Perceiving Cybercrime: Appearance, Challenges and Legal Reaction

Thamraj Ghorsad

M.Tech, Department of Computer Science & Engg.,
Radha Raman Engineering College, Bhopal.
RGPV University, Bhopal
raj.ghorsad@gmail.com

Abstract:

The emergence of the Internet in the late 1980s led to the evolution of cyberspace as a fifth domain of human activity and in last two decades, Internet has grown exponentially worldwide. India too has witnessed significant rise in cyber space activities and usage of internet so much so that it has not only become one of the major IT destinations in the world but has also become the third largest number of Internet users after USA and China. Such phenomenal growth in access to information and connectivity has on the one hand empowered individuals and on the other posed new challenges to Governments and administrators of cyberspace.

1. Introduction

Cyber space has unique characteristics *viz.* anonymity and difficulty of attribution, coupled with enormous potential for damage and mischief. This characteristics not only adds to the vulnerabilities but also makes cyber security a major concern across the globe since it is being exploited by criminals and terrorists alike to carry out identity theft and financial fraud, conduct espionage, disrupt critical infrastructures, facilitate terrorist activities, steal corporate information and plant malicious software (malware) and Trojans. The emergence of cloud and mobile technology has further complicated the cyber threat landscape. Moreover, with the advent of sophisticated and malicious cyber tools physical damage on critical infrastructure and systems are

inflicted and systematically information from targeted systems are stolen. All this makes cyber security an issue of critical importance with profound implications for our economic development and national security. Given the growing threats to cyber assets and all pervasive inter-connected information systems, countries around the world are engaged in actions for ensuring security of their cyber space.

Cyber security, a complex issue, cuts across domains and national boundaries and makes it difficult to attribute the origin of cyber-attacks. It, therefore, calls for a strategic and holistic approach requiring multi-dimensional and multi-layered initiatives and responses.

2. Monikers in Cybersecurity and Cybercrime

Cybercrime and cybersecurity are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cybersecurity35 addresses cybercrime as one major challenge underlines this.

Cybersecurity36 plays an important role in the ongoing development of information technology, as well as Internet services. 37 Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.38 Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cybersecurity thus requires a comprehensive approach.39 Cybersecurity strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of

cybercrime.40 The development and support of cybersecurity strategies are a vital element in the fight against cybercrime.41 The legal, technical and institutional challenges posed by the issue of cybersecurity are global and farreaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.42 In this regard, the World Summit on the Information Society (WSIS)43 recognized the real and significant risks posed by inadequate cybersecurity and the proliferation of cybercrime. The provisions of §§ 108-110 of the *WSIS Tunis Agenda for the Information Society44*, including the Annex, set out a plan for multistakeholder

3. Development of computer crime and cybercrime

The criminal abuse of information technology and the necessary legal response are issues that have been discussed ever since the technology was introduced. Over the last 50 years, various solutions have been implemented at the national and regional levels. One of the reasons why the topic remains challenging is the constant technical development, as well as the changing methods and ways in which the offences are committed.

3.1 The 1960s

In the 1960s, the introduction of transistor-based computer systems, which were smaller and less expensive than vacuum-tube based machines, led to an increase in the use of computer technology.112 At this early stage, offences focused on physical damage to computer systems and stored data.113 Such incidents were reported, for example, in Canada, where in 1969 a student riot caused a fire that destroyed computer data hosted at the university.114 In the mid 1960s, the United States started a debate on the creation of a central data-storage authority for all ministries.

3.2 The 1970s

In the 1970s, the use of computer systems and computer data increased further.119 At the end of the decade, an estimated number of 100 000 mainframe computers were operating in the United States.120 With

falling prices, computer technology was more widely used within administration and business, and by the public. The 1970s were characterized by a shift from the traditional property crimes against computer systems121 that had dominated the 1960s, to new forms of crime.122 While physical damage continued to be a relevant form of criminal abuse against computer systems,123 new forms of computer crime were recognized. They included the illegal use of computer systems124 and the manipulation125 of electronic data.126 The shift from manual to computer-operated transactions led to another new form of crime – computer-related fraud.127 Already at this time, multimillion dollar losses were caused by computer-related fraud. 128 Computer-related fraud, in particular, was a real challenge, and lawenforcement agencies were investigating more and more cases.129 As the application of existing legislation in computer-crime cases led to difficulties,130 a debate about legal solutions started in different parts of the world.131 The United States discussed a draft bill designed specifically to address cybercrime.

