BAOU
Education for All

Dr. Babasaheb Ambedkar
Open University
(Established by Government of Gujarat)

PGDCL-201
Cyber Crime and Offences

Post Graduate Diploma in
Cyber Law

(PGDCL)

2021

Cyber Crime and Offences

Dr. Babasaheb Ambedkar Open University

Cyber Crime and Offences

Course Writer

Dr Peter Ladis — Chankaya National Law University,
Patna, Bihar

Mr Kumar Gurav — Chankaya National Law University,
Patna, Bihar

Content Reviewer

Dr Deesha Khaire — Gujarat National Law University,
Gandhinagar

Content Editor

Prof. (Dr.) Nilesh K. Modi — Professor & Director,
School of Computer Science
Dr. Babasaheb Ambedkar Open University,
Ahmedabad

ISBN:

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr. Babasaheb
Ambedkar Open
University

PGDCL-201

Cyber Crime and Offences

Block-1: Nature of Cyber Crimes

Block-2: Legislative Framework of Cybercrimes

Block-3: Types of Cyber Crimes

Block-4: International Law on Cyber Space

Block-1

NATURE OF CYBER CRIMES

Unit 1: MEANING AND DEFINITION OF CYBER CRIMES

1

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- History and Evolution of Cyber crime
- Nature and Scope of Cyber crime
- How doctrine of actus rea and mens rea play a role in cyber crimes

1.2 INTRODUCTION

Cyber crime is a collective term encompassing both ‘cyber contraventions’ and ‘cyber offences’. The word ‘cyber’ is synonymous with a computer, computer system or computer network. Thus, cyber crime may be defined as any illegal act that involves a computer, computer system or computer network, i.e., any illegal act for which knowledge of computer technology is essential for its perpetration, investigation or prosecution.

In a broad context, cybercrime refers to any crime that includes a computer, computer network, mobile phone, or other electronic devices, either as a target or as a weapon or associate. As a consequence, any illegal activity carried out with or against such computer devices and in cyberspace is known as a cyber crime. The purpose or intention to inflict an accident, like all illegal acts, is one of the components, although it is not limited to any particular category. Stealing computer hardware is the beginning of illegal crime in the cyber world, and it leads to the conversion, modification, or loss of computer data in order to damage Internet users.

1.3 CYBER SPACE AND IT EVOLUTION

Crime isn’t a particular event that can be studied, interpreted, or represented in a single paper. It can be seen in every part of the world and in every social class. People of all ages, income classes, and backgrounds are among the perpetrators and victims. It’s impossible to say what’s going on with it. It has multiple causes. Its therapies are speculative and debatable. Computer-related offences, also known as cybercrime, are the most recent of all the crimes.

In 1984, William Gibson coined the phrase “cyber space” in his science fiction novel “Neuromancer.” Essentially, it refers to the interactive world in which computer operations take place. Cyberspace is a world without borders. It does not have any geographical borders.The geographical positioning of machines and people using the internet has no effect on the internet address, making national boundaries irrelevant.The territorial limits of nations and the technological frontiers are unrelated. Since nations claim control over persons, activities, and happenings arising within their jurisdiction on the basis of geographical nexus, when territorial borders lose their significance, a well-established concept of international law is jeopardized. As a result, cyberspace contradicts the well-established concept of international law that citizenship and statehood are characteristics of authority over physical space and individuals.

Information technology is one of the world's fastest-growing markets. Rapid developments are emerging in the information technology sector as it moves from a control structure to one of liberalization and globalization. Knowledge is being regarded as a critical resource for country growth. The Indian government has taken a number of steps and interventions to implement effective automation in order to improve productivity and ensure the development of high-quality goods and services. The presence of qualified personnel is a plus factor. For the government, business, and industrial sectors, timely availability of credible, reliable, and coherent information on various accounts is crucial. Organizations in India are planning to face the burden of handling a changing world. To do this, processes and technologies must collaborate closely with the enterprise to include qualitative evidence at the required levels and at the right time for decision-making.Via the collection, organization, preservation, and distribution of information not only at the point of origin but also at various other relevant locations using appropriate communication infrastructure, information technology plays a significant role in this. In simple terms, the Internet is a global network of computers of various types, ranging from notebook computers to display computers, that connects 2 million computers across 13,300 networks to serve over 50 million users worldwide. The 'World Wide Web,' or digital superhighway, is another term for this. A 'Website' is a term used to describe each individual network on the internet.

1.4 HISTORY AND EVOLUTION OF CYBER CRIMES

All who uses palmtops and microchips today will be shocked to find that the first popular computer was installed in the 1950s, and the scale of the computer was so huge that it took up the whole space, and they were too costly to run. The use of these machines was inaccessible to a vast majority of people, and only a limited number of specialists had extensive access to them and the expertise to operate them. At the turn of the twenty-first century, personal computers became more affordable and commonplace in India. After World War II, the US Department of Defense developed the Internet with the intention of developing a network that could operate in the event of a catastrophe or war and safely exchange information. ARPANET was the first network, and with the introduction of Transmission Control Protocol/Internet Protocol, the World Wide Web, and Hypertext, the internet became a global phenomenon. The accuracy and diversity of knowledge have improved as the Internet has risen in popularity. However, no one expected the possibilities that the internet would bring to tech-savvy offenders at the moment.

In India, the state-owned Videsh Sanchar Nigam Limited introduced internet services in 1995, and the government ended VSNL's monopoly in 1998, opening the sector to private operators. At the time, internet usage in India accounted for 0.1 percent of the total population; however, India has now surpassed China as the second-largest country in terms of internet access, with 33.22 percent of the population accessing the internet.

In common law systems, the mechanism of criminalizing individual conduct considered to be detrimental to the public generally takes time. Until undesirable acts are identified as "terrorism," traction acquired by issue detection and demands exercised by special interest organizations may easily cover decades. This mechanism can be exacerbated in certain cases by the emergence of such "catalyst events" that draw the public's and lawmakers' attention.[1]

In the year 1820, the first cybercrime was registered. That's not surprising given that the abacus, which is believed to be the oldest version of a device, has been used in India, Japan, and China since 3500 B.C. The era of modem machines, on the other hand, started with Charles Babbage's analytical engine. The loom was founded by Joseph-Marie Jacquard, a cloth maker in France, in 1820. This system required a series of steps in the weaving of special fabrics to be replicated. Employees at Jacquard became concerned that their traditional work and livelihoods would be jeopardized as a result of this.[2]

[1] Abraham D. Sofaer, Seymour E, .The Transnational Dimension of Cyber Crime Terrorism, Hoover Institution Press, 2001.

[2] http://cybercrime.planetindia.net/intro.htm

Legislators became more concerned about computer crime in the 1980s as businesses became more focused on computers and as trigger incident cases revealed major vulnerabilities to computer crime violations. Criminals can also securely encrypt material that constitutes proof of their illegal activities, archive it, and even distribute it without fear of law enforcement detection. A cyber crime scene will now span from the regional point of victimization (e.g., the victim's personal computer) to every other point on the globe, further complicating police investigations.In effect, digital technology has significantly altered the criminal justice environment so that enterprising and opportunistic offenders have deliberately turned to the computer to perform their unlawful actions in circumstances where the device functions as the tool of the crime, the medium by which the crime is committed, as well as cases where the victim's computer, or computer system, is the victim's computer, or computer system.

As previously mentioned, the presence of modern computing technologies helps cyber criminals in cases where the device's function is incidental to the crime, such as when the machine is used to archive and secure information linking the perpetrator to illegal activities. The perpetrator, to a large extent, relies on the lack of technical capabilities in law enforcement to effectively execute the offences and escape undetected, which is a commonality in these types of crimes.Based on the analytical data available on investigators' self-assessed expertise in this field, computer offenders will have good cause to be confident about their chances of escaping capture.[3]

If we move closer to the twenty-first century, it will be clear that technological advances have opened the way for anyone who uses computer technologies today to enjoy modern and wonderful conveniences in their everyday lives, spanning from how to teach, shop, entertain, and develop a deeper understanding of market strategy and job flow.Our everyday lives have been permanently altered as a result of exponential developments in information technology. These advances allow us to interact over long distances in a matter of seconds and to collect and arrange vast volumes of data almost instantly, tasks that would otherwise be tedious and costly.However, the technical marvels that have enhanced the quality of our lives

[3] Stambaugh, H., et. al, Electronic Crime Needs Assessment for State and Local Law Enforcement, National Institute of Justice Report, Washington, Dc: U.S. Department of Justice, March 2001.Available at : https://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf

can be seen as a double-edged sword. Although computer technology has provided countless people with greater conveniences, it has also provided offenders with new opportunities.

1.5 DEFINITION OF CYBER CRIME

The Indian legislature has not specified cyber crime in any legislation, including the Information Technology Act of 2000, which deals with cyber crime. However, in general, the term "cybercrime" refers to any criminal action that is carried out over the internet or through the use of technology.

Cybercrimes are described by Dr Debarati Halder and Dr K. Jaishankar as "offences committed against persons or groups of individuals with a criminal purpose to deliberately damage the victim's identity or inflict physical or mental harm, or loss, to the victim directly or indirectly, using electronic telecommunication networks such as the Internet (chat rooms, emails, notice boards, and groups)".[4]

We don't have a clear description of cybercrime; however, the following are some general definitions:

"Criminal acts carried out by means of computers or the Internet," according to the Oxford Dictionary.[5]

"Those species of cyber crime whose genus is traditional crime and where the machine is either an object or target of the criminal conduct".[6]

"Any criminal or other offence encouraged by or requiring the use of electronic communications or computer systems, including any computer or the Internet, or either one or both of them" is classified as "cyber crime".[7]

Professor S.T. Vishwanathan had cited three definitions of Cybercrimes in his book *'The Indian Cyber Laws with Cyber Glossary'* which are as follows:-

- Any illegal activity in which a computer is a tool or object of the crime, i.e., any crime, the means or purpose of which is to influence the function of a computer.

[4] http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf (Accessed on 28th February, 2021)

[5] http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 28th February, 2021)

[6] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Accessed on 28th February, 2021)

[7] http://cybercrime.org.za/definition (Accessed on 28th February, 2021)

- Any incident associated with computer technology in which a victim suffered or could have suffered a loss; and a perpetrator, by intention, made or could have made a gain.
- Computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to the automatic transmission of data.[8]

1.6 NATURE AND SCOPE OF CYBER CRIME

Criminality is a psychologically mediated phenomenon. We will never be able to survive in a world without cybercrime, no matter how hard we try. In fact, if we haven't yet been able to get the crime rate down to a desirable level in the real world, how would we hope to do so in the virtual world, which is comparatively more unreal, infinite, and legally less controllable? However, the existence, scale, and meaning of crime in a particular society vary over time.The idea of a crime-free society is a fallacy, and crime cannot be isolated from society. As a consequence, the essence of a crime is dictated by the nature of a culture.

The complexity of a culture determines the complexity of the criminality that occurs in its environs. It is important and vital to check all of the causes that affect and lead to crime in order to comprehend crime in a society. The social and political institutions of society must grasp violence and the steps that can be taken to minimize it. When analyzing the nature and scope of a crime, the prevention and disciplinary steps taken by the machinery to control crime and criminal behaviour in society are not taken into account.

Technology advances have created new social and political issues in society, and rather than aiding the state in managing the crisis. They have created a new complicated scenario that is difficult to grasp and much more difficult to adapt existing legislation to. The state apparatus lacks the tools and expertise required to fight modern crime.

In the last three or four decades, computers have totally changed the human culture. It has not only made life simpler, but it has also significantly aided the physical, economic, and cultural integration of various parts of the world. Computer technology

[8] S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary, 2001, p. 81.

has allowed people to have access to information from all over the world when sitting in a room. Time and space barriers are no longer a problem due to new technologies. However, with the incredible benefits of using machines today, a jurisdictional problem has arisen in the legal system.

One component of transnational transactions over the internet that is difficult to assess is Jurisdiction. When courts were faced with questions of authority law, they were unable to determine the correct venue to hear lawsuits concerning cybercrime because the cyberspace or virtual universe became borderless when opposed to the real world, making it exceedingly difficult to monitor cybercrime.We are unable to solve the issue of cyber crime using local equipment because our machinery is incompatible with dealing with transnational crimes. Since cybercrime is so distinct from other forms of crime, the legislation in effect in the jurisdiction is inadequate to control it.

As a result, the global existence of cybercrime has made it impossible to control and fight. The advent of internet technology has provided us with many benefits, including the potential to cope with potential challenges and expand at an accelerated pace, but it has also provided offenders with the opportunity to commit crimes at the least amount of risk of detection. The internet has proven to be a boon to society’s deviant actions. The idea of cybercrime has risen in importance, and we are now facing a major challenge from its impact on global culture. Because of our growing dependency on technology, human civilization is becoming more vulnerable to cybercrime.

Since cybercrime has become a worldwide epidemic, nationwide generalization of crime is no longer possible in the current situation. Our definition and enforcement of cybercrime must be regional, not global. Only by enacting new legislation and preparing global prevention and defence measures would we be able to protect our society from this evil known as “Cyber Crime”.

