Cybercrime

Cybercrime, or **computer-oriented crime**, is a crime that involves a computer and a network.[1] The computer may have been used in the commission of a crime, or it may be the target.[2] Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".[3] Cybercrime may threaten a person or a nation's security and financial health.[4] Issues surrounding these types of crimes have become high-profile, particularly those regarding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming.[3]

There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".[3] Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state is sometimes referred to as cyberwarfare.

A report (sponsored by McAfee), published in 2014, estimated that the annual damage to the global economy was $445 billion.[5] Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US.[6] In 2018, a study by Center for Strategic and International Studies (CSIS), in partnership with McAfee, concludes that close to $600 billion, nearly one percent of global GDP, is lost to cybercrime each year.

Cyber Crime?
Any crime with the help of computer and telecommunication technology.
Any crime where either the computer is used as an object or subject. [1]

Classifications

Categories of Cyber Crime

1. Cybercrimes against persons
2. Cybercrimes against property
3. Cybercrimes against government
1. Against a Person
Cyber stalking
Impersonation
Loss of Privacy
Transmission of Obscene Material
Harassment with the use of computer

2. Against Property
Unauthorized Computer Trespassing
Computer vandalism
Transmission of harmful programmes
Siphoning of funds from financial institutions
Stealing secret information & data
Copyright

3. Against Government
Hacking of Government websites
Cyber Extortion
Cyber Terrorism
Computer Viruses[2]

Some Other Crimes
Logic Bombs
Spamming
Virus, worms, Trojan Horse
E-Mail Bombing
E-Mail abuse etc.
Computer crime encompasses a broad range of activities.[8]

Financial fraud crimes[edit]

Main article: Internet fraud

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- Altering in an unauthorized way. This requires little technical expertise and is a common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;
- Altering or deleting stored data;

Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. These types of crime often result in the loss of private information or monetary information.

Cyberterrorism[edit]

Main article: Cyberterrorism

Government officials and information technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. There is a growing concern among government agencies such as the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) that such intrusions are part of an organized effort by cyberterroristforeign intelligence services, or other groups to map potential security holes in critical systems.[9] A cyberterrorist is someone who intimidates or coerces a government or an organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.

Cyberterrorism, in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda piece on the Internet that there will be bomb attacks during the holidays can be considered cyberterrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing, etc.[10]

Cyberextortion[edit]

Main article: Extortion

Cyberextortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cybercrime extortionists are

increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack.[11] However, other cyberextortion techniques exist such as doxing extortion and bug poaching.

An example of cyberextortion was the attack on Sony Pictures of 2014.[12]

Cyberwarfare[edit]

The U.S. Department of Defense (DoD) notes that the cyberspace has emerged as a national-level concern through several recent events of geostrategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. The December 2015 Ukraine power grid cyberattack has also been attributed to Russia and is considered the first successful cyber attack on a power grid.[*citation needed*] Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.[13]

Computer as a target[edit]

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world, in general, is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet. It is seldom committed by loners, instead it involves large syndicate groups.

Crimes that primarily target computer networks or devices include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

Computer as a tool[edit]

Main articles: Internet fraud, Spamming, Phishing, and Carding (fraud)

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend.[14]

Crimes that use computer networks or devices to advance other ends include:

- Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime)
- Information warfare
- Phishing scams
- Spam
- Propagation of illegal obscene or offensive content, including harassment and threats

The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions.

Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware.[15] Or, they may contain links to fake online banking or other websites used to steal private account information.

Obscene or offensive content[edit]

The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances, these communications may be illegal.

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world.

Online harassment[edit]

See also: Cyberbullying, Online predator, Cyberstalking, and Internet troll

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation.

