International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Cyber Crime: International Organized Crime- An Overview

Shiksha Dahiya

Assistant Professor, Schoool of Law, GD Goenka University, Gurgaon
Guest Faculty, law Centre-2, Faculty of Law, University of Delhi
+9050478492 Email: shikshadahiya11@gmail.com

Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.

Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

The Internet is one of the fastest-growing areas of technical infrastructure development. Today, information and communication technologies (ICTs) are omnipresent and the trend towards is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs.

The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries.

ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements. In turn, ICT applications may release technical and human capacity and enable greater access to basic services. In this regard, online identity theft and the act of capturing another person's credentials and/or personal information via the Internet with the intent to fraudulently reuse it for criminal purposes is now one of the main threats to further deployment of e-government and e-business services.

The costs of Internet services are often also much lower than comparable services outside the network.13 E-mail services are often available free of charge or cost very little compared to traditional postal services.14 The online encyclopaedia Wikipedia15 can be used free of charge, as

can hundreds of online hosting services.16 Lower costs are important, as they enable services to be used by many more users, including people with only limited income. Given the limited financial resources of many people in developing countries, the Internet enables them to use services they may not otherwise have access to outside network.

DEFINING CYBERCRIME

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 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.

An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal? Where exactly does cybercrime take place? Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified.

In 1996 the Council of Europe, together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime. Around the world, civil libertarian groups immediately protested provisions in the treaty requiring Internet service providers (ISPs) to store information on their customers' transactions and to turn this information over on demand. Work on the treaty proceeded nevertheless, and on November 23, 2001, the Council of Europe

Convention on Cybercrime was signed by 30 states. The convention came into effect in 2004. Additional protocols, covering terrorist activities and racist and xenophobic cybercrimes, were proposed in 2002 and came into effect in 2006. In addition, various national laws, such as the USA PATRIOT Act of 2001, have expanded law enforcement's power to monitor and protect computer networks.

TYPES OF CYBERCRIME

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual. Also at this end of the spectrum is the growing crime of identity theft. These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the Internet. Another part of this type of crime involves individuals within corporations or government bureaucracies deliberately altering data for either profit or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These range from spam, hacking, and denial of service attacks against specific sites to acts of cyberterrorism—that is, the use of the Internet to cause public disturbances and even death.

Identity theft and invasion of privacy

Cybercrime affects both a virtual and a real body, but the effects upon each are different. This phenomenon is clearest in the case of identity theft. In the United States, for example, individuals do not have an official identity card but a Social Security number that has long served as a de facto identification number. Taxes are collected on the basis of each citizen's Social Security number, and many private institutions use the number to keep track of their employees, students, and patients. Access to an individual's Social Security number affords the opportunity to gather all the documents related to that person's citizenship—i.e., to steal his identity. Even stolen credit card information can be used to reconstruct an individual's identity. When criminals steal a firm's credit card records, they produce two distinct effects. First, they make off with digital information about individuals that is useful in many ways. For example, they might use the credit card information to run up huge bills, forcing the credit card firms to suffer large losses, or they might sell the information to others who can use it in a similar fashion. Second, they might use individual credit card names and numbers to create new identities for other criminals. Although identity theft takes places in many countries, researchers and law-enforcement officials are plagued by a lack of information and statistics about the crime worldwide. Cybercrime is clearly, however, an international problem.

Internet fraud

Schemes to defraud consumers abound on the Internet. Among the most famous is the Nigerian, or "419," scam; the number is a reference to the section of Nigerian law that the scam violates. Although this con has been used with both fax and traditional mail, it has been given new life by the Internet. In the scheme, an individual receives an e-mail asserting that the sender requires help in transferring a large sum of money out of

Nigeria or another distant country. Usually, this money is in the form of an asset that is going to be sold, such as oil, or a large amount of cash that requires "laundering" to conceal its source; the variations are endless, and new specifics are constantly being developed. The message asks the recipient to cover some cost of moving the funds out of the country in return for receiving a much larger sum of money in the near future. Should the recipient respond with a check or money order, he is told that complications have developed; more money is required. Over time, victims can lose thousands of dollars that are utterly unrecoverable.