As a result, the threat of cyber warfare/terrorism poses a significant threat to the planet and its institutions. Terrorism groups employ robotics to promote hate and attract militants, who are then trained using teaching tools. They’re also introducing blogs and websites that teach them how to use arms and make bombs, among other things.

1.7 DOCTRINE OF MENS REA AND ACTUS REUS IN CYBER CRIME

Mens Rea and Actus Reus are the two most important concepts of conventional crime. “Such a consequence of human actions as the statute aims to prohibit,” is defined as Actus Reus.[9] To be called a felony, there must be a commission or omission. Mens rea roughly refers to “a guilty state of mind.”[10] The most significant aspect of crime is the mental component. The behavior remains the same, but the state of mind turns it into a*‘reus’* and therefore an assault. About any crime necessitates the existence of a behavioural factor of some kind.[11]In the case of cybercrime, assessing the mens rea is exceedingly complicated.

In cybercrime, it’s crucial to ascertain the hacker’s mental state and whether or not the hacker was aware that the access was unauthorized. Thus, the hacker would not need to have intended to target a “Unique Device,” as long as the unauthorized access was to “any computer.” It gets easier for the hacker to show that he is an outsider with no power to enter because he is aware of the situation. However, where a hacker already has little authority, as in the case of a company executive, establishing that he violated his boundaries and was also aware of the fact that he was violating them becomes challenging.

Actus is the Latin term for “action.” Since the entire act is performed in intangible contexts, reus in cybercrime has become a task. The suspect can leave any fingerprints in the machine itself, but demonstrating that in court would be a herculean task for the law enforcement apparatus, since it must be in actual shape or at least in a form that is admissible in testimony.[12]

1.8 CHARACTERISTICS OF CYBER CRIME

Cybercrime varies greatly from conventional crime in terms of definition. In comparison, as a result of the advent of Internet technologies, this activity has earned much more serious and unregulated exposure than typical crime. As a consequence, it is important to analyze the particular features of cybercrime.

[9] J.W.C. Turner, Kenney’s Outlines of criminal law (19th Edition University Press, Cambridge 1966) 17. also at Talat Fatima, Cyber Crime (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68

[10] R.C. Nigam, “Law of Crimes in India”, Principals of criminal Law, Vol 1, (Asia Publishing House, 1965) 6.

[11] Talat Fatima, Cyber Crime (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68

[12] Ibid.

- ***People with advanced expertise*** – Since cybercrime can only be conducted by technology, one must be highly knowledgeable about the internet, machines, and the internet in order to commit such a crime. People who conduct cybercrime are well-educated and have a detailed knowledge of how to manipulate the internet, making it impossible for police to apprehend them.
- ***Geographical problems*** – In cyberspace, there are no geographical borders. A cyber criminal can commit a crime in another part of the world while sitting in some part of the world. For example, a hacker in India might compromise a system in the United States.
- ***Digital Universe*** – The process of cybercrime takes place in cyberspace, but the perpetrator is physically situated outside of cyberspace. The criminal's entire activity when committing the crime takes place in the virtual universe.
- ***Collection of Evidence -*** Owing to the complexities of cyber fraud, collecting facts and prosecuting it before a court of law is exceedingly challenging. When committing cybercrime, the perpetrator invokes the jurisdiction of many nations while still hiding in a secure location where he cannot be identified.
- ***Unimaginable scale of violence***- Cybercrime has the capacity to cause injuries and death on an unimaginable scale. Cyberbullying, cyber pornography, and other crimes have a vast scope, and they can easily ruin websites and steal company records.

1.9 LET'S SUM UP

In this chapter, we have studied the evolution of cyber crime following how various authors have defined the term *'cyber crime'* as there isn't a clear definition under the Informaton Technology Act, 2000. We have also seen the scope of cyber crime in the present era along with how actus rea and mens rea play a pivotal role with respect to cyber crime. Finally, we ended the discussion with the different characteristics of cyber crime.

1.10 FURTHER READING

- S.T. Viswanathan, *The Indian Cyber Laws with Cyber Glossary*, 2001, p. 81
- Rhiannon Williams, "The Biggest Ever Cyber Attacks and Security Breaches", The Telegraph, Available on http://www.telegraph.co.uk/technology/internet-security/10848707/The-biggestever-cyber-attacks-and-security breaches.html.

- See “Is Cyber-Terrorism the New Normal?” Available athttp://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the meaning of cyber crime?**

The Indian legislature has not specified cyber crime in any legislation, including the Information Technology Act of 2000, which deals with cyber crime. However, in general, the term “cybercrime” refers to any criminal action that is carried out over the internet or through the use of technology.

2. **What is Actus rea and Mens rea?**

Mens Rea and Actus Reus are the two most important concepts of conventional crime. “Such a consequence of human actions as the statute aims to prohibit,” is defined as Actus Reus.To be called a felony, there must be a commission or omission. Mens rea roughly refers to “a guilty state of mind.”

3. **What are the different characteristics of cyber crime?**

Cybercrime varies greatly from conventional crime in terms of definition. In comparison, as a result of the advent of Internet technologies, this activity has earned much more serious and unregulated exposure than typical crime. The different characteristics of cyber crime are:

- People with advanced expertise
- Geographical problems
- Digital Universe
- Collection of Evidence
- Unimaginable scale of violence

1.12ACTIVITY

“Criminal activities in the cyber world are quite easier and most challengeable”- Explain the statement in the light of the Information Technology Act, 2000. (2000-2500 words)

Unit 2: CLASSIFICATION OF CRIMES AGAINST INDIVIDUALS

2

Unit Structure

2.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Overview of the crimes affecting individuals
- Privacy in the technology driven world and the IT Act
- Cyber Stalking

2.2 INTRODUCTION

The rapid strides in technological developments, especially in the fields of electronics and information technology, have heralded a new age in human life. However, technological innovations are not only helpful to humans; they also have detrimental implications. While technical advances such as telephones, cars, computers, cell phones, and other technologies have offered conveniences and other advantages, they have also provided new opportunities for offenders and wrongdoers. A significant number of young and misguided children are exploiting the internet and mobile phones for entertainment while causing a slew of problems for others, some of which are illegal in nature. Many offenders are also using machines as a means to promote illegal acts, such as theft, the selling or dissemination of child pornography, the sale of cocaine, and so forth. There is also systematic patent piracy and misuse of intellectual property rights.

The exponential development and application of the internet are transforming people's lives and supplying offenders with new methods of action. Criminals and criminals all over the world profit immensely from the Internet, e-mail, and other related technologies. The anonymity offered by modern networking modes such as e-mail, chat rooms, and other facets of the internet infrastructure helps offenders to work freely.Drug groups and jihadists all over the world now have new resources in the shape of these networks for organizing and extending their operations beyond their respective national boundaries. Criminals are even messing with the machine to see how they can use it in a different direction to carry out their crimes.

Criminals exploiting networks and information technology for nefarious ends have left all facets of human activity open to cybercriminals. For example, if a computer programmer is effective in changing a patient's medical order kept in a hospital's computer, the patient's life could be jeopardized.A similar incident occurred in the United Kingdom, where the life of a 10-year-old child was put in peril. Cyber offenders are exchanging huge sums of money on a large scale. Frauds involving credit cards and ATMs are becoming more popular. People's anonymity has not been untouched. For e.g., when a senior television journalist went to withdraw money from an ATM in Delhi years ago, she wanted to get cozy with her male colleague. Their off-screen antics were filmed on the hidden camera and then shared in the offices of numerous TV stations.[13]The private video of Pamela Anderson and ex-husband Tommy Lee having sex was widely circulated online in another well-known Anderson Tape Cyber Scandal. These tapes are, without a doubt, the most popular stolen video of all time.[14] In dealing with the criminals operating in the evolution of criminality, law enforcement agencies and society must face new challenges.

2.3 CRIMES AFFECTING INDIVIDUALS

Of course, it is difficult to include a comprehensive and exhaustive list of the different kinds of illegal activity that occur in cyberspace because criminals are actively experimenting to discover new ways to commit crimes. The events in the cyber world are constant, and we are seeing a new form of cyber crime almost every day. Per contra, we will be discussing the different types of crimes affecting individuals in the present era. How the cyber crimes affect the individuals will then be very clear as most of them do affect the individuals too.

2.4 INVASION OF PRIVACY

Computers are the most significant means of protecting confidential and official records and personal knowledge in today's world. It helps you to store, manipulate, and transfer data even faster than any other concurrent record-keeping device. The Internet will now gather all sorts of information about a person that he might not be able to collect himself.When a person seeks medical attention in a hospital, for

[13] https://timesofindia.indiatimes.com/home/sunday-times/deep-focus/the-death-of-privacy/articleshow/991395.cms
[14]Ibid.

example, the hospital’s machine receives his entire medical history and records. Similarly, a businessperson stores all details about his purchases in his machine.Any person who has access to this data, whether allowed or not, may use or misuse it.

Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[15] Right to privacy is more of an implied obligation. It is the *‘right to be let alone’.*[16] Right is an interest recognized and protected by moral or legal rules. It is an interest, the violation of which would be a legal wrong. Respect for such interest would be a legal duty. It is the basic principle of jurisprudence that every right has a correlative duty, and every duty has a correlative right. But the rule is not absolute. It is subject to certain exceptions in the sense that a person may have a right, but there may not be correlative duty. Nevertheless, it would be prudent if the issues related to privacy (and confidentiality) are viewed as *‘right along with duties’.*

Allowing retained data to flow openly through the network carries the risk of jeopardizing an individual’s life and safety, as well as a nation’s protection. Individuals’ right to privacy is recognized as a constitutional right in virtually every country. The availability of data in cyberspace, whether by hacking or other means of access, can result in a criminal invasion of privacy. It also infringes the right to privacy secured by Article 21 of the Indian Constitution.The Supreme Court has ruled clearly that the right to life requires the right to privacy.[17] Every person has a right to privacy, according to Article 12 of the United Nations Declaration of Human Rights.

Unsolicited requests from banks, telecom providers, and others for a deposit, credit card, or even a new connection, according to experts, led to “enemic violation of privacy of mobile telephony users at all times and hours” and significantly damaged citizens’ constitutional rights.Personal data of subscribers is now commonly used by mobile service providers and telemarketers for commercial purposes as a product for sales marketing at the personal and financial expense of subscribers. Personal data provided by a subscriber to a cell telephone service company should be classified as private, and service providers should be forbidden from transmitting that data to other entities for commercial purposes by regulation.

[15] Westin, AF, Privacy and Freedom, 1967, London: Bodley Head.

[16] Warren and Brandeis ‘The Right to Privacy’ (1890) Harvard Law Review, IV (5).

[17] Mr. X Vs. Hospital 'Z' = 1988 AIR S.C.W. 3662; State of Maharashtra Vs. M.N. Mardikar, AIR 1991, SC 207; People's Union for Civil Liberties, V. Union of India; Kharak Singh Vs. State of U.P., 1964, ISCR, 332.

2.5 LAW OF PRIVACY: AN INDIAN PERSPECTIVE

Though the Indian Constitution has not guaranteed the right to privacy as a fundamental right to the citizens but nevertheless, the Supreme Court has come to the rescue of a common citizen, time and again, by construing *'right to privacy'* as a part of the right to *'protection of life and personal liberty'.* The right to privacy could be read into Article 21, which states that *'no person shall be deprived of his life or personal liberty except according to procedures established by law'.* In this context of personal liberty, the Supreme Court has observed that *'those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of law'.*[18]

In the case of *State vs Charulatha Joshi,*[19]the Supreme court recognized privacy rights and held that *'the constitutional right to freedom of speech and expression conferred by Article 19(1)(a) of the Constitution which includes the freedom of the press is not an absolute right. The press must first obtain the willingness of the person sought to be interviewed, and no court can pass any order if the person to be interviewed expressed his unwillingness'.*

In *People's Union for Civil Liberties (PUCL) vs Union of India,*[20]the Supreme Court held that the telephone tapping by Government under Section 5(2) of the Telegraph Act amounts infraction of Article 21. Right to privacy is a part of the Indian Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed *'except according to the procedure established by law'.*

In *Ram Jethmalani vs Union of India,*[21] the Supreme Court had dealt with the right to privacy elaborately and held as under:

'Right to privacy is an integral part of right to life. This is a cherished constitutional value, and it is important that human beings should be allowed domains of freedom that are free of public scrutiny unless they act in a lawful manner. The solution for the problem of abrogation of one zone of constitutional values cannot be the creation of another zone of abrogation of constitutional values. The notion of fundamental rights,

[18] Ram Narain v. State of Bombay, 1952 SCR 652: AIR 1959 SC 459: 1959 SCJ 679.

[19] State v. Charulatha Joshi, (1999) 4 SCC 65; See also Prabhu Dutt v. Union of India, AIR 1982 SC 6; Sheela Barse v. State of Maharashtra, (1987) 4 SCC 373.

[20] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

[21] Ram Jethmalani v. Union of India, (2011) 8 SCC 1.

such as a right to privacy as part of right to life, is not merely that the State is enjoined from derogating from them. It also includes the responsibility of the State to uphold them against the actions of others in the society, even in the context of the exercise of fundamental rights by those others'.

