8 Understanding the Significance of Cyber Security

Dr. Omkar Sonawane*
Independent Researcher.
*Corresponding Author: dromkarphd@gmail.com

Abstract

Cyber-attack is the further extension of the execution phase, where a terrorist carries out cyber-attack on the adversary. There is a range of cyber-attacks that can be carried by the terrorist. Cyber-attacks can be executed at any given moment with stealth and speed. Cyber-attack includes credit card theft, debit card fraud, cyber extortion, criminal intimidation, attack on critical infrastructure, hacking and defacement of government websites and webpages, ransomware attack, DDoS attack, SQL attack, lethal virus attack, deleting databases, crypto currency fraud and installing spyware. The motive for a cyber-attack depends upon the goal of the terrorist organisation and its technical capability, and access to technology, combined with the technical expertise of the hacker. In a cyber-attack, the terrorist uses the computer and internet as weapons and cyber-attack tools as a method of delivery.

Keywords: Cyber-Attack, Cyber Crime, Cyber Warfare, Cyber Security, ICT, Hacking.

Introduction

Cyber-attacks that are executed on a large scale receive considerable publicity and attention from the new media. It results in loss of revenue and loss of reputation for the government and companies that are into data businesses, banking, financial institutions, technology companies, research centres and data management servers. In this entire episode, the government plays a minimal role as the technological domains mostly fall under the control of corporate and private enterprises.

Information and Communication Technology, also known as information technology, has permeated into our social lives in different forms. Human exchanges and its interactions are increasingly driven by the technological innovations and have expanded their reach in all corners of our society. ICT is also shaping human relations through social media platforms and other communication channels that provide services of communications. ICT is an umbrella term that specifies and has a unified approach to communication and integration of telecommunication, telephone, wireless signals, computer systems, computer networks, hardware, software, storage, mobile devices, and audiovisual systems and various other electronic gadgets and equipment's. It not only enables an individual to access information, store data, manipulate and transmit information anywhere around the world, but also brings the world closer at unimaginable speed.

Role of Information System

The term ICT has been in currency since 1980's and gained attention, when it was first used in a report addressed to the government of United Kingdom by Dennis Stevenson in the year 1997. Since then, the term has been widely used in the United Kingdom academic curriculum, until it was replaced by much broader term 'computing' in September 2013. Information technology today can largely be conceived as application of computer and telecommunication equipment's to store, transmit, retrieve and manipulate data for variety of purposes, such as business communication and enterprise communication, which includes the governments, military, individual and society as a whole.

Although, the term ICT is popularly used for computers and computer networks, it also encompasses other information distribution systems like radio, television, telephone, smart TV, smart phones, smart watches, satellite phone, Bluetooth devices, laptops, computer desktops, wireless technologies that include; Wi-Fi, hotspot and peer to peer exchanges. The electronic devices, which have the capability to send and retrieve data, to and from the servers or computer networks, also fall into this category.

Traditionally radio, television, telegram and print media were the broad mediums of communication. The advent of information technology dramatically changed the way these technologies operated and functioned. The analogue television has now transformed into digital television, known as the smart TV. The various communication mediums like printed newspapers have transformed into digital newspapers, traditional FM radios into digital, email has replaced old telegrams. Traditional mode of tele-communication has now turned into online formats, such as video call or video conference call. Not all these digital technologies and digital transformations would have been possible without the advancement of

ICT. It has left a profound impact upon human race and the way in which they organise their lives.

The UNESCO has defined ICT as, “A form of technology that is used to transmit, process, store, display, share or exchange information by electronic means. IT includes not only traditional technologies like radio and television, but also modern ones like cellular phones, computer and network, hardware and software, satellite systems and so on, as well as the various services and applications, associated with them, such as video conferencing”.

While the Technology of Association of America (ITAA) defines it as “The study, design, development, and implementation, support or management of computer-based information systems, particularly software applications and computer hardware”. ICT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit, and securely retrieve information.

