VOL.4 ISSUE 3
DROIT PENALE: INDIAN LAW JOURNAL ON CRIME & CRIMINOLOGY
ISSN: 2456-7280

DEVELOPMENT OF TECHNOLOGY: IT'S IMPACT ON CRIME AND LEGAL RESPONSE

- Shivani, Ankita Chawla & Bhawna[1]

ABSTRACT

Development of technology is the process of research and development of science. Many emerging technologies are expected to become generally applied in the near future. Crime facilitated through technology encompasses a wide variety of offences that pose different levels of threat to consumers, business, and more generally, society at large. Development has lead to the invention of Nano technology and others. Cyber crime has taken the top most position, in relation to crimes committed using technology. In cyber crimes children has taken major part. Law has taken many steps in regard to prevent and investigate cyber crimes. Even though there are many laws and regulations the issues relating to sovereignty, legal jurisdiction continue to hinder its effective implementation, thereby rendering the Criminal Justice Process and System ineffective.

This paper aims at bringing out the various issues relating to technology and crime; the Justice System, such as problem relating to investigation and detection, Judicial Processes and Justice delivery mechanisms.

Keywords – Advance technology, Crime, Criminal Justice, Judicial effectiveness

Introduction

Crimes committed using technology is not a careless matter in this world. Technology has given rise to many inventions which made humans get relief from their work tensions in solving complex problems, doing routine and repetitive tasks. On the other hand we should also know that invention has made humans depend upon technology to a large extent. Almost everything in our lives are gradually becoming cyber technology development. Thus, crimes have entered into the cyberspace as well. The growth in the number and variety of technology related crimes, particularly computer-related crimes, echoes the exponential increase in the number of Internet users and the

[1] Student, Geeta Institute of Law, Panipat

expansion of e-commerce globally. Organized crime groups are broadening their exploitation of technological vulnerabilities by targeting individuals and businesses that rely on technology, e-commerce and the on-line storage of valuable personal, financial and intellectual property data.

Computer-related crimes pose significant and growing threats globally because many are sophisticated, effective and malicious. For example, spam has evolved from a time- and resource-wasting nuisance to a medium through which individuals can distribute malicious software programs, also known as "malware." Individuals now increasingly use unsolicited email, or spam, to distribute viruses, worms, spyware and Trojan horse software. Spam directed at computer programs/files, instant messaging systems, web logs and cellular phones makes these tools vulnerable to worms, viruses, and fraud. Some viruses facilitate the illicit access of the personal or sensitive data stored on the devices. For cellular phones, new text messaging technology enables senders to conceal their identity, allowing impersonated messages that can facilitate spam, fraud and viruses. Malware enables criminals to use the cellular phone without the user's knowledge or gain access to the phone's personal data. The exploitation of these technologies is expected to increase in the forthcoming years. Spam also poses a threat to wireless game consoles, personal data assistants (PDA) and Voice over Internet Protocol (Vo I P).[2]

In Internet "pharming," hackers exploit vulnerabilities in the domain name system (DNS) server software and then illicitly redirect Internet traffic to targeted websites. Pharming can also occur when a user's computer system is compromised by malware. As a result, when users wish to access a legitimate site, they are unknowingly redirected. Redirected false sites are used for phishing. Pharming poses an ongoing threat to consumers and businesses as it can target a broad number of financial institutions' users and wait within the computer for the user to access financial services. Criminals are forming more and larger botnets, or networks of computers with broadband Internet connections that are compromised by malware and are thus "software robots or zombies." These remotely-controlled attack networks undertake a variety of crimes: sending spam or phishing e-mails, hosting spoofed websites for

[2]Interpol and Law Enforcement: Response to Transnational Crime: Andre Bossard, Secretary-General (red.) Interpol

pharming scams, and distributing viruses or Trojan horse software to facilitate on-line extortion or compromise more home computers for larger botnets. Individuals involved in on-line "carder networks" illegally buy and sell stolen personal and financial information. Some networks sell blank credit cards, the algorithms necessary to encode a credit card's magnetic strip or lists of botnets. These networks facilitate counterfeit credit card manufacture and identity theft. In Operation FIREWALL for example, 28 individuals were arrested from eight U.S. states and several countries who were involved in selling about two million credit card numbers in two years, causing losses of over US$4 million.