2.6 PRIVACY IN THE TECHNOLOGY DRIVEN WORLD

Privacy in the technology-driven world is a difficult proposition. Technology has become a kind of double-edged sword. On the one hand, it quips the person to safeguard his privacy, and on the other, it helps in blowing the privacy cover one may have had.

There are means to capture the digital footprints of the user (customer), who is browsing the Internet for various personal reasons. It all begins with capturing the Internet Protocol (IP) address. It is a kind of *personally identifiable information* that is automatically captured by another computer when any communications that is automatically captured by another computer when any communications link is made over the Internet. The computer resource in use could easily be identified as it has been given a unique IP address (static or dynamic) by the Internet Service Provider (ISP). Whenever a person browses, visits a site, sends an e-mail or chats online, he leaves his distinctive IP address behind. It is possible either by searching IP registration databases or by conducting a traceroute to determine an approximate physical location of an IP address.

2.7 INFORMATION TECHNOLOGY ACT AND PRIVACY

Regrettably, Indian laws are essentially vague on the issue of privacy rights. Even the Indian Information Technology Act of 2000, which was passed to "provide legal recognition for transactions carried out by way of electronic data exchange and other means of electronic communication," lacks sufficient protections to protect the right to privacy.However, section 72 of the Act provides a provision for punishment for violation/breach of confidentiality and privacy in the restricted sense of any person unlawfully and without the permission of the person concerned revealing any electronic record, book, log, correspondence, records, papers, or other material to which he had access under any of the provisions of the Act.

Section 72 has a limited application only. It confines itself to the acts and omissions of those persons who have been conferred powers under this Act, rules or regulations made thereunder. The ides behind the said provision is that the person who has secured access to any such information shall not take unfair advantage of it by disclosing it to the third party without obtaining the consent of the disclosing party. An obligation of confidence arises between the *'data collectors/data controller'* and a *'data subject'.* In case of unauthorized disclosure of such information, the said person shall be punished with imprisonment for a term, which may extend to two years, or with fine, which may extend to one lakh rupees, or with both.

Besides Section 72 of the Act, there is a clause under section 74 of the Act that specifies that anyone who intentionally produces, publishes, or otherwise makes available a Digital Signature Certificate for some fraudulent or unlawful intent shall be punished with imprisonment of up to two years, a fine of up to one lakh rupees, or both.

In furtherance, Section 72A has been inserted by the new amendment act, which talks about punishment for disclosure of information in breach of lawful contract. This provision creates liabilities for service providers, including an intermediary. It is in fact, a kind of data protection measure, wherein a service provider who has secured access to any material containing personal information about a person, discloses such information without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain to such a person.

Here, the issue of confidentiality and privacy as enumerated in Sections 72 and 72A of the IT Act should be read along with the reasonable restrictions imposed by Article 19(2) on right to *'freedom of speech and expression'* as enunciated in Article 19(1)(a) of the Constitution of India.

The Organization for Economic Co-operation and Development (OECD) issued recommendations in 1980, advising countries all over the world to follow sound data privacy policies in order to escape unreasonable limitations or data flows through borders.[22] In 1990, the United Nations adopted a series of guidelines for governing computerized data files.[23]

2.8 VOYEURISM

‘Voyeurism’ is described as “a sexual pervert’s act who gains joy from secretly watching sexual acts?” ‘Voyeur’ is a term used to identify someone who has a morbid curiosity in other people’s bodies or objects.The rules of Section 67 of the IT Act, 2000 and others do not extend to such heinous acts. There is a serious lacuna in the Indian Information Technology Act,2000 as it relates to the protection of privacy of individuals in the region.If the said provision is to be successfully invoked, the prosecutor must demonstrate that the accused’s photos were released on the internetin the form of a CD or via the internet.

The right to privacy is implied in the Indian Constitution under Article 21, which states the universal right to life, as the Supreme Court of India first acknowledged in 1964. However, the decision only applies to the state and is covered under the Human Rights Act, which contributed to the creation of national and state human rights commissions. In the absence of a categorical clause, law enforcement authorities usually accept that cybercrime against women comes under the rules of the Information Technology Act of 2000, the Indecent Representation of Women (Prohibition) Act of 1987, and certain parts of the Indian Penal Code.

The provisions of section 67 of the IT Act deal with the printing, dissemination, or causing to be published of any obscene material. Its spectrum contains lascivious content, information that appeals to obscene desires, and information that has the power to deprive or degrade those who are likely to hear, see, or read it. Inconsistencies created by other rules are overridden by the IT Act. Section 292 of the Indian Penal Code, which governs the selling and dissemination of indecent material such as brochures and pamphlets, is another statute that tackles the issue. Conviction will result in a three-year sentence and a fine set by the court. The Indecent Representation of Women (Prohibition) Act, 1987 attempts to put an embargo to this trend of advertising, magazines, literature, drawing, figures, and

[22] Guidelines of OECD for protection of privacy and transborder flows of personal data, Paris, 1980
[23] UN General Assembly, Resolution No. 45/95, dated 14 December, 1990.

other means of speech. However, the maximum penalty is just two years imprisonment and a fine of Rs. 2000.

The 2013 criminal law amendments, inter alia many other provisions, has incorporated Section 354-C to the Indian Penal Code, 1860 with the definition of Voyeurism. Let us have a look at this provisiton:

> **Section 354-C: Voyeurism:** Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image1 shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.
>
> **Explanations**
>
> 1. For the purpose of this section, “private act” includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy and where the victim’s genitals, posterior or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the victim is doing a sexual act that is not of a kind ordinarily done in public.
> 2. Where the victim consents to the capture of the images or any act, but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section.

The existing provisions of Indian law, according to legal experts, are not adequate enough. They claim that new technology should be used for good, and that in situations where “human rights are infringed and unsuspecting people are filmed to appeal to voyeuristic interests of others,” the legislation should include stringent punishments, such as imprisonment for both the cameraman and the seller. They further advocate an amendment to the IT Act, as it actually only requires ACPs or Deputy Superintendents of Police (DSPs) to prosecute those crimes. This restriction is unfair since there is a lack of officers up to the rank of ACP or DSP, and hence such a rule restricts police personnel. However, after the 2013 Crminal Law Amendments, FIR can be filed now in the Police Station and the Procedures are as per the provisions of the Code of Criminal Procedure, 1973.

2.9 THEFT OF IDENTITY

The term “theft of identity” or “identity theft” applies to acts of deception, theft, forgery, misrepresentation of fact, and impersonation, among other things, that include the use of another person’s identifying details. It erodes customer trust in the legitimacy of commercial transactions and infringes on personal privacy. Identity fraud may involve items like having a credit card and taking out loans in someone else’s name.The hiring of an apartment, non-payment of bills, acquiring a cellular phone service, buying a car, taking out a home loan, and other forms of illegal activities fall into this group. A more extreme form of ‘identity fraud’ happens where a thief commits a robbery in a victim’s home and leaves a felony record behind. The internet has developed into a simple, low-cost, and successful way of accessing the identity of innocent victims.

SMS spoofing is a modern form of cybercrime that comes under the umbrella of identity theft. In this type of fraud, the perpetrator uses web-based tools to send a message from a device to an innocent person by specifying another person’s name in the form of his or her cell phone number. It seems to the receiver that the message was received by the victim himself.

Section 66C of the Information Technology Act, 2000 deals with punishment for identity theft. This provision is meant to protect the identity of a user in the online medium. The prime objective of this section is to protect the privacy of all or any online users, including their personal information or data.

The perspective of the said provision is not to merely protect the information residing in a computer resource but to protect the authentication details of any person in the form of electronic signatures (including digital signatures), passwords, PINs, biometric identifiers or any such other unique identification feature. The offence of *‘identity theft’* is completed when there is a dishonest or fraudulent downloading, copying or extraction of the electronic signature, password or any other unique identification feature of any other person. In other words, the moment personal information is downloaded, copied or extracted of any person – dishonestly or fraudulently, *mens rea* comes into existence. Whether the offender makes use of such downloaded, copied or extracted personnel information will be the *actus reus* component of the crime. As per Section 66C of the Act, the offender shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to a fine which may extend to rupees one lakh.

2.10 CYBER STALKING

Stalking has long been a part of our history. It's an act ofstrutting stiffly or haughtily' or 'approaching someone undercover or without revealing one's name.' In our culture, telephone stalking, especially by children, is a widespread phenomenon. Initially, the stalking was dismissed as a mild case, with no need for state or congressional action.Minor infractions such as harassing phone calls, unnecessary gifts, excessive chasing, and so on were either ignored or dealt with by other legal provisions of law.

Cyber stalking is a form of stalking in which an electronic medium, such as the internet, is used to threaten or contact another person without their permission. The word "cyber stalking" refers to the use of electronic media as a stalking weapon, such as the internet, e-mail, SMS, MMS, and so on. Cyber stalking is typically anonymous and can be carried out by someone anywhere in the world. It does not pose a physical danger or inflict abuse.There are a number of stalking tactics that a person may use to intimidate others even though they do not share a geographical boundary. It can have a multitude of physical, mental, and psychological effects on the survivor, which can be debilitating in some situations. Since more people are using the internet in their everyday lives, the possibility of cyber stalking is on the rise.

While Indian law acknowledges cyber stalking, there is no clear legislation in place to resolve this issue. There are no clauses in the Information Technology Act of 2000 that fix cyber stalking, cyber bullying, or cyber harassment. It's a blatant mistake on the part of the administration. However, the Information Technology Amendment Act, 2008, directly addressed Cyber Stalking under Section 66A, i.e., Punishment for sending offensive messages through communication service, etc.However, critics argued that section 66A would be used as a mechanism to limit individual freedom of speech and expression, in breach of India's Constitution's Article 19(1), and in 2015, the Supreme Court of India struck down Section 66A of the Information Technology Amendment Act 2008, in the case of *Shreya Singhal vs Union of India,*[24] arguing that it was "grossly misapplied by the authorities."

As a result, the Information Technology Amendment Act, 2008 does not address stalking directly. However, the problem is treated as an"invasion of an individual's privacy," rather than the regular cyber offences discussed in the IT Act 2008. Hence, Sections 72 and 72A of the Information Technology Amendment Act, 2008 are the most commonly used provisions in India for regulating cyber stalking.

2.11 LET'S SUM UP

In this chapter, we have studied the classification of crimes affecting individuals along with the significance of right to privacy and the constitutional aspects related to it. In furtherance, we have also seen an overview of the crimes affecting individuals such as voyeurism, identity theft, cyber stalking and the provisions pertaining to the same under IT Act.

2.12 FURTHER READING

- Yar, M. (2006). *Cybercrime and society*. SAGE Publications Ltd, https://www.doi.org/10.4135/9781446212196
- Paul Bocij. (2004). Cyber Stalking: Harassment in the Internet Age and How to protect your family
- John Q. Newman. (1999) Identity Theft: The Cybercrime of the Millennium
- Susan W. Brenner. (2010) Cybercrime: Criminal Threats from Cyberspace (Crime , Media, and Popular Culture)

2.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is Cyber Stalking?**

[24] Shreya Singhal v. Union of India, (2013) 12 S.C.C. 73

Cyber stalking is a form of stalking in which an electronic medium, such as the internet, is used to threaten or contact another person without their permission. The word “cyber stalking” refers to the use of electronic media as a stalking weapon, such as the internet, e-mail, SMS, MMS, and so on.

2. **What is the meaning of Identity Theft?**

The term “theft of identity” or “identity theft” applies to acts of deception, theft, forgery, misrepresentation of fact, and impersonation, among other things, that include the use of another person’s identifying details.

3. **Which provision of IT Act protects voyeurism?**

Section 67 of the IT Act protects voyeurism. It deals with the printing, dissemination, or causing to be published of any obscene material. Its spectrum contains lascivious content, information that appeals to obscene desires, and information that has the power to deprive or degrade those who are likely to hear, see, or read it.

2.14 ACTIVITY

Discuss the procedure and safeguards provided under IT Act for crimes affecting individuals along with case laws? (2000 words)

Unit 3: CLASSIFICATION OF CRIMES AFFECTING ECONOMY

3

Unit Structure

3.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Overview of crimes affecting economy
- Different kinds of cybercrimes using the computer and Internet
- Legal provisions pertaining to it

3.2 INTRODUCTION

E-commerce is the use of the Internet for the purpose of industry and commerce growth. The widespread use of the internet for commerce and industry has aided the growth and advancement of emerging technology and communication networks. The speed and cost-effectiveness are the main benefits. Electronic shopping, also known as e-commerce, has made it possible for people to do business across national borders without having to worry about time or distance. These scientific advancements, however, are not without their drawbacks. Since such large sums of money are exchanged in e-commerce, suspects are likely to be drawn in. Criminals that are armed with advanced electronic gadgets have a lot of options when it comes to carrying out their illegal operations.Today, terrorists use malware to conduct acts of spying, cyber theft, data frauds, and vandalism on a wide scale.