There are instances where committing a crime using a computer can lead to an enhanced sentence. For example, in the case of United States v. Neil Scott Kramer, Kramer was handed an enhanced sentence according to the U.S. Sentencing Guidelines Manual §2G1.3(b)(3) for his use of a cell phone to "persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct." Kramer appealed the sentence on the grounds that there was insufficient evidence to convict him under this statute because his charge included persuading through a computer device and his cellular phone technically is not a computer. Although Kramer tried to argue this point, the U.S. Sentencing Guidelines Manual states that the term computer "means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

In the United States alone, Missouri and over 40 other states have passed laws and regulations that regard extreme online harassment as a criminal act. These acts can be punished on a federal scale, such as US Code 18 Section 2261A, which states that using computers to threaten or harass can lead to a sentence of up to 20 years, depending on the action taken.[16]

Several countries outside of the United States have also created laws to combat online harassment. In China, a country that supports over 20 percent of the world's internet users, the Legislative Affairs Office of the State Council passed a strict law against the bullying of young people through a bill in response to the Human Flesh Search Engine.[17][18] The United Kingdom passed the Malicious Communications Act, among other acts from 1997 to 2013, which stated that sending messages or letters electronically that the government deemed “indecent or grossly offensive” and/or language intended to cause “distress and anxiety” can lead to a prison sentence of six months and a potentially large fine.[19][20] Australia, while not directly addressing the issue of harassment, has grouped the majority of online harassment under the Criminal Code Act of 1995. Using telecommunication to send threats or harass and cause offense was a direct violation of this act. [21]

Although freedom of speech is protected by law in most democratic societies (in the US this is done by the First Amendment), it does not include all types of speech. In fact, spoken or written "true threat" speech/text is criminalized because of "intent to harm or intimidate." That also applies for online or any type of network related threats in written text or speech.

Drug trafficking[edit]

Darknet markets are used to buy and sell recreational drugs online. Some drug traffickers use encrypted messaging tools to communicate with drug mules. The dark web site Silk Road was a major online marketplace for drugs before it was shut down by law enforcement (then reopened under new management, and then shut down by law enforcement again). After Silk Road 2.0 went down, Silk Road 3 Reloaded emerged. However, it was just an older marketplace named Diabolus Market, that used the name for more exposure from the brand's previous success.[22]

Combating computer crime[edit]

It is difficult to find and combat cyber crime's perpetrators due to their use of the internet in support of cross-border attacks. Not only does the internet allow people to be targeted from various locations, but the scale of the harm done can be magnified. Cyber criminals can target more than one person at a time. The availability of virtual spaces [40] to public and private sectors has allowed cybercrime to become an everyday occurrence.[41] In 2018, The Internet Crime Complaint Center received 351,937 complaints of cybercrime, which lead to $2.7 billion dollars lost.[42]

Investigation[edit]

A computer can be a source of evidence (see digital forensics). Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a logfile. In most countries[43] Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide Data Retention Directive (applicable to all EU member states) states that all e-mail traffic should be retained for a minimum of 12 months.

There are many ways for cybercrime to take place, and investigations tend to start with an IP Address trace, however, that is not necessarily a factual basis upon which detectives can solve a case. Different types of high-tech crime may also include elements of low-tech crime, and vice versa, making cybercrime investigators an indispensable part of modern law enforcement. Methods of cybercrime detective work are dynamic and constantly improving, whether in closed police units or in international cooperation framework.[44]

In the United States, the Federal Bureau of Investigation (FBI)[45] and the Department of Homeland Security (DHS)[46] are government agencies that combat cybercrime. The FBI has trained agents and analysts in cybercrime placed in their field offices and headquarters.[45] Under the DHS, the Secret Service has a Cyber Intelligence Section that works to target financial cyber crimes. They use their intelligence to protect against international cybercrime. Their efforts work to protect institutions, such as banks, from intrusions and information breaches. Based in Alabama, the Secret Service and the Alabama Office of Prosecution Services work together to train professionals in law enforcement through the creation of The National Computer Forensic Institute.[46][47][48] This institute works to provide "state and local members of the law enforcement community with training in cyber incident response, investigation, and forensic examination in cyber incident response, investigation, and forensic examination."[48]

Due to the common use of encryption and other techniques to hide their identity and location by cybercriminals, it can be difficult to trace a perpetrator after the crime is committed, so prevention measures are crucial.[41][49]

