Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 8, Issue. 1, January 2019, pg.131 – 143

A Survey of Cybercrimes, Investigations and Penal Laws Imposed on the Criminals

[1]Wisam Shakir Hussain; [2]Nebras Jalel Ibrahim

wisamalkhshali@gmail.com; eng_nebrasjalel84@yahoo.com
[1]College Education for Pure Science – Diyala University - Iraq
[2]Presidency of Diyala University- Iraq

***Abstract:** Cyber-crime, once the domain of disaffected genius teenagers as portrayed in the movies "War Games" and "Hackers," has grown into a mature and sophisticated threat to the open nature of the Internet. "Cyber-criminals," like their non-virtual traditional criminal counterparts, seek opportunity and are attracted to vacuums in law enforcement. The news media is filled with reports of debilitating denial of service attacks, defaced web sites, and new computer viruses worming their way through the nation's computers. However, there are countless other cyber-crimes that are not made public due to private industry's reluctance to publicize its vulnerability and the government's concern for security. Along with the phenomenal growth of the Internet has come the growth of cyber-crime opportunities. As a result of rapid adoption of the Internet globally, computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few. Law enforcement officials have been frustrated by the inability of legislators to keep cyber-crime legislation ahead of the fast-moving technological curve. At the same time, legislators face the need to balance the competing interests between individual rights, such as privacy and free speech, and the need to protect the integrity of the world's public and private networks. Further complicating cyber-crime enforcement is the area of legal jurisdiction. Like pollution control legislation, one country cannot by itself effectively enact laws that comprehensively address the problem of Internet crimes without cooperation from other nations. While the major international organizations, like the OECD and the G-8, are seriously discussing cooperative schemes, many countries do not share the urgency to combat cyber-crime for many reasons, including different values concerning piracy and espionage or the need to*

address more pressing social problems. These countries, inadvertently or not, present the cyber-criminal with a safe haven to operate. Never before has it been so easy to commit a crime in one jurisdiction while hiding behind the jurisdiction of another. In section II of this article, we begin by providing an overview of cyber-crimes, the state of the law, and cyber-crime perpetrators and their motivations. Then, in section III we discuss in detail three major computer crimes and analyze how the different statutory subsections are applied depending upon the technical details of the crime itself. Just as a murder prosecution is dependent on how the crime was committed, different hacking techniques trigger different federal anti-computer crime subsections. We begin with a discussion of the various denial of service attacks and the applicable statutes. Next we discuss the technical details of several hacking techniques and apply the relevant statutory subsections to the specific techniques. Finally, we explore the various types of computer viruses and how viral "payloads" and the class of the targeted computer will determine which federal subsection can be applied to the crime. In section IV, we discuss proposed legislative changes to the Computer Fraud and Abuse Act and related privacy concerns.

1. Introduction

What is a cyber-crime? Law enforcement experts and legal commentators are divided. Some experts believe that computer crime is nothing more than ordinary crime committed by high-tech computers and that current criminal laws on the books should be applied to the various laws broken, such as trespass, larceny, and conspiracy. Others view cyber-crime as a new category of crime requiring a comprehensive new legal framework to address the unique nature of the emerging technologies and the unique set of challenges that traditional crimes do not deal with; such as jurisdiction, international cooperation, intent, and the difficulty of identifying the perpetrator. Another source of confusion is the meaning of "hacker" and "cracker" and the distinction behind their motivations. The following section will elaborate on the differences between the two and their relevance to federal criminal statutes. Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network.[1] The computer may have been used in the commission of a crime, or it may be the target.[2] Cybercrimes can be defined as: "Offences that are committed against individuals or groups 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 (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".[3] Cybercrime may threaten a person or a nation's security and financial health.[4] Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming.[3] There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".[3] Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation state is sometimes referred to as cyberwarfare. A report (sponsored by McAfee), published in 2014, estimated that the annual damage to the global economy was $445 billion. [5] Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US.[6] In 2018, a study by Center for Strategic and International Studies (CSIS), in partnership with McAfee, concludes that close to $600 billion, nearly one percent of global GDP, is lost to cybercrime each year.[7]

