WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Crime

Chitra, Reshma Umair

Amity University Lucknow

ABSTRACT

The growth in cybercrime has emerged as an urgent issue around the world, impacting people, institutions, and governments equally. With the advancement of technology and our increasing dependency on online platforms, cybercriminals are taking advantage of loopholes to indulge in a variety of crimes. These range from identity theft, where individual information is hacked and used for nefarious ends; financial scams, which include unauthorized transactions and fake schemes; and data breaches, where sensitive data is accessed without permission. Investigation and prosecution of cybercrime by law enforcement agencies are very challenging. The anonymous nature of the internet and the application of advanced technologies complicate the identification of perpetrators. In addition, cybercrime frequently transcends borders, necessitating international cooperation to fight effectively. In spite of all these challenges, there are steps that can be taken to avoid and reduce cybercrime. Creating awareness on best practices in cybersecurity is important, as is putting in place technology solutions like firewalls and encryption. Global collaboration among law enforcement agencies is also important in information sharing and coordinating efforts to fight cybercrime.

In summary, the growth of cybercrime calls for an all-encompassing strategy to mitigate the threats and challenges that it presents. Through the knowledge of the forms of cybercrime, the effects on society, and the challenges to law enforcement, we can strive to make the digital world safer. This calls for a collective effort by individuals, organizations, and governments to make cybersecurity a priority and take active steps towards prevention and mitigation of cybercrime.

Keyword: cybercrime, hacking, internet fraud, cyberterrorism, digital arrest, ransomware, cyber law and regulations.

Introduction

New technologies give rise to new opportunities for crime but relatively few new forms of crime. What separates cybercrime from other forms of criminality? Clearly, one distinction is the employment of the digital computer, but technology itself is not enough for any separation that may occur between various areas of criminal enterprise. There is no need for a computer in order for fraud to be carried out, to traffic in child pornography and intellectual property, to steal an identity, or to invade someone's privacy. All such activities predated the ubiquity of the "cyber" prefix. Cybercrime, particularly using the Internet, is an extension of current criminal activity with some new illegal activities.

Most computer crime is an assault on information regarding persons, corporations, or governments. While the assaults are not occurring on a physical body, they are occurring on the personal or corporate virtual body, that is, the collection of informational characteristics that delineate individuals and institutions on the Internet. That is, in the age of the internet our virtual selves are ubiquitous aspects of daily life: we are a collection of numbers and identifiers across various computer databases controlled by governments and corporations. Cybercrime underscores the centrality of networked computers in our lives, as well as the instability of such seemingly firm facts as individual identity.

A key feature of cybercrime is its nonlocal nature: events can take place in jurisdictions far apart. This is a serious challenge for law enforcement because hitherto local or even national crimes now need international coordination. For instance, if someone uses child pornography on a computer within a nation where child pornography is not prohibited, is that someone committing an offense in a state where such pornography is illegal? Where precisely is cybercrime being committed? Cyberspace is merely an enriched form of the area where a telephone call occurs, somewhere in between the two individuals who are communicating. Being a global network, the Internet provides criminals with several places to hide in the physical world and also within the network. But just as people who move on the ground leave traces that a good tracker can use, cybercriminals leave hints about their identity and location even though they try to cover them up. To pursue such leads beyond national borders, however, international cybercrime agreements need to be ratified.

TYPES OF CYBER CRIME

In 2000, the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders classified cybercrimes into five categories: unauthorized access, damage to computer data or programs, sabotage to hinder the functioning of a computer system or network, unauthorized interception

of data within a system or network, and computer espionage.[1]Cybercrime takes on a gamut of actions. On the one hand, there are offences involving basic invasions of business or individual privacy, including intrusions into the integrity of data stored in cyber repositories and applications of illegally sourced digital data for harassing, harming, or black-mailing an enterprise or a person. The new cyber capabilities have provoked heated discussions. Pegasus spyware, for example, to its developer, the Israeli cyber-intelligence company NSO Group, is marketed to government security and law enforcement agencies only and only in order to assist in rescue missions and the fight against criminals like money launderers, sex- and drug-traffickers, and terrorists. However, the smartphone-based spyware, which can download sensitive information without manifestly leaving a trace of its operation, has been globally employed surreptitiously by governments to monitor politicians, government officials, human rights activists, dissidents, and reporters. It was even utilized to monitor Saudi journalist and U.S. resident Jamal Khashoggi months prior to his murder and dismemberment by Saudi agents in October 2018. Also on this end of the spectrum is the increasing crime of identity theft.