Prevention[edit]

The Department of Homeland Security also instituted the Continuous Diagnostics and Mitigation (CDM) Program. The CDM Program monitors and secures government networks by tracking and prioritizing network risks, and informing system personnel so that they can take action.[50] In an attempt to catch intrusions before the damage is done, the DHS created the Enhanced Cybersecurity Services (ECS) to protect public and private sectors in the United States. The Cyber Security and Infrastructure Security Agency approves private partners that provide intrusion detection and prevention services through the ECS. An example of one of these services offered is DNS sinkholing. [50]

Legislation[edit]

Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries, such as the Philippines, laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington. They proceeded to lure the two Russian men into the United States by offering them work with this company. Upon completion of the

interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cybercriminals when weak legislation makes it impossible otherwise.[51]

Then-President Barack Obama released in an executive order in April 2015 to combat cybercrime. The executive order allows the United States to freeze assets of convicted cybercriminals and block their economic activity within the United States. This is some of the first solid legislation that combats cybercrime in this way.[52]

The European Union adopted directive 2013/40/EU. All offences of the directive, and other definitions and procedural institutions are also in the Council of Europe's Convention on Cybercrime.[53].

It is not only the USA and the European Union who are introducing new measures against cybercrime. ON 31 May 2017 China announced that its new cybersecurity law takes effect on this date.[54]

Penalties[edit]

Penalties for computer-related crimes in New York State can range from a fine and a short period of jail time for a Class A misdemeanor such as unauthorized use of a computer up to computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison.[55]

However, some hackers have been hired as information security experts by private companies due to their inside knowledge of computer crime, a phenomenon which theoretically could create perverse incentives. A possible counter to this is for courts to ban convicted hackers from using the Internet or computers, even after they have been released from prison – though as computers and the Internet become more and more central to everyday life, this type of punishment may be viewed as more and more harsh and draconian. However, nuanced approaches have been developed that manage cyber offenders' behavior without resorting to total computer or Internet bans.[56] These approaches involve restricting individuals to specific devices which are subject to computer monitoring or computer searches by probation or parole officers.[57]

Awareness[edit]

As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals increasingly attempt to steal that information. Cybercrime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information continues to grow in importance. According to the FBI's Internet Crime Complaint Center in 2014, there were 269,422 complaints filed. With all the claims combined there was a reported total loss of $800,492,073.[58] But cybercrime does yet seem to be on the average person's radar. There are 1.5 million cyber-attacks annually, that means that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute, with studies showing us that only 16% of victims had asked the people who were carrying out the attacks to stop.[59] Anybody who uses the internet for any reason can be a victim, which is why it is important to be aware of how one is being protected while online.

Intelligence[edit]

As cybercrime has proliferated, a professional ecosystem has evolved to support individuals and groups seeking to profit from cybercriminal activities. The ecosystem has become quite specialized, including malware developers, botnet operators, professional cybercrime groups, groups specializing in the sale of stolen content, and so forth. A few of the leading cybersecurity companies have the skills, resources and visibility to follow the activities of these individuals and group.[60] A wide variety of information is available from these sources which can be used for defensive purposes, including technical indicators such as hashes of infected files[61] or malicious IPs/URLs,[61] as well as strategic information profiling the goals, techniques and campaigns of the profiled groups. Some of it is freely published, but consistent, on-going access typically requires subscribing to an adversary intelligence subscription service. At the level of an individual threat actor, threat intelligence is often referred to that actor's "TTP", or "tactics, techniques, and procedures," as the infrastructure, tools, and other technical indicators are often trivial for attackers to change. Corporate sectors are considering crucial role of artificial intelligence cybersecurity.[62][63]

Diffusion of cybercrime[edit]