1.1 The State of the Law

Congress has approached computer crime as both traditional crime committed by new methods and as crime unique in character requiring new legal framework. For example, Congress has amended the Securities Act of 1933 to include crimes committed by a computer. However, Congress has also enacted a comprehensive new computer fraud and abuse section that can easily be amended to reflect changes in technology and computer use by criminals. In fact, the U.S. [8] Congress has enacted statutes that widen the scope of traditional crimes to specifically include crimes involving computers, or categorize them as entirely separate offenses.[9] For example, the main federal statutory framework for many computer crimes is the Computer Fraud and Abuse Act ("CFAA"). The statute is structured with an eye to the future so that it can be easily amended to reflect changes in technology and criminal techniques. The statute has already been amended several times to close unintended loopholes created by judicial interpretation. In its current form, the statute is very broad in scope, reflecting the government's resolve to combat cyber-crime at every level.2.1 Applications of Virtual Reality in Sports

1.2 The Perpetrators—Hackers and Crackers

a. Hackers

"Hacker" is a term commonly applied to a "computer user who intends to gain unauthorized access to a computer system." Hackers are skilled computer users who penetrate computer systems to gain knowledge about computer systems and how they work. The traditional hacker does not have authorized access to the system. Hacking purists do not condone damage to the systems that are hacked. .[10] According to The Jargon Dictionary, the term "hacker" seems to have been first adopted as a badge in the 1960s by the hacker culture surrounding The Tech Model Railroad Club ("TMRC") at Massachusetts Institute of Technology when members of the group began to work with computers. The TMRC resents the application of the term "hacker" to mean the committing of illegal acts, maintaining that words such as "thieves," "password crackers," or "computer vandals" are better descriptions. In the hacking "community," it is considered better to be described as a "hacker" by others than to describe oneself as a "hacker." Hackers consider themselves members of an elite meritocracy based on ability and trade hacker techniques and "war stories" amongst themselves in Usenet forums, local or regional clubs, and national conferences, such as the annual Def Con Computer Underground Convention held in Las Vegas. [11]

b. Crackers

A "cracker" is a hacker with criminal intent. According to The Jargon Dictionary, the term began to appear in 1985 as a way to distinguish "benign" hackers from hackers who maliciously cause damage to targeted computers. Crackers maliciously sabotage computers, steal information located on secure computers, and cause disruption to the networks for personal or political motives.

Estimates made in the mid-1990's by Bruce Sterling, author of The Hacker Crackdown: Law and Disorder on the Electronic Frontier, put "the total number of hackers at about 100,000, of which 10,000 are dedicated and obsessed computer enthusiasts. A group of 250-1,000 are in the so-called hacker 'elite', skilled enough to penetrate corporate systems and to unnerve corporate security."

In the eyes of the law, hacking and cracking are not always treated the same way. Depending upon the method of intrusion, the type of computer that was broken into, the hacker's intent, and the type and amount of damage, different statutes and penalties will apply. There are many ways to approach a discussion on hacking. In this article, we will structure the discussion on hacking techniques within the framework of the statutory elements to provide an understanding of how the different techniques trigger different statutes and penalties. [12] We begin with an overview of hacking and an explanation of several common hacking techniques. Then, we discuss the relevant criminal code that can be applied depending on the nature of the hack.

1.3 Why People Hack

- **Hacktivism**

In recent years, according to the Department of Justice's National Infrastructure Protection Center, there has been a rise in what has been dubbed "hacktivism." Hacktivists launch politically motivated attacks on public web pages or e-mail servers. The hacking groups and individuals, or Hacktivists, overload e-mail servers by sending massive amounts of e-mail to one address and hack into web sites to send a political message. [13] In 1999, for example, the homepages for the White House, the U.S. Department of the Interior, White Pride, the United States Senate, Greenpeace, and the Klu Klux Klan were attacked by political activists protesting the site's politics. One such group is called the "Electronic Disturbance Theater," which promotes civil disobedience on-line to raise awareness for its political agenda regarding the Zapatista movement in Mexico and other issues. Also, during the 1999 NATO conflict in Yugoslavia, hackers attacked web sites in NATO countries, including the United States, using virus-infected e-mail and other hacking techniques. On February 7, 2000, the official web site of the Austrian Freedom Party was hacked to protest the inclusion of Jörg Haider and his party into a coalition Austrian government. [14]

