RESEARCH REVIEW JOURNALS
Volume-04
Issue-06
June-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Technology Influence the Evolution of Cyber Crime

Sandeep Kumar

Research Scholar Law, Kurukshetra University Kurukshetra

ARTICLE DETAILS

Article History
Published Online: 04 June 2019

Keywords
Cyber Crime, Terrorism, Technology

ABSTRACT

We are well ware with different-different form of Terrorism in the world. Till now we have heard about terrorism from Bomb Blast and Many other ways but now a new terrorist has come which is computer based terrorism. Here is the evolution of Cyber Crime in the world with the dependency of human being on computer. This kind of terrorism can destroy all the human based system in a spam. Today, cyber crime has caused lot of damages to individuals, organizations and even the government. Cybercrime detection methods and classification methods have come up with varying levels of success for preventing and protecting data from such attacks. Several laws and methods have been introduced in order to prevent cybercrime and the penalties are laid down to the criminals. However, the study shows that there are many countries facing this problem even today and United States of America is leading with maximum damage due to the cybercrimes over the years. With the technology increasing, criminals don't have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their lap. Their weapons aren't guns anymore; they attack with mouse cursors and passwords.

1. Introduction

Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy. Generically, cyber law is referred to as the Law of the Internet.Cyber law is any law that applies to the internet and internet-related technologies. Cyber law is one of the newest areas of the legal system. This is because internet technology develops at such a rapid pace. Cyber law provides legal protections to people using the internet. This includes both businesses and everyday citizens. Understanding cyber law is of the utmost importance to anyone who uses the internet. Cyber Law has also been referred to as the "law of the internet."Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.IT law does not consist a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a key element of IT law. The area of software licence is controversial and still evolving in Europe and elsewhere.

All too often, Internet crime is taken as a 'white-collar' crime and the perpetrators are treated as people with errant behaviour rather than as criminals. As far as successful convictions go, in India, only the case of a call centre employee in Noida who used the credit card number of an overseas customer to buy himself a personal computer, comes to mind. In the Delhi MMS case, Baazee.com CEO Avnish Bajaj was arrested, Some copies of the digital clip featuring the sexual activities of two Delhi school students had been auctioned through his site. There was much hullabaloo, and even high-power interventions from US authorities on behalf of the CEO, who is an American citizen. The matter is now before the courts.

Last year, the FBI's Operation Web Snare led to the arrests or convictions of more than 150 individuals. Last week, a teenager in South Wales, UK, who duped more than 100 people into paying tens of thousands of sterling pounds for non-existent goods as part of a deceptively simple fraud on eBay was sentenced to 12 months' detention and training. While in the West, securing e-commerce is a priority, in India, pornography has been taken very seriously, especially under Section 67 of the IT Act. Anyone caught surfing porn sites or storing obscene images or text in their computer faces five years in prison and a fine of Rs 1 lakh for the first conviction, The second time invites double that punishment. However, as expected, pornographic sites are a major draw for many Internet users, periodic heavy-handed raids by the police on cyber cafés notwithstanding. As Nitya, Ramakrishnan points out: "The police targets those who have no power to put something on the Net. Police, as such. is not the answer to moderating content on the Net. Some kind of non-coercive supervisory mechanism is needed, it would include self moderation and parental/peer supervision.

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behavior alongside some novel illegal activities.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age

RRIJM 2015, All Rights Reserved

our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

In Minority Report, the police use psychic technology to arrest and convict murderers even before they commit a crime. Since the Hollywood movie is a work of science fiction, set in Washington DC in 2054, we have no way of finding out if such a technology will exist. As of now, one is only too aware of computers being used by criminals for nefarious activities. It was only last month that 12 persons were arrested in Pune for allegedly transferring Rs 1.5 crore from a multinational bank to their own accounts, opened under fictitious names. Before that a medical student had been arrested in Bangalore. He had defrauded people by using a website to advertise the sale of inexpensive laptops. He received the payments but did not deliver the laptops. There is no doubt that criminals are exploiting advances in cyber technology to commit crimes, both small and big. In Kurukshetra, a zonal Manager of a reputed organization being and cheated by Delhi based Company on Phone Call and told him to deposit 7500 Rs. in their A/C but the products they send are not actual as they have talked. In many other Cases use of Credit Cards and Debit Cards of other Person is very commonly Cyber Criminal.