3.3 HACKING

In general, the word “computer hacking” refers to the act of manipulating, vandalism, or spying in order to gain access to a computer device. After large-scale use of computer networks by government, military, and commercial organizations, cyber criminals realized the value of hacking.

The hacking strategy is based on the connectivity and security mechanism that a network or device uses in general. Hacking has historically been accomplished by the use of popular passwords, physical monitoring of the device, or confidence tricks. Following the introduction of the internet, modern hacking and computer manipulation devices have been created. The following are some of the most popular hacking techniques:

a) IP-spoofing

An individual uses this strategy to gain unauthorized access to computers or networks by impersonating an approved and trusted device within the infiltrated network. Modification of IP addresses in data packet headers sent to an incoming portion of the network's router is how it's achieved. The routers are unable to differentiate between data sent from the outside and data sent from within the network. At present, newer routers and firewalls also claim to defend against this kind of threat.

b) DNS-spoofing

The "Domain Name Service" (DNS) is a service that maps host names to IP addresses. The act of 'DNS-spoofing' is the development of a false hotsmask during the resolution of the internet. The name of the host must be resolved to its IP address for any internet connection, and this is achieved by connecting with a DNS-server, which holds the hotsmasks in databases. Hackers try to intercept contact and send bogus hostname mappings to the victim's device when performing DNS spoofing attacks. This is conveniently accomplished by using malicious site applets that the attacked user has downloaded. The user's contact can be rerouted and transmission data captured as soon as the applet is enabled.

c) Web Spoofing

'Web spoofing' is less difficult than IP and DNS spoofing, which take more advanced technical skills. It is based on an optical illusion in which characters in hyperlinks on web pages appear to make an address look legitimate but actually lead to a wrong web site.By changing the letter '0' in the address www.micrsoft.com, for example, a hacker may build an incorrect web site. The majority of users did not presume any malicious intent.

3.4 KINDS OF HACKERS

a) Scamps:

Hackers do so for pleasure and have no intention of harming anybody.

b) Pioneers:

These are mostly young men who are intrigued by innovative new technology and pursue them without really knowing what they would discover.

c) Vandals:

Such hackers do harm for no personal gain.

d) Explorers:

Breaking into a computer machine is normally a pleasurable experience for such hackers.

e) Addicts:

Such individuals are physically addicted to hacking and abusing information technologies.

3.5 LEGAL PROVISIONS UNDER IT ACT

Hacking is a crime under sections 66 and 70 of the Indian Information Technology Act, 2000, and is punishable with imprisonment for up to three years, a fine of up to two lakh rupees, or both. However, if the hacking is performed on a secure device, the penalty is more serious.

It is necessary to note that under Indian law, a hacker who gains unauthorized access to another's computer will not be punished.It is only punishable if an intruder enters and then "destroys, deletes, or modifies any knowledge residing in a computer property, or diminishes its worth or usefulness, or harms it in any way." Unauthorized entry is only punishable if it is rendered into a "Protected system," as specified by Section 70 of the Act.

3.6 VIRUS/MALICIOUS PROGRAMMES

Viruses, worms, Trojan horses, logic bombs, hoaxes, and other malicious programmes are designed to harm the victim's computer system. They are:

a) Virus:

The virus is a malicious programme that infects an executable file and causes it to function in a different way than it was intended. It can spread by attaching itself to executable files such as application programmes, operating systems, macros, scripts, the boot sector of a hard disk or floppy disc, and so on.

b) Worms:

Worms are malicious programmes that cause harm by multiplying and spreading copies of themselves. It does not change or delete any files, unlike viruses. It releases a worm into the internet, which slows or clogs the network because the worms keep multiplying, affecting and then sending copies to other computers.

c) Trojan Horse:

It is a seemingly innocent programme that is typically used by hackers to collect data such as passwords, credit card numbers, and other sensitive information. Such a programme can be transmitted to the victim's computer by an outsider or downloaded by the victim inadvertently from another computer, assuming it is a useful programme.

d) Logic Bomb:

It is also a malicious programme executable at a particular event. It marks the program to go into an infinite loop, crash the computer, delete data files or causes some other kind of damage to the computer or its data.

e) Hoax:

It's just a false warning about the existence of a malicious program.

Since the internet is based on the interconnection of computer networks, it is easier to send viruses or malicious programs. The most popular way for viruses and malicious programs to spread is via the internet and e-mail. Distance is no longer an issue because the whole planet has become a village.

3.7 COMPUTER SABOTAGE

The machine has grown in value as states, businesses, and individuals become increasingly reliant on computers for data storage. The days of sabotage being committed by physically damaging machines or shooting or blasting a structure are long gone. Also, insiders have the ability to inflict sabotage by using electrical short circuits or saline solution on the hardware. Computer attacks and extortion are becoming more common as people become more reliant on computer networks and information technologies. Since vast amounts of sensitive and classified documents and records are stored on computer hard disks, hackers now have the ability to steal these data and information and then use blackmail to extort money from businesses and individuals.

3.8 COMPUTER FRAUD

The term “computer fraud” refers to common economic crimes committed by criminals using computer networks and internet access. Initially, computer frauds were restricted to data manipulation, tampering of invoices, account balances, data theft, wage payment, and so on. With the invention of the internet, computers all over the world are linked, and the potential for fraud has grown beyond national boundaries.

Certain intrinsic characteristics of the internet, such as transparency, cost-effectiveness, scope, challenges in authenticating identification, and so on, have made it difficult to detect fraudulent activity. A fake investment plan that seems legitimate and real can be advertised all over the world in seconds and at a low cost using the internet and e-mail services. As a result, it is much easier for a cyber fraudster to locate a huge number of gullible users using Internet services. The risk of such fraud is also evident in the area of e-commerce, where products and services are purchased electronically, and purchases are made using credit cards or other similar payment methods.

The Information Technology Act, 2000, made changes to the Indian Penal Code to include electronic frauds in the same category as conventional frauds. In addition, the Information Technology Act, 2000 contains provisions against fraud. For e.g., ‘tampering with computer source of text’ is punishable under Section 65 of the Act. ‘Hacking of computer system’ is punishable under Section 66 of the Act. The illegal acts of “misrepresentation” and “breach of secrecy and privacy,” respectively, are covered by sections 71 and 72 of the Act. Apart from section 100 of the Criminal Procedure Code, section 76 of the Act prescribes particular methods for the confiscation of devices used in electronic crimes, such as computers, computer systems, floppies, floppy disks, tapes, drives, and all other attachments associated dangers. Similarly, the majority of countries have enacted new legislation or amended existing legislation to make cyber fraud illegal.

3.9 COMPUTER COUNTERFEITING

Software theft is somewhat similar to computer counterfeiting. For the whole world, the validity of any document related to e-commerce is extremely important. Computer-assisted advanced printing technology is now assisting offenders in the production of counterfeit money notes, judicial and non-judicial stamps. Such paper counterfeiting is made possible by digital technologies.

Previously, provisions of the Indian Penal Code, such as Sections 417 (cheating), 465 (forgery), 471 (using as genuine a forged document known to be forged), 467 (forgery of valuable security, etc., or to gain money), etc., dealt with computer fraud and counterfeiting. However, under Section 74 of the Information Technology Act, 2000, strict rules have been made to deal with theft, forgery, and counterfeiting of digital signatures only. Section 74 of the Act deals with digital signatures only, which is one of the IT Act’s major flaws.

3.9 THEFT OF TELECOMMUNICATION SERVICE AND MOBILE CLONING

Because of recent technological advances, telecommunication systems are now heavily reliant on computer networks. The repeater system, exchange, telephone networks, and other computer networks use similar technologies. As a result, it is easier for a hacker to gain access to the contact network’s infrastructure and make false calls or offer free services to others.The exponential increase in the use of mobile phones has opened up a new area for illegal activity. Criminals normally break the encryption to link the handset to the service provider or use the phone for their own purposes. ‘Mobile Phone Cloning’ is a modern form of cybercrime that adds a new layer to the field of cybercrime. “Mobile Phone Cloning” is a crime in which “security data from one phone is re-programmed into another phone so that calls can be made from all phones but only the original is billed.”

3.10 COPYRIGHT INFRINGEMENT AND SOFTWARE PIRACY

Copyrights refer to an author’s or producer’s exclusive right to do or authorize others to do such actions for the publishing or commercial exploitation of copyright content, which may include a novel, literature, theatrical, musical, paintings and other creative works, cinematograph video and sound recording, and so on. Such a right is known as quid pro quo, because it is the benefit provided to the creator in exchange for his invention or intellectual property. As a result, the commercial use of copyright materials by unauthorized individuals is considered “piracy,” and is a felony against the author as well as society.

Copyright piracy is one of the most common cyber crimes perpetrated in cyberspace. Copyright preservation for publishers or creators of books, audio or video cassettes, and software programs remains one of the most difficult challenges facing law enforcement agencies all around the world. Intellectual property rights, like computer software, must be protected in order for our useful skills and lives to continue to expand. It is important for legal guardians to provide effective and sufficient protection to writers’ interests so that they can benefit from their intellectual creations.

Advanced computing technology has made it possible to pirate copyrighted works in vast quantities and at a low price. Because of widespread video theft, an original video CD of a Hindi film worth Rs. 200 is now available in the market for just Rs. 20. Since manufacturing is faster, the danger associated with physical distribution is often reduced by online distribution, piracy has been promoted and abetted on a wide scale by the internet. Apart from the tech industry, piracy has a major impact on the film and music industries. Because of the widespread proliferation of pirated copies and online downloads, the recording industry’s entire survival is in jeopardy.

For the preservation of copyright in India, the Copyright Act of 1957 was passed. The description “literary work” involves computer systems, charts, and compilations, and computer databases, according to section 2 (o) of the Act. In the case of violation of copyrights and software piracy, a legal suit can be filed to obtain an injunction, punitive damages, and benefits accounts. A criminal investigation can also be brought under the terms of Sections 63-70 of the same Act, in addition to civil proceedings.

3.11ECONOMIC ESPIONAGE

For the storage and processing of data and trade secrets, commercial and business organizations are increasingly reliant on computers. Because of this reliance on machines, the complexity of economic espionage in cyberspace has grown. Several incidents of business secrets being stolen from reputable firms and sold to competitors have been reported all over the world. These offences have been seen involving both outsiders and employees of such businesses. Employees in private organizations are occasionally enticed by rivals to purchase trade secrets. Hacking is often done by an outsider for the purpose of collecting trade knowledge for illegal purposes.

3.12 TAX EVASION AND MONEY LAUNDERING

Money laundering is an illegal enterprise in which criminal proceeds are given the illusion of legality. To gain the requisite credibility, the criminals must first cut their hard-earned money and then spend it in another transaction. For example, a notorious criminal in Mumbai who makes money by extortion is frequently seen investing his illicit funds in Bollywood’s film and music industries. Money laundering is difficult by using traditional form of cash.As a result, foreign criminals involved in drug trafficking, smuggling, and other illicit activities faced significant challenges in transporting large sums of money. In these cases, they use ‘Hawala’ tactics, in which a criminal sitting in Dubai can pass money to Mumbai via Hawala agents in a matter of hours. For this, an agent in Dubai accepts cash and sends a message in code words to the individual concerned in Mumbai via the internet or mobile. As such, the money is exchanged without the possibility of being intercepted or falling into the hands of law enforcement officers.

With the rise of e-commerce, tax evasion has now become much simpler. Since the volume of digital cash or e-cash in an individual’s hands is not traceable in normal conditions, it has become almost impossible for a taxman or any law enforcement agency to keep track of a person engaging in e-income commerce’s and spending. Following technical advancements in the cyber space, conventional anti-tax and anti-money laundering systems, as well as laws, have been unsuccessful in various countries around the world.

3.13 CYBER SQUATTING

Cyber squatting is a practice in which website names are blocked on the internet and later traced by unscrupulous individuals for commercial gain. Cyber squatting mostly affects well-known private entities, actors, and key government institutions. To combat the illegal act, the United States of America passed the Anti-cyber Squatting Consumer Protection Act of 1999. The Act further amends Section 43 of the Trademark Act of 1946 to impose legal liability on anybody who registers, uses, or traffics in a domain name. The Act also establishes a penalty for violators and the offender is liable to pay damages and profits, as well as statutory damages ranging from $1,000 per domain, at the discretion of the judge.

3.14 INTERNET MARKETING FRAUD

Net frauds are the most recent form of cybercrime to emerge on the internet. Many fake businesses set up websites and recruit members via the internet as part of their business model. New members are paid a fee and invited to bring in more members in exchange for a commission. When the number of participants becomes unmanageable, the firms close their doors and disappear, duping all of their customers. The promised commission for adding new candidates, as well as the original payment, was forfeited by the victim members.

3.15 LET’S SUM UP

In this chapter, we have studied the classification of crimes affecting the economy along with the legal provisions pertaining to it. In furtherance, we have also seen an overview of such crimes such as hacking, cyber squatting, computer sabotage etc., and the provisions under IPC and IT Act.