- **Employees**

According to a study conducted in 1999 by Michael G. Kessler & Associates Ltd., disgruntled employees are the greatest threat to a computer's security. Employees that steal confidential information and trade secrets account for thirty-five percent of the theft of proprietary information. In fact, data suggests that serious economic losses linked to computer abuse have been and continue to be attributed to current and former employees of the victimized organization rather than to outside hackers with modems. Internet Security Systems' Chris Klaus estimates that over eighty percent of the attacks on computer systems are committed by employees. [15] According to recent FBI assessments, disgruntled insiders are a principal source of computer crimes. Insiders do not need a great deal of knowledge about their target computers, because their inside knowledge of the victim's system allows them unrestricted access to cause damage to the system or to steal system data. A Computer Security Institute/FBI report notes that fifty-five percent of survey respondents reported malicious activity by insiders. Employees who exceed their authorized use and intentionally cause damage are just a liable as an outside hacker who intentionally causes damage. However, § 1030(a) of the CFAA does not criminalize damage caused by authorized persons and company insiders that was reckless or negligent.[16] Only outside non-authorized hackers are liable for any damage caused, whether it was negligent, reckless, or intentional.

- **Recreational Hackers**

"Recreational hackers" break into computer networks for the thrill of the challenge or for bragging rights in the hacking community. While hacking once required a fair amount of skill or computer knowledge, the recreational hacker today can now download attack scripts and protocols from the Internet and launch them against victim sites with little knowledge of the systems they are attacking. There are countless web sites on the Internet that provide "newbies" (inexperienced hackers, or "wannabes") with detailed instructions on hacking techniques and downloadable, do-it-yourself hacking tools. [17] In recent years, the hacker's attack tools have become more sophisticated and easier to use. For example, in 1999 hackers defaced the Anniston Army Depot, Lloyd's of London, and the U.S. Senate and Yahoo home pages to demonstrate to the hacking community their ability to hack into third-party servers and to highlight the servers' vulnerabilities.

- **Web Site Administrators and Web Pages**

It is usually considered a passive and harmless exercise to visit a web site. The user requests information and the server responds to the request by sending out packets of requested data back to the user's computer. However, web sites can also access a lot of hidden background information from the user. For example, Privacy.net has a web site that will show users all of the information that can be taken from their individual computer. [18] The remote web site can determine the following information about a visitor:

(a) The IP address the user is accessing the web site from;

(b) The number of prior visits to the web site, and the dates;

(c) The URL of the page that contained the link to get the user to the web site;

(d) The user's browser type and operating system and version;

(e) The user's screen resolution;

(f) Whether JavaScript and VBScript are enabled on the user's computer;

(g) How many web pages the user has visited in the current session;

(h) The local time and date; and

(i) FTP username and password, if there is one.

Privacy advocates have pressured web browser developers to address security concerns by enabling users to significantly enhance their privacy by adjusting the security level on their browsers. The extent of information that a web site can retrieve from a visitor without violating the CFAA is still uncertain. Section 1030(a) (C) proscribes the intentional access of a computer without, or in excess of authority to obtain information. When a person visits a web site, how much information has that person reasonably "authorized" the web site to obtain? This question may be answered by a court in one of the cases filed against Real Networks over its gathering of user data. It is also possible for a web programmer to enable a web page to send an e-mail to a predetermined address just by visiting the page through a JavaScript exploit in Netscape Navigator Versions 2.0 through 4.0b1. For example, if a person visits such a web site, hidden within the hypertext markup language ("HTML") is code that will cause the person's e-mail program to send an e-mail to the web site with the person's e-mail address in the "from" slot. [19] Theoretically, this exploit would allow a web site to collect all of the e-mails from persons who visit their web site. Internet Explorer and Netscape Navigator provide security warnings to users before they send the mail if the security level is set at a higher level.

1.4 Types of Attacks

In this age of automation and connectivity, almost all organizations are vulnerable to cybercrimes. Here are the most common targets for cybercrimes: [20]

- Military and Intelligence Attacks

Espionage agents may target military and intelligence computers. National security increasingly depends on computers. Computers store information ranging from the positioning of Air Force satellites to plans for troop deployment throughout the world. Espionage agents have learned that they can get what they want from computers.

- Business Attacks

Businesses may be the target of their competitors. The worldwide economic competition is becoming more and more fierce. Industrial espionages have become a growing threat because of the competition among national economies. Even "friendly" nations in the past have become our economic enemies.

- Financial Attacks

Professional criminals may target Banks and other financial organizations for financial gain. These days, our money may seem to be nothing but bits in a computer, numbers on a screen, and ink on an occasional bank statement. We tend to depend on more on computer to pay our bills and deposit our checks electronically. Theft and fraud cases are also increasingly done electronically as well.