The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. According to Jean-Loup Richet (Associate Professor at the Sorbonne Business School), technical expertise and accessibility no longer act as barriers to entry into cybercrime.[64] Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, hacking is cheaper than ever: before the cloud computing era, in order to spam or scam one needed a dedicated server, skills in server management, network configuration, and maintenance, knowledge of Internet service provider standards, etc. By comparison, a mail software-as-a-service is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for spam.[65] Cloud computing could be helpful for a cybercriminal as a way to leverage his or her attack, in terms of brute-forcing a password, improving the reach of a botnet, or facilitating a spamming campaign.[66]

Importance of Cyber Law In India

The computer-generated world of internet is known as cyberspace and the laws prevailing this area are known as Cyber laws and all the users of this space come under the ambit of these laws as it carries a kind of worldwide jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology. In short, cyber law is the law governing computers and the internet.

The growth of Electronic Commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce. All these governing mechanisms and legal structures come within the domain of Cyber law.

Cyber law is important because it touches almost all aspects of transactions and activities and on involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal angles.

Cyber Crime is not defined in Information Technology Act 2000 nor in the National Cyber Security Policy 2013 nor in any other regulation in India. Hence, to define cyber-crime, one can say, it is just a combination of crime and computer. In other words ‘any offence or crime in which a computer is used is a cyber-crime’. Even a petty offence like stealing or pick pocket can be brought within the broader purview of cybercrime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cybercrime.

Cyber law encompasses laws relating to:
· Cyber crimes
· Electronic and digital signatures
· Intellectual property
· Data protection and privacy

Cyber space includes computers, networks, softwares, data storage devices(such as hard disks, USB disks etc), the internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Need For Cyber Law

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.

In today's highly digitalized world, almost everyone is affected by cyber law.

For example:
Almost all transactions in shares are in demat form.
Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
Government forms including income tax returns, company law forms etc. are now filled in electronic form.
Consumers are increasingly using credit/debit cards for shopping.
Most people are using email, phones and SMS messages for communication.
Even in "**non-cyber crime**" cases, important evidence is found in computers/cell phones eg: in cases of murder, divorce, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.
Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc. are becoming common.
Digital signatures and e-contracts are fast replacing conventional method of transacting business.[3]

Cyber Laws In India

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

The existing laws of India, even with the most compassionate and liberal interpretation could not be interpreted in the light of the emergency cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgement found that it shall not be without major threats and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence, the need for enactment of relevant cyber laws.

None of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email id not "legal" in our country. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for Cyber law.

World and Cyber Laws

The Great firewall of China monitors every moment in cyber space and protect to publish any offensive content.
China have an hold on every content which is harmful of dangerous for the government of China.
Brazil is considered world's biggest airport for Hackers.
Iran is also a dangerous country for the Netizens. He also have a Crime Police unit for crime in Cyber Space.

Importance of Cyber Laws

We are living in highly digitalized world.
All companies depend upon their computer networks and keep their valuable data in electronic form.
Government forms including income tax returns, company law forms etc are now filled in electronic form.
Consumers are increasingly using credit cards for shopping.
Most people are using email, cell phones and SMS messages for communication.
Even in "non-cyber crime" cases, important evidence is found in computers/ cell phones e.g. in cases of divorce, murder, kidnapping, organized crime, terrorist operations, counterfeit currency etc.
Since it touches all the aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace therefore Cyber law is extremely important.[4]

Conclusion

To sum up, though a crime free society is perfect and exists only in illusion, it should be constant attempt of rules to keep the criminalities lowest. Especially in a society that is dependent more and more on technology, crime based on electronic law-breaking are bound to increase and the law makers have to go the extra mile compared to the impostors, to keep them at bay.

Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even Dos or DDos) are all technologies and per se not crimes, but falling into the wrong hands with an illicit intent who are out to exploit them or misuse them, they come into the array of cyber-crime and become punishable offences.

Hence, it should be the tenacious efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes. It should be the duty of the three stake holders viz. i) the rulers, regulators, law makers and agents ii) Internet or Network Service Suppliers or banks and other intercessors and iii) the users to take care of information security playing their respective role within the permitted limitations and ensuring obedience with the law of the land.