suffer data corruption, or lose operational capacity. Cyber security breaches may cause the release of Client information or confidential business information, impede investment, subject Adviser to regulatory fines or financial losses and/or cause reputational damage. The standard of liability described in Paragraph will apply to any Client losses related to a breach in cyber securities. I'm highly appreciate to **SJTU** to give me opportunity for this season. I would like to looking forward for further any bootcamp. For leaning more Courses.

Table of Contents

Introduction

In a world driven more and more by big data, social networks, online transactions, information stored or managed via internet and automated processes performed through the use of IT systems, information security and data privacy are permanently facing risks. With the development of new tools and techniques, cyber-crime is consistently increasing in terms of number of attacks and level of damage caused to its victims. Developing new ways to gain unauthorized access to networks, programs and data, attackers aim to compromise the confidentiality, integrity and availability of information, building their targets from single individuals to small or medium sized companies and even business giants. Every year seems to bring a bigger number of attacks overall, but also a bigger number of attacks defeating the security of extremely large companies, thus affecting the information security, business continuity and customers' trust. The increasing trend has reached new peaks in 2014, universally known as "the year of cyber-attacks", but the authors believe this is not to be the apogee unless countermeasures are taken at a global scale. This article has the purpose of revealing results, trends and patterns noted by the authors through the analysis of the attacks reported in the last three years, and to present countermeasures that should be taken as for supporting the improvement of security and the decrease of world-wide cyber-crime. The article is structured in three main parts: it begins by presenting the general view of cyber-crime from the perspective of specialized literature, international law, as well as historical facts and continues through revealing the main results and interpretation of the study performed over the last three years' reported attacks. It ends by drawing some of the main countermeasures that companies may undertake in order to ensure improvement of controls covering the information confidentiality, integrity and availability, while decreasing the security breaches.

Types of cyber crimes

Hacking

It is an offence to hack a computer system which belongs to other individuals or organizations. Hacking puts the victim in a very vulnerable position as there are risks of exposing all the confidential information in a computer system. It is a punishable offence and the laws regarding hacking are quite strict.

Cyber-defamation

The internet can be used to spread misinformation just as easily as information. Websites can present false or defamatory information especially in forums and chat rooms, where users can post messages without verification by moderators. IT is vital to highlight the increased danger presented by false or misleading information. Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a world-wide range.

Cyber-extortion

Cyber-extortionists create harmful soft-wares and often threat individuals or organizations. With those soft-wares they can cause serious damage to the threatened individuals or organizations. They offer 'protection' in exchange of money otherwise they destroy or expose all financial and security information. These cyber-extortionists can be regarded as the new age cyber-mafias.

E-mail bombing

E-mail bombing refers to sending a large number of e-mails to the victim resulting in the victim's e-mail account (in case of an individual) crashing. This kind of things are done to harass someone purposefully.

Cyber-terrorism

The term cyber-terrorism was coined in the 1980s by Barry C. Collin. It is defined as the premeditated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. Cyber-terrorists can do unimaginable harm to a group of people or a state. They can get into a telephone network during an emergency and shut it down causing more casualties. Suppose, a situation similar to 9/11 has arisen and emergency personnel are being deployed. Meanwhile, the terrorists can hack into emergency communication system and redirect all orders, give false information etc. Thus, the situation will worsen. In USA, FBI has separate Cyber Security Unit (CSU) who works to protect the nation from such attacks. Cyber-terrorists target transportation, telecommunication, financial data etc. Thus, a war can be won without shooting even a single bullet.

Cyber Attack Statistics

What are the costs and impact of cyber-attacks for businesses?
The global cost of cyber-attacks is expected to grow by 15% per year and is expected to reach over $10 trillion. A growing part of this cost is Ransomware attacks, which now cost businesses in the US $20 billion per year.

How well are organizations prepared for cyber-attacks?

In a recent survey, 78% of respondents said they believe their company's cybersecurity measures need to be improved. As many as 43% of small businesses do not have any cyber defenses in place. At the same time, organizations of all sizes are facing a global cybersecurity skills shortage, with almost 3.5 million open jobs worldwide, 500,000 of them in the US alone.