- Terrorist Attacks

Terrorists may target any organization but especially government and utility company computers. Their purposes could be to paralyze the government or cause disastrous accidents.

- Grudge Attacks

Any company can be the target of its own employees or ex-employees. Similarly, universities may be the target of their students and former students. Their goals are for revenge.

- "Fun" Attacks

Any organization can be the target of crackers, sometimes they're seeking for the intellectual challenge, and sometimes they are professionals who may do it to be hired.

1.5 Types of Cyber Crimes and Prevention

Cybercrimes can be classified in many ways. You might divide them by who commits them and what their motivation might be. Or, you might divide these crimes by how they are committed. Here, I have chosen to divide computer attacks by the types of computer security that ought to prevent them. There are four types of computer security: [21]

- Physical security is protection of the physical building, computer, related equipment, and media (e.g., disks and tapes).
- Personnel security includes preventing computer crimes. That is to protect computer equipment and data from a variety of different types of people, including employees, vendors, contractors, professional criminals and others.
- Communications security is to protect software and data, especially when it passes from one computer to another computer across a network connection.
- Operations security is protection of the procedures used to prevent and detect security breaches, and the development of methods of prevention and detection.

2. Applicable Federal Criminal Statutes

2.1 User-level Hack

In the above scenario, Hacker has broken numerous laws. Hacker would be liable under 18 U.S.C. § 1029(a) which prohibits the knowing possession of a "telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services" with the intent to defraud. Hacker modified the modem and the lineman's handset, also known as a "beige box." Also, Hacker may be liable for a violation of 18 U.S.C. § 1343, which prohibits the intentional scheming to obtain "money or property by means of false or fraudulent pretenses" by "wire." In United States v. Freeman, the court held that the use of a "blue box" to bypass long distance charges is a taking of property under § 1343. [21] Hacker intentionally schemed to take "property" from the phone company or the victim whose phone line he tapped with the beige box. A violation of the subsection carries a prison term of not more than five years. One of the difficulties prosecutors face with many of the subsections under § 1030(a) is the requirement for "damage," which is defined as a loss aggregating at least $5,000 in value during a one year period. If only the text of a web page is altered in the attack, and the system is not "damaged," then meeting the $5,000 threshold may be difficult. The subsections that penalize only the "access" with no damage requirement, § 1030(a) [22], have an easier burden to meet. However, unless the hacker has broken into a computer that contains restricted data; has received information valued at more than $5,000; committed acts in the furtherance of another criminal or tortious act; or committed acts for commercial or private financial gain, the crime is only a misdemeanor. The three subsections that measure a threshold value of at least $5,000 for information, anything of value, or damage, are often difficult to prove in the type of hack explained above. If the web site that Hacker altered was located on a computer that is used by or for the government of the United States, then he could be liable for a misdemeanor violation of 18 U.S.C. § 1030(a) [23], which criminalizes the intentional access of such non-public computers. Hacker could be charged with a misdemeanor violation of 18 U.S.C. § 1030(a)(2)(C), which protects any information intentionally obtained from a protected computer. The "information" he obtained would be the web site owner's user name and password, along with any other information he may have viewed. The courts have held that "accessing" of information is not limited to taking the information. "Access" applies to the "intent" to access, not the "intent" to damage the protected computer. Viewing the information on the computer is considered "access." In other words, the mens rea for this crime is the intent to access the computer and there is no requirement for the actual transport of the information. Also, if Hacker defaced the web site with a "url redirect" to his own company's web site, then the charge could be bumped up to a felony for those acts considered for commercial advantage or private financial gain. Prosecutors may be able to charge Hacker with a violation of 18 U.S.C. § 1030(a) [24] if they can show he obtained something of value worth more than $5,000 or § 1030(a) [25] if they can show Hacker caused $5,000 or more damage. Under § 1030(a), merely viewing the information may not meet the statute's definition of "obtaining" information. Congress intended to punish the theft of information, not merely punish unauthorized access. In United States v. Czubinski, an Internal Revenue Service employee was charged with the unauthorized access of confidential income tax records. However, the court found that he only viewed the information and did not use the information in any manner. The First Circuit Court of Appeals held that the information obtained "is the showing of some additional end—to which the unauthorized access is a means—that is lacking here." However, in Hacker's case, he did use the user information he obtained as a means to the additional end of hacking the web site.