3.16 FURTHER READING

- Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. Measuring the Cost of Cybercrime. In The Economics of Information Security and Privacy. Springer Berlin Heidelberg, 265–300.
- Sam Brand and Richard Price. 2000. The economic and social costs of crime. Home Oce London
- Kshetri, Nir. (2006). The simple economics of cybercrimes. Security & Privacy, IEEE. 4. 33 - 39. 10.1109/MSP.2006.27.

- M. Riek, R. Bohme, and T. Moore. 2015. Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. Dependable and Secure Computing, IEEE Transactions on PP, 99 (2015), 1–1. DOI:http://dx.doi.org/10.1109/TDSC. 2015.2410795

3.17 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is computer hacking?**

The word “computer hacking” refers to the act of manipulating, vandalism, or spying in order to gain access to a computer device.

2. **What is computer fraud?**

The term “computer fraud” refers to common economic crimes committed by criminals using computer networks and internet access.

3. **What is Trojan Horse?**

It is a seemingly innocent program that is typically used by hackers to collect data such as passwords, credit card numbers, and other sensitive information. Such a program can be transmitted to the victim’s computer by an outsider or downloaded by the victim inadvertently from another computer, assuming it is a useful program.

3.18 ACTIVITY

Elucidate the different kinds of crimes affecting economy along with the legal provisions pertaining to it. (2000-2500 words)

Unit 4: CLASSIFICATION OF CRIMES AGAINST SOCIETY AT LARGE

4

Unit Structure

4.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Overview of the cybercrimes affecting nations and society at large
- Shortcomings of provisions and definitions under IT Act, 2000
- Future prospects and needs

4.2 CRIMES AFFECTING NATIONS

a) Cyber Terrorism

Cyber Terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives. It is a combination of cyberspace and terrorism. There isn't an appropriate definition for Cyber Terrorism which can be accepted worldwide. However, a universally acknowledged definition of Cyber Terrorism is 'A criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and/or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda'.

Cyber terrorism is the use of technology and the internet to create and spread terrorism. It is a more modern type of terrorism, and an illegal act carried out to threaten or coerce a country or its citizens into pursuing political or social objectives. To be classified as cyber terrorism, an attack must threaten or inflict violence against individuals, goods, or the government, and/or cause fear of harm among those who are affected.

The use of computer and internet networks for terrorist purposes has raised the challenge of cyber crime to the national and international community's defence. Government departments use computers to provide and communicate useful data in the transportation, medical, defence, finance, and financial services industries. Such sensitive material is not impenetrable to outsiders. They are vulnerable to attacks by hackers and terrorists, and the valuable information they provide, if intercepted, may have catastrophic consequences for the stability of their respective countries.The thiefs of the world today with the aid of a keyboard to do more serious harm to an organization or a government than a gun or a missile.

Terrorists are using new information systems to devise tactics, collect money, generate propaganda, and exchange messages among themselves in order to carry out their plans.

b) Cyber Warfare

Another source of controversy is the use of computers by defence forces during a conflict. Most armies around the world are now entirely reliant on electronic networks for all types of defensive and offensive activities, and cyber warfare has become an integral part of military strategy. Cyber espionage to collect information about the enemy's army, as well as cyber attacks to immobilize the enemy by disrupting their information infrastructure, are also looming high.The protection of a server storing Army strategic information is a newer problem for defence authorities. The issue of electronic warfare security is now before the main international law authorities to be resolved effectively.

c) Unaccredited Calls

There are many illegal agencies running all over the world that make unaccredited international telephonic calls, causing damage to respective countries' exchequer. When an individual receives such calls, no telephone number appears on the caller ID panel of the handset. In India, phone companies like BSNL and MTNL are struggling miserably in their efforts to monitor such calls, which have uncovered a foreign SIM cloning industry that has enabled ISO calls between India and Saudi Arabia using cloned SIM cards.

In another incident, the CBI apprehended two engineers, Ashok and Suresh, who were involved in a net-heist and were using the internet to make international calls as if they were local calls. Five exchanges were confiscated in Chennai, and one such device was discovered in Hyderabad.The CBI team discovered advanced computer devices, as well as mobile handsets, wired wireless sets, switches, modems, and other equipment, connecting to internet broadband cables. They lifted foreign calls transmitted into India via Voice Over Internet Protocol (VOIP or Net telephony) and distributed them into the BSNL or MTNL networks using software-based exchanges.The BSNL and MTNL were robbed of an estimated Rs. 400 crore by such operators.

4.3 CRIMES AFFECTING SOCIETY

a) *Racial Propaganda*

The political leaders and their groups are often seen using computers and media networks to spread their political message. Terrorists and antisocial organizations aren't far behind in using electronic and internet networks to spread social and communal hatred ideology among the people.For example, Pakistani television networks are frequently seen spreading political and social propaganda among Kashmiris in order to instigate an indirect war. Terror groups and other radical organizations all over the world have begun to use the internet to distribute social and communal messaging among their target groups, thanks to the global spread of internet networks. Such acts of terrorism are much more successful than conventional terrorism approaches.

b) *Pornography*

Pornography and paedophilia dissemination on the digital internet is one of the most serious machine and internet network abuses. Paedophiles have been given a simple way to organize and spread derogatory and obscenity materials around the world thanks to the internet networks. The suspecting children's quick access to these paedophiles through the internet leaves them vulnerable to abuse.

As more classrooms and homes become wired to the internet, children now have convenient access to the internet.As a result of this incentive, children are more likely to have free access to inappropriate content that are readily accessible on the Internet.Such materials that include sexually suggestive photographs or explanations, plead hatred and bigotry, crime, substance addiction, and other criminal acts are more likely to mislead students.Cyber criminals now have a simple way to befriend a kid in a chat room without revealing his name, then manipulate him. As a result, the internet has become extremely hazardous to youth. However, it is not appropriate to keep children completely off the internet since the internet contains a wealth of valuable knowledge and instructional resources for children. On the internet, you can find useful stuff like online friendships, pen pals, and so on.Parental monitoring is necessary to prevent them from abusing the internet and falling into the hands of paedophiles and other poor actors who promote illegal acts.

Section 67 of the Information Technology Act, 2000 discusses about publishing of information which is obscene in electronic form. The ingredients of offence under the said provision are:

- Publication or transmission in the electronic form,
- Any material lascivious or appeals to the prurient interest,
- Tendency to deprave and corrupt persons,
- Likely-audience,
- To read, see or hear the matter contained or embodied in electronic form.

It is important that while interpreting this provision, the court may exercise the interests of our contemporary society and particularly the influence of the obscene material in electronic form on it. For this purpose, even the State Governments may have to apprehend perpetrators of *'cyber obscenity'* by invoking local State legislation's accordingly. In the case of *Prakas (Dr.) vs State of Tamil Nadu,*[25] the petitioner was detained under Section 3(1) of the Tamil Nadu Prevention of Dangerous Activities of Bootleggers, Drug Offenders, Goondas, Immoral Traffic Offenders and Slum Grabbers Act. The main grounds of detention against the petitioner were that he was indulging in offences under Section 67 of the IT Act, 2000, Section 4 and 6 of the Indecent Representation of Women (Prohibition) Act, 1986 and under Section 27 of the Arms Act, 1959. The petitioner challenged his detention under Article 32 of the Indian Constitution.

The petition was dismissed, as the Supreme Court did not find much merit in the plea that the delay of two days in furnishing translated copies of documents had caused any prejudice to the detenu. It held that the contents of the letter received from members of the public *pro bono publico,* were not extraneous or irrelevant.

In furtherance, to combat cyber pornography, additionally, Section 67A was introduced under IT Act that talks about the punishment for publishing or transmitting material containing sexually explicit act etc. The ingredients of offence under the said provision are:

- Publication or transmission in the electronic form,
- Any material containing sexually explicit act or conduct.

[25] Prakash (Dr.) v. State of Tamil Nadu, (2002) 7 SCC 759.

It is significant to note that publication or transmission in the electronic form includes dissemination, storage and transmission of information or data in electronic form.

In view of the ease with which obscene content can be replicated, misused and distributed over the Internet using all kinds of information technology and communication tools – it was felt by the lawmakers to move beyond *'likely audience'* test of Section 67 and to provide more stringent mechanism to combat obscenity in the electronic form.

The term *'sexually explicit act or conduct'* has been qualified by the word *'explicit'* meaning thereby that mere *'obscene act or conduct'* may not fall under this provision. For punishment under this section, *'publication or transmission of sexually explicit act or conduct'* is an essential ingredient. Hence the difference between Section 67 and 67A depends on the nature of obscene content.

	Section 67	**Section 67A**
Nature of offence	Punishment for publishing or transmitting obscenity in electronic form	Punishment for publishing or transmitting sexually explicit act or conduct
Applicability	Generic	Specific
Test of Obscenity	Likely audience test to prove obscenity	No likely-audience test. Whether content in question – is it patently or grossly explicit?
Punishment	First conviction – 3 years, and fine which may extend to five lakh rupees. Second conviction – 5 years and fine which may extend to 10 lakh rupees.	First conviction – 5 years, and fine which may extend to 10 lakh rupees. Second conviction – 7 years and fine which may extend to 10 lakh rupees

The amendment Act has incorporated the *Exception* as provided under Section 292 of IPC as proviso in the Sections 67 and 67A.

The Supreme Court in *Kamlesh Vaswani vs Union of India,*[26] has been approached to direct the respondents to block the pornography websites, platforms, links or downloading by whatever other Internet means or name in order to prevent easy access whether in private or public. The questions are twofold: (a) whether, pornography can be blocked in absolute forms? and (b) whether blocking of adult pornography is violative of freedom of speech and expression as enshrined under Article 19(1)(a) of the Indian Constitution? Interestingly, during the proceedings before the court, the respondent did block 847 websites, allegedly depicting child pornography content but had to hastily withdraw the order as majority of the listed website on examination found to carry only adult pornography content.

The issues referred to publication or transmission of obscene information in electronic form has to be also looked at from the perspective of *'extra-territorial'* jurisdiction and Internet technologies, keeping in view that *'obscenity'* is no longer a local and static phenomenon. It is now global and dynamic in nature and thus needs strict interpretation of statute.

4.4 CERTAIN SHORTCOMINGS

Despite the fact that there are certain definitions of contraventions and crimes, as well as their fines and sentences, certain questions remain unsolved. Many procedural forms and methods of crime identification and deterrence have seen less consideration from legislators. These flaws can be discussed under the headings below.

a) ***Power of Police to Enter and Search Limited to Higher Officers and to Public Places:***

While the Act grants police officers up to the rank of Deputy Superintendent of Police (DSP) broad powers to access and search public places without a warrant and to apprehend without a warrant anybody who is legitimately accused of having committed, committing, or about to commit any crime under the Act, this authority is restricted to "public places" only.These felony offences can also be committed or are being performed on a wide scale from private residences and other private locations. Since police departments do not have enough DSP level officers to handle too many

[26] Kamlesh Vaswani v. Union of India, (2016) 7 SCC 592

investigations, the Act's requirement that only an officer of the rank of DSP can prosecute the case or conduct a search and seize is also a major restriction. Furthermore, such sweeping powers of search and seizure can result in violations of privacy and human rights.

b) Lacks Definition of Cyber Stalking and Harassment:

Hacking, damage to electronic source code, publication of pornographic material, and violation of a security device are all covered in Chapter XI of the Act, which is titled "offenses." Cyber stalking and other forms of violence, on the other hand, was completely ignored.

c) Improper definition of Hacking:

The meaning of "hacking" in section 66 (1) of the Act does not correspond to the generally accepted concept. The meaning of section 66 (1) is so broad that any conduct an individual engages in over the internet could be protected by the section's mischief. In addition, the term "wrongful loss" is not specified in the Act. Furthermore, there are no prescribed metrics for demonstrating the declining value of content.

d) Lacks of Steps for Checking Internet and Copyright Piracy:

Despite the fact that such infringements have been rampant since the invention of the internet, there seems to be an act of reasonable steps in the field of verifying the theft of copyright of music, lyrics, images, and other works in the Act. Violations of intellectual property rights and piracy in the cyberspace will result in a variety of civil penalties.

e) Lack of International Cooperation:

Since the effect and scope of cybercrime are global, any attempt made at the national level cannot be considered frivolous. Until proactive measures are taken at the international level by international collaboration, it is impossible to check terrorist activities perpetrated through the internet by aliens living and working from other countries. Achieving such constructive global partnership is also a long way off.

f) Lack of Appropriate Guidelines for Investigation:

In the world of cybercrime, conventional investigative techniques are incapable of detecting and collecting data. Since the cyber world is rapidly evolving, the legislation must be updated to keep up. Aside from amending the Indian Evidence

Act of 1872 and the Bankers Book Evidence Act of 1891, new strategies for making electronic documents admissible as evidence in a court of law are needed. The current techniques used by the police are also in the early stages of growth.

