White Collar Cyber Crime v. Blue Collar Crime

Puja Paul Srivastava
Faculty of Law, Jayoti Vidyapeeth Womens University, Rajasthan
Jaipur, India

Abstract

Cyberspace is virtual world where everything is present but no one present, in other words we can also say it is a world of fictitious bodies, who enter do work, play, chat and go away but not physically. This fast moving nowhere present world is now effecting the present moving world and the effect is so deep that the present world’s entire crime can actually be performed in virtual world. But a very big question arises that how to control this crime, as neither the crime nor the criminal is traceable easily being virtual. Another big issue is that which law shall be applied whether new law for new crime or old tested law for virtual world crime. In India for dealing traditional crimes Indian Penal Code, 1860 is sufficient and for cyber crime where computer is either tool or target Information Technology Act, 2000 is present. The author has tried to deal with all the issues in detailed manners which are raised here. Author has also dealt with some new types of cybercrime which are upcoming in today’s world.

Keywords: Cyber Crime, Blue Collar Crime

I. INTRODUCTION

Cyber Law basically refers to entire legal and regulatory aspect of Internet; more specifically Cyber Law can be defined as law governing computer and internet. IT revolution resulted in phenomenal increase in number of cybercrime in cyberspace, the term cyberspace was coined by William Gibson in his science fiction novel ‘Neuromancer’ in the year 1984. The novel tells the story of a washed-up computer hacker where in a setting which is not physical hired by an anonymous employer to pull off the ultimate hack. Cyber space is a conceptual hallucination where they carried business transactions, worked, play games, and broke the law. Research report of 2013 says that India has third largest number of Internet users after China and the United States, and its users are significantly younger than those of other emerging economies, but little did anyone suspect that online activities that are uncontrolled would give way to new type of opportunity to companies to give solution which are costly for safety and exposure on Internet.

First noticed Cyber crime and Law: - First public noticed cyber crime1 was done by Vladimir Leonidovich Levin, born on March 11, 1971, a biochemistry graduate of St. Petersburg's Tekhnologichesky University in mathematics, led a Russian hacker group in the first international bank robbery over a network. Vladimir, who worked for AO Saturn, a trading company in St. Petersburg, befriended a former St. Petersburg bus driver who had turned entrepreneur in San Francisco, according to recently unsealed court documents. Levin allegedly told his new friend he had found out how to wire transfer money out of Citibank's computer system. Twice already, he allegedly bragged, he had squirreled substantial amounts into his own account in Finland. Court documents said Levin's colleague became a partner in what would become a multinational hacker ring. Just a few weeks later, transfers were made to BankAmerica accounts held by Primorye (roughly translated as "Shoreland" in Russian) Corp. and Shore Corp., both of San Francisco. The companies were owned by Levin's friend Jevgenij Korolkov. By this time, Citicorp officials had begun to suspect foul play and started questioning Korolkov. Korolkov left the country but apparently was not deterred. Instead, the two pressed on and recruited new partners around the globe, authorities say. By October 1994, he broke into Citibank's computerized cash management system and attempted forty illegal transactions to California, Israel, Germany, Holland, and Switzerland. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers and then obtained a list of customer codes and passwords. In July 1994 customers complained of $400,000 mysteriously "disappearing" from two Citibank accounts. Citibank's security system flagged two transfers in August 1994, one for $26,800 and another for $304,000. Bank officials then contacted the FBI, who tracked Levin as he trespassed on Citibank's system and made more illegal transfers. He logged on 18 times over a period of few weeks and between June and October 1994 transferred more than $10 million in funds from three Citibank corporate customers to bank accounts through wire transfers to accounts his group controlled in the United States, Finland, Netherlands, Germany, and Israel. Court documents allege he accomplished the illegal transfers by dialing into Citibank's cash management system. Citibank indicated that Levin gained access to the company's cash management system through valid accounts that weren't protected by encryption. There had been speculation that someone inside Citibank served as Levin's accomplice. Citibank, however, denied such claims and evidence to the contrary never surfaced. The system allowed Citibank customers to initiate their own fund