2.2 "Root-Access" Hack

In a "root access" hack, the potential for serious crime escalates because of the information that can be obtained, the damage that can be caused, and the value of data obtained. One way to analyze § 1030(a) is to first look at the type of computer that was targeted. If the computer was a federal government computer or a computer used by or for the federal government, then § 1030(a) could apply. [26] However, in the example above, Hacker most likely targeted a private ISP computer. The next step in the analysis is to determine if the hacker obtained information, obtained anything more than $5,000 in value, or damaged the protected computer. At the point when Hacker exploited a hole in the "sendmail" program, he did not obtain any information, nor did he arguably obtain anything of value, or do over $5,000 damage to the computer at this point. However, Hacker's next move, downloading the password files, is clearly obtaining information under 18 U.S.C. § 1030(a)(2)(C) and Hacker is liable for a misdemeanor unless the prosecution can show that the value exceeds $5,000, was for personal gain, or was committed in furtherance of another crime. Section 1030(a) [27] was meant to protect privacy where the value of the information, although lacking quantifiable monetary value, is nevertheless valuable in terms of privacy. Also, during congressional hearings on the CFAA, Senator Leahy noted that if: The information obtained is of minimal value, the penalty is only a misdemeanor. If, on the other hand, the offense is committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000, the penalty is a felony." If Hacker downloaded an entire batch of passwords, the prosecution may be able to argue that the aggregate value of the web site's security was more than $5,000, triggering § 1030(a) liability. Hacker's theft and possession of the credit card numbers is a violation of several statutes. First, Hacker could be liable under 15 U.S.C. § 1644(b), which proscribes the transport of stolen credit cards. In United States v. Callihan, the court held that the defendant didn't "transport" the credit card when he gave the credit card number over the phone. [28]

2.3 Malicious Code - Viruses, Worms and Trojans

The relevant and tested federal anti-virus statutes are 18 U.S.C. § 1030(a)(5)(A) and 18 U.S.C. § 1030(a)(2). If a virus is loaded into a computer by an e-mail attachment, and the author intended to cause "damage" to the recipient computer, then 18 U.S.C. § 1030(a)(5)(A) is applicable. Section 1030(a)(5)(A) prohibits the knowing transmission of a program, code, or command, that results in intentional damage without authorization to a protected computer. [29] If the virus author did not intend to cause damage to the computer, but rather the code accidentally damaged the computer as a result of the e-mail transmission, then as an alternative to the above statute, the author may be prosecuted under 18 U.S.C. § 1030(a)(5)(B) which covers reckless damage to a computer as a result of unauthorized and intentional access. The penalties for both § 1030(a)(5)(A) and (B) are the same -- up to five years in prison. A negligence standard would be considered too low for an intentional act, as provided by 18 U.S.C. § 1030(a)(5)(C), which is a misdemeanor. If the recipient of the virus forwards the virus on to another person via e-mail, then his mental state, or mens rea, will determine his culpability. If he is unaware that there is a virus, then he will not have the requisite mental state. If he is aware that there is a virus, then he could face § 1030(a)(5)(A) liability because he intentionally sent the virus. [30] However, if he was aware there was a virus attached to the e-mail, but he thought it was a harmless prank, for example, then his act could be reckless negligent; mental states that can trigger § 1030(a)(5) sanctions. There is a possibility that a virus may not reach federal jurisdiction if the virus was transmitted to a stand-alone computer by diskette. Section 1030(a)(5) covers only "protected computers," those that are "used in interstate or foreign commerce or communication." If the computer has a modem or a fax server loaded on it, then the prosecution could argue that it is a protected computer because it is a computer "which is used in interstate or foreign commerce or communication." However, if the virus is loaded onto a non-networked computer that, for example, is used in a small office for billing and the virus is placed on it by a diskette, a strong argument can be made that it is not a protected computer under federal jurisdiction because it is not a computer “which is used in interstate or foreign commerce or communication.” However, if the virus is loaded onto a computer and causes any of the enumerated damages in § 1030(e)(8), then action against the attacker might be brought under the statute.

3. Handling Computer Crime

3.1 Steps Taken After the Breach

The first step is to assess the situation. You need ask following question:

a. What is the severity level of the intrusion?

b. Who will be involved in the investigation?

c. Who is responsible for determining future actions?