Transaction-based crimes like fraud, child pornography trafficking, digital piracy, money laundering, and counterfeiting fall somewhere in the middle of the spectrum. These are targeted crimes with targeted victims, but the perpetrator conceals himself in the relative anonymity of the Internet. A second component of this kind of crime is the manipulation of data by individuals in corporations or government bureaucracies for profit or political purposes. On the other side of the coin are crimes that attempt to interfere with the actual functioning of the Internet.

These include everything from spam, hacking, and denial of service attacks on particular sites to cyberterrorism—that is, the exploitation of the Internet to create public disturbances and even kill. Cyberterrorism targets the employment of the Internet by nonstate actors to influence a country's economic and technological infrastructure. Public consciousness of the menace of cyberterrorism has increased exponentially since the September 11 attacks of 2001.

-> Identity theft and invasion of privacy

Cybercrime impacts both a virtual body and a real one, but differently. This is best illustrated in the case of identity theft. In the United States, for instance, one does not possess an official identity card but rather a Social Security number that has been a de facto identification number for a long time. Taxes are levied based on every citizen's Social Security number, and several private organizations employ the number to monitor their workers, students, and patients. Possession of a person's Social Security number provides the possibility of collecting all the papers pertaining to the individual's citizenship—i.e., to steal his identity. Even pilfered credit card details can be utilized to rebuild a person's identity. When thieves steal a company's credit card records, they create two different impacts. They first steal digital data about people that is valuable in numerous ways. For instance, they may use the credit card data to accumulate enormous bills, causing the credit card companies to incur significant losses, or they may sell the data to others who can utilize it in the same manner. Second, they may employ their own credit card names and numbers to establish other criminals' new identities. As an illustration, a criminal would call the card's issuing bank if he stolen a credit card and request an address change for the account to his own. Then, the criminal can obtain a passport or driver's license with his picture but the name of the victim. With a driver's license, the offender can readily obtain a new Social Security card; it is then easy to open bank accounts and take out loans—all on the victim's credit history and background. The original card owner may not even know this until the debt is so large that the bank calls the account owner. Only then does the identity theft become apparent. While identity theft occurs in most nations, researchers and law enforcement are plagued with a lack of stats and info regarding the crime globally. Cybercrime is undoubtedly, however, an international issue.

->Internet Fraud

Warren Buffett has stated that cybercrime is the "number one problem with mankind",[2] and that it "poses real risks to humanity"[3]. Cybercrime affects both a virtual body and a corporeal one but in a different way. The best example can be seen with the case of identity theft. In the US, for example, one doesn't have an official identity card but a Social Security number which has been de facto identification number for decades. Taxes are imposed on the basis of each citizen's Social Security number, and a number of private agencies use the number to track their employees, students, and patients. Having someone's Social Security number offers the potential for gathering all the documents related to the individual's citizenship—i.e., to steal his identity. Even stolen credit card information can be used to reconstruct an individual's identity. When burglars steal a business's credit card records, they have two different effects. They first steal computer information about individuals that is worth a lot in many different ways. For example, they can use the credit card information to rack up gigantic bills, which the credit card companies then lose money on, or they can sell the information to others who can use it the same way. Second, they can use their own credit card names and numbers to create new identities for other criminals. To illustrate, a criminal would place a call to the issuing bank of the card if he swiped a credit card and have an address changed on the account to his. Then, the criminal can procure a passport or driver's license with his image but the victim's name. With a driver's license, the criminal can easily get a new Social Security card; from there, it is simple to open banking accounts and borrow loans—all on the victim's credit record and history. The owner of the original card might not even be aware of this until the debt is so huge that the bank phones the owner of the account. Only then does the identity theft reveal itself. Though identity theft does take place across the majority of countries, stats and information and are plagued regarding the crime of the world's law enforcement. Cybercrime, however, certainly is a world problem.

---

[1] Sukhai, Nataliya B. (8 October 2004). "Hacking and cybercrime". *Proceedings of the 1st annual conference on Information security curriculum development*. New York, NY, USA: ACM. pp. 128–132. doi:10.1145/1059524.1059553. ISBN 1-59593-048-5. S2CID 46562809. Archived from the original on 18 July 2024. Retrieved 10 December 2023

[2] "BUFFETT: This is 'the number one problem with mankind'". *Business Insider*. Archived from the original on 9 June 2023. Retrieved 17 May 2021.

[3] "Warren Buffett: 'Cyber poses real risks to humanity'". *finance.yahoo.com*. 30 April 2019. Archived from the original on 2 June 2023. Retrieved 17 May 2021.

->Hacking

While invading privacy to find cybercrime is effective when the crimes involve stealing and exploiting information, from credit card numbers and personal information to file sharing of commodities—music, video, or child pornography—what about crimes that seek to destroy the very functionality of the machines that comprise the network? Hacking's actual story dates to the 1950s, however, when phreaks ("phone freaks") first took over pieces of the global phone networks and were placing unauthorized long-distance calls, establishing special "party lines" for other phreaks. With the explosion of computer BBSs in the late 1970s, the underground phreaking culture started to form into quasi-structured groups of hackers who graduated from the telephone network to "hacking" corporate and government computer network systems.

