Study of Security Breaches in Internet- Cyber Crime

[1]Aditi Rawal
[1]Computer Science and Engineering
[1]IES IPS Academy
Indore, India

Abstract: Cyber-age is the era of Internet & computers where most of the things are actively done over the network starting from online dealing to the transaction online. Since the web is understood as the worldwide stage, be it enterprise, national defence system, shopping or online banking system etc all the database information of these web services are kept isolated from the outside world of tampering though the services of web permit an individual to connect with other countless computers easily to transmit and collect information, messages and data. Unfortunately, this connectivity also lead the path for hackers and offenders to setup a trap for the users so that they will fall prey to the unethical and malicious software and thus providing their personal information and become prone to cyber threats. Threats to the cyber universe which is posed by the enormous rise in the digitization has raised an eye of the whole nation by generating global cause of concern, termed as Cyber Crime. This paper presents the relevant study of attacks on the cyber as the inspiration behind these attacks are processed knowingly and hence affects the integrity and efficiency of the information. Also explaining the impacts caused by these crimes keeping in mind the present day activities that have occurred and highlighting the necessity of being cyber safe and how such criminal tasks could become troublesome, this paper also reviews the laws pertaining to the Cyber Criminals coined as "CYBER LAW".

Index Terms **- Cyber Crime, Security, Unauthorised Access, Cyber threats, Cyber law**

I. INTRODUCTION

The invention of Computer and the expansion of Internet has not only made the human's life easier but also have accomplished large improvements starting from an individual to the large organizations which deals in the field of research, expertise, communication and surgery across the globe. And in this current era and technology-driven age where utilizing the time in fast manner in order to improve the performance, Internet which is a collection of interconnected networks through the use of standard protocols of communication has made it all possible. Unfortunately, these also have given birth to a new environment for crime. Everyone praises the use of Internet but as it is being said that, there are two sides of coin and so is cyber crime and cyber use. Since decades, either for personal benefits or for other's benefit, computer users are using the computer for the imprecise purposes. And because of these erroneous acts, keeping our personal information secure and private is becoming more problematic. The thing is, highly confidential details are becoming more accessible to public databases as we are largely interconnected today than ever. For almost everyone, our data is achievable due to this interconnection and this leads to the negative stigma on the use of technology and considered it as dangerous as practically, our information can be available to the hackers for a price. Technology of modern age continues to promise to keep our data secure however there are threats to this security and the main danger is the threat of Cyber Crimes. Cybercrime is defined roughly as carrying out a misdeed with the help of a computer or the Internet. The Internet is described as "the collection and the interconnection of many computer and telecommunications amenities, enveloping gear and functioning programs, which constitutes to the interconnected maze of systems throughout the world that works through the use of Transmission Control Protocol/Internet Protocol, or any other protocols, for broadcasting data of all kinds either by cable or radio" [1] .In other words, The term cyber crime can be described as a deed which has been wrongly committed or omitted in a way to violate the law forbidding it and strict actions and punishments could be imposed upon those convictions. Other view the cyber crime as, Criminal does the activity of illegally trespassing into the computer system or into the database of another, modification of content or theft or sabotage of data and equipments. [2]. In other words, Cyber crime enters the world of cyber and encompasses the network of computers because of which one can do any task such as fraud commitment, child pornography and its trafficking, lost of intellectual property, violating privacy using digitization of data, stealing personalized information from electronic devices.[3]. It describes various security threats, encryption methods and The connectivity of the large mesh of computers which attach each and every users together allows an individual to accumulate, collect and convey messages, data and information but sadly, furthermore it leads to the broadcasting also to the lawless people and the users become victim to the unknown world i.e. delineation of cybercrime lives. But a distinction should be made compulsorily between a customary misdeed which is enacting by the computers or the Internet and a misguidance that mainly aims at the technology [4]. Now points to the term "Cyber Law". It doesn't have a rigid description, but in broad term, we can explain it as the governing power to the cyber space. Cyber laws are the governing rules and regulations that is laws that supervises the cyber area. Cyber Crimes, theft, stealing private information, digital and electronic signatures, data securities and privacies etc are comprehended by the Laws of Cyber [5]. The General Assembly of UN suggested the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce" (UNCITRAL) Model.