Cyber Attack Examples

Here are a few recent examples of cyber-attacks that had a global impact.
Kaseya Ransomware Attack
Kaseya, a US-based provider of remote management software, experienced a supply chain attack, which was made public on July 2, 2021. The company announced that attackers could use its VSA product to infect customer machines with ransomware.
The attack was reported to be highly sophisticated, chaining together several new vulnerabilities discovered in the Kaseya product: CVE-2021-30116 (credentials leak and business logic flaw), CVE-2021-30119 (XSS), and CVE-2021-30120 (two-factor authentication flaw). The malware exploiting these vulnerabilities was pushed to customers using a fake software update labelled "Kaseya VSA Agent Hot Fix".
The attack was carried out by the Russian-based REvil cybercrime group. Kaseya said less than 0.1% of their customers were affected by the breach, however, some of them were managed service providers (MSP) who used Kaseya software, and the attack affected their customers. A short time after the attack, press reports said 800-1500 small to mid-sized companies were infected by REvil ransomware as a result of the attack.
SolarWinds Supply Chain Attack
This was a massive, highly innovative supply chain attack detected in December 2020, and named after its victim, Austin-based IT management company SolarWinds. It was conducted by APT 29, an organized cybercrime group connected to the Russian government.
The attack compromised an update meant for SolarWinds's software platform, Orion. During the attack, threat actors injected malware, which came to be known as the Sunburst or Solorigate malware—into Orion's updates. The updates were then distributed to SolarWinds customers.
The SolarWinds attack is considered one of the most serious cyber espionage attacks on the United States, because it successfully breached the US military, many US-based federal agencies, including agencies responsible for nuclear weapons, critical infrastructure services, and a majority of Fortune 500 organizations

Types of Cyber Attacks

While there are thousands of known variants of cyber attacks, here are a few of the most common attacks experienced by organizations every day.
There are many types of malwares, of which ransomware is just one variant. Malware can be used for a range of objectives from stealing information, to defacing or altering web content, to damaging a computing system permanently.
Banking trojans—steals financial and credential information for banking websites
Mobile Malware—targets devices via apps or SMS
Rootkits—gives the attacker complete control over a device's operating system
These attacks don't provide the attacker with access to the target system or any direct benefit. They are used purely for the purpose of sabotage, or as a diversion used to distract security teams while attackers carry out other attacks. Phishing and Social Engineering Attacks
Social engineering is an attack vector that relies heavily on human interaction, used in over 90% of cyberattacks. It involves impersonating a trusted person or entity, and tricking individuals into granting an attacker sensitive information, transferring funds, or providing access to systems or networks.
Phishing attacks occur when a malicious attacker obtains sensitive information from a target and sends a message that appears to be from a trusted and legitimate source. The name "phishing" alludes to the fact that attackers are "fishing" for access or sensitive information, baiting the unsuspecting user with an emotional hook and a trusted identity.
Man-in-the-Middle (MitM) attacks are breaches that allow attackers to intercept the data transmitted between networks, computers or users. The attacker is positioned in the "middle" of the two parties and can spy on their communication, often without being detected. The attacker can also modify messages before sending them on to the intended recipient.

Legal issues of new and emerging technologies

To prepare for and mitigate the impact of emerging technologies on cybercrime, Estonia could consider broad anti-cybercrime capacity building; seek legal, regulatory and organizational agility; and invest in technological expertise, skills and research.