The term cybercrime is loosely used to describe “any crime committed using a computer and the Internet to steal a person’s identity or sell contraband or stalk victims or disrupt operations with malevolent program.” In the Pune cyber crime case, the employees of a call centre got the Personal Information Numbers of the customers and through Internet banking transferred the amounts into their personal accounts. The bank certainly showed “lack of due diligence,” and the call centre employees are liable under Section 66 of the ITA-2000since “information residing inside a computer” was affected injuriously.The IT Act 2000, enacted on June 9 that year, was one of the early legislations against cybercrime. With India emerging as a major IT destination for outsourcing, the Act should be constantly updated to keep up pace with the changing technology. As Nitya Ramakrishnan, a lawyer, points out:“The IT Act gives draconian powers to the police to seize and enter. In the virtual world of IT, data and responsibility are difficult to demarcate and given this nebulous nature, policing is either excessive or no action is taken. The law is a step behind technology and it will have to be intelligently culled and applied to various situations. There has to be an internationally accepted standard affixing responsibility of cyber data.” A major lacuna in the Act is that Intellectual property issues have not been adequately touched and even the rightto privacy has not been dealt with,” says Ali Naqvi, another Delhi- based lawyer.“There is need to define ‘access’ more clearly and the sanctity of ‘click- wrap contracts,’ that appear during the setup of a software program or online service and that requires the user to click a button to agree to the terms of the license, is still not clear. Also there is too much power given to the police, as the police can arrest someone even if they believe that a crime is about to be committed.” Incidentally, the Cyber Appellate Tribunal envisioned in the Act has not been setup. While the main fear of cybercrime is with regard to credit card fraud, it actually forms only one of the many ways in which criminals use computers and Internet. Overall, the police has been able to solve cases of cybercrime, especially those concerning BPO industries, and Nasscom has come up with the plan of creating a list of all BPO employees, to track their where about even as they change jobs. This should help prevent crimes.

A simple and common computer-related crime which involves changing data prior to or during input to a computer. Data can be changed by anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transporting computer data. Minimize the risk of diddling by applying internal security controls.A Trojan horse involves the placement of unwanted computer instructions in a program so that the host computer will perform some and undesired/unauthorized function. Minimize the risk of attack by a Trojan Horse by implementing security control measures for all incoming data containing hidden content.A logic bomb is a computer program executed at a specific time to cause damage to computer programs or data. Logic Bombs often enter a computer system using the Trojan horse method, but differ because their presence is detected only after the bomb “blows up.” Minimize the risk by using security methods that verify the system for inappropriate content.Impersonation in the workplace may be accomplished as easily as taking an authorized user’s place at an unattended terminal which has not been logged off. However, in impersonation usually requires that the intruder has access to two or three pieces of information:

- User I.D. or account number;
- Password of the authorized user.
- A dial port number (ie. Computer’s telephone number), if access is attempted from a remote location.

Minimize the risk of unauthorized access by implementing security measures and password maintenance. Passwords should be of adequatelength to maximize security and maintenance systems should force a chance of passwords at regular intervals.Impact of Cybercrime is Technological developments appear in a row. The trend shows that internet technology is used to help work and Conduct business activities. This activity includes students, students, employees, and the upper classes. Cyber technology is a system that is implemented to facilitate fast and instant relationships. If the system does not have a defense, then this will be a threat and target from wild parties. The use of information technology is to provide benefits to the community also has the opportunity to be misused to commit crime both ordinary and professional which has an impact on massive financial losses. Negative impacts can lead to the collapse of the social order system, the paralysis of the country's economy, the weakness of the defense system and can also be used for terror devices. Cybercrime is a crime that is most detrimental to state finances. Each country has established several laws to regulate the law of cybercrime. Education in information technology and national defense has been included in the curriculum in universities. It will explain the impact caused by cybercrime. Introduction various types of information technology in digital form are popular, and in demand by the world community, the internet is one of them. With the internet, there are various kinds of applications that can be used by computer users such as to communicate, find