Although the term hacker predates computers and was used as early as the mid-1950s in connection with electronic hobbyists, the first recorded instance of its use in connection with computer programmers who were adept at writing, or "hacking," computer code seems to have been in a 1963 article in a student newspaper at the Massachusetts Institute of Technology (MIT). Following the first computer systems being connected to several users over telephone lines in the early 1960s, hacker began to mean those who accessed computer networks without permission from either another computer network or, as personal computers were developed, from their own computer systems. While it is beyond the scope of this article to describe hacker culture, the majority of hackers have not been criminals in the sense of being vandals or of looking for illicit financial gain. Rather, the majority have been young, intellectually curious individuals; many of these individuals have become computer security architects. But as some hackers looked for fame among their peers, their actions resulted in well-defined crimes. Specifically, hackers started invading computer systems and then boasting to each other about their actions, exchanging stolen documents as trophies to validate their claims. These actions escalated as hackers not only invaded but sometimes took over government and corporate computer networks.

->Computer viruses

The intentional spread of harmful computer viruses is another form of cybercrime. In reality, it was the crime of choice for the first individual to be convicted under the Computer Fraud and Abuse Act of 1986 in the United States. On November 2, 1988, Cornell University computer science student Robert Morris released a software "worm" onto the Internet from MIT (as a visitor on campus, he wished to be unknown). The worm was a test self-replicating and propagating computer program that exploited weaknesses in some e-mail protocols. Because of an error in its programming, instead of sending only copies of itself to other computers, this software continued to duplicate itself on every infected machine, consuming all the available computer memory. Prior to finding a fix, the worm had disabled about 6,000 computers (an estimated tenth of the Internet). Though Morris's worm took time and millions of dollars to be fixed, there were few business implications of the event, because the Internet wasn't yet established as a feature of economic activity. That Morris's father directed computer security for the U.S. National Security Agency directed the press to approach the event as more of a high-tech Oedipal tragedy than as a harbinger of things to come. Since then, increasingly dangerous viruses have been concocted by anarchists and misfits from places as varied as the United States, Bulgaria, Pakistan, and the Philippines.

->Digital Arrest

Digital arrest is a type of online scam where the perpetrator pretends to be a law enforcement official to cheat victims. The common practice is contacting someone on the phone, falsely reporting they are involved in criminal activity regarding a package of illicit products, drugs, fake documents, or other banned items. In other versions, the scammers target the victim's friends or family members, claiming the victim is in custody for criminal activity or an accident. Victims are then manipulated into staying on camera and keeping to themselves, while the fraudsters gather personal and financial data under the pretext of an official investigation, eventually transferring the victim's funds to money mule accounts.

To identify and avoid the fraud, beware of unsolicited phone calls from alleged law enforcement officials asking for instant payments or individual information. Official law enforcement authorities hardly make investigations in such a way. Check the identity of the caller independently by contacting the concerned agency directly through formal means. Keep in mind, the government agencies never digitally arrest anyone, it's not allowed.

->Cyberterrorism

The term *cyberterrorism* refers to acts of terrorism committed through the use of cyberspace or computer resources.[4] Cyberterrorism is the commission of acts of terrorism by means of cyberspace or computer assets. Computer network and personal computer disruption acts by viruses, worms, phishing, malicious software, hardware, or programming scripts are all forms of cyberterrorism.

Government officials and information technology (IT) security professionals have reported a large rise in network issues and server scams since 2001. In the United States there is a growing concern from organizations like the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA).

->Ransomware

Ransomware is a type of malware used in cyberextortion to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid. Ransomware is a global issue: 153 countries were affected by this type of attack in 2024[5]. Ransomware is a form of malware employed in cyberextortion to limit access to files, at times demanding permanent data destruction unless a ransom is paid. Ransomware is an international problem: 153 countries were hit by this kind of attack in 2024. The number of attacks is increasing every day, and in 2024 there were 5,263 attacks. And this is the number of significant and successful attacks with serious damage, the number of all attacks and attempts to attack, including in automatic mode in 2021 was more