Since the invention of the agriculture in the Fertile Crescent, the humanity has witnessed continuous technological developments. Such developments affect the human society in positive and negative ways. For example, an airplane allows the quick transportation of passengers, whereas an atomic bomb provides its users with an opportunity to destroy entire nations. The governments put efforts to regulate technology in such a way as to enhance its positive effects and ameliorate its negative consequences. For example, there are governmental regulations related to the use of cookies (i.e., small files which are stored on a user's computer), drones, wearable devices (e.g., smart watches and Google Glass), and social networking platforms. The regulation of new and emerging technologies is not an exception.
The legal issues related to "New and Emerging Technologies" (NET) fall within the scope of the laws regulating the use of data, evidence, creative works, and inventions. We will further focus on four such laws:
Privacy law, i.e., the law that regulates the collection, use, processing, and disclose of personal information. Under most privacy laws, personal information is defined as information which identifies an

individual or allows an individual to be identified; The law of evidence, i.e., the law that governs the proof of facts in legal proceedings; Copyright law, i.e., the law that governs the ownership and use of creative works Patent law, i.e., the law that regulates the rights to inventions.

PRIVACY ISSUES

The privacy issues related to NET can be grouped into two categories, namely, (1) security vulnerabilities threatening the privacy of NET users and (2) the use of NET for unlawful surveillance (see Fig. 1). These two categories are examined in Sections 2.1 and 2.2, respectively. The first category relates to privacy issues caused by security vulnerabilities of NET. Such security vulnerabilities may include, for example, weak authentication, insufficient encryption, and insecure firmware. The second category of issues refers to the use of NET for unlawful surveillance. For example, thieves may use crowdsensing for detecting when a victim is not at home. The term "crowdsensing" refers to sharing data collected by sensing devices with the aim to measure the phenomena of common interest.

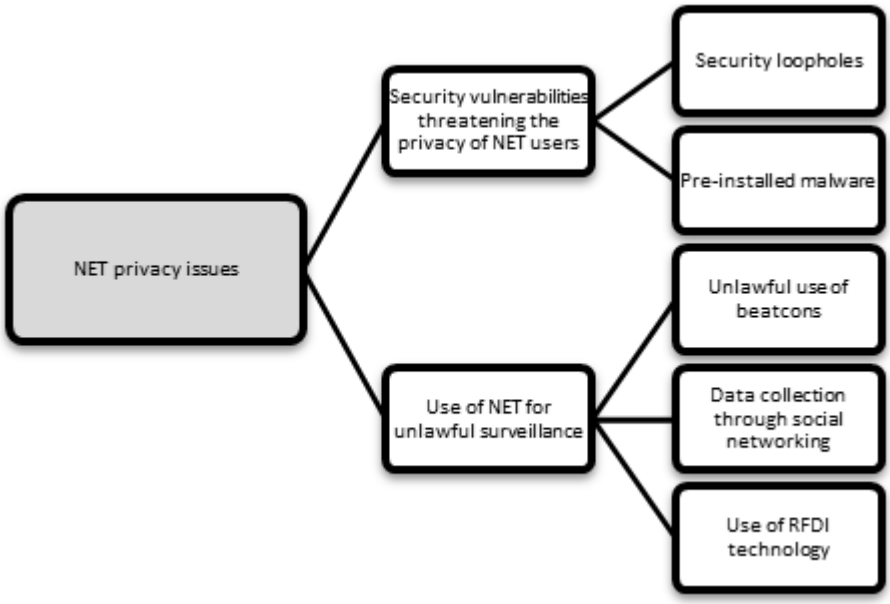
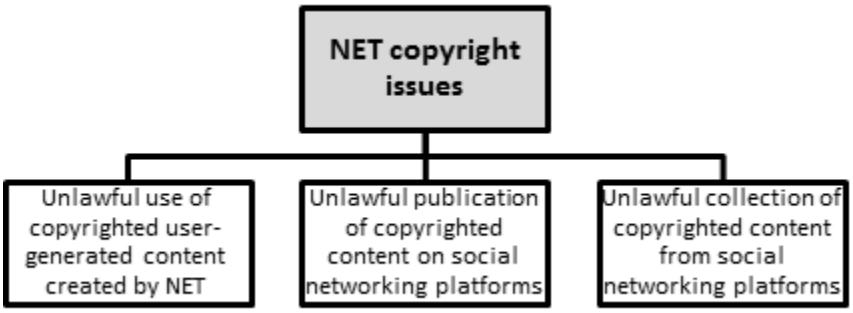