The more such questions have been addressed in advance by the adoption of a written security policy, the more quickly and accurately the effects of the breach can be ameliorated. The second step is to repair damage and prevent recurrence. The organization may have to seek help from outside expertise. In the past, following a serious breach, the government is one choice for an organization when investigating computer crime. [31] With the number of computer crimes growing each year, the resources of most governmental agencies have been overburdened. They have insufficient personnel resources to handle the load and inadequate technical expertise to thoroughly research the cases. Private companies specializing in the field of network security now offer computer crime and forensic evidence services. Such specialists must have the specific knowledge base to efficiently and quickly complete investigations, with a background in recovery and analysis of computer forensics, formal investigations, and the relevant laws. Cybercrimes may be subject to the investigation of the NCCS (The FBI’s National Computer Crimes Squad):

1. Intrusions of the Public Switched Network (the telephone company).
2. Major computer network intrusions.
3. Network integrity violations.
4. Privacy violations
5. Industrial espionage.
6. Pirated computer software.
7. Other crimes where the computer is a major factor in committing the criminal offense.

3.2 Methods of Investigations

Initial assessment includes a careful examination and inventory of all potentially affected systems. The important first step is determining if a criminal still has control of any relevant computer. [32] If they are still logged on, an important decision is to decide whether to terminate the user. Leaving the intruder on the system may provide a better opportunity of profiling and ultimately identifying and apprehending the attacker. On the other hand, if investigator decides to lock the user out and disconnect the system from network they can often limit the damage to what the malicious user has already accomplished. As a general rule, an investigator should not let the attacker know that they are being disconnected or tracked due to unauthorized access. [33]

3.3 Recommendations Because of Laws

Cybercrimes can involve criminal activities that are traditional in nature, such as theft and fraud. However, Cybercrime is different from the traditional crime. Business and governments need legal protection and technical measures to protect themselves from those who would steal or destroy valuable information. Self-protection is not sufficient to make cyberspace a safe place to conduct business. The rule of law must be enforced. At present, the state of global legal protection against cybercrime is weak. There are following suggestions: [34]

i. Firms should secure their networked information. Laws to enforce property rights work only when property owners take reasonable steps to protect their property in the first place.
ii. Government should assure that their laws apply to cybercrimes. National governments remain the dominant authority for regulating criminal behavior in most places in the world.
iii. Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security. To be prosecuted across a border, an act must be a crime in each jurisdiction.

4. Conclusions

All those using the internet should meticulously follow a few basic tips to prevent cybercrime. Some of these key steps include:

- Strengthen your home network

It is highly recommended that you start with a strong encryption password and a virtual private network (VPN). A VPN can encrypt all traffic leaving your devices until it arrives at its destination. Even if cybercriminals manage to hack your communication line, they will not intercept anything but encrypted data. It is always a good idea to use a VPN whenever you use a public WiFi network.

- Use strong passwords

Never repeat your passwords on different sites and keep changing them regularly. Create complex passwords by combining at least 10 letters, symbols, and numbers. Using a password management application will help keep your passwords locked down.

- Keep your software updated

Updating your software is particularly important for your internet security software and operating systems. Very often, cybercriminals use known exploits, or flaws, in your software to access your system. Patching those flaws and exploits can prevent you from becoming a cybercrime target.

- Take necessary measures to protect yourself against identity theft

Identity theft takes place when someone illegally obtains your personal details through deception or fraud, typically for economic gain. You could be tricked into giving personal details over the internet, or a thief could steal your mail to access account information. That is why it is important to protect your personal information. A VPN can also help to safeguard the data you receive and send online, particularly when accessing the internet on public WiFi.

- Understand that identity theft can happen anywhere

You should always be on the smarter side and obtain all the knowledge required for protecting your identity even when traveling. Some of the things you can do to help keep criminals from getting your private information on the road include keeping your travel plans off social media networks and using a VPN when accessing the internet over your hotel’s WiFi network.

- Install a good antivirus program

Ensure that you have a robust antivirus in place to counter hacker attacks and other cybercrimes and also ensure safety. Comodo Free Antivirus Software has been specifically designed to drive away unexpected threats and offer all-around security. The main aim of this virus protection software is to safeguard data and protect it from unauthorized access. Comodo Free Antivirus is capable of automatically containing malicious or unknown files. It plays a vital role in preventing cybercrimes from damaging your computer or stealing your data.

References

[1]. Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[2]. *Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392.* ISBN 978-0-201-70719-9.