RRIJM 2015, All Rights Reserved

news and do business. Software development triggers cybercrime. Initially, the software used to commit crimes is software for system repair. In repairing the system, software must look for errors in the system. This software is converted to look for weaknesses in the system to be hacked so that when the system experiences weakness, this tool will work well. The development of information and communication technology certainly adds to the trend of world technological development with all forms of human creativity. The development of technology extends to various fields where people can quickly obtain the information anytime. Companies in doing business depend a lot on banks because they have an online transaction system. Without realizing it, online transactions can cause enormous losses for the business person. The mistake that often occurs is neglect of maintaining privacy and account. Business can also be done anywhere as long as there is internet access. Even important information is stored on a computer and can be accessed anywhere because the data is stored online. It is also what causes cybercrime. The bank also runs the banking process using internet access. For example, ATM has its network that can be accessed by customers anywhere. If cybercrime perpetrators can enter the ATM system, funds owned by customers will be lost one by one. The use of computers will also be disrupted so that the banking process cannot run smoothly. Information related to customer data can be misused.

By its very nature, cybercrime must evolve to survive. Not only are cyber security experts constantly working to close hacking loopholes and prevent zero-day events, but technology itself is always evolving. This means cybercriminals are constantly creating new attacks to fit new trends, while tweaking existing attacks to avoid detection. To understand how cybercrime might evolve in the future, we look back to understand how it emerged in the past.

Cybercrime's origins are rooted in telecommunications, with "hacker" culture as we know it today originating from "phone phreaking," which peaked in the 1970s. Phreaking was the practice of exploiting hardware and frequency vulnerabilities in a telephone network, often for the purpose of receiving free or reduced telephone rates. As landline networks became more security savvy—and then fell out of favor—phone phreaking became less and less common. But it hasn't been phased out completely. In 2018, a phone phreaker staged a series of creepy attacks in New York City Wi-Fi kiosks, reminding us that the phreaks may have been forgotten, but they are certainly not gone.

Cybercrime as we currently think of it began on November 2, 1988 when Robert Tappan Morris unleashed the Morris Worm upon the world. Much like Dr. Frankenstein, Morris did not understand what his creation was capable of. This type of self-replicating program had never been seen before outside of a research lab, and the worm quickly transformed itself into the world's first large-scale distributed denial of service (DDoS) attack. Computers worldwide were overwhelmed by the program and servers ground to a halt. Although Morris quickly released the protocol for shutting the program down, the damage had been done. In 1989, Morris was the first to be prosecuted and charged in violation of the Computer Fraud and Abuse Act.

Although you may get general consensus among criminal defense lawyers that cybercrime has been the most recent radical change in criminal behavior, it is unlikely you'll receive the same consensus when it came to defining what cybercrime actually was. Nevertheless, broad consensus would most probably agree that cybercrime is a term of language used to describe "criminal activity that utilizes an element of a computer or computer network".

Thus, essentially there are two separate and distinct elements to cybercrime. On the one hand you have an element of exploiting weaknesses in the computer operating system or computer network. On the other hand you have an element of exploiting social fabric of a computer network, whereby a criminal makes use of the computer network to infiltrate the trust of other users of that computer network for profit or gain. Although these different elements of what constitute cybercrime may not seem overly important, they do have an impact when you look at the evolution and development of cybercrime.

2. Pre-2000 cybercrime

prior to the turn of the millennium large scale cybercrime centered on or around one-man operated criminals exploiting the weaknesses in the computer operating system or computer network. In most cases these crimes were committed by computer nerds who felt challenged to prove that they could beat the system. We coined the term hacker for just such a nerd, but rarely was there a financial gain element to the criminal behavior. While a great deal of financial damage could actually result, not to mention the potential for the security risks that resulted, this one-man band criminal lacked the motive and intent of traditional criminal gangs. In short, cybercrime was infantile and largely seen as a practical joke or game by those who committed it. Criminal defense tactics at this time was also largely based on the fact that no real intentional damage was done and, in a large number of cases, the penalty for the crime was showing how the computer system had been hacked by the hacker.