ATM Fraud

Computers also make more mundane types of fraud possible. Take the automated teller machine (ATM) through which many people now get cash. In order to access an account, a user supplies a card and personal identification number (PIN). Criminals have developed means to intercept both the data on the card's magnetic strip as well as the user's PIN. In turn, the information is used to create fake cards that are then used to withdraw funds from the unsuspecting individual's account. For example, in 2002 the New York Times reported that more than 21,000 American bank accounts had been skimmed by a single group engaged in acquiring ATM information illegally. A particularly effective form of fraud has involved the use of ATMs in shopping centres and convenience stores. These machines are free-standing and not physically part of a bank. Criminals can easily set up a machine that looks like a legitimate machine; instead of dispensing money, however, the machine gathers information on users and only tells them that the machine is out of order after they have typed in their PINs. Given that ATMs are the preferred method for dispensing currency all over the world, ATM fraud has become an international problem.

Wire fraud

The international nature of cybercrime is particularly evident with wire fraud. One of the largest and best-organized wire fraud schemes was orchestrated by Vladimir Levin, a Russian programmer with a computer software firm in St. Petersburg. In 1994, with the aid of dozens of confederates, Levin began transferring some $10 million from subsidiaries of Citibank, N.A., in Argentina and Indonesia to bank accounts in San Francisco, Tel Aviv, Amsterdam, Germany, and Finland. According to Citibank, all but $400,000 was eventually recovered as Levin's accomplices attempted to withdraw the funds. Levin himself was arrested in 1995 while in transit through London's Heathrow Airport (at the time, Russia had no extradition treaty for cybercrime). In 1998 Levin was finally extradited to the United States, where he was sentenced to three years in jail and ordered to reimburse Citibank $240,015. Exactly how Levin obtained the necessary account names and passwords has never been disclosed, but no Citibank employee has ever been charged in connection with the case. Because a sense of security and privacy are paramount to financial institutions, the exact extent of wire fraud is difficult to ascertain. In the early 21st century, wire fraud remained a worldwide problem.

File sharing and piracy

Through the 1990s, sales of compact discs (CDs) were the major source of revenue for recording companies. Although piracy—that

is, the illegal duplication of copyrighted materials—had always been a problem, especially in the Far East, the proliferation on college campuses of inexpensive personal computers capable of capturing music off CDs and sharing them over high-speed ("broadband") Internet connections became the recording industry's greatest nightmare. In the United States, the recording industry, represented by the Recording Industry Association of America (RIAA), attacked a single file-sharing service, Napster, which from 1999 to 2001 allowed users across the Internet access to music files, stored in the data-compression format known as MP3, on other users' computers by way of Napster's central computer. According to the RIAA, Napster users regularly violated the copyright of recording artists, and the service had to stop. For users, the issues were not so clear-cut. At the core of the Napster case was the issue of fair use. Individuals who had purchased a CD were clearly allowed to listen to the music, whether in their home stereo, automobile sound system, or personal computer. What they did not have the right to do, argued the RIAA, was to make the CD available to thousands of others who could make a perfect digital copy of the music and create their own CDs. Users rejoined that sharing their files was a fair use of copyrighted material for which they had paid a fair price. In the end, the RIAA argued that a whole new class of cybercriminal had been born—the digital pirate—that included just about anyone who had ever shared or downloaded an MP3 file. Although the RIAA successfully shuttered Napster, a new type of file-sharing service, known as peer-to-peer (P2P) networks, sprang up. These decentralized systems do not rely on a central facilitating computer; instead, they consist of millions of users who voluntarily open their own computers to others for file sharing.File sharing brought about a fundamental reconstruction of the relationship between producers, distributors, and consumers of artistic material.

Counterfeiting and forgery

File sharing of intellectual property is only one aspect of the problem with copies. Another more mundane aspect lies in the ability of digital devices to render nearly perfect copies of material artifacts. Take the traditional crime of counterfeiting. Until recently, creating passable currency required a significant amount of skill and access to technologies that individuals usually do not own, such as printing presses, engraving plates, and special inks. The advent of inexpensive, high-quality colour copiers and printers has brought counterfeiting to the masses. Ink-jet printers now account for a growing percentage of the counterfeit currency confiscated by the U.S. Secret Service. In 1995 ink-jet currency accounted for 0.5 percent of counterfeit U.S. currency; in 1997 ink-jet printers produced 19 percent of the illegal cash. By 2014 almost 60 percent of the counterfeit money recovered in the U.S. came from ink-jet printers. The widespread development and use of computer technology prompted the U.S. Treasury to redesign U.S. paper currency to include a variety of anti-counterfeiting technologies. The European Union currency, or euro, had security designed into it from the start. Special features, such as embossed foil holograms and special ribbons and paper, were designed to make counterfeiting difficult. Indeed, the switch to the euro presented an unprecedented opportunity for counterfeiters of preexisting national currencies. The great fear was that