In a newer version of traditional extortion, criminals hack computer systems containing valuable and/or sensitive data, like credit card numbers. The data are then either ransomed back to the company or the criminal offers to exchange silence regarding the vulnerability for a fee. An increasingly popular extortion scheme involves either threatening to launch or actually launching denial-of-service (D o S) attacks or directed denial-of- service (DD o S) attacks against businesses. These attacks, often undertaken through botnets, involve overloading computer networks/servers with enormous amounts of data to disrupt or interrupt service to users. Corporate or intellectual property information is also vulnerable to espionage. In May 2005 for example, a number of middle level managers and private investigators from several companies in Israel were charged with planting Trojan horse software in competitors' computers to access confidential information. Internationally, some criminal groups, according to the United Kingdom's National High-Tech Crime Unit, are also showing increasing interest in using the Internet for pay-perview child pornography. Organized crime has also began the use technology to intimidate criminal rivals, or instill fear in communities to prevent the reporting of organized crime-related activities or testifying to a witnessed crime.[3] For example, individuals can use e-mail, the Internet or other electronic communications devices, like cellular phones with cameras, to slander, threaten, harass or "cyber stalk" another person. Threats can be posted in chat groups and personal information can be manipulated or simply released to violate personal privacy. With technology to enable

[3]Interpol and Law Enforcement: Response to Transnational Crime: Andre Bossard, Secretary-General (red.) Interpol

anonymity and security in communication, this type of intimidation poses challenges to law enforcement. Certain technologies and innovations have facilitated the production and distribution of child pornography. For example, computer software can digitally alter images of child pornography to enhance or change the image, for example sexualizing content by removing clothing. Similarly, in contrast to software that digitally ages missing children, images of child pornography can be created by "de-aging" images of adult pornography. With developments in animation, digitally-created child pornography may become widespread. Criminals have been known to use steganography to conceal information, like child pornography, and distribute it in a secure fashion. 4 Technology facilitates increasingly secure, anonymous and rapid communication, through tools like encryption software, wireless devices, encrypted cellular phones and anonymous re-mailers that forward e-mails without revealing their origins. Criminal groups exploit tools like this to plan and undertake criminal activities, such as drug trafficking, without physical interactions, thereby reducing the risks of detection and prosecution.

Technology: It's Impact On Crime

Cyber crime poses serious risks on the society. Even as protective technologies as evolved, never modes of cyber technologies may be misused in the years to come. Dr Toni Makkai, Director of the Australian Institute of Criminology, in his publications looking at the future environment in which Australians will use information and communications technologies and how this environment will provide opportunities for illegality and infringement of current regulatory controls. The reports are 'Future directions in technology-enabled crime: 2007-09', the most recent publication in the AIC's Research and public policy series, and 'The future of technology-enabled crime in Australia', number 341 in the Trends & issues in crime and criminal justice series.

The reports identify developments that may facilitate technology-based crime.[4] These include:

- globalization and the emergence of new economics
- increased widespread use of broadband services and mobile and wireless technologies

[4]Cyber Crime and Information Warfare-Dr Peter Grabosky; Australian Institute of Criminology, ACT

- increased use of electronic payment systems
- Changes in government use of technology to allow the public to conduct transactions securely, including participation in democracy.

The most likely areas in which opportunities for illegality may arise include fraud, identity related crime, computer viruses and malicious code, theft of information, dissemination of objectionable material online, and risks of organized crime and terrorism. Children, who are most at risk, learn about computers and the Internet at an early age. But just as you wouldn't let children cross a busy road without some safety rules, you shouldn't send them onto the information superhighway without teaching them the rules of the road. Too many dangerous people can reach children and adults through the Internet. Today's technology is a wonderful tool, but you must know how to use it safely.

Not only children are pray to cyber crime, even adults are also in quiet large. Even with the knowledge also adults are falling in this crime world. Both adults and children are mainly exposed to prone [sex pictures], even though it is strictly prohibited in cyber cafe, there are two ways who give encouragement doing things which are restricted: one is, encouraged by the owner of the cyber cafe and by the peer group friends. On the other hand it is bad curiosity with bad boldness which insists peoples including children to get involved in this crime world.

Above all, these major and serious problem is faced in internet, mostly children are playing major role as a pray to criminals and children have also themselves become criminal not only outside, even in their own house and schools. Children are spending their valuable time with money in cyber cafe, which is an easy availability all over their environment.