[3]. Halder, D., & Jaishankar, K. (2011) Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

[4]. *Steve Morgan (17 January 2016).* "Cyber Crime Costs Projected To Reach $2 Trillion by 2019". *Forbes.* Retrieved 22 September 2016.

[5]. Cybercrime costs global economy $445 billion a year: report". *Reuters. 9 June 2014.* Retrieved 17 June 2014.

[6]. Cybercrime— what are the costs to victims - North Denver News". *North Denver News. 17 January 2015*. Retrieved 16 May 2015.

[7]. *Lewis, James (February 2018).* "Economic Impact of Cybercrime - No Slowing Down"(PDF).

[8]. *Gordon, Sarah (25 July 2006).* "On the definition and classification of cybercrime"(PDF). Retrieved 14 January 2018.

[9]. *Laqueur, Walter; C., Smith; Spector, Michael (2002).* Cyberterrorism. *Facts on File. pp. 52–53.* ISBN 9781438110196.

[10]. Cybercriminals Need Shopping Money in 2017, Too! - SentinelOne". *sentinelone.com. 28 December 2016*. Retrieved 24 March 2017.

[11]. *Lepofsky, Ron.* "Cyberextortion by Denial-of-Service Attack" (PDF). *Archived from* the original (PDF) *on 6 July 2011.*

[12]. *Mohanta, Abhijit (6 December 2014).* "Latest Sony Pictures Breach : A Deadly Cyber Extortion". Retrieved 20 September 2015.

[13]. *Dennis Murphy (February 2010).* "War is War? The utility of cyberspace operations in the contemporary operational environment" (PDF). *Center for Strategic Leadership. Archived from* the original (PDF) *on 20 March 2012.*

[14]. Cyber Crime definition".

[15]. Save browsing". *google.*

[16]. 2011 U.S. Sentencing Guidelines Manual § 2G1.3(b)(3)". *28 October 2013.*

[17]. United States of America v. Neil Scott Kramer". Retrieved 23 October 2013.

[18]. "South Carolina". Retrieved 16 May 2015.

[19]. "1. In Connecticut, harassment by computer is now a crime". *Nerac Inc. 3 February 2003. Archived from* the original *on 10 April 2008.*

[20]. "Section 18.2-152.7:1". *Code of Virginia. Legislative Information System of Virginia*. Retrieved 27 November 2008.

[21]. Jump up to:a b Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, ABC-CLIO, 2010, pp. 91

[22]. "We talked to the opportunist imitator behind Silk Road 3.0". *7 November 2014*. Retrieved 4 October 2016.

[23]. Jump up to:a b c *Weitzer, Ronald (2003). Current Controversies in Criminology. Upper Saddle River, New Jersey: Pearson Education Press. p. 150.*

[24]. *David Mann And Mike Sutton (6 November 2011).* ">>Netcrime". *British Journal of Criminology. 38 (2): 201–229.* CiteSeerX 10.1.1.133.3861. doi*:*10.1093/oxfordjournals.bjc.a014232. Retrieved 10 November 2011.

[25]. "A walk on the dark side". *The Economist. 30 September 2007.*

[26]. "DHS: Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children". *Dhs.gov. 3 August 2011*. Retrieved 10 November 2011.

[27]. *DAVID K. LI (17 January 2012).* "Zappos cyber attack". *New York Post.*

[28]. *Salvador Rodriguez (6 June 2012).* "Like LinkedIn, eHarmony is hacked; 1.5 million passwords stolen". *Los Angeles Times.*

[29]. Rick Rothacker (12 October 2012). "Cyber attacks against Wells Fargo "significant," handled well: CFO". Reuters.

[30]. "AP Twitter Hack Falsely Claims Explosions at White House". Samantha Murphy. 23 April 2013. Retrieved 23 April 2013.

[31]. "Fake Tweet Erasing $136 Billion Shows Markets Need Humans". Bloomberg. 23 April 2013. Retrieved 23 April 2013.

[32].

Richet, Jean-Loup (2013). "From Young Hackers to Crackers". International Journal of Technology and Human Interaction. 9 (1).

[33]. *Richet, Jean-Loup (2011). "Adoption of deviant behavior and cybercrime 'Know how' diffusion". York Deviancy Conference.*

[34]. *Richet, Jean-Loup (2012). "How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry Into Cybercrime". 17th AIM Symposium.*