3.3 The 1980s

In the 1980s, personal computers became more and more popular. With this development, the number of computer systems and hence the number of potential targets for criminals again increased. For the first time, the targets included a broad range of critical infrastructure.134 One of the side effects of the spread of computer systems was an increasing interest in software, resulting in the emergence of the first forms of software piracy and crimes related to patents.135 The interconnection of computer systems brought about new types of offence.136 Networks enabled offenders to enter a computer system without being present at the crime scene.137 In addition, the possibility of distributing software through networks enabled offenders to spread malicious software, and more and more computer viruses were discovered.138 Countries started the process of updating their legislation so as to meet the requirements of a changing criminal environment.139 International organizations also got involved in the process. OECD140 and the Council of Europe141 set up study groups to analyse the phenomena and evaluate possibilities for legal response.

3.4 The 1990s

The introduction of the graphical interface ("WWW") in the 1990s that was followed by a rapid growth in the number of Internet users led to new challenges. Information legally made available in one country was available globally – even in countries where the publication of such information was criminalized.142 Another concern associated with online services that turned out to be especially challenging in the investigation of transnational crime was the speed of information exchange.143 Finally, the distribution of child pornography moved from physical exchange of books and tapes to online distribution through websites and Internet services.144 While computer crimes were in general local crimes, the Internet turned electronic crimes into transnational crime. As a result, the international community tackled the issue more intensively. UN General Assembly Resolution 45/121 adopted in 1990145 and the manual for the prevention and control of computer-related crimes issued in 1994.

3.5 The 21st Century

As in each preceding decade, new trends in computer crime and cybercrime continued to be discovered in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as "phishing",147 and "botnet attacks",148 and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as "voice-over-IP (VoIP) communication"149 and "cloud computing".150 It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to
cybercrime high priority.

4. Types of Cybercrime/attack - methodology and impact

Most of the Internet frauds reported in the country are relating to phishing, usage of stolen Credit Cards / Debit Cards, unauthorized fraudulent Real Time Gross Settlement (RTGS) transactions, fictitious

offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds etc.

When the Committee desired to know the mode of occurrence and prevention of various types of cyber-crimes existing/emerging around the world and in our country, the Department, in their written reply, furnished the following information:-

- HACKING
- DENIAL OF SERVICE ATTACK
- VIRUS DISSEMINATION
- SOFTWARE PIRACY
- PORNOGRAPHY
- IRC Crime
- CREDIT CARD FRAUD
- PHISHING
- SPOOFING
- CYBER STALKING
- CYBER DEFAMATION
- THREATENING
- SALAMI ATTACK
- NET EXTORTION

HACKING

The act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access. Hacking is also the act by which other forms of cyber-crime (e.g., fraud, terrorism, etc.) are committed. Hacking in simple terms means illegal intrusion into a computer system without the permission of the computer owner/user.

DENIAL OF SERVICE ATTACK

This is an act by the criminal, who floods the band width of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide.

VIRUS DISSEMINATION

Malicious software that attaches iitself to other software. (virus, worms, Trojan Horse, Time bomb,Logic Bomb, Rabbit and Bacterium are the malicious soft wares)

SOFTWARE PIRACY

Theft of software through the iillegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. Retail revenue losses worldwide are ever increasing due to this crime Can be done in

various ways such as end user copying, hard disk loading, Counterfeiting, Illegal downloads from the iinternet etc.

PRONOGRAPHY

Pornography is the first consistently successful ecommerce product. It was a deceptive marketing tactics and mouse trapping technologies. Pronography encourage customers to access their websites. Anybody including children can log on to the internet and access website with pronography contents with a click of a mouse.

IRC CRIME

Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere the world can come together and chat with each other Criminals use it for meeting coconspirators. Hackers use it for discussing their exploits / sharing the techniques Paedophiles use chat rooms to allure small children.