E-Commerce: The increasing use of telecommunications, particularly the development of ecommerce, is steadily increasing the opportunities for crime in many guises, especially IT related crime.

Globalization: Globalization does not mean globalized welfare at all. Globalized information systems accommodate an increasing number of trans-national offences. The network context of cyber crime makes it one of the most globalized offences of the present and the most modernized threats of the future.

Legal Responses For Technological Crimes

The Criminal Justice System:

The criminal justice system [CJS] is a systematized form, to render justice; it is also represents the organized societal response to crime. In the eyes of the general public, criminal justice is viewed as a glittering land mark in the annals of crime history & portrays the sanctum sanctorum of justice. The unimpeachable faith is responded in the Criminal Justice System as an institution in the social welfare, equality, morality & highly a droned doctrines & dogmas.

Indian Response: Information Technology Act-2000

The Parliament of India has passed its first Cyber law, the Information Technology Act, 2000 which provides the legal infrastructure for E-commerce in India. The said Act has received the assent of the President of India and has become the law of the land in India.

At this juncture, it is relevant for us to understand what the IT Act, 2000 offers and its various perspectives.

The object as defined therein is as under:-

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto." [5]

Towards that end, the said Act thereafter stipulates numerous provisions. The said Act aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The said Act further states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal

[5] The Information Technology Act, 2000

validity and enforceability. The said Act purports to facilitate electronic intercourse in trade and commerce, eliminate barriers and obstacles coming in the way of electronic commerce.[6]

Need For International Harmonization Of Cyber Laws

People usually are impressed by the illusory overlap between Internet space and international space. Notwithstanding the fact that information systems are linking Continents, islands, residents and communities into a giant virtual network, states and areas preserve their 7 traditional sovereignty. McConnell International's metaphor (2000, p. 8) said that: "In the networked world, no island is an island." At this turning point, the globally connected Internet has made cyber crime a trans-border problem. The "international dimension" (Wasik, 1991, pp. 187-201), "trans-national dimension" (Sofaer & Goodman, 2005) or "global dimension" (Grabosky, 2004, pp. 146-157) of cyber crime is universally perceived. While law is always territory-based, the tool, the scene, the target, and the subject of cyber crime are all boundary independent. Domestic measures will certainly be of critical importance but not sufficient for meeting this worldwide challenge. International coordination and cooperation are necessary in fighting offences commonly prohibited by every country. Many international organizations have been making efforts to harmonize actions within their forums; for example, Sieber (1996, 1998), United Nations Crime and Justice Information Network (UNCJIN, 1999), Police Commissioners' Conference Electronic Crime Working Party (2000), Sofaer et al. (2000), Putnam and Elliott (2001), Schjølberg & Hubbard (2005), and so on.

INTERPOL'S Efforts

Many international organizations qualify for professional organizations, because their goals and activities are focused on certain specific issues; these organizations include Interpol, the International Telecommunications Union, etc. However, professional efforts here primarily mean substantial actions in the field of cyber security protection and cyber crime prevention. Although some other organizations also greatly

[6]India's Information Technology Act, 2000; By Pavan Duggal (editorial advisor, Inomy.com, and Advocate,Supreme Court of India

contribute to coordinating cyber security protection, their emphasis is not necessarily on the law. By this standard, this section only analyzes the actions of the International Criminal Police Organization (Interpol). , Interpol also takes distinct actions to prevent cybercrime, cooperating with credit-card companies to combat payment fraud by building a database on Interpol's web site (Police Commissioners' Conference Electronic Crime Working Party, 2000, p. 64).

Regional Efforts

There are many regional international organizations, with a narrow or broad coverage of states, more or less making efforts to maintain cyber security and harmonize international measures to combat cyber crime. This section will introduce only four of these organizations, which have taken typical actions in combating cyber crime.

(i) The Asia-Pacific Economic Cooperation (APEC)

In the Asia-Pacific region, the APEC coordinates its 21 member economies to promote cyber security and to tackle the risks brought about by cyber crime (APEC, 2003). The APEC has conducted a capacity-building project on cyber crime for member economies in relation to legal structures and investigative abilities, where the advanced APEC economies support other member-economies in training legislative and investigative personnel.