II. CLASSIFICATION OF CYBER CRIMES

Cyber crimes are the crimes which are not generated today but they have their existence since the time when Cyber Space was first ever produced. The first Cyber Crime was detected in the year 1820, it was evolved from simple Morris worm to the dangerous ransom ware and it is defined as the crime or the offences in which PCs and internet both are included and takes place over the internet which are committed against an individual or group of people. Over the years, government has laid down many laws in respect to curb these cyber crimes but yet because of the criminal motives and the increasing volume of these criminal activities as there is no need to have physical appearance to commit the crime, it still leads to the damage of reputation of the victim or make a way to mental or physical harm either directly or indirectly and may threaten a person's or country's security and health financially using these modern technologies(Such as chat rooms, notice boards, emails). As the crime that occurs on the internet never let victims and the offender to come in direct contact, it cause heavy loss and it usually happens from the countries where there are weak cyber laws or no cyber laws in a chance of never getting caught. With the advent of websites and cyber space, it also increases the crimes on the mesh system of internet. Therefore, this paper also presented all kinds of threats that are harmful to the network world and hence classified it on the basis of subject of the crime, the organization or the people against whom the crime is committed and on the temporal nature of the crimes that are committed online.

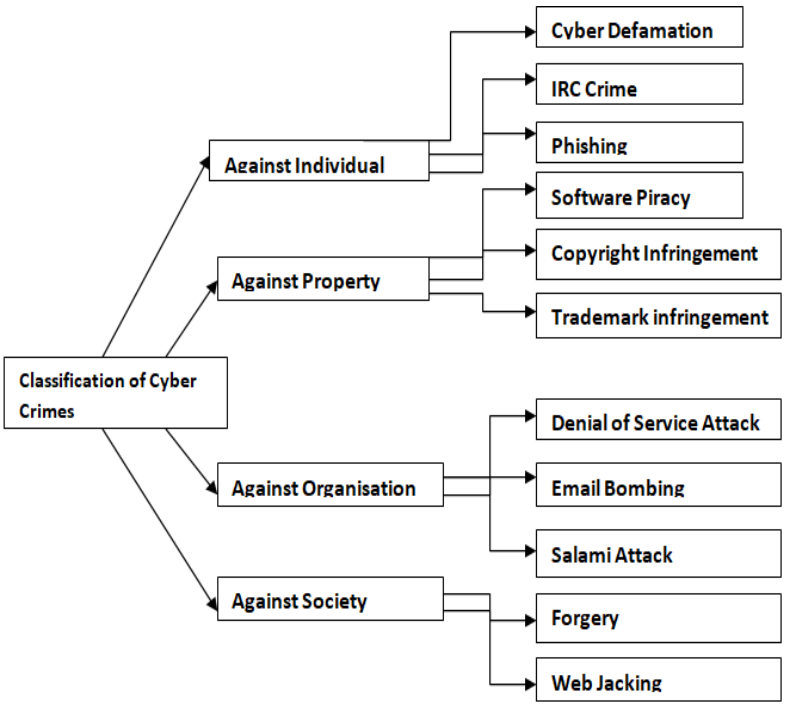

Fig.1 Classification of Cyber Crimes

1. Cyber Crime against Individual*:* Crimes which are carried out against an individual person in a manner to harm a person's image, status, or his reputation of good image therefore incorporate some sorts of violations like transmitting of Child exploitation entertainment or harassment etc. It includes Cyber Defamation, E-mail satirizing, Malicious code, IRC Crime (Internet Transfer Chat), Credit Card Fraud, Phishing, Dissemination, Net Extortion, Trafficking, E-mail spoofing Scattering of revolting material including Software Theft, Indecent exposure etc these all are the potential harms that greatly affects an individual.

1.1 Cyber Defamation: The freedom of interacting and communicating with each other through the use of social media without any barriers has not only brought the revolution in the technical world but this freedom is sometimes misunderstood by some personal grudges' people commonly termed as 'trolls' who post defamatory, unnecessary, false statements, wrongfully and intentionally publishing words about a person that means defaming them in the cyber space which may tarnish their reputation, good name, person's status and lowering their respect is called as Cyber Defamation.