---

1 Global digital measurement and analytics firm Comscore has said in a report.
2 Decided on February 24, 1998
transfers to other banks; daily turnover was about $500 billion. Authorities said that to avoid causing suspicion, Levin dialed in from his house in Russia late at -2- night. Conducting transactions during New York business hours would less likely raise alarms. Levin apparently used valid user IDs and passwords of other banks, among them Banco del Sud in Argentina and Bank Artha Graha in Indonesia. How he got those passwords, given Citibank's extensive security, is unclear. Inside help seems likely, but Citibank claimed that no employees were involved. When Citibank noticed the transfers, they contacted the FBI authorities, who were working with Citibank tracked Levin making illegal transfers. They were further assisted by Russian telephone company employees, who helped them trace the source of the transfers to Levin’s employer in St. Petersburg, Russia. Levin was finally arrested at Heathrow airport, London in March 1995 as he stepped off an incoming flight from Moscow. Thirty months later in 1997, he was extradited to New York - the extradition and the actual charges underscore the legal problems encountered with the multi-jurisdictional nature of cyber-crime. Vladimir fought extradition for 30 months, but lost, and was transferred to the US for trial. When Levin was extradited to the U.S. in 1997, he was described in the newspapers as the mastermind behind the Internet's first- ever bank raid. Some security experts dispute that claim, however. Levin, they say, used telecommunications systems, not the Internet, to break into Citibank. He was able to intercept Citibank customers' phone calls and, as the customers authenticated their accounts by punching in their account numbers and PINs, obtain the information he needed to commit the fraudulent transactions. Levin pleaded guilty in January 1998 and admitted using passwords and codes stolen from Citibank customers to make transfers to his accounts. Citibank was able to recover all but $400,000 of the $10 million that was siphoned from its accounts. Finally, in February 24, 1998 a U.S. judge sentenced Levin to three years in prison, and ordered him to pay Citibank $240,015. Four members of Levin's group pleaded guilty to conspiracy to commit bank fraud, and served various sentences. While Citibank spokespeople have indicated that Levin gained access to the company's cash management system through valid accounts that weren't protected by encryption, there has been speculation that someone inside Citibank served as Levin's accomplice. Citibank denies such claims and evidence to the contrary has never surfaced. This rapidly increasing crime is increasing very fast as per data of authorities.

Cyber security: - US President Barack Obama said cyber crime is the most serious crime that is faced as Nation and America’s economic prosperity in 21st century and this is also a matter of public safety and security 3. ‘Web War I” for first took place in 2007 between Russian and Estonia where network collapsed, satellites spin out of control, chemical plants exploded and power grid failed, Ergma4 says she spent years studying nuclear energy and watched the world transform as it wrapped itself around the advent of nuclear technology. For her, information warfare is a similar defining moment in world history. "When I look at a nuclear explosion and the explosion that happened in our country in May, I see the same thing,” she says. “Like nuclear radiation, cyberwar doesn’t make you bleed, but it can destroy everything”, more example in June 2010 worm “stuxnet” discovered initially like simple Malware but later found to carefully designed not buy rough but with resources of nation to destruct system to help control equipments at nuclear plant of Iran. In 2009 the US government admitted that software had been found that could shut down the nation's power grid and Mr Hypponen5 said that he was aware of an attack - launched by infected USB sticks - against the military systems of a NATO country."Whether the attacker was successful, we don't know,” he said.

Viruses and Worms

Trojan horse: - It is virus which has damaging instruction set which will enable remote user to assume control of user system like “black orifice” downloaded by e-mail deals security of window and control targets computer.

Password Sniffer: - Program that record name and password of Internet users when someone enter password they enter computer and can tamper any files there in. A virus that modify computer programs changing file. Once computer connected to other computer through Internet , floppy, direct computer connection it affect.

Melissa Virus: It has 80 pornographic websites through mail which says important message from it affected 1000 Fortune companies, look like message from friend.

Worms: - It is standalone programs and replicated without human intervention.

Example. “I love you bug” - According to anti-virus software producer McAfee, the ILOVEYOU virus had a wide range of attacks:

- It copied itself several times and hid the copies in several folders on the victim's hard drive.
- It added new files to the victim's registry keys.

3President on Securing Our Nation’s Cyber Infrastructure

4 Ene Ergma speaker of the Estonian parliament

5 Mikko Hypponen, chief research officer at security firm F-Secure
Cyber Murder: - First<sup>6</sup> online murder will happen by end of year, warned US firm. In a series of high-profile stunts, Barnaby Jack hacked into cash machines to make them spew money, and exploited a flaw in an insulin pump. He died last year just before he was about to demonstrate how pacemakers could be hacked.

The former US vice-president Dick Cheney – who has a long history of heart problems – revealed last year that the wireless function had been disabled on his implanted defibrillator because of concerns that outsiders could hack the network and provoke a heart attack.

Examples-Patient admitted to New York Hospital fully computerized, cracker entered into system as a result modified date of patient medicine that was 60 mg insulin which was modified to 260 MG when nurse injected the injection and patient died. Also, in a series of high-profile stunts, Barnaby Jack hacked into cash machines to make them spew money, and exploited a flaw in an insulin pump. He died last year just before he was about to demonstrate how pacemakers could be hacked. The former US vice-president Dick Cheney – who has a long history of heart problems – revealed last year that the wireless function had been disabled on his implanted defibrillator because of concerns that outsiders could hack the network and provoke a heart attack.

Phishing: - Using spoof (humorous copy of film) email directing people to fake website to fool them into financial details so criminal can access their account. They send out e-mails that appear to come from legitimate websites such as eBay, PayPal, or other banking institutions. The e-mails state that your information needs to be updated or validated as eBay, PayPal, or other banking institutions. The email is not crime under law as offence and there shall be punishment prescribed for that offence. Debate on cyber crime where computer is tool or a target in cyberspace is twofold on the basis of following basic question.