3. Post-2000 cybercrime

once we had all got over the fact that there was no millennium bug after all (probably the biggest cybercrime hoax of all time), cyber criminal had organised and focused their attention elsewhere. Yes, the geek element of hacking still existed – as still does today – but now hardened criminal gangs had worked out that the Internet was a safe domain, with much less risk, with which to operate and generate large profits.

In short, criminal gangs had introduced a professional element into the world of cybercrime. No longer were we looking at geeky exploitation of weaknesses in computer operating/networking systems, things had now developed to criminal gangs making use of computer networks to infiltrate and take advantage of the trust of other users of that computer network for huge financial gain. Because of this radical change in the nature of cyber criminal activity, law makers and criminal defense lawyers began to see developments which reflected these changes. Primarily these included new cyber crimes, such as:

* Cyber-extortion – where criminal gangs threatened to close down internet-based businesses if protection money

RRIJM 2015, All Rights Reserved

was not paid. Worse still, threats can also be made to infiltrate the businesses security system to access financial or personal information stored therein that may then be used for financial gain

* information theft – similar to that set-out above, only no prior approach is made to try and extort protection money and a computer network is infiltrated with the purpose of obtaining information relating to the users, whether they be an individual user of business

* Fraud – fraud has many guises on the internet, from the famous e-mails promising millions in advance fees to the sale of unmarketable quality goods. What is usually fairly consistent is an unsolicited e-mail approach by the fraudster to their victim.

* Identity theft – identity theft is where the cyber criminal steals their victims identity and then transacts, usually via the Internet in the name of the victim. More often than not this will include an element of credit card fraud.

* Exploitation of children, etc – unfortunately many view the act of cybercrime as either harmless fun (such as hacking) or for financial gain (such as credit card fraud). However, there is also a very real and extremely nasty side to cyber crime – taking advantage of weaker members of our society. Almost weekly we now hear of cyber criminal gangs who have been caught with child pornography.

* Intellectual property theft – strangely many computer network users do not see the illegal downloading of software and intellectual property as constituting a criminal act. In fact it is anything but. Billions of dollars are being lost each year on illegal software and intellectual property downloads that are putting sever financial constraints on the companies that manufacture these products, many of whom are young start-ups themselves. Nevertheless, unlike other forms of cyber crimes, governments have been quick to respond to the actions of those who illegally download movies, music or software from the Internet and so, many argue, criminal defense procedures against such persons are probably the most successful and front-line of all.

* phishing and vishing – both phishing and the more recent vishing is obtaining financial information, such as bank account records or credit card details, by sending what look like authentic messages to the recipient informing them they need to comply with certain procedures to reactivate their account. Once the information has been obtained, the criminal then defrauds the victim.

References

[1]. Dainik Tribune 12/09/1999 (lakshmi prashad pant.)
[2]. The Tribune 14/05/2005 (Roopinder Singh)
[3]. Royal Canadian Mounted Police
[4]. LaFave, Wayne R., Jerold H. Israel, Nancy J. King, and Orin S. Kerr. (2015). Criminal Procedure, 4th edition. Thomson Reuters.
[5]. Maras, Marie-Helen. (2014). Computer Forensics: Cybercriminals, Laws and Evidence, Second edition. Jones and Bartlett.
[6]. Maras, Marie-Helen. (2016). Cyber criminology. Oxford University Press.
[7]. Maras, Marie-Helen. Cyber law and Cyber liberties. Oxford
[8]. University Press, forthcoming, 2020.
[9]. Miles, Tom. (2018). U.N. investigators cite Facebook role in Myanmar
[10]. Crisis. Reuters, March 12, 2018.
[11]. Odhiambo, Sharon Anyango. (2017). Internet shutdowns during elections. Africa up Close, Wilson Center.
[12]. Ohlin, Jens David. (2013). Targeting and the Concept of Intent. Michigan Journal of International Law, Vol. 35, 79-130.
[13]. Rahman, Rizal. (2012). Legal jurisdiction over malware-related crimes:
[14]. From theories of jurisdiction to solid practical application. Computer Law & Security Review 28 (2012) 403-415.
[15]. Sandle, Tim. (2016). UN thinks Internet access is a human right. Business Insider, 22 July 2016.

RRIJM 2015, All Rights Reserved