counterfeit currency would be laundered into legal euros. Fortunately, it was not the problem that some believed it would be.

Child pornography

With the advent of almost every new media technology, pornography has been its "killer app," or the application that drove early deployment of technical innovations in search of profit. The Internet was no exception, but there is a criminal element to this business bonanza—child pornography, which is unrelated to the lucrative business of legal adult-oriented pornography. The possession of child pornography, defined here as images of children under age 18 engaged in sexual behaviour, is illegal in the United States, the European Union, and many other countries, but it remains a problem that has no easy solution. The problem is compounded by the ability of "kiddie porn" Web sites to disseminate their material from locations, such as states of the former Soviet Union as well as Southeast Asia, that lack cybercrime laws. Some law-enforcement organizations believe that child pornography represents a $3-billion-a-year industry and that more than 10,000 Internet locations provide access to these materials.The Internet also provides pedophiles with an unprecedented opportunity to commit criminal acts through the use of "chat rooms" to identify and lure victims. Here the virtual and the material worlds intersect in a particularly dangerous fashion. In many countries, state authorities now pose as children in chat rooms; despite the widespread knowledge of this practice, pedophiles continue to make contact with these "children" in order to meet them "off-line." That such a meeting invites a high risk of immediate arrest does not seem to deter pedophiles. Interestingly enough, it is because the Internet allows individual privacy to be breached that the authorities are able to capture pedophiles.

Hacking

While breaching privacy to detect cybercrime works well when the crimes involve the theft and misuse of information, ranging from credit card numbers and personal data to file sharing of various commodities—music, video, or child pornography—what of crimes that attempt to wreak havoc on the very workings of the machines that make up the network? The story of hacking actually goes back to the 1950s, when a group of phreaks (short for "phone freaks") began to hijack portions of the world's telephone networks, making unauthorized long-distance calls and setting up special "party lines" for fellow phreaks. With the proliferation of computer bulletin board systems (BBSs) in the late 1970s, the informal phreaking culture began to coalesce into quasi-organized groups of individuals who graduated from the telephone network to "hacking" corporate and government computer network systems.

One such criminal was Kevin Mitnick, the first hacker to make the "most wanted list" of the U.S. Federal Bureau of Investigation (FBI). He allegedly broke into the North American Aerospace Defense Command (NORAD) computer in 1981, when he was 17 years old, a feat that brought to the fore the gravity of the threat posed by such security breaches. Concern with hacking contributed first to an overhaul of federal sentencing in the United States, with the 1984 Comprehensive Crime Control Act and then with the Computer Fraud and Abuse Act of 1986.

Computer viruses

The deliberate release of damaging computer viruses is yet another type of cybercrime. In fact, this was the crime of choice of the first person to be convicted in the United States under the Computer Fraud and Abuse Act of 1986. On November 2, 1988, a computer science student at Cornell University named Robert Morris released a software "worm" onto the Internet from MIT (as a guest on the campus, he hoped to remain anonymous). The worm was an experimental self-propagating and replicating computer program that took advantage of flaws in certain e-mail protocols. Due to a mistake in its programming, rather than just sending copies of itself to other computers, this software kept replicating itself on each infected system, filling all the available computer memory. Before a fix was found, the worm had brought some 6,000 computers (one-tenth of the Internet) to a halt. Although Morris's worm cost time and millions of dollars to fix, the event had few commercial consequences, for the Internet had not yet become a fixture of economic affairs. That Morris's father was the head of computer security for the U.S. National Security Agency led the press to treat the event more as a high-tech Oedipal drama than as a foreshadowing of things to come. Since then, ever more harmful viruses have been cooked up by anarchists and misfits from locations as diverse as the United States, Bulgaria, Pakistan, and the Philippines.