1. What constitutes cyber crime as opposed to Physical crime?

2. Application of traditional crimal law administration on cyber crime, whether just and equitable?

On first debate there are some consensus either computer is tool or target. There are divergent views, done through Internet therefore need of international dimensions for avoiding “International warfare of IT” and to judge the damage done. Cyber crimes are misnomer both crimes include conduct therefore it would be relevant to find out similarities and differences between the two.

Similarities and Differences -

1. Requirement of guilty mind –Both cyber crime and physical crime have requirement of guilty mind. Examples sending virus with email intentionally crime but unknowingly sending such mail is not crime under-

a. Section 65 - Tampering with computer source documents<sup>7</sup>.

---

<sup>6</sup> Report by US security firm IID that predicted the first murder via “hacked internet-connected device” by the end of 2014

---

<sup>7</sup> Whoever knowingly or intentionally conceals, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be supplied in furtherance of any criminal activity, shall be punished with imprisonment of either description for a term which shall not be less than five years but which may extend to ten years and with fine which may extend to one lakh rupees or with both such imprisonment and fine. The Court may, if it thinks fit, order that the fine shall be collected by attachment of the property of the person convicted.
b. Section 66 - Hacking with Computer System.

c. Section 67 of Information Technology Act – Punishment for publishing or transmitting obscene material in electronic form.

2. Jurist Salmond says wrongful Act arise with two distinct questions:

Q1. How did he do that act? And

Q2. Why did he do it?

First show intention and second motives. But the question is that how to check whether particular act is crime. Examples- A fire shot at bush thinking of tiger but it was a man who died question whether he is liable? He is not liable as no intention to kill man.

Person is said to do offence of attempt to commit offence when he

- intent to commit particular offence
- made preparation to do act towards the commission
- may not be step to committing offence but one done during course of committing offence
- Must be proximate to offence. Possibility proximity not in relation to time but intention.

Five punishments are recognized by IPC 1860 –

1. Death,
2. Imprisonment of life, imprisonment rigorous and simple,
3. Forfeiture of property and
4. Fine,

Crime in context of Cyberspace: - Virtual world crimes are different from real world. Cyber world is virtual though is a reality. Here unimaginable crimes happen in speed. Moot point is whether same blue collar crime principle is applied here; arguments say that there is division of thought. School in support says –

1. Cyber crime is nothing but physical crime happening in computer world.
2. As in physical world cyber crime are done by individual or groups, just the medium is different.
3. As traditional principles have handled situations too well they are capable of handling new technology as well.
4. Technological advancement itself is good tool to track convict.

School not in support says-

1. Cybercrime is potential to do uncontrollable damage and needs strict regulations.
2. Done by anonymous person who are skilled in opening password and security and can vanish without trace.
3. Cybercrime are transnational and involve complex prosecution.
4. Crime of obscenity and pornography has potential scope to push people to do crime in physical world, like Rape.
5. Technology is fast changing hence need different enforcement system to tackle crime.

Punishment under IT Act:-

1. Imprisonment but not mentioned rigorous or simple.
2. Fine as per damage suffered.
3. Confiscation under section 76 of Information Technology Act, 2000 of floppy, computer, tape, pen drive etc.
4. Residue penalty under section 45 of Information Technology Act, 2000 whomsoever contravenes provision of art and for which no separate penalty provided in the Act shall be liable to pay not exceeding 25000/-. 
5. Non interference with other law under section 77 even if is confiscation or penalty imposed. Actt shall not interfere with other punishment if applied for the time being in force.

II. CONCLUSION

Thus with a vast discussion and comparison made above we can come up to the conclusion that India has variety of Law to deal all the crimes but the special type of cyber crime which looks normal like any blue collar crime

kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

(1) Whoever with the intent of cause or knowing that is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

(3) Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

(4) Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is

(5) Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is
is not that easy to deal with as collection of evidences is different from what in blue collar crime, because the netizens are in a fictitious world, crime has been performed in the fictitious world then how to draw something real from everything fictitious. Next Indian Penal Code has definitions to every crime but what about crime which are not even defined in IPC. Talking about crimes which are defined in Indian Penal Code like murder which is cyber murder in cyberspace is also not easy to deal with as evidence collection and proving the person accused for murder is tough because cyberspace has no limitation and the person sitting across seven seas can also perform it easily. Internet has no boundaries but law of present world's law have distinct boundaries. IT Act which is for cyberspace is quite loose as far as punishment are concerned, then in this way it does not justify with the present world laws. Therefore it is required that a new cross border law should be made especially for crime of cyberspace and the countries at large should join hands to root out this global problem.

REFERENCES
[1] Bare Act, Indian Penal Code, 1860