Fig. 1 Privacy issues related to NET

What is the issue?
Digital systems and Information Communication Technology (ICT) have become critical in all areas of economic activity in Europe and beyond. Access to the internet and an uninterrupted flow of information now underpins many businesses and the day-to-day functioning of societies.
Ethical issues

Copyright issues related to Net
The term "copyright" can be defined as "the exclusive right of the author or producer of a literary, scientific, or artistic work to publish and reproduce it." (Kraak and Ormeling, 2011, p. 182) The copyright issues arising related to NET can be categorized into the following three categories (See Fig. 3):

Unlawful use of user-generated content created by NET;
Unlawful publication of copyright content on social networks; and
Unlawful collection of copyrighted content from social networks.



Specific Case/crime in Bangladesh Act low processes

Cyber Crime and Legal Fabric of Bangladesh

Today we often come across terms like ‘cyber crimes’, ‘net crimes’, ‘computer-fraud’, ‘cyber extortion’ etc. With the advent and advancement of internet, a new type of crime has developed. It is most commonly known as the cybercrimes. The term cyber generally means computer network or virtual reality. So, cybercrime can simply be defined as crime which involves cyberspace or computer network or a protected computer system. As our modern age is entirely dependent on network-based facilities, a slight inconvenience on its part can cause a lot of problems. A single misplacement of information or a single wrong stroke on a keyboard button can literally cause great havoc and destruction. Though these technologies have empowered us to do a great deal of things, it has also put us in a vulnerable position. We have created these things but now we are sometimes helpless in front of our own creation. Honest mistakes may happen but some people are intentionally taking advantages of these weaknesses. What they are doing is called cybercrime. They become active in the cyberspace and then use trickeries and evil methods to materialize their malicious desires which are often very harmful to individuals and group of individuals. These cybercrimes are dangerous in nature and always pose serious threat to privacy at personal, public or national level.

What exactly is cybercrime?
“Offences that are committed against an individual or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss to the victim directly or indirectly using modern telecommunication networks such as internet (chat rooms, emails, notice boards or groups) and mobile phone (SMS/MMS).’’
Cyber criminals are most commonly known as hackers. The term “hacker” is now so overused that it has come to be applied to anyone who breaks into computer systems. But this is not entirely correct. There is a difference between hackers and crackers, although the term “cracker” has never caught on with general public.

Cyber-crimes in Bangladesh

Bangladesh, despite being a third world country, has seen a technological revolution. A Bangladeshi teenager has very easy access to computers and other devices. And so, they get enough opportunity to engage in hacking. Hacking has already become a major problem in Bangladesh. Young people are getting more and more interested in hacking for the thrill in it. Not just young people, even the mainstream media is so often engaged in the hacking and exposing private information.

The Mahmudur Rahman case is one of the leading cases in terms of cybercrimes in Bangladesh and may be referred as the first cybercrime case in Bangladesh. Mahmudur Rahman, the founder of a Bangladeshi newspaper named Amar Dash was sued in line with a High Court directive for publishing reports on Skype conversation between former International Crimes Tribunal chairman Justice Md Nijamul Huq and an expatriate legal expert in December, 2012. He was sued along with the Amar Desh publisher Hashmat Ali on December 13, 2012.

On 15/02/2012 a group of alleged Bangladeshi hackers named 'Black Hat Hackers' hacked more than 25000 Indian websites which included important sites such as the website of the Border Security Forces (BSF). Propaganda activities are also considered as cyber-crimes in some instances. Propaganda is information which is biased and misleading in nature used to promote or publicize a particular political cause or ideology. It creates agitation and panic among the public. For example, we can mention the 2012 Ramu Violence in Cox's Bazar. Someone with a fake Facebook account posted a photo of desecration of the Holy Quran on its wall. The fake account was under a Buddhist male name. This post agitated the common Muslim people of that area and they, without verifying the authenticity of the Facebook account, attacked innocent Buddhist dwellers of that area. Many Buddhist temples, monasteries and households were destroyed. So, it is clear that Bangladesh is not free from the threat of cyber-crimes. Everyday new forms of cyber-crimes are happening and if it goes unchecked, law and order situation will worsen.