(ii) The Council of Europe (COE)

The Council of Europe has been working to tackle rising international anxiety over the risks brought about by the automatic processing of personal data since the early 1980s. In 1981, the Council of Europe implemented the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108, 26 January 1981), which was revised according to the Amendment to Convention ETS No. 108 Allowing the European Community to Accede, 15 June 1999, and the Additional Protocol to Convention ETS No. 108 on Supervisory Authorities and Trans-border Data Flows, 8 June 2000. The Convention recognized the desirability "to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing,"

and the necessity "to reconcile the fundamental values of the respect to privacy and the free flow of information between peoples" (Preamble). The Convention covers the protection of personal data in both the public and private sectors.

(iii) The European Union

The EU took a series of actions to tackle cyber crime through impelling a coordinated law enforcement and legal harmonization policy. Civil liberty has also been a focus in the anti-cyber crime field. In April 2002, the Commission of the European Communities presented a Proposal for a Council Framework Decision on Attacks against information systems, and this proposal constitutes the case of the Decision of 24 February 2005.

(iv) The Organization of American States (OAS)

As other regional organizations, the Organization of American States (OAS) with 35 member states is also highly concerned about the issue of cyber crime. Through its forum for the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA), the OAS has long recognized the central role that a sound legal framework plays in combating cyber crime and protecting the Internet. Such recognition has prompted the REMJA to recommend the creation of the Group of Governmental Experts on Cyber crime (The Group of Experts) in March 1999.

Other Multi-National Efforts

Unlike professional organizations that are limited to a more specific field of concern, and unlike regional organizations that are limited to a more specific location of states, the multinational international organizations care for affairs of a broader range and take actions in a broader territorial environment. This section recounts the efforts of three of the multi-national organizations.

(i) The Commonwealth of Nations

The Commonwealth of Nations took a direct and timely action in the harmonizing laws of its member states. In October 2002, the Commonwealth Secretariat prepared the "Model Law on Computer and Computer Related Crime" (Bourne, 2002, p. 17). Within the Commonwealth's 53 member countries, the "Model Law" has had a wide influence on domestic legislation. Through this model law, the Convention on Cyber

crime has become one of the legislative choices in substantive criminal law, covering the offences of illegal access, interfering with data, interfering with computer systems, and illegal interception of data, illegal data, and child pornography.

(ii) *The Group of Eight (G8)*

Since the mid-1990s, the Group of Eight (G8) has created working groups and issued a series of communiqués from the leaders and actions plans from justice ministers. At the Halifax Summit 1995, the Group of Seven recognized "that ultimate success requires all Governments 10 to provide for effective measures to prevent the laundering of proceeds from serious crimes, to implement commitments in the fight against trans-national organized crime At the Denver Summit 1997, the Group of Eight proposed to strengthen their efforts to realize the Lyon recommendations, by concentrating on punishing high-tech criminals, and promoting the governments' technical and legal abilities to react to trans-territorial computer crimes.

(iii) The Organization for Economic Cooperation and Development (OECD)

With its 30 member countries, the OECD addressed computer security for several decades. In 1983, an expert committee was appointed by the OECD to discuss computer crime phenomena and criminal-law reform (Schonberg& Hubbard, 2005). Offences against confidentiality, integrity or availability listed in the 1985 OECD document included unauthorized access, damage to computer data or computer programs, computer sabotage, unauthorized interception, and computer espionage. In December 1999, the OECD officially approved the Guidelines for Consumer Protection in the Context of Electronic Commerce (Department of Justice, 2000, p. 27), representing member states' consensus in the area of consumer protection for e-commerce: consumers should be protected in e-commerce not less than the protection they enjoyed within traditional commerce (Department of Justice, 2000, p. 27).

Conclusion

Technology can be the best friend of human but with a condition that we use them properly. We use social media, in our daily life; today it is full of negativity. Today a Facebook post can lead riots in different communities; a photo shopped picture of a girl can defame her in social media. ATMs, PCO, Net banking etc are all modern

technology which are very helpful to human but only till cyber crime doesn't take place. A cyber criminal can empty your account within the time you take for blinking eyes. Today rate of cyber crimes is increasing day by day on a very alarming rate and government is still sleeping. Today the only way to eradicate cyber crimes is public awareness and strict law implementation. It's high time for police to get themselves Hi-Tech as to get rid of these cyber criminals. As technology is advancing and crimes are also advancing the law needs to be upgraded to meet the challenges of crimes arising out of this. This periodic revision of law with genuine interest to curb losses from these crimes are the need of the hour. In addition to this efforts must be to train all the segments of the criminal justice system in understanding and combating such crimes.