4.5 FUTURE PROSPECTS AND NEEDS

India’s modest start in the world of cyberspace can be attributed to the passage of the Information Technology Act, 2000. This initiative is both timely and fitting, as India is now recognized as a global pioneer in the field of information technology. However, the scope of cyber legislation must be expanded to include an increasing number of cyber operations. The problem could be addressed by amending the Indian Penal Code to reflect the evolving nature of cybercrime. Legislative attention is also needed in the field of data security.Such legislative acts are required to protect Indian computer and internet users, as well as their right to privacy, including Indian organizations, corporations, business firms, and individuals.

The Indian Parliament has not dealt with procedural issues properly, such as inquiry and evidence evaluation. Sections 76, 78, and 80 of the Act deal with investigation, capture, search, and detention, as well as making the rules of the Criminal Procedure Code applicable to such admission, search, and arrests by responsible authorities. In this regard, certain required changes to the Indian Penal Code and the Indian Evidence Act have been introduced.However, since criminals are better trained than law enforcement officers, law enforcement agencies continue to face problems. Surveillance, search and arrest, forensic elements, proof gathering in transnational situations, and other issues include well-defined rules in today’s world.

Special courts for the prosecution of cyber criminals should be created, and the judges who preside over them should be adequately and technically qualified to test facts technologically. Efforts can be made to raise public consciousness and create capacity within representatives of law enforcement departments and the criminal justice administration.In the police force, an adequate number of highly trained detective officers and forensic technicians should be hired, and a special cell should be established to efficiently deal with cyber crimes.

4.6 LET'S SUM UP

In this chapter, we have studied the cybercrimes affecting nations and society at large along with the shortcomings in the Information Technology Act, 2000. In furtherance, we have also seen the future prospects and needs or amendments needed in the Information Technology Act for the betterment of the society.

4.7 FURTHER READING

- Cybercrime and Society – By MajidYar, SAGE publication India Pvt. Ltd, NewDelhi.
- Cybercrime: Criminal Threat from Cyberspace. Goodman and Brenner, "Emerging Consensus on Criminal Conduct on Cyberspace", International Journal of Law and information technology, Vol. 10 No 2, Oxford University press 2002.
- Black , G. Patrick and Hawk, Kenneth R. (2010) Computer and Internet crimes, San Francisco, California [Online] available from <http://www.fd.org/pdf_lib/WS2010/WS2010_Computer_Crimes.pdf>
- Eric J. Sinrod and William P. Reilly (2000) cybercrimes: a practical approach to the application of federal computer crime laws; Santa Clara university school of law Journal vol16, number 2 [Online] available from < http://www.sinrodlaw. com/CyberCrime.pdf>

4.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the ingredients of Section 67 of the IT Act, 2000?**

The ingredients of offence under the said provision are:

- Publication or transmission in the electronic form,
- Any material lascivious or appeals to the prurient interest,
- Tendency to deprave and corrupt persons,
- Likely-audience,
- To read, see or hear the matter contained or embodied in electronic form.

2. **What is the meaning of unaccredited calls?**

When an individual receives such calls, no telephone number appears on the caller ID panel of the handset. This is generally known as unaccredited calls. In India, phone companies like BSNL and MTNL are struggling miserably in their efforts to monitor such calls, which have uncovered a foreign SIM cloning industry that has enabled ISO calls between India and Saudi Arabia using cloned SIM cards.

3. **What is Cyber Terrorism?**

Cyber Terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country’s government or citizens in furtherance of political or social objectives.

4.9 ACTIVITY

Elaborate on the cybercrimes affecting the nation and society at large along with case laws/case studies? (1500-2000 words)

Block-2

LEGISLATIVE FRAMEWORK OF CYBERCRIMES

Unit 1: LEGAL ISSUES AND FRAMEWORK OFINTERCEPTING WiFi TRANSMISSIONS

1

Unit Structure

1.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- WiFi Technology
- How privacy is infringed using WiFi Technology
- Eavesdropping on WiFi and Legal Framework

1.2 INTRODUCTION

WiFi stands for wireless fidelity (wireless) and refers to a set of protocols that enable computers and other devices to link to local area networks wirelessly. WiFi technology proliferation is a success story in standards growth, representing a demand worth more than $750 million per quarter globally (Infonetics Research). As a standard feature, most computer systems, especially laptops, come with WiFi-compliant hardware and software. Even the cheapest laptop sold at Wal-Mart, for example, comes with WiFi. Furthermore, the equipment used to set up your own WAN—using the same computers and Internet service—costs less than $100.

A variety of organizations have decided to make WiFi connectivity open to anybody who wants to use it. Dartmouth College has free WiFi in the campus; Panera Bread and several CompUSA shops around the country have free WiFi; and Bradley International Airport in Connecticut and Ft. Lauderdale Airport in Florida also have free WiFi. WiFi is no longer a technology used solely by the technologically sophisticated early adopters; it has clearly entered the mainstream in terms of acceptance and application.

1.3 WiFi TECHNOLOGY

WiFi is part of the IEEE (I-triple-E), or Institute of Electrical and Electronics Engineers. The IEEE is a standards-setting organization that established the 802 families of standards. These specifications define a framework—physical media and operating characteristics—that allows two or more devices to communicate in a network. The 802.3 protocol, which is the Ethernet interface, is the most well-known of all specifications. The Ethernet protocol specifies a physical networking method for use in a local area network (LAN). Ethernet is also the networking mode for the vast majority of computer networks; nearly every computer sold now has an Ethernet jack for connecting to an Ethernet network. The vast expansion of computer networks in companies, classrooms, and government buildings is most likely due to the popularity of the 802.3 specification.

IEEE's 802.11 specificationsare seeing a similar surge in popularity and growth. The 802.11 protocol is a set of wireless local area network standards (WLANs). It specifies the form of physical communication between network devices, similar to the 802.3 standards, except instead of communication over a physical connection via cabling, the 802.11 standard specifies the communication between devices through infrared and radio frequency (RF) transmissions.While infrared has been useful in some situations—for example, short-range wireless printing—it has been overshadowed by the use of radio frequency transmissions.

Each computer on a WiFi network must have a wireless card or an 802.11 compliant radio transceiver in order to link to the network. Some computers have built-in wireless cards, while others need an extra wireless card, while still others will need to use a PCMCIA slot or a USB port to access one. A transceiver tuned to a specific frequency, as specified by the 802.11 standard, is included inside this wireless card. An access point is a system that functions as a connector between devices on the wireless network and others on the wired local area network.The access point is configured by the network user, and authentication and encryption solutions are available—most security features are disabled by default. The wireless card in a computer (or other device) communicates with the access point to transmit data and network management information over the selected radio frequency.

1.4 AUTHENTICATION AND PRIVACY IN THE 802.11 STANDARD

It's worth noting that both authentication (who is able to connect to the network) and anonymity (who is allowed to access details off the network) are discussed in the 802.11 guidelines. Users of WiFi systems, on the other hand, seldom take the time to correctly install their WiFi network. A cellular network is not the same as a physical-wired network. To link to a physical network, one must first have physical access to the network. As a consequence, physical authentication is critical for authenticating users in a physical network.Wireless networks, on the other hand, do not remain conveniently enclosed inside the walls of a building—authentication is used to determine who is placed on a WLAN.

“The service used to determine the status of one station as a part of the collection of stations permitted to associate with another station,” according to the 802 guidelines. (R2003) ANSI/IEEE Std 802.11, 1999 Edition) As a result, there must be a way to restrict entry to a certain WLAN—and there is. One approach is to use MAC address authentication to control access. The access point maintains a list of approved MAC addresses during this process. WLAN connections would be enabled for network interface cards with MAC addresses on the accepted list. The entry point would not let you in if your name isn't on the list.

Another method for controlling authentication is encryption. WLANs can be programmed to use a range of encryption schemes, the most popular of which are WEP and WPA. By restricting the decryption of WLAN signals, encryption regulates authentication. To decode the signal, approved users must have the requisite secret key—indeed, they must have the correct credentials to bind to the access point at all. To assist the user with authentication, one would presume the equipment would allow either MAC access control or one of the encryption schemes by design. This is not the case, though. The default configuration of most access points is known as Open Device Authentication in the 802.11 protocol. Any system that requests authentication can be authenticated and connected to the WLAN using this scheme. Excluding the fact that more reliable methods of authentication exist—MAC filtering and encryption—the 802.11 protocol describes open framework authentication as the default setting for 802.11 applications.

1.5 PRIVACY

The routing of information protects secrecy in a wired LAN. On a LAN, routers and switches monitor the flow of data such that computers on the LAN receive either data that is directly addressed to them or data that is broadcast to all devices. Eavesdropping on a wired network, on the other hand, can be impossible, requiring physical access to the network and/or direct access to the computer of interest. If anyone wanted to listen in on data traffic on the cable between computer X and the network switch, for example, the eavesdropper would only be able to see traffic transmitted to computer X.

Inside a WLAN, data is transmitted over RF transmissions to all computers connected to the WLAN; data is not limited to moving in specific cables to a single computer. Since RF cannot be contained, data intended for any of the devices in a WLAN can be viewed at a much higher level without having physical access to the network. Furthermore, the radio waves produced by the access points often surpass the confines of the space or building in which they are located and intended for use.

1.6 EAVESDROPPING ON WiFi

Eavesdropping on WiFi communications does not take a lot of experience or ability, and the equipment, both hardware and software, is readily accessible. There are a range of tech products that can both locate and listen in on WiFi transmissions. For the most part, these software packages are fully legal network analyzers that network operators use to debug networks and detect unwanted access points.

Any non-encrypted contact over the WAN can be snatched from the airwaves and shown. Limiting who connects to a network makes the entire network secure, specifically the details on other computers on the network, but it does little to deter people from intercepting unencrypted transmissions. Transmissions must be encrypted to prevent the contents of the transmission from being accessed by any 802.11-equipped computer.

1.7 LEGAL FRAMEWORK

We must examine how current regulations apply to WiFi technologies in order to fully comprehend the legitimacy of WiFi eavesdropping. As we'll see, federal laws governing the interception of different forms of electronic messages don't seem to extend to WiFi transmissions.

- ***The Electronic Communications Privacy Act (ECPA)***

Despite the fact thatWiFi messages come within the definition of electronic communications as established by the ECPA, the signals sent by WiFi devices are open to the general public unless they are secured. As a consequence, the interception of non-encrypted WiFi signals that are not transmitted by a common carrier is not protected by ECPA.

Under the ECPA, WiFi messages will be called “electronic communications.” The Electronic Communications Privacy Act (ECPA) forbids the interception of all electronic communications, regardless of the physical medium of transmission (USC 18 §2510). “Any transmission of signs, messages, writing, pictures, sounds, data, or intelligence of any kind conveyed in whole or in part by a cable, antenna, electromagnetic, photoelectronic, or photo-optical device that affects interstate or international commerce,” according to the ECPA.In the past, judges have used a vague description of what constitutes interstate commerce.As a consequence, using WLANs to transfer data, particularly when connecting to the Internet, would be called “electronic communications” under the ECPA.

A data trespasser is someone who gains unauthorized access to a protected computer and therefore has no fair sense of privacy in any contact sent to, from, or from the protected computer (USC 18 § 2510). It’s worth noting that, like the CFAA, this concept makes no allowances for wireless eavesdroppers who don’t need entry. The ECPA (USC 18 §2511 (1)(a)) punishes someone who “intentionally intercepts, endeavours to intercept, or procures some other entity to intercept or endeavour to intercept any cable, oral, or electronic contact.”

Despite the fact thatWiFi transmissions fall under the ECPA’s concept of electronic communications, the statute exempts electronic communications that are easily accessible to the general public.Typical WiFi broadcasts have a lot of characteristics that make them easily available to the general public.As a result, it seems that the ECPA does not apply to most WiFi transmissions.

WiFi transmissions are not scrambled or encrypted, for instance. The 802.11 standard’s default configuration is open device authentication with no encryption.As a result, 802.11 WiFi networks do not follow these requirements in their default configuration, with no encryption allowed. Next, WiFi broadcasts do not use modulation techniques whose basic parameters have been kept hidden from the public in order to protect the secrecy of such correspondence. The IEEE 802.11 protocol is open to the public. Furthermore, the requisite hardware and software are not limited or regulated objects, and the hardware is often used as a regular feature in many computers.

Only WiFi messages transmitted over a single carrier’s contact channel are covered by the ECPA. A national carrier is a company that charges the general public for communication services. The ECPA would apply to a number of well-known carriers that operate WiFi networks. The ECPA, on the other hand, does not apply if the WiFi network in question is operated by a private citizen or other entity that is not in the business of providing internet services. See *Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998)* (defendant did not provide electronic communication service to the public and therefore could not be sued under the ECPA).

- ***Telecommunications Act***

Since WiFi messages may be accessed by the general public, the Telecommunications Act would not seem to regulate WiFi interceptions. "No person not allowed by the sender shall intercept any radio communication and divulge or publish the presence, contents, substance, purport, consequence, or sense of such intercepted communication to another person," according to the Telecommunications Act. This clause would not refer to accessing, disclosing, printing, or using the contents of any radio correspondence broadcast by any station for the general public..." 605 of the United States Code (emphasis added).