Table 1: Information and Computer Technology

Information	Technologies
Creation	Personal Computers, Digital Camera, Scanner, Smartphone
Processing	Calculator, PC, Smartphone
Storage	CD, DVD, Pen Drive, Microchip, Cloud, Harddisk, SSD
Display	PC, Smart TV, Projector, Smartphone. LCD/LED Screens
Transmission	Internet, Tele conference, Video conference, Radio.
Exchange	Email, SMS, MMS, Video Chat, Text Chat, Peer to Peer

Source: Created by Author

Thus, in the age of ICT, it is difficult to imagine a society without computers. It has penetrated in our lives so widely that it would now seem life impossible without the computer. Further, the invention of internet has made the computer a powerful medium of communication and emerged as a dominant force in communication, e-commerce, information and entertainment over the past few decades. The progress and advancement in the field of IT has blurred the space, time, physical boundaries, nationality, citizenships, colour and ideology and has brought the world closer on common virtual platform.

Implication of ICT in 21st Century

21st century is often defined as the age of information, because of the way in which information governing almost every possible sphere has transformed the nature of social, business and strategic intercourse across the world. The widespread use of ICT is not just a coincidence, but it is now a reality which been accepted and endemic to all aspects of our daily lives. Industries today, have realised the potential and capability of IT as it has provided them competitive edge and potential to increase profit margins and customer satisfaction. Information technology has made a direct impact upon the way these businesses function and operate. A simple email

conversation to a telephonic conference to connecting organization worldwide has unified the global market to a great extent. Similarly, the retail industry, education sector and healthcare systems is increasingly using ICT and rapidly evolving with greater usage of ICT in its operations. Let us take a look as to how ICT has permeated our lives and these sectors.

- **ICT in Retail**

ICT has greatly revolutionised the retail industry and the ways of operations. Internet has provided a direct line of communication between the retailers and the consumers and allowed retailers to be made available to consumers day and night, 24 hrs a day, interacting with customers, when they are ready to shop. Retailers now heavily depend upon IT to manage their communications, inventory, track customer habits, track order, orders status, delivery of goods and services and online feedback on products and customer's experiences. Many retailers have extended their online platforms by going mobile. The choice of having mobile application and websites has gained huge popularity among consumers, allowing them to shop outside physical retail location. They woo consumers by offering discounts, promotions, sales update that motivates consumer to make online purchases.

- **ICT in Education**

Historically, access to education was a privilege of few. Attempt to universalize education by various governments under the constitutional framework did not materialise in improving the accessibility to education, as millions of children still continued to be left deprived of basic education to which they did not have access too. However, this picture flipped with ICT causing a revolution in the education sector.

ICT has enabled access to information, thereby allowing the masses to empower themselves. By accessing the information freely without any hindrance together with a choice to learn and relearn on matter and subjects of their choices and interests. Such exchange of information has promoted interdisciplinary studies which have now resulted into many such social innovations and technological development. Online education today offers convenience and adaptability to customise the education process and cater to individual student's according to their needs, goals, learning capability and schedule. IT supports interactions, feedback and experience via teleconference, online chats and digital application, which further enhances student and faculty's interaction, thereby consolidating academic relations. It has transformed education into a global hotspot wing with range of courses being made available online. Today, one can take part in any global discussion online with participants taking part from all around the world cutting across different time zones, regions and nationalities. Thus, in the age of ICT ideas have truly become global and hence education plays vital role in our society.

- **ICT in Business**

ICT has made significant impact on businesses and business community and its standardization has made the boom in e-commerce possible. Lowering the transactional cost of operations and increasing speed of logistics along with easy reach to customers and vendors has acquired huge attention and popularity in the field of e-commerce. By creating a set of benchmark for transmitting, marketing and presenting the information electronically, the business has ushered its revenues on an unprecedented scale. One could not imagine global business environment without the use of information and communication technology. In a way, ICT coupled with globalization has transformed the world into a global village, truly extending its global reach and presence across different regions and corners of the world.

Internet and the World Wide Web in particularly are useful in creating virtual communities that become ideal target markets. A virtual community involves the online gathering of people who share a common interest or belief and choose to gather online rather than physically in physical environments. ICT has not only collaborated with businesses around the global, but has also contributed to its development and transformation. This has given rise to big tech companies and multinational corporations. The larger benefit of IT also extends to general welfare of society where digital payments of tax refunds, retirement salaries and welfare support are carried out digitally, saving costs and its transactions being carried out securely.