Spam, Stenography and E-mail Hacking

E-mail has spawned one of the most significant forms of cybercrime—spam, or unsolicited advertisements for products and services, which experts estimate to comprise roughly 50 percent of the e-mail circulating on the Internet. Spam is a crime against all users of the Internet since it wastes both the storage and network capacities of ISPs, as well as often simply being offensive. Yet, despite various attempts to legislate it out of existence, it remains unclear how spam can be eliminated without violating the freedom of speech in a liberal democratic polity. Unlike junk mail, which has a postage cost associated with it, spam is nearly free for perpetrators—it typically costs the same to send 10 messages as it does to send 10 million.

One of the most significant problems in shutting down spammers involves their use of other individuals' personal computers. Typically, numerous machines connected to the Internet are first infected with a virus or Trojan horse that gives the spammer secret control. Such machines are known as zombie computers, and networks of them, often involving thousands of infected computers, can be activated to flood the Internet with spam or to institute DoS attacks. While the former may be almost benign, including solicitations to purchase legitimate goods, DoS attacks have been deployed in efforts to blackmail Web sites by threatening to shut them down. Cyberexperts estimate that the United States accounts for about one-fourth of the 4–8 million zombie computers in the world and is the origin of nearly one-third of all spam.The FBI has estimated that BEC scams have cost American businesses about $750 million. Sometimes e-mail that an organization would wish to keep secret is obtained and released.

In 2014 hackers calling themselves "Guardians of Peace" released e-mail from executives at the motion picture company

Sony Pictures Entertainment, as well as other confidential company information. The hackers demanded that Sony Pictures not release The Interview, a comedy about a CIA plot to assassinate North Korean leader Kim Jong-Eun, and threatened to attack theatres that showed the movie. After American movie theatre chains canceled screenings, Sony released the movie online and in limited theatrical release. E-mail hacking has even affected politics. In 2016, e-mail at the Democratic National Committee (DNC) was obtained by hackers believed to be in Russia. Just before the Democratic National Convention, the media organization WikiLeaks released the e-mail, which showed a marked preference of DNC officials for the presidential campaign of Hillary Clinton over that of her challenger Bernie Sanders. DNC chairperson Debbie Wasserman Schultz resigned, and some American commentators speculated that the release of the e-mail showed the preference of the Russian government for Republican nominee Donald Trump.

Sabotage

Another type of hacking involves the hijacking of a government or corporation Web site. Sometimes these crimes have been committed in protest over the incarceration of other hackers; in 1996 the Web site of the U.S. Central Intelligence Agency (CIA) was altered by Swedish hackers to gain international support for their protest of the Swedish government's prosecution of local hackers, and in 1998 the New York Times's Web site was hacked by supporters of the incarcerated hacker Kevin Mitnick. Still other hackers have used their skills to engage in political protests: in 1998 a group calling itself the Legion of the Underground declared "cyberwar" on China and Iraq in protest of alleged human rights abuses and a program to build weapons of mass destruction, respectively. In 2007, Estonian government Web sites, as well as those for banks and the media, were attacked. Russian hackers were suspected because Estonia was then in a dispute with Russia over the removal of a Soviet war memorial in Tallinn.

Criminality and Famous Outlaws

Defacing Web sites is a minor matter, though, when compared with the specter of cyberterrorists using the Internet to attack the infrastructure of a nation, by rerouting airline traffic, contaminating the water supply, or disabling nuclear plant safeguards. One consequence of the September 11 attacks on New York City was the destruction of a major telephone and Internet switching centre. Lower Manhattan was effectively cut off from the rest of the world, save for radios and cellular telephones. Since that day, there has been no other attempt to destroy the infrastructure that produces what has been called that "consensual hallucination," cyberspace. Large-scale cyberwar (or "information warfare") has yet to take place, whether initiated by rogue states or terrorist organizations, although both writers and policy makers have imagined it in all too great detail.

Cybersecurity plays an important role in the ongoing development of information technology, as well as Internet services. 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.

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. 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. The development and support of cybersecurity strategies are a vital element in the fight against cybercrime.

The legal, technical and institutional challenges posed by the issue of cybersecurity are global and far- reaching, 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).