Legal fabric of Bangladesh regarding cyber-crimes

The ***Information and Communication Technology (ICT) Act, 2006*** came in force on 8 October, 2006. Subsequently, the government amended the Act in 2008 and in 2009. For the better application of the Act, the government passed Information Technology (Certificate Authority) rules in 2010. But these laws alone are not enough. To face the challenges growing in cyber space it is essential to amend the existing laws such as *the Penal Code 1860, the Evidence Act 1872, the Contract Act 1872* etc. It is hoped that these Acts will be modified in accordance with the demand of time. However, there are some provisions in the ICT Act, 2006 which mention penalties for various cyberspace related crimes. For instance, *section 54 (1)* of this Act declares the offences concerning cyberspace. Then, *section-54(2)* says, "If any person commits offences under sub-section (1) of this section, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to taka ten lakhs, or with both".

We can also look at *section-56* which says-

"If any person—

(a) with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, does any act and thereby destroys, deletes or alters any information residing in a computer

resource or diminishes its value or utility or affects it injuriously by any means;

(b) damage through illegal access to any such computer, computer network or any electronic system which do not belong to him; then such activity shall be treated as hacking offence;

(c) whoever commits hacking offence under sub-section (1) of this section, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to taka one crore, or with both."

We can see that law has taken the matter of cyber-crimes in consideration and there are some strict rules regarding it.

A day in the life of a lawyer

Lawyers are some of the most hardworking people out there. They put in many more hours of work compared to those in other professions. In fact, what you might see on TV, like lawyers relaxing, chatting and enjoying lunch with clients, is not realistic. The truth is, lawyers work between 50 and 60 hours weekly on average.

Main responsibilities

The everyday responsibilities of a lawyer may consist of the following:

- Advising clients
- Interpreting laws and applying them to specific cases
- Gathering evidence for a case and researching public and other legal records
- Representing clients in court
- Examining legal data to determine advisability of defending or prosecuting lawsuit
- Presenting evidence to defend clients or prosecute defendants in criminal or civil litigation
- Preparing and drafting legal documents e.g., legal briefs, wills, deeds, mortgages, leases etc.
- Negotiating settlements
- Supervising legal assistants
- Act as agent, trustee, guardian, or executor for businesses or individuals

Even if they have to dedicate more hours to work every day, lawyers will aim to help their clients with their legal concerns. In some cases, their work can really change their lives, whether it is clearing them of charges or helping them get compensation. It is, in fact, this knowledge that their work affects other people's lives that motivates them to work harder and at times, longer than others

Conclusion

Cybercrime is obviously the latest form of the crimes which is very difficult to suppress. But its difficulty must not prevent us from taking adequate measures against the cyber-criminals. Only law is not enough and so, we must nurture ethics and morality in our private and communal lives. As our youngsters are prone to misdirection, they must be given proper guidance and care. The state has to take all possible measures to thwart any kind of cyber-invasion which may put the lives of people in danger. Continuous vigilance and upgrading counter-measures are some of the must-dos for the government. Common people should also be careful in using computer systems and online facilities. Hopefully, our awareness and constant battle against cyber-crime will result in success.

References

1. Md. Sarwar Alam Sajjad, 'Cyber Crime and Legal Fabric of Bangladesh' (*Bangladesh Law Digest*, August 12, 2015)
2. Dr. Debarati Haldar and Dr. K. Jaishankar
3. Bangladesh cybercrime tribunal

Sources

1. *Penal Code 1860, the Evidence Act 1872, the Contract Act 1872* etc.
2. *Information and Communication Technology (ICT) Act, 2006*
3. *https://bdlawdigest.org*
4. *https://www.lawinsider.com/clause/cyber-incident-reporting*
5. *https://en.prothomalo.com/topic/Cyber-Crime*
6. *https://www.simplylawjobs.com/*