1.2 IRC Crime*:* Internet Relay Chat (IRC) is an open protocol and is a form of synchronous conferencing that allows the people around the world for group communication by coming together under a single platform and chat with each other; it also allows users to exchange text messages and point to point communication through private message. Cyber attackers uses the chat rooms for meeting, hackers use it for discussion; paedophiles use it to allure children. This crime takes place by the attackers through chatting by winning one's confidence and later starts harassing them which leads to blackmailing people for ransom and if the innocent denied paying the requisites amount, then the criminal threatened the to upload victim's naked pictures or video on the websites. Some people uses the IRC in the promise of fake jobs and fake lotteries and later runs with the money thus become IRC Crime..

1.3 Phishing*:* Phishing is a cyber attack of trying to gather private information using disguised e-mails and websites as a weapon. The main target is to make email recipient falls into false belief that the messages is something they needed or falsely claiming to be an authorised legitimate organisation maybe a request from their bank or to scam the victim into submitting their personal information that will lead to identity theft by making them clicking a link or download an attachment..

2. Cyber Crime against Property*:* Another type of cyber crime is the Crimes of the cyber space which are against all types of property. These includes the incorporation of PC vandalism (obliteration of others' property), Threatening, Salami Attacks, Intellectual Property Crimes. This kind of crime is usually prevalent in the monetary establishments and financial institutions or with the end target of carrying out financial crimes. The important component of this sort is the type of offence that the amendment is small to the point that it would go unnoticed and unobserved.

2.1 Software Piracy: Software Piracy is the stealing of authorised secured software. Its penalties apply to the users that illegally produce copyrighted works and under these copyright laws, it occurs due to the unauthorised copying, use, downloading, distribution, modified or selling of software without payments is the common way of pirated software users. It also includes the distribution of the software over multiple systems when the license is only bought for the one as well as redistributing it. Unfortunately, allowing pirated software is another scenario, here the end recipients may notice red flags that specifies pirated ones especially if the digital media which is being acquired is wrapped in hidden containers, for example CD sleeves or no name packages of disk.

2.2 Copyright Infringement: Copyright infringement over the internet means, the use of the activities which are secured by the copyright laws without the consent and permission or the acknowledgement and infringing some exclusive claims which are granted to the lawful copyright holder, such as the distribution of the work (content, image, pictures, design, software etc), right to reproduce, display, hosting or performing the authorised works.. The lawful copyright owner is the only person who has the right of creating works, distributing etc. .

2.3 Trademark infringement*:* It is explained as the availing of a service mark or trademark unauthorized by breaching of exclusive rights secured by trademark with no consent of trademark owner. This case usually arises when a website's trademark somewhat looks similar or confusingly similar to a trademark which is owned by another website owner in respect to the same products or services that come under the registration.

3. Cyber Crime against Organisation- This is the third type of cyber crime which is strongly associated with the organisation and association. Cyber terrorism is one distinct kind of crime in its kind. The advancement of the web has depicted about the standard of Cyber world that it is being utilized by a single person and groups to show the importance of international governments in order to threaten the citizens of a nation. This crime by itself leads into terrorism when human being "cracks" into the governing systems or the military oriented site.

3.1 Denial of Service Attack: DoS attack is an attack in which there are multiple requests on a network server which it cannot handle. It typically floods the servers with traffic so that legitimate users no more able to use them. It may lead to system instability or even paralysis. Though it doesn't result in theft, it can cost the organisation a great amount of time and money to handle. Call flooding is an example of DoS where an attacker floods necessary or unnecessary heavy traffic because of which either performance of the entire business drops or breaks down occurs.

3.2 Email Bombing*:* It is one type of Net Abuse, where large numbers of emails and messages such as malformed messages, fake messages and insert it into certain network session with the purpose of service malfunction. are sent to an email address in order to overflow or flood the server and mailbox. Call teardown and toll fraud are the examples of spoofed messaging. An attacker creates spoofed messages on the server to force password assault until he receives authorization. If the client use default password or easily guessed password then it is quiet easier for an attacker to attack maliciously by using password dictionary.

3.3 Salami Attack*:* Salami attack is also termed as Salami slicing. it is a series of minor data security attacks in which the attackers use an online database to seize the victim's necessary private information like card details, bank details, credit card details etc. that together results in large attack. For example- Every time an attacker from every account reduces very little amounts over a period of time which ultimately sums up and becomes bigger amount. In this attack, no complaint is file as these are difficult to track and detect and the hackers remain free from any legal proceedings as the clients have no idea of the slicing.