CREDIT CARD FRAUD

You siimply have to type credit card number into www page off the vendor for online transaction If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.

NET EXTORTION

Copying the company's confidential data in order to extort said company for huge amount.

PHISHING

It is technique of pulling out confidential information from the bank/financial institutional account holders by deceptive means.

SPOOFIING

Getting one computer on a network to pretend to have the identity of another computer, usually one with special access privileges ,, so as to obtain access to the other computers on the network.

CYBER STALKING

The Criminal follows the victim by sending emails, entering the chat rooms frequently.

CYBER DEFAMATION

The Criminal sends emails containing defamatory matters to all concerned of the victim or post the defamatory matters on a website. (disgruntled employee may do this against boss, ex-boys friend against girl, divorced husband against wife etc)

THREATENING

The Criminal sends threatening email or comes in contact in chat rooms with victim. (Any one disgruntled may do this against boss, friend or official)

SALAMI ATTACK

In such crime criminal makes insignificant changes in such a manner that such changes would go unnoticed. Criminal makes such program that deducts small amount like 2.50 per month from the account of all the customer of the Bank and deposit the same in his account. In this case no account holder will approach the bank for such small amount but criminal gains huge amount.

5. Conclusion

It can be seen that the threat of computer crime is not as big as the authority claim. This means that the method s that they introducing to combat it represents an unwarranted attack on human rights and is not proportionate to the threat posed by cyber-criminals. Part of the problem is that there are no reliable statistics on the problem; this means that it is hard to justify the increased powers that the Regulation of Investigatory Powers Act has given to the authorities. These powers will also be ineffective in dealing with the problem of computer. The international treaties being drawn up to deal with it are so vague that they are bound to be ineffective in dealing with the problem. It will also mean the civil liberties will be unjustly affected by the terms of the treaties since they could, conceivably, imply that everybody who owns a computer fitted with a modem could be suspected of being a hacker. The attempts to outlaw the possession of hacking software could harm people who trying to make the internet more secure as they will not be able to test there systems.

6. Reference

[1] http://threatchaos.com/2009/03/stay-calm-peoplecyber- crime-does-not-reap-1-trillion-in-profi ts/.

[2] http://www.theregister.co.uk/2005/11/29/cybercrime/.

[3] http://www.tmcnet.com/usubmit/2009/03/20/4072706.htm.

[4] http://www.fortiguardcenter.com/papers/VB2006_ Dirty_Money_on_the_Wires.pdf.

[5] http://www.fortiguardcenter.com/papers/VB2007_ Menace_II_the_Wires.pdf.

[6] Survey by Aon Ltd, 2005.

[7] http://www.telegraph.co.uk/news/worldnews/europe/ france/4547649/French-fi ghter-planes-grounded-bycomputer- virus.html.

[8] http://en.wikipedia.org/wiki/50_Cent_Party.

[9] Dupuis-Danon, M.-C. Finance Criminelle.

[10] http://counterterrorismblog.org/House%20Homeland%203-31-09%20Statement.pdf.

[11] http://en.wikipedia.org/wiki/Internet_censorship_in_ Iran.

[12] http://news.bbc.co.uk/2/hi/middle_east/8099579.stm.

[13] http://en.wikipedia.org/wiki/Internet_censorship_in_ the_People's_Republic_of_China.

[14] http://en.wikipedia.org/wiki/Golden_Shield_Project.

[15] http://en.wikipedia.org/wiki/Green_Dam_Youth_ Escort.

[16] http://www.messagelabs.co.uk/mlireport/MLI_Report_March_Q1_2008.pdf.

[17] http://telegraph.co.uk/news/worldnews/europe/ france/4547649/French-fi ghter-planes-grounded-bycomputer- virus.html.

[18] Verdelho, P. The effectiveness of international co-operation against cybercrime: examples of good practice. For the Project on Cybercrime of the Council of Europe, 2008.

[19] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[20] Interview with the author, 2009.

[21] In its 2008 Internet Crime Report, the IC3 (the US computer crime online report platform for the public) reckons it received 275,284 complaints in 2008 and referred 72,940 of those to law enforcement agencies. In the report only six resolved cases are documented, five of which pertain to auction fraud, and all involve perpetrators located in the US