Today, one can instantly transfer funds to any global destination at click of a button. The power of internet has allowed businesses to grow rapidly by extending their reach to customers with the help of its websites and webpages. Backend offices are increasing in numbers and are working 24x7 with its offices and employees being spread and cut across different nationalities and regions of the world. E-commerce has also helped people living in rural areas and has provided them the opportunity to market their unique goods and products that bring them livelihood. The online e-commerce platforms like amazon, Flipkart, Snapdeal, Walmart, eBay and aggregated taxi apps like Uber and Ola have gained immense popularity amongst masses and have reduced complexities to a great extent.

Figure 1: The use of ICT in various sectors

Need of Information Security

Information has become so highly substantial, that it has gained the status of asset as well as weapon at the same time. The role of IT primarily involves researching, creating, developing, and executing new technologies for the business enterprise and its consumers, such as government, military, individual and society. The main objective of the IT is to develop technological solutions for the enterprise and business in general. IT acts as a vehicle in order to store data, transport data, and retrieve data from one unit to another.

Information Security not only secures communication security but also network security. Communication security focuses on the protection of business enterprise, organisation, government and individual's data, content and technology. In addition, the data security and data confidentiality forms the integral and critical component to information security. Notable features of the information security include:

- Risk Assessment
- Digital Forensics
- Vulnerability Assessment
- Disaster Management & Data Recovery
- Audits of IT
- Security Program Development
- Network Vulnerability Assessment
- Web Applications Testing
- Mobile Application Testing
- Gap Analysis
- General Audits
- Penetration Testing

When data is interpreted in a particular context to give it a visual form, it is known as information. For example, 121023 can be initially seen as data, but the meaning of it is presently unknown. Upon data interpretation one can figure out this information which would be a date of birth of an individual or date of a particular historical event or date for a particular event which is yet to happen in future. Thus, it can be truly said, data that carries value qualifies to be information. Hence, information security can be also called as data security. The primary role of information security is to safeguard information from any potential breach or violation.

With the advent of computer and IT combined with the birth of world wide web, a new dimension to range of human experiences have been added and are rapidly evolving with complex technologies that carry loads of information. These new digital

experiences created online, while interacting with computer and network systems in many ways can be understood as cyber space or the extension of human psychological spaces online. Cyberspace today has converted a zone of transition from the physical world towards a virtual world.

Insights of Cyber Crime

ICT today has become an integral part of our daily lives. It enhances one's capability by allowing people to communicate across the world, search for information at a click of a button and shop online without the need to go outsides of your homes and offices. This has led to the society's reliance on technology, which only is increasing day by day. With such reliance on technology, it can be said that internet has now generated many risks and threats online. It has allowed criminals and criminal organization to increase their reach and scale up traditional crimes and digital crimes, where computer systems have become their targets. These digital crimes can now be said to be known as Cyber Crime.

Cybercrime can be referred as criminal exploitation of the internet, which involves a computer and a network. It can be further defined as a crime, which is done using the computer, network or the internet. This includes anything from stealing millions of rupees from an online bank account to creating, distributing virus on the computer systems, networks, copying confidential data information, cheats businesses, citizen and government over the internet. Lucrative financial gains are the key to persistent cybercrimes threats. Specific types of cybercrime involve criminal organizations who are making online profits, from online thefts and extortions.

Cybercrime encompassed almost every areas of society and has affected people of all ages in many different ways leaving victims helpless, worried and vulnerable. It is increasing at a very fast rate as compared to traditional crime, which is now estimated to be in billions. Due to this nature of cybercrime, anyone can be a victim to it, which could be anyone from, a young woman who is harassed and bullied online to a senior citizen, who has been scammed for money through a false online retirement pension scheme.

Cybercrime encompasses a wide range of activities, which can be broken into two categories:

- The crimes that characterize viruses and denial of service attack by targeting computer networks or devices.
- Another set of crimes that involve the use of computer networks to engage in attacking individuals or a group of individuals. This category of crimes consists of stalking, phishing, fraud, or identity theft.

Summary

Cyber-attacks are rapidly evolving with advancement of technology in the field of internet and computing. Cyber attackers leverage these innovations in order to achieve their desired goals. Depending upon the nature of the attack and scale of impact, cyber terrorists can carry out a range of cyber-attack. All these attacks demand a different set of skills and expertise from the hacker (hacking groups). Let us look into some of these cyber-attacks. The following are some of the main types of attacks that are frequently carried out by perpetrators.