Here the focus is on Cyber Terrorism:-

Cyber terrorism has been around since the late 1980's, however the number of internet terrorism have only increased since the September 11 2001.Cyber Terrorism involves two words which has their own meaning on its own.

- Cyber is actually a prefix but it's commonly presumed to be the internet or virtual reality.
- The application of the word cyber can be seen in words such as cyber bullying, cyber crime, cyber fraud, cyber racism and so on and so forth. Usually, with the word cyber, it refers to be an act carried out through the internet.
- Terrorism means acts carried out by individuals, a group or an organization to create fear with underlying reasons such as politics, religion or ideological goal.

According to Paul Strassman, an expert of information warfare, in an interview with Business Online Asia stated that Cyber Terrorism is an extension of terrorism and it takes advantage of the fact that our society is increasingly becoming dependent on the Internet.Cyber Terrorism is applied mostly to civilian information infrastructures with the ultimate objectives that are either ideological or political. He went on to state that the most attractive objective in cyber terrorism is to bring the Internet down.

According the Federal Bureau of Investigation states that "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. However, this is not the only definitions there are more definitions that are given by authors and other heads of security such as U.S. Department of State

who define terrorism as "Premeditated politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents" and then personality like James Lewis from the Center for Strategic and International Studies defined cyber terrorism as: "The use of computer network tools to shut down critical national infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population".

High Profile Attacks

There have been several cases which reinforce the fact that the internet is also not a very safe place. The main reason why one would want to attack something or someone through the internet is due to the fact that everyone is depending on the internet. And hence, every information today is available and stored online. Hence, why would one even consider breaking into a house or bank? They can just access the information through a touch of a keyboard. Hence, this method is more and more prevalent. There are certain cases which took internet by storm. They serve as the perfect examples to understand the situation and causalities of cyber terrorism in this modern day society.

- **Sven Jaschan:**
  - a German college student who confessed as the author of Netsky worms and Sasser computer worms, hasdunleashed a virus in 2004 on his 18th birthday that has resounding effects all around the world. Microsoft placed a $250,000 bounty on his head.
- **Presidential-Level Espionage**
  - During the 2008 presidency run, suspected hackers from China or Russia attacked the computer systems used in the campaigns of both Barrack Obama and John McCain. which include emails and sensitive data used in the campaign.
- **India:**
  - India has reported 13,301 cyber security breaches in 2011. However, the biggest cyber attack that the country had faced occurred on July 12, 2012 where hackers penetrated the email accounts of 12,000 people, which include high officials from Defense Research and Development Organization (DRDO), the Indo-Tibetan Border Police (ITBP), Ministry of Home Affairs, and the Ministry of External Affairs.
- **Iran:**
  - Iran was subjected to cyber attacks on June 2010 when its nuclear facility in Natanz was infected by Stuxnet, a cyber worm that was believed to be a combined effort of Israel and the United States, though no one claimed responsibility for its inception. The worm destroyed Tehran's 1000 nuclear centrifuges and set back the country's atomic program by at least two years, as it spread beyond the plant and infected over 60,000 computers as well. The Iranian government was also accused of its own cyber attacks to the United States, Israel and other countries in the Gulf Arabs, including

their alleged involvement in the hacking of American banks in 2012.

- **Project Chanology:**
  - The biggest protest movement against the Church of Scientology was conducted by Anonymous, a leaderless group of internet-based hacktivist that originated from 4chan. The Project Chanology originated from the church's attempt to remove the material from the highly-publicized interview of Tom Cruise, a prominent member of the church, in the internet in January 2008.
- **Against Indian Parliament:**
  - In year 2001, Indian Parliament was attacked with the help of information technology. Accused forged an official gate pass with the logo of Ministry of Home Affairs and other information along with the layout of Indian Parliament. Police found out a laptop from main accused Md. Afzal and S. Hussein Guru and also found out that they did it through a Pakistani Internet Service Provider. They controlled the identity and E-mail system of Indian Army.

Indian Law and Cyber Terrorism

In India there is no law, which is specifically dealing with prevention of malware through aggressive defence. Thus, the analogous provisions have to be applied in a purposive manner. The protection against malware attacks can be claimed under the following categories:

- Protection available under the Constitution of India, and
- Protection available under other statutes.