4. **Crime against society**-Cyber crime against society is the fourth type which is related to the society. It includes class fraud, forgery, digital psychological oppression, cyber terrorism, sale of illegal articles, web jacking, net extortion, contaminating the youth through indecent, cyber contraband, money related crimes, salami attacks, data diddling and logic bombs. Imitation of the currency notes, income stamps, mark sheets etc can be forged using PCs and high quality printers and astounding scanners. Logic bomb is the crime which is in incorporated and hackers of the web jacking obtain entrance and gains full control over the entire website, and thus change the content of website either for political gain or for money.

4.1 Forgery-Forgery is a illegal and criminal act which is considered as a crime in all jurisdictions within the United States, it is defined as an act which is intentionally done and deliberately committed by a person through falsifying something or when a person changes or modifies a written document with the intention of cheating and deceiving that is defrauding , misleading , altering electronic documents, misrepresentation of a product or item or generating false signature, currency, revenue stamp etc.

4.2 Web Jacking-In this attack, someone seeks the control of website illegally by taking over the domain and thus creates a fake website whenever the user visits or clicks the link, he will soon be redirected to a fake page and the actual page of the website is never touched. It is simple the cyber criminal has cloned the website and makes you believe that it is the authenticate site only. This attack's main aim is to gain complete control over the website so that it could modify, deletes etc the actual content of the webpage according to him.

5. Cyber Crime against Data- In this attack, the main motive of the criminal is to gain overall control over the data and information so that they can use it for personal grudges or gains by altering the data, modifying its content and stealing the necessary information. It includes Data theft, Data Modification and Data Interception.

5.1 Data interception- A criminal monitors the streams of data to or from a destination in order to collect the information. This may have an aim of only gathering the data and later support the attacks. It involves usually sniffing of the traffic over the network but sometimes observes data streams such as radio. In this, the attacker is passive and only detects regular communication but these attackers also sometimes attempt to influence the data nature which is being transmitted.

5.2 Data modification- The main aim of data on the web is to ensure that it cannot be altered or modified in transit. Distributed networks along with the ease of transmission of data also bring the malicious third party which tampers the data as it moves between sites. In this, an unauthorised party intervenes on the network and modifies the data before transmitting it again. One of the example is, attacker change the dollar amount of banking transaction from $200 to $12,000. In a replay attack, a fully set of authenticate data is interjected onto the network channel again and again. An example would be to repeat, twelve thousand times, an authenticate $200 bank account transferring transactions.

5.3 Data Theft- It is defined as the theft when the important information is duplicated illegally and used for some personal gain because by false displays, they made users to provide their private information such as information related to card, social security numbers, passwords or other confidential corporate information. And as it is illegally obtained, when the hackers get apprehended, then it is more probably that he or she will be prosecuted according to the law.

6. Cyber Crime against Network- This is the dangerous attack as it involves the criminal motives over the network channel. The path of communication or interaction in this cyber space majorly depends on the network and if the stream of information flowing over the channel gets stolen or modified or disrupted then both the end parties will lose their crucial information. Example of this attack are network interference, network sabotage etc.

6.1 Network Interference: It is the interruption in the network as attackers or the hackers disrupt the functioning of the network by inputting, deleting, destroying, altering, damaging and transmitting the network data.

6.2 Network Sabotage: Data Sabotage includes the attackers by making small and hidden twists on the computer systems as when services of the web got delivered over the internet or purposefully installed at the time of manufacturing, then the spoiled hardware or software leads to the cause of concern because these tweaks are unnoticed and results in the disruption of the processes that eventually will work in the favour of the hackers.

7. Cyber Crime against Access- This is the unauthorised and illegally getting the access in order to harm the integrity of the data and provides an unauthorised way of capturing credentials, identities and access. It includes virus dissemination, accessing crimes etc. This is difficult to detect by normal users as the malicious software gets attached to the normal softwares which looks like real websites.

7.1 Access Crime: Unauthorized Access or Hacking is nothing but attempting the unauthorised information illegally in order to bypass the mechanisms of security of an information system or network because when someone gets the access to a program, website, server, application, service, or other system using someone else's account or other methods it leads to the threat to the integrity of the data.