- **Denial of Service:** This attack involves the creation of web traffic, diverts web traffic to a particular computer system or server that confuses handling legitimate requests, and denies access to the legitimate user.
- **Hacking:** It involves the use of a computer in order to intrude the computer system and network by gaining unauthorised access to the system with the intent to cause harm or steal data.
- **Cracking:** Is the act of breaking into the computer system, without the knowledge of the user and tampering data or confidential information.
- **Carding:** Involves the fraudulent use of the debit card or a credit card. Terrorist make unauthorised use of ATM cards to gain monetary benefits, which is done by withdrawing money from the bank accounts or purchasing commodities on e-commerce platforms.
- **SQL Injection:** A cyber-attack injects a malicious SQL statement into the computer system. These SQL statements control the database server. The attacker carries out SQL injection attack in order to bypass web applications' security measures. The attack affects web application, web pages and a website that uses SQL database and SQL statements such as MySQL, Oracle, and SQL Server.
- **Social Engineering Attack:** It is a malicious activity carried out through human social interactions. It initially gathers information about the victim through human and psychological manipulation. Once the information is gained, the attacker tries to establish a connection with the victim in order to gain the victim’s trust. After gaining the trust of the victim, the attacker then seeks access to his/her computer system or network. Once access gained to the computer system or network, the attacker maintains access to the system and later uses the system, in order to launch a cyber-attack.
- **Ransom Ware Attack:** It is a malicious cyber-attack, where the victim computer and database are either locked or encrypted. Here access is denied to the computer. The attacker then demands ransom and such payment are to be made in crypto currencies such as bit coin. After successful payment, the

attacker unlocks the computer. If the victim does not opt to pay the attacker, the malicious code executes its script and deletes data from the computer. The health sector is particularly vulnerable to Ransom Ware attack. Ransomware attack is purely for monetary benefits.

- **Zero-Day Attack:** Also known as zero-day exploit, it is computer software vulnerability. The computer software vulnerability is found and exploited by the attacker, even before the creator releases the security patch for the exploit. Zero days have high commercial value, and are often found and sold in black markets. Zero day exploit gives advantage to the attacker as the creator does not discover the problem, and there is no security patch for the exploit. Zero day in computer software may even continue to exist over extended periods if the creator fails to identify and plug the gaps in the software.
- **Cryptography Attack:** In cryptography attack, cyber terrorists use encryption technology in order to carry out cyber-attacks. Terrorists use encryption, high frequency encryption voice data links, codes, encrypted algorithms, in order to carry out a sophisticated cyber-attack on the adversary. It becomes a herculean task for cyber experts and law enforcement agencies to decrypt the information that is being transmitted live by the terrorist. Terrorists have been found to use 512 bit symmetric encryption technology over the network.
- **Advanced Persistent Threat:** It involves the use of advanced and sophisticated cyber-attack to gain access to the network. Once access to the network is gained, the attacker maintains access to the system and remains silent over the network for long periods. Such an attack in done in order to steal data from the system rather than cause harm to the system. Advanced Persistent threat attacks are used against the organisation and individuals that have high value information. Such high value information sectors include information technology, nuclear, defence and manufacturing sectors which are of national and international importance.
- **Critical Infrastructure Attack:** Critical infrastructures are the core component of the infrastructure and vital assets of the government which help human life function in an orderly and peaceful manner. The USA Patriot Act 2001 provides a definition of critical infrastructure. It categorizes systems and assets both, physical and virtual and crucial to the national security as critical infrastructure. Further, it mentions that information related to national security, economic security, public health or safety, or any combination of these matters constitutes important infrastructure of a nation.

Core components of critical infrastructure include dams, electricity grids, energy sector, telecommunication sector, gas and oil pipelines, transportation sector, chemical industries, defence industries, sewage management, nuclear sector, health,

agriculture, banking and finance. Attack on critical infrastructure involves carrying out cyber-attacks on industrial control systems, which can cause havoc and give a false sense of security to the public. Attack on CI can cause large-scale disruption and put cities, states and nations at risk.