[4] Parker D (1983) *Fighting Computer Crime,* U.S.: Charles Scribner's Sons.
[5] *"Ransomware Trends 2024: Insights for Global Cybersecurity Readiness". www.cyberpeace.org. Retrieved 15 April 2025*

than 300 million attacks in the world. Almost a third of the significant attacks (1,424) in 2024 hit industrial enterprises (up 15% to 2023), hitting critical infrastructure and services, leading to significant losses. In some instances, attacks on healthcare facilities also left human victims. Between 2016 and 2021 ransomware resulted in the deaths of between 42 and 67 Medicare patients due to the treatment challenges caused, in 2024 an attack on UK pathology provider Synovus caused thousands of surgeries and appointments to be cancelled. Ransom demands in attacks are also constantly and significantly rising. According to the 2022 Unit 42 Ransomware Threat Report, in 2021 the average ransom asked in Norton cases was $2.2 million (an increase of 144%), and victims whose personal data found its way into the information dumps of the dark web increased by 85%. Losses in 2021 and 2022 amount to almost $400 million. The average ransom payment in 2024 is $5.2 million, the two largest being demanded from healthcare organizations - $100 million from India's Regional Cancer Centre (RCC) and $50 million from Synovus.

Cybersex trafficking

Cybersex trafficking is the transportation of victims for such purposes as coerced prostitution or the live streaming of coerced sexual acts or rape on webcam.[6] Cybersex trafficking involves the movement of victims for the purpose of coerced prostitution or streaming live coerced sexual activity or rape on webcam. Victims are kidnapped, threatened, or tricked and moved to "cybersex dens". The dens can be anywhere where the cybersex traffickers have a computer, tablet, or phone with internet access. Perpetrators utilize social media networks, video conferences, dating sites, online chat rooms, apps, dark web sites, and other sites. They employ online payment platforms and cryptocurrencies to conceal their identities. Millions of reports of cybersex crimes are submitted to authorities every year. New laws and police practices must be implemented to fight this form of cybercrime.

There are a total of 6.3 million cybersex trafficking victims estimated, based on a recent International Labour Organization report. This figure comprises approximately 1.7 million child victims. One example of cybersex trafficking is the 2018–2020 Nth room case in South Korea.

Cyber Law

Cyber law or information technology law encompasses the study of issues pertaining to the use of the internet electronic devices, for communication and computer networks. Cyber law deals with issues like agreements, cybercrimes, protection of data, privacy rights, jurisdiction in cyberspace and legal principles in the digital space. Its relevance is in the protection of people's and companies' rights to have a safe online environment.

Cyber law in India

In the era of India's fast growth, cyber law has emerged as a vital part of the legal system. It encompasses various legal issues in the digital world concerning the use of electronic devices, computer networks and the growing usage of social media. It is crucial in safeguarding the rights of individuals and organizations in the world providing a secure and trustworthy online environment.

Information Technology Act, 2000 (IT Act):

The IT Act of India is the pillar of cyber law and addresses categories of cybercrimes, lays down penalties for crimes related to unauthorized gaining entry into computer systems pilfering information, hacking, cyber terrorism and dissemination of unsuitable or offensive content on the internet.

The Digital Personal Data Protection Act, 2023 (DPDPA):

The DPDPA focuses on regulating data collection, processing, storage and usage while bolstering privacy safeguards with an emphasis on securing minor consent through the permission of guardian.

Conclusion

In summary, cybercrime is a complex and constantly changing threat that requires a unified and multi-pronged strategy to counter. With more and more reliance on digital technologies in every sphere of life, the threat of cybercrime expands, and the effects can be tremendous. To tackle cybercrime effectively, strong cybersecurity systems need to be implemented, laws and policies need to be formulated and enforced, and global cooperation needs to be encouraged. By so doing, we can safeguard our digital wealth, secure sensitive data, and facilitate trust in the digital economy. A safer and more secure digital world ultimately calls for an all-hands-on-deck approach by individuals, organizations, and governments to remain informed, adjust to evolving threats, and cooperate to avoid and reduce the risk of cybercrime. By putting cybersecurity first and proactively working to combat these dangers, we can create a more secure and robust digital future.

Data is a central part of the perpetration of most cybercrimes and susceptibility to cybercrime. Although data gives users of it (people, private businesses, organizations, and governments) countless opportunities, these advantages can be (and have been) used by some for criminal ends. In particular, data gathering, storage, processing, and dissemination both facilitate much cybercrime and the massive gathering, storage, utilization, and dispersion of data without users' effective informed choice and consent and requisite legal and security safeguards. Furthermore, aggregation, processing, and transmission of data are at magnitudes governments and organizations are not equipped to handle, posing a host of cybersecurity threats. Privacy, data protection, and systems, networks, and data security are mutually dependent. In light of that, in order to defend against cybercrime, there is a need for security that will guard data and user's privacy.

[6] *Carback, Joshua T. (2018). "Cybersex Trafficking: Toward a More Effective Prosecutorial Response". Criminal Law Bulletin.* ***54*** *(1): 64–183.* p. 64.