7.2 Virus Dissemination: Virus Dissemination is the maligned software that attaches itself to other softwares in a manner of infecting and destroying the entire system of the victim by spoiling the operations of the system and affecting the data which is stored either by deleting or altering it. It comprises of three types that is Greay hat hackers, White hat hackers and Black hat hackers. The software that destroys the system's privacy are viruses, time bomb, rabbit, worms, Trojan horse etc. Virus and the worms are similar as they both does their work of attacking without the knowledge of the user.

III. IMPACTS OF CYBER CRIME

Crime is the evil force in our society. It is omnipresent phenomenon and it is not new; it was always the characteristic features existed in the societies so far whether it is civilized or uncivilized. One should bear in mind that the social concern for this threat is not because of its behaviour but due to the potential harm it causes to the society. The impact of the harm it poses to the society is unbearable if strict actions are not taken in consideration. It affects an individual, private organisation and industries, teenager, market values, consumers etc. Some of the effects are given below.

3.1 Impact on Business Organisation: According to the Department of Law and Justice, it has disclosed around 74 million people in United States who are the victims of the cyber crime which causes the loss of $32 billion financially. The target of the breaching is to steal the financial requisite data of both the business and customers, to refuse services to the company or install a virus which will hide monitors all the activities carried out online.

3.1.1 Cost for Protection- Business organisations have to pull out their wallets in order to secure them because it costs in identifying the risks, building and buying new and protected softwares. Not only have these, but it often required to hire a cyber security analyst who will invent customised way of safety. Also, the systems must be tested and maintained regularly to ensure that they are efficient against emanating attacks online.

3.1.2 Lost Sales- It can't be said that cyber crimes are for the thieves only; it has also started involving cyber-activist. Cyber-activist are the online protestors who link themselves to something and does the work of shutting down company's online activities of transferring messages about company's practices. There are two reputed companies PayPal and MasterCard which was attacked by dozens of people. Though it did not experience full shut down but because of the Denial of Service Attack, it results in losing of the sales and less revenue.

3.2 Impact over Consumer Behaviour and Trust*:* With the invention of e-commerce, its commercial and criminal side also got born which affects greatly the way we shop online. Cyber attackers interferes into user space and tries to break the logic of the website, which will ultimately lead the frustration among the end users and also got discouraged to utilize the site on long term. Fraudulent is the site which is in question but the mastermind of the hidden attack remains unrecognized that lose the confidence of the customer in site and on internet. Corporations should understand that these threats have strategic implementations to all their customers and thus need to have proper measures to eliminate them significantly. According to the reports given by the Better Business Bureau Online, online shoppers over 80% cited security as their primary concern. About 75% of the users terminate the transaction online whenever asked for credit card information. The view of the internet riffled with fraud of credit card and protection hazard is increasing which is a serious bottleneck for e-commerce. Credibility of e-business is of utter importance but being unsafe or scattered makes the online shoppers reluctant to the online transactions.

3.3 Impact over Teenagers and Youth*:* The greatest impact is on the teenagers and youth because of the fear of Cyber Bullying. Teens and the youths spend usually hours online every day chatting or messaging on the social websites like Facebook, Orkut, and Twitter etc. The affect of cyber crime among the children often leads to humiliation, depression and then suicide.

3.3.1 Cyber Bulling- It is negative outcome of the online interaction between youngsters. Bully people sometimes post embarrassing or inappropriate photos of their victims so that lies and rumours spread about that person will get insulted in order to satisfy personal grudges. Sometimes text messages also become the weapon of harassment.

3.3.2 Sexual Solicitation- It is a great cause of concern for one's life. Sexual solicitation occurs on social networking sites or in chat rooms when a person whose age is above 18 or a peer or fake person who is not an adult gets engage in a sexual relationship online. A teen may be said to reveal personal information, view nudes or pornography, or discuss something online related to sex. More than 70% of the teens who got solicited sexually online are girls. In some extreme cases, teens took their lives because of sexual solicitation.

3.4 Impact over National Security*:* In this era, the defence system of the country relies heavily upon the super computers. Information Warfare, attacks on the network, exploitation and breaching of the protected data is not a new challenge in the security of defence system but after 9/11 it has gained utter importance. The Internet has 90% mess and only 10% well maintained security systems. When interveners find that these systems are easy to crack, they hack into the system and gather the most important information of the country, thus providing it to the terrorists so that those criminals can execute their murderous plan. Because of the advanced technology, attackers does not have a need to be in same country to commit such crimes and what fuels their pocket is the wide spread corruption in these countries.