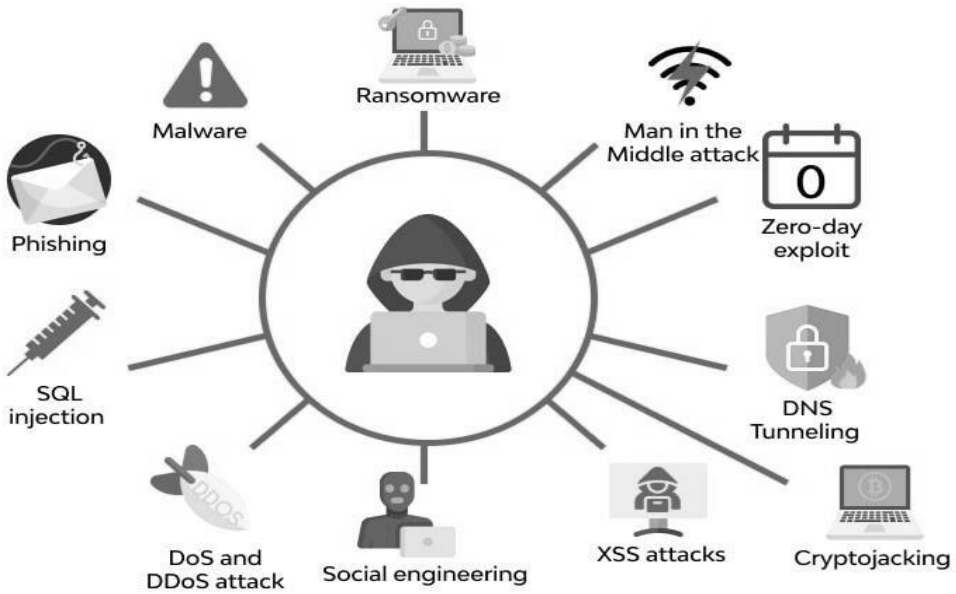

Figure 2: Distinct categories of cyber threats online.

Conclusion

The nature of cybercrime does not only remain an external threat, but it has also acquired a local character. This has been explained by the gradual rise in number of cybercrimes in different cities of India with figures from national crime records bureau and other related documents. The chapter has analysed the pattern of crime and the legal provisions under which it was registered in different cities. This suggests that most number of cases have been registered under Information Technology Act, while crimes registered under Indian Penal Code are lesser. Metropolitan cities like Mumbai, Pune, Bengaluru and Delhi constitute the major cities facing cybercrime, while some of the non-industrial states like Uttar Pradesh and Bihar have also reported a considerable number of cases.

It can be noted that the motives behind committing cybercrimes are conventional in nature; it is the only difference in medium. In a way, cyberspace has allowed socially insensitive elements to leverage it for their ill-informed motives. All these have cumulatively contributed in a pressing burden on enforcement agencies and state machinery to put in place better infrastructure and address the growing concern. The growing cybercrime has affected both, private and public sector, leaving critical and sensitive infrastructure vulnerable.

References

1. Abaimov, S., & Martellini, M. (2020). Cyber Arms Security in Cyberspace. Boca Raton: CRC Press.
2. Akhgar, B. Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities (B. Brewster, Ed.). Switzerland: Springer International Publishing.
3. Andress, J., & Winterfeld, S. (2013). Cyber Warfare Techniques, Tactics and Tools for Security Practitioners (L. Ablon, Ed.). Syngress Press.
4. Arora, S., & Arora, R. (2021). Cyber Crimes & Laws (4th Edition). Delhi: Taxmann Publication Pvt Ltd.
5. Bartlett, J. (2018). PEOPLE VS TECH, THE. Faridabad: Thomson Press India Ltd.
6. Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). Cyber security policy guidebook. Hoboken, NJ: John Wiley & Sons.
7. Bernik, I. (2014). Cybercrime and Cyber Warfare. John Wiley & Sons.
8. Bhushan, M., Rathore, R., & Jamshed, A. (2018). Fundamental of Cyber Security (1st ed.). New Delhi: BPB Publications.
9. Braiker, H. B. The September 11 Syndrome. McGraw Hill.
10. Dr. Sharanjit. (2014). Anti-Terror Laws in India. New Delhi: Regal Publications.
11. Gaber, H. (2020). 2020 Cyber Security and Cyber Law Guide. Edmonton: HSM Press.
12. Geetha, M. K., & Raman, S. Cyber Crimes And Fraud Managment (1st ed.). Chennai: Macmillan.