- ***Computer Fraud and Abuse Act***

Since the Computer Fraud and Abuse Act (CFAA) is mainly based on manipulating (Kern, 2004) computer networks, it does not tend to extend to the intercept of WiFi signals. While there does not seem to be any direct case law on the subject, passively monitoring a WiFi contact would not appear to include manipulating the person's device in the sense that the word is commonly known. The first six major legislative breaches deal with gaining improper access to a computer device, while the seventh deals with rendering threats of harm to a safe system (the following things have been paraphrased for clarity):

a) Unauthorized access to a device containing classified government records.
b) Obtaining financial information from a financial institution or card issuer, any US government papers, or information from a secure computer relating to domestic or international trade without permission or beyond permitted access.
c) Deliberately and without permission accesses any nonpublic device of a United States department or organization.
d) Accesses a secure device without permission or exceeds permitted access in order to conduct or further a crime with the intent to defraud.

e) Gains access to a secure device and deliberately disseminates malicious code or causes injury, whether purposely or accidentally, or tries to obtain access that will result in a loss of $5000 or more, bodily injury, medical care alteration, a threat to public safety, or disruption to a government structure.

f) Traffics in any password or related information from which a device can be accessed without permission, knowing and with intent to defraud, if— (A) such trafficking involves interstate or international commerce; or (B) such computer is used by or by the United States Government.

g) Any person who transmits any message involving any attempt to inflict harm to a protected device with the intent to extort money or other valuables.

Eavesdropping on WiFi may be achieved passively, with the eavesdropping device emitting no outgoing info. To collect data carried on radio frequency transmissions, no link to an access point is necessary.

1.8 FOURTH AMENDMENT EXPECTATION OF PRIVACY IN WLANs

Despite the fact that Congress has opted not to pass laws banning the surveillance of WiFi traffic, cyber fraud agents are also prohibited from performing unlawful searches under the Fourth Amendment as law enforcement officers. Only those areas in which the target of the search has shown an actual (subjective) presumption of privacy and the expectation is one that society is willing to consider as “fair” are protected by the constitution (Katz v. United States, 389 U.S. 347, 361 (1967)). Although an individual has a constitutionally-protected expectation of privacy in his home,“[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection” (Katz, 389 U.S. at 351).“The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares” (California v. Ciraolo, 476 U.S. 207, 213 (1986)). “Nor does the mere fact that an individual has taken measures to restrict some views of his activities to preclude an officer’s observations from a public vantage point where he has a right to be and which renders the activities clearly visible” Id. (citing United States v. Knotts, 460 U.S. 276, 282 (1983)).

The argument then becomes whether a fair presumption of privacy in electronic messages exchanged through WiFi exists under the Fourth Amendment. While the case is yet to be resolved, the best opinion seems to be that such a privacy expectation would not be fair under the Fourth Amendment.It is a fundamental feature of WiFi communications that, at the user's discretion, may be encrypted and thereby easily hidden from public view. As a consequence, if a person decides not to use the built-in encryption—which is expressly defined in the WiFi standard—courts are likely to infer that the WiFi user has given up any fair assurance of privacy(see United States v. Granderson, 182 F. Supp. 2d 315, 321–22 (2001) defendant had no reasonable expectation of privacy when conducting drug activities behind a boarded-up window that had a slot between the boards since the defendant easily could have shielded his activities from public view by taking simple and obvious steps).

1.9 LET’S SUM UP

In this chapter, we have studied the meaning and how WiFi technology works along with understanding as to how privacy is infringed due to the usage of this technology with the help of the US laws. Furthermore, we also studied on eavesdropping on WiFi and legislative framework of the same along with the fourth amendment expectation of privacy in WLANs.

1.10 FURTHER READING

- Kern, Benjamin D. 2004. Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law. Santa Clara Computer and High Technology Law Journal.
- Jain, B. 8,736 phone and e-mail accounts tapped by different government agencies in July. September 17th 2011. Available at: http://articles.economictimes.indiatimes.com/2011-09-17/news/30169231_1_phone-tap-e-mail-accounts-indian-telegraph-act
- Chaudhary, A. BlackBerry’s Tussle with Indian Govt. Finally Ends; BB Provides Interception System. http://www.medianama.com/2013/07/223-

blackberrys-tussle-with-indian-govt-finally-ends-bb-provides-interception-system/

- Report of the Group of Experts on Privacy. Available at: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the meaning of WiFi?**

WiFi stands for wireless fidelity (wireless) and refers to a set of protocols that enable computers and other devices to link to local area networks wirelessly.

2. **What is the meaning of authentication?**

Authentication is defined in the 802 standards as “The service used to establish the identity of one station as a member of the set of stations authorized to associate with another station.”

3. **How are WLANs set up?**

WLANs can be programmed to use a range of encryption schemes, the most popular of which are WEP and WPA. By restricting the decryption of WLAN signals, encryption regulates authentication. To decode the signal, approved users must have the requisite secret key—indeed, they must have the correct credentials to bind to the access point at all.

4. **What does 802.11 standard state?**

The 802.11 standard clearly articulates that additional privacy measures, primarily authentication measures such as MAC filtering and encryption, are needed to prohibit any other 802.11 equipped device from connecting to the wireless access point

1.12 ACTIVITY

Elucidate how WiFi signals are interrupted, along with a few case studies. (1500-2000 words)

Unit 2: CYBER SECURITY AND INTERNATIONAL LEGAL ASPECTS

2

Unit Structure

2.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Cybersecurity in U.S.
- U.S. Comprehensive National Cybersecurity strategy
- International comprehensive cybersecurity strategy

2.2 INTRODUCTION

Cyberspace, like a virtual battleground, has become a battleground for the appropriation of personal data, espionage of scientific, economic, and commercial assets of companies that fall prey to competitors or foreign powers, disruption of services essential to the economy and daily life, compromise of information related to our sovereignty, and even assassination.

This "virtual battleground" in cyberspace has only increased global security visibility and has had a significant effect on global political stability, cutting a vast swath across physical territorial borders and affecting the security of people, private companies, societies, and global nation-state governance and stability.The Internet is integral to many international trade and enterprise growth activities in both developed and developing countries. For example, digital technology underpins Canada's entire economy, with 87 percent of commercial businesses dependent on the Internet to do business in 2012.

Individuals can use the Internet to mobilize and inform others about current political activities or events affecting others in a specific community and can operate individual water systems. The Internet offers a nearly anonymous avenue for world people whose freedom of expression is limited or forbidden, where individuals can communicate without government interference and intrusion, use the Internet to rally and warn others about current political developments or events involving others in a particular society, and run individual water systems. People and factions with sinister agendas that wish to destabilize or overthrow governments or perform acts of terrorism, on the other hand, can gain access to and use the same rights.

2.3 WHAT IS CYBERSECURITY IN U.S.?

The legal playing field on which local, state, and federal institutions in the United States, foreign organizations, and European Union (EU) member states target their legal bat to oversee, rule, and defend their defined tangible and intangible properties from cybercrime, espionage, and assault brings common terminology into play, which at first glance seems to be equivalent because the players wear the same uniforms.However, upon closer examination, some players have merely adopted a term without ever assigning a particular meaning to that term, while others have adopted a specific definition that does not correspond to any scientific or actual statistical context. In all events the willingness of all players to recognise their strengths and disadvantages, to produce sound gaming statistics and to create an easy-to-understand rules book which is technically reasonable and smooth to use, will not be able to develop and provide standardized concepts compatible with overall strategy, legal framework and theoretical grounds.

The development and adoption of specific meanings for the primary terms of art dealing with the protection of various informational structures and their physical and virtual devices, all of which are interconnected through the Internet, has been defined as a necessary component if and when cybersecurity is established as a discipline. The experimental method, which involves the repeatability of experiments based on precise meanings and conditions, will be extended to the study of cybersecurity as a result of this development.“It’s essential to provide specific meanings. It would not be necessary to raise the degree of rigour until a precise collection of items can be studied carefully and clearly.”

Recognizing that standardized and globally accepted definitions for significant and repeating terms of art affecting cybersecurity do not yet exist among global nation-states, businesses, and individual stakeholders, an examination of the relevant U.S. and international legal environments must identify, at the very least, what has been identified as a definition, or the lack thereof, for the aforementioned terms of art.What exactly does the term “cybersecurity” imply, and is that meaning broad enough to be applicable across borders? Is that term widely agreed across the globe, or is it finite, exclusive, and exclusive to only a few nation-states? The expression “cybersecurity” tends to be used interchangeably, just as the term “glue.”As we all know, not all glues are made equal, which means that the additives used in particular forms of glue will decide whether the glue sticks or not, or, even worse, will muck it up and produce more complications than remedies. Definitions can be compared in the same way.Because of the breadth and reach of coverage, a concept of cybersecurity must properly consider and resolve the physical and virtual existence of the objects be protected.

Cybersecurity is a multifaceted challenge, and regulatory and legislative analyses of cybersecurity problems must differentiate not only between various cyber threat entities, such as nation-states, terrorist groups, terrorists, and malicious hackers but also between different forms of cyber threats. Threats to vital facilities, which could result in a loss of life or substantial economic damage, and threats to intellectual property, which could affect our nation's long-term prosperity, are examples of cyber threats.

2.4 CURRENT U.S. COMPREHENSIVE NATIONAL CYBERSECURITY STRATEGY

In general, new federal and state cybersecurity policies have evolved in response to abuses and malicious activities in particular economic markets, either directly or indirectly.Despite the fact that a slew of bills has recently been introduced to establish a standardized umbrella federal cybersecurity legal structure that will protect all government and private computer and network networks, none of them has been effectively implemented into legislation.In February 2003, the White House released The National Strategy to Protect Cyberspace, which was the first national cybersecurity policy released by the White House under then-President George W. Bush. Bush defined, suggested, and stressed the role of a public–private relationship in implementing the national strategy to protect cyberspace, as well as the importance of private sector engagement.Bush's cyberspace policy prioritized five issues: (1) establishing a strategic cyberspace security council, (2) a cyberspace threat and risk prevention initiative, (3) a cyberspace security awareness program, (4) a roadmap to protect federal cyberspace, and (5) national and international cyberspace collaboration.

The Comprehensive National Cybersecurity Initiative (CNCI) began as a classified offshoot of Bush's National Strategy, despite the fact that these five policy goals would not result in the passage of any substantive legislation.The Center for Strategic and International Studies (CSIS) named a Commission on Cybersecurity for the 44th Presidency ("Commission") in December 2008, which released a report with three main findings: "(1) Cybersecurity is already a significant national security issue for the United States; (2) decisions and activities must protect privacy and civil liberties; and (3) only a holistic national security policy that encompasses all domestic and foreign facets of cybersecurity can make us safer."

President Barack Obama released a revamped and modified CNCI as National Security Presidential Directive 54 on March 2, 2010, in response to the CSIS Commission's findings, which specifically discussed cybersecurity of federal networks, both classified and civilian; required the use of EINSTEIN 2, an intrusion prevention system, across all federal systems; and decreased government spending.In the absence of a legally binding cybersecurity standard, the Obama White House released Executive Order (EO) 13636, Strengthening Critical Infrastructure Protection, on February 12, 2013, which defines a national policy on cyber intrusions, describes the essence and extent of the United States' national policy on critical infrastructure security, and establishes a mechanism for information sharingand coordination with private entities to enhance and better protect critical infrastructure assets, defines critical infrastructures and critical infrastructure sectors, and directs the development of standards and a framework for improved cybersecurity of critical infrastructures.The EO also orders the Secretary of the Department of Homeland Security to protect citizens' privacy and civil rights and to ensure their participation in the operation and enforcement of the Order's mandates by implementing the Fair Information Practice Guidelines and other related "privacy and civil rights policies, standards, and mechanisms."

2.5 INTERNATIONAL COMPREHENSIVE CYBERSECURITY STRATEGY

Although a number of international organizations are forming alliances among member countries around the world, the United Nations (UN) and the North Atlantic Treaty Organization (NATO) are two international bodies whose activities are raising global concern about cybersecurity, increased growth, and access to Internet connectivity (NATO). NATO's activities in support of its politico-military mission to provide diplomatic and unified security for its European members are coordinated and supplemented by the UN.

a) *UN Cybersecurity Policy and Strategy*

The United Nations (UN) is an international organization established on October 24, 1945, with the goals of maintaining peace, establishing “good ties among nations,” assisting “nations in working together to improve the lives of poor people,” and coordinating nations’ efforts to “achieve these goals.” There are officially 193 countries that are part of the United Nations.The UN, as an international body, effectively functions as a “standard entrepreneur” and agent of change to its member nations and the world at large, offering analysis and proposed models on a range of topics, including cybersecurity and international Internet regulation, since it has no jurisdiction over its member nations to implement its global mandate.The UN Charter specifies six main institutions to act and self-govern: the General Assembly, Security Council, Economic and Social Council, Trusteeship Council, International Court of Justice, and a Secretariat (Chapter 3, Article 7). Chapter 4, Article 22 allows the principal organs to join additional committees or subsidiaries to assist them in carrying out their responsibilities as appropriate. 60 Chapter 9, Article 57,61 establishes the use of specialist organizations controlled by interagency agreements issued by the Economic and Social Council in accordance with Chapter 10, Article 63.