IV. CYBER LAWS

Cyber Crime is no longer limited to time; space, individual or group of people as these cyber gives the criminal a new way to rob the users online and thus generates immoral, criminal wrongs. And therefore there should be some legal provisions which will provide assurance to the users regarding their security, deterrence and punishment to the criminals. The misuse of the services provided online has created the need of the enforcement and implementation of the laws which will abide the rules to either curb or deduce these cyber crimes. Thus, Cyber laws play very important role as it observes all the transactions and activities that takes place online. And to deal with all types of digital crimes, Indian Parliament has implemented an act that is "The Information Technology Act, 2000 (also called as IT Act)". The IT Act has some positive aspects, that are-

1. Electronic mail is now declared as authenticate and valid form of transmission.
2. Electronic certificates and digital signatures have been considered valid after the enactment of IT Act.
3. It also has led to issue digital certificates by letting business to become Certifying Authorities.
4. It also has given right to the government for issuing notices through e-governance online.
5. Communication between end parties could be done easily on the internet.
6. It also has introduced the concept of digital signatures which will correctly verify the identity of an individual.
7. This act also guarantees a remedy in form of money to the company.

This table contains some of the sections of the IT Act, 2000 along with the offences.

. Table 1: Following are the sections under IT Act, 2000 [5]

Offences	Sec. Under IT Act 2000
Temping and Concealing with source documents of the computers	Section 65
It has the ability to issue the guidelines regarding block of the sites that threatens the security	Section 69A
Un-authorized gaining control over the protected system.	Section 70
Sanctions for misrepresentation.	Section 71
Breach of security, privacy and confidentiality	Section 72
Publishing Fake electronic signature and digital certificates.	Section 73
Fraudulent purpose gets published	Section 74
Intermingling of Offences.	Section 77A
Companies commit the offences	Section 85
Transmits the threatening mails	Section 503 IPC
Bogus web pages, Frauds occur under Cyber Space	Section 420 IPC
Web Jacking.	Section 383 IPC
E-mail Spoofing.	Section 463 IPC
Online sale of Ammunitions	Arm Act
Criminal duplication by anonymous interaction groups.	Section 507 IPC
Obscene materials get published in electronic form	Section 67-

V. CONCLUSIONS

In conclusion, it can be understood that the attack over the distributed systems which are connected through Internet has increased by 260% since 1994, and with these alarming rise in cyber crimes we need more detecting technologies along with educating and providing adequate knowledge regarding its pros and cons to the users for being remain unharmed by these crimes. It is true that Internet offers criminals several ways for intrusions and to understand the behaviour of these attackers, there are three ways for taking concrete measures: Cyber laws, Policy making and Education. The main of this paper was to spread awareness among the common people in respect to these heinious crimes, if anyone falls in the prey of cyber attacks without any fear and worry about its impact, there are also laws which are there in support to them.

References

[1] Casey, "*E. Digital Evidence and Computer Crime*": Forensic Science, Computers and the Internet. London: Academic Press, Pp. 5-19, 2011.
[2] Hemraj Saini ,T.C.Panda and Yerra Shankar Rao ,"*Cyber-Crimes and their Impacts: A Review*" ,IJERA, Pp 202-203,2012
[3] Dacey, Raymond & Gallant, Kenneth S. "Crime control and harassment of the innocent, " Journal of Criminal Justice, Elsevier, vol. 25(4), pages 325334,1997
[4] Richards, James." *Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators. Boca Raton, FL*": CRC Press, Pp. 21-54, 1999
[5] Animesh Sarmah, Roshmi Sarmah and Amlan Jyoti Baruah, "*A brief study on Cyber Crime and Cyber Law's of India*", IRJET, Pp 1633-1634, 2017
[6] Sumanjit Das and Tapaswini Nayak, "*IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES*", IJESEt, vol 6, Pp 147-151, 2013
[7] Kshetri, Nir, "*Pattern of global cyber war and crime: A conceptual framework,* " Journal of International Management, Elsevier, vol. 11(4), Pp 541-562 ,2005
Whitman, Michael E. & Mattord, Herbert J.," *Principles of information security* "(2nd ed.). Boston: Thomson Course Technology, Pp. 205-249, 2005