Protection under the Constitution of India:

- The protection available under the Constitution of any country is the strongest and the safest one since it is the supreme document and all other laws derive their power and validity from it. If a law satisfies the rigorous tests of the Constitutional validity, then its applicability and validity cannot be challenge and it becomes absolutely binding. The Constitutions of India, like other Constitutions of the world, is organic and living in nature and is capable of molding itself as per the time and requirements of the society.

Protection under other statutes:

- The protection available under the Constitution is further strengthened by various statutory enactments. These

protections can be classified as:

- Protection under the Indian Penal Code (I.P.C), 1860, and
- Protection under the Information Technology Act (ITA), 2000.

The Information Technology (Amendment) Act 2008 has made the provision for cyber terrorism under Section 66F. It provides Life Sentence, though definition is not considered comprehensive. This section is a combination of Section 66 [Computer related offences] and Section 70 [Protected System] of the Act. What separates section 66F from other sections is degree and nature of the offence.

To overcome such casualties caused by the internet based criminals, several policies and regulations are being formulated. So in the recent years several conferences and meetings are held around the world to come up with solutions and alternatives. This year, we were fortunate enough have attended a conference on digital security and digital empowerment. CyFy 2016, was held in Delhi and we were honoured to have attended it and understood the crusts of digital security and the different threats.

CyFy – "Digital Asia: Scripting the New Governance Order"

CyFy is emerging as an indispensable marketplace of ideas where tomorrow's issues are discussed. The 2015 edition of CYFY had over 100 experts from 33 countries and six continents to discuss issues ranging from cyber arms control and critical information infrastructure protection to digital empowerment and bringing the next billion online.

The main theme of CyFy – "Digital Asia: Scripting the New Governance Order" Digital Economy: Taking stock of legal, regulatory and economic aspects of digital development in India and the Asia Pacific, as well as the development of frontier technologies in the financial sector and Internet of Things.CyFy 2016 will also highlighted the role of technology in creating and destroying global cyber regimes, and examined the role of non-state actors in cyberspace.

The conference was a two day event at Taj Mahal Hotel, New Delhi. People from the Federal Bureau of Investigation, The US State Department of Homeland Securities, dignitaries from Ministry of External Affairs and Foreign Affairs, UN and several other dignitaries from various countries gathered here to talk about something which is in this modern industrial society an important issue - Cyber Security and different policies that are present to tackle this problem.

The 2016 edition of CyFy highlighted the political, economic and strategic questions that revolve around cyberspace.The panel had dignitaries belonging from different backgrounds. The diversity present on the panel made it more interesting and gave different perspectives on one situation.The discussions and the little debates that took place was enlightening to the students who were present.

The programme of the conference included panels, roundtables, and interactive sessions covering five main

areas:
1.Digital Economy
2.International Engagement
3.Security, Access and Inclusion
4.Capacity building.

Each day there were four to five panels which tackled several issues which are related to cyberspace.

Ways to overcome Organized Crime

Various international entities, along with other state and non-state actors have worked to stop transnational crime. However, it has been quite difficult to do so. Scholars argue that "countries are ill equipped to effectively respond to global criminal activities…globalization has been far more beneficial to non-state actors, including smugglers, drug traffickers, and other global criminal networks, than it has been to nation states. The hierarchical structure of countries is a liability in an increasing decentralized, global society. Furthermore, globalization has diminished the ability of states to exercise effective jurisdiction over their territories and to regulate trade and other activities" (Payne, 2013: 270). In addition, states are often unable to successfully stop all transnational crime that affects their own state, and internationally. It is often very expensive to halt transnational crime, and governments do not have the necessary budgets (Payne, 2013).

Nevertheless, there are many ways that they have tried to halt illegal activities. One of the key organizations working to combat transnational crime is the International Criminal Police Organization, or Interpol, which is working out of France. Interpol is understood to be a "global clearinghouse for police information that assists countries in criminal cases" (Payne, 2013: 270), and "is the world's largest international police organization, with 190 member countries" (INTERPOL, 2014). In terms of its responsibilities in their fight against transnational crime, "Interpol collects and analyses data, supports global crime investigations, organizes operational working meetings among countries, and organizes regional and global conferences on a wide range of criminal activities" (Payne, 2013: 270). Interpol (2014) explains that they "work to ensure that police around the world have access to the tools and services necessary to do their jobs effectively. We provide targeted training, expert investigative support, relevant data and secure communications channels."