The Internet Governance Forum (IGF) and the International Telecommunication Union (ITU) are two of the most relevant international multi-stakeholder advisory bodies working under the United Nations umbrella, tasked with investigating, collaborating, and consulting on global issues affecting Internet governance and cybersecurity.Although neither the IGF nor the ITU has the power to enact or implement legislation, they both serve as “think tanks” that collaborate and gather information, feedback, and analysis from a range of outlets, including scholars, private enterprise, government agencies, the general public, advocacy organizations, and others, in order to propose best industry practices for remaining cyber secure and keeping the internet safe.

The IGF is an online multi-stakeholder forum where public and private people and organizations from around the world can gather to discuss topics and concerns that affect Internet governance. The IGF was founded in 2006 by the UN Secretary-General, who is also the head of the UN Secretariat, “to assist the UN Secretary-General in carrying out the mandate from the World Summit on the Information Society (WSIS) with regard to convening a new multi-stakeholder policy discussion forum.”In relation to the IGF, the ITU is an UN-affiliated organization with “191

Member States and more than 700 Sector Members and Associates." In its position as the UN's leader for information and communication technology, the ITU represents three main sectors: Standardization, growth, and radio communication.Cyber attacks against member constituencies and processes are one of the most serious issues facing the world today, according to a consensus of UN members. Since the Russian government first submitted a cybercrime resolution to the General Assembly in 1998, and an explosive growth boom on the Internet started in 1998, 77 Maurer pins raised UN interest and escalation of cyber challenges to the forefront.

b) NATO Cybersecurity Policy and Strategy

Following continuing Soviet threats to the stability of newly formed nations seeking to rebound from the destruction of World War II, the North American Treaty ("Treaty") was signed on April 4, 1949, resulting in the establishment of NATO. NATO now consists of 28 European and North American countries.NATO has provided politico-military assistance, training, education, and peacekeeping to member nations who have been targeted or are engaged in external conflict since its establishment. Although NATO prioritizes peace in settling future disputes among nations, the Treaty imposes a clear measure of alliance unity by tying adverse action on all members in the event of an attack on one of them. Article 5 of the North American Treaty reflects this critical pillar:

The Parties agree that if an Armed Attack is carried out against one or more of them in Europe or North America, the Parties shall assist the Parties, if an Armed Attack takes place in any case, in exercising their right to individual and collective self-defense, recognized in Article 51 of the Charter of the United Nations, and that the Party or Parties attacked therefrom shall assist.

Cyber threats, which NATO tackles independently via its members' networks, an articulated cybersecurity strategy81, and the NATO Cooperative Cyber DefenseCenter of Excellence in Tallinn, Estonia, can be prompted by this unity in security to NATO members.On December 27, 2013, the United Nations explicitly stated that behaviour in cyberspace is governed by international law83, bolstering the effect and current applicability of NATO's Article 5 in the event of nation-sponsored or launched cyberattacks against NATO members.

c) EU Data Protection

The European Union (EU) is an economic and political international organization made up of 28 European member states whose members govern collectively by a series of interconnected structures, the most important of which are the Euro Parliament, the Council of European Union (EU Council), and the European Commission (EU Commission).The Euro Parliament, according to its website, is made up of representatives who are directly elected by EU citizens every five years.
Along with the Council of the European Union ("the Council"), Parliament is one of the EU's key law-making organs. The European Parliament holds three core functions:

- Debating and passing European laws, with the Council.
- Scrutinizing other EU institutions, particularly the Commission, to make sure they are working democratically.
- Debating and adopting the EU's budget, with the Council.

The European Union Council is a governing body made up of national ministers from each EU member country who meet to "adopt laws and coordinate policies." The EU Council is responsible for authorizing the annual budget, implementing EU legislation, organizing member countries' economic strategies, enforcing negotiations between the EU and other nations, establishing EU international and security policies, and promoting coordination between prosecutorial and law enforcement agencies.
The legislative authority that the EU's governing bodies exercise is founded on two main treaties that grant them the authority and power to issue legislation, orders, resolutions, advice, and opinions. A released directive, as opposed to a law, is "a statutory act that lays out an aim that all EU countries must meet."Specific nations, on the other hand, must determine how to proceed."On October 24, 1995, the Euro Parliament and EU Council released Directive 95/46/EC (the "Information Security Directive") on the protection of personal data of individuals and the free flow of such data within the EU, according to former Article 7(a) of the Treaty of European Union.
In recent years, the EU Court of Justice has interpreted the language of Article 7(f) of the Data Protection Directive with that of Article 8 of the EU Charter to provide a distinct and powerful individual right to data protection that precludes laws of member states that seek to release personal data without the consent of the data subject.The EU Commission released its proposal on the issuance of regulation on

January 25, 2012, in response to the dynamic nature of the Internet and the constantly changing technological development impacting the collection, use, and distribution of electronic data, as well as the potential erosion of the Data Protection Directive's ability to protect personal data.The draft law has five key components: (1) geographical reach, which guarantees a constitutional right to data security regardless of the geophysical position of the enterprise or its servers; (2) international transactions allowed where data protection is guaranteed; (3) compliance, which requires substantial penalties for foreign companies who do not comply with EU data protection rights; and (4) development of substantive guidelines for the security of personal data exchanged with law enforcement by cloud storage data processors, providing specific rules on responsibilities and liabilities.

Despite the lack of an EU law, the European Court of Justice recently approved the principle of the "freedom to be lost" based on existing Data Security Directive provisions. The European Court of Justice ordered Google, Inc. and its foreign branches ("Google") conducting business with the EU to respect individual EU citizen requests to remove personal data from Google search engines on May 13, 2014.

2.6 LET'S SUM UP

In this chapter, we have studied how cybersecurity has been defined in U.S. along with the comprehensive National Cybersecurity Strategy and its historicial development. Further, we also have studied the U.N. cybersecurity policy and strategy along with NATO and U.S. policy and strategy.

2.7 FURTHER READING

- European Parliament, Directorate General for Internal Policies Policy Department A: Economic and Scientific Policy, Industry, Research and Energy. September 2013. "Data and Security Breaches and Cyber-Security Strategies in the E.U. and Its International Counterparts." IP/A/ITRE/NT/2013-5, PE 507.476, 41. Available at http://www.europarl.euro.eu
- NATO Cooperative Cyber Defence Center of Excellence. 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare, 45. Available at http://issuu .com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381#

- For further information concerning the ITU and its recommendations, see http://www.itu.int, International Telecommunications Union. April 2008. “Series X: Data Networks, Open Systems Communications and Security,” 2.

2.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the meaning of cybersecurity?**

Cybersecurity is a multifaceted challenge, and regulatory and legislative analyses of cybersecurity problems must differentiate not only between various cyber threat entities, such as nation-states, terrorist groups, terrorists, and malicious hackers but also between different forms of cyber threats.

2. **What are IGF and ITU?**

The Internet Governance Forum (IGF) and the International Telecommunication Union (ITU) are two of the most relevant international multi-stakeholder advisory bodies working under the United Nations umbrella, tasked with investigating, collaborating, and consulting on global issues affecting Internet governance and cybersecurity.

3. **What are the three core functions of European Parliament?**

The European Parliament holds three core functions:

- Debating and passing European laws, with the Council.
- Scrutinizing other EU institutions, particularly the Commission, to make sure they are working democratically.
- Debating and adopting the EU’s budget, with the Council.

2.9 ACTIVITY

Elucidate NATO, U.N. and U.S. Cybersecurity policies and strategies in detail (2500-3000 words).

Unit 3: MAPPING THE COSTS OF CYBER CRIME

3

Unit Structure

3.1 LEARNING OBJECTIVE

In this chapter, we will learn-

- Cost of cybercrime through research data presented by UK agencies.
- How to handle the cybercrime situation.

3.2 INTRODUCTION

The word "cybercrime" is not a legal term. As a result, it holds some contextual mutability, such as ‘cyberspace' criminality (Gibson 1982, 1984) and ‘the transformation of illicit or dangerous behavior by networked infrastructure' (Gibson 1982, 1984). (Wall 2007: 10). As a result, cybercrime may refer to the use of computers to aid in the commission of "traditional" crimes, either within specific structures or through global networks. It may also involve cybercrimes that are entirely mediated by technology, referred to as "third generation" cybercrimes (Wall 2007: 10). Such cybercrimes, such as spam e-mail, are purely a product of the Internet and would not occur otherwise. Many of the so-called cybercrimes that have sparked outrage over the last decade, though, are not actually offences in the legal sense. In essence, the suffix of "crime" is applied to actions that do not easily fall into the scope of criminal law. As a consequence, there isn't necessarily a legal justification for such "cybercrimes." They are more contentious harms that fall outside of the criminal justice system's control and practice, such as cyber-rape (MacKinnon 1997) and virtual reality vandalism (Williams 2006).

Despite the fact that ‘What is the essence and scale of cybercrime?' seems to be a straightforward query, it is actually difficult to respond in terms of frequency and distribution throughout societies. Crime prevention programs, on the other hand, are typically based on statistics that can accurately represent both the kinds of offenses that are being committed and the frequency at which they are occurring. Similarly, the degree to which crime rates have reduced, or not, is a clear indicator of the success of criminal justice responses.A collection of consistent, accurate data will help advise and assess policy responses to cybercrime. Attempting to map and quantify cybercrime is appealing for this primary purpose. While the security group is "prone to leap to management while bypassing calculation," as Wade Baker put it, "measurement allows management."

Estimates of crime costs will aid the government in achieving the best effect on crime with the least amount of money spent. The statistics will be used to measure and monitor measures aimed at minimizing crime. They will assist the government in prioritizing measures that have the largest effect on crime-related damage, rather than just the amount of crimes (Home Office, 2000, p 7).The Home Office has previously published research examining the costs of traditional crimes such as burglary and violent crimes. Previously, the Home Office conducted reports on the costs of traditional offences like robbery and violent crimes. A research by the Home Office (2013b) measured the social and economic consequences of organized crime. Cyber terrorism, on the other hand, has not been included in all such figures to date due to the difficulties in accurately estimating costs. In light of the emerging challenges posed by cyber-enabled and cyber-dependent offences, it is now necessary to examine the effects of new digital crime forms and aim to measure the costs they have on the UK economy.The study on the effects of crime has taken an iterative approach, with revisions released as approaches and expense forecasts have changed. This has enabled cost of crime analysis to guide progress in future research while also providing an easy-to-access summary of the most well-known cost figures for the research community. In order to form an overall view of the cost of crime, the costs of crime study has concentrated on the economic cost to the UK per incident, and has separately used figures of the prevalence of crime.The costs considered in this study were divided into three categories: costs in preparation, costs as a result, and costs in reaction.

3.3 ECONOMIC CONCEPTS

The Costs of Cyber Crime Working Group funded a study to create a costs of cyber crime system to outline and help explain the multiple assessments of cyber crime costs based on the lessons learnt from the literature review exercise and a commitment to encourage accuracy in future study. Dr. Adam Bossler, in collaboration with Home Office Analysis and Insight, worked on this initiative.The system strategy was built on previous Home Office studies into the effects of crime, and the costs were broken down into the same three categories:

- costs in preparation

- costs as a resultand
- costs in reaction.

This section introduces the economic principles that underpin the system, followed by a summary of the framework itself. The report's subsequent chapters address how researchers should use the methodology to ensure that prospective research projects are complementary and clear in approach. The definition of economic cost was used in this project to illustrate the full effect of cyber fraud on the UK economy. HM Treasury's Green Book advice from 2003 was used to develop economic principles.The idea of opportunity cost is a central economic concept used in the system for calculating the effects of cybercrime. This applies to "the worth of the most valuable of alternate purposes," which simply means the value of assets or services if they were put to other uses rather than being attributed to cybercrime in this situation. The definition of opportunity cost helps researchers to value the capital, such as people or money, that would be freed up if cyber crime did not occur in the United Kingdom. It is therefore necessary to understand the principle of transfer payments and their position within the system. If there is no product or service in exchange, transfer payments exist in an economy. Subsidies and casinos are examples of such transactions. Transfer fees are not used in the costs of crime context because they are not considered a societal expense and are merely financial transfers within the UK economy. Fines handed out to enterprises for not adequately protecting data from cybercriminals are an example of transfer fees related to the costs of cyber crime; this is not seen as a cost to the economy, but rather as a financial burden to businesses.

Furthermore, under recommendations from the Home Office's costs of crime work, reimbursement premiums to victims of cybercrime are not included in the costs of cybercrime scheme. Insurance lawsuits were left out so the sharing of funds between insurers and insurance providers, as well as payments from insurance companies to victims, was not considered a societal cost. Insurance claims, on the other hand, are not included in the cyber crime framework's charges, but insurance management expenses are.They are the costs of insurance providers' personnel, facilities, and supplies, and they pose an opportunity loss to society because these services would be opened up and used elsewhere in the economy if cyber terrorism did not exist.

3.4 COSTS OF CYBER CRIME FRAMEWORK

Costs have been divided into three groups that reflect the different levels of how victims experience the costs of cyber crime