Along with the efforts of Interpol in conduction with other criminal investigation entities throughout the world, another tool that has been used to fight transnational crime has been the role of the international treaties and conventions with regards to countering global crime. One of the most related conventions with regards to transnational crime is the United Nations Convention Against Transnational Organized Crime which is "a global agreement that outlaws bank secrecy, keeps prosecutors worldwide in contact by email, allows international arrest warrants to be sent by e-mail, provided for videoconferences to allow witnesses to testify without have to travel around the world, and creates international witness protection programs" (Payne, 2013: 270).

The United Nations Convention Against Transnational Organized Crime was "adopted by General Assembly resolution 55/25 of 15 November 2000" (UNODC, 2014). The UN Convention was put into force in 2003. This document is seen as an important addition to the fight against transnational crime, and is being put in place in many different ways, such as helping with legal aid, setting up extradition for those accused of committing a crime (Albanese, 2013), as well as other points mentioned above.

But in addition to the UN Convention Against Transnational Organized Crime, the UN also passed "The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children in 2003 (UNODC, 2003). This Protocol is very important, as "[i]t is the first global legally binding instrument with an agreed definition on trafficking in persons" (UNODC, 2003). The UN has also passed a number of additional protocols, such as the Protocol Against the Smuggling of Migrants by Land, Sea, and Air, and other protocols such as the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition (UNODC, 2003). These protocols have aided in bringing addition attention to these criminal issues, and offering a wide range of support for the ending of such transnational crime.

However, the sharing of information is not always effective. For example, the United States government has attempted to increase the collection and sharing of information with regards to criminal organizations. The U.S. with regards to cooperation efforts with El Salvador, "the FBI released lists of suspected gang-member deportees to a special unit within the Salvadoran national police, which then disseminated the list across the country's law enforcement agencies. However, according to interviews conducted…the police unit responsible for disseminating the information did not properly communicate, or in some cases refused to communicate, the names of suspected gang members to other police agencies. There are many reasons for such breakdowns in communication, including distrust about how the information will be used" (Dudley, 2012: 9-10).

Conclusion

There are constant pressures on the criminal justice system to take on roles for which it has traditionally not been equipped. Given the widespread belief that the world is under siege by criminal organizations, those pressures are likely to increase. The popular view is that the world is facing a new criminal threat - new crimes and enormous increases in the number and technological sophistication of old crimes to which it must respond. Yet a criminal justice should always be conservative, hesitating to follow fad and fashion. And, arguably, the degree to which there is a new, greatly expanded criminal challenge has been exaggerated, perhaps grossly. Probably the most important lesson to be drawn is that the real criminal justice challenge lies in understanding the twilight zone where crime and business interact, often to their mutual benefit. That is a zone where regulatory and alternative instruments may be better suited than traditional criminal justice approaches that were created largely to deal with crimes involving involuntary redistribution of wealth.

References

Albanese, J. S. (2013). Deciphering the Linkages Between Organized Crime and Transnational Crime. Journal of International Affairs, Fall/Winter 2012, Vol. 66, No. 1, pages 1-16.

Haken, J. (2011). Transnational Crime in an Organized World. Global Financial Integrity. February 2011. Available Online: http://test.revenuewatch.org/rwiresources.071811/sites/default/files/Transnational_crime_web.pdf

INTERPOL (2014). Overview. Available Online: http://www.interpol.int/About-INTERPOL/Overview

Mittleman, J.H. & Johnston, R. (1999). The Globalization of Organized Crime, The Courtesan State, and the Corruption of Civil Society, Global Governance, pages 103-126.

Payne, R. (2013). Global Issues. New York, New York. Pearson.

UNODC (2014). United Nations Convention Against Transnational Organized Crime and the Protocols Thereto. Available Online: http://www.unodc.org/unodc/treaties/CTOC/

Drug trafficking. (2016). Unodc.org. Retrieved 23 November 2016, from https://www.unodc.org/unodc/en/drug-trafficking/

Drug Trafficking/Distribution - FindLaw. (2016). Findlaw. Retrieved 23 November 2016, from http://criminal.findlaw.com/criminal-charges/drug-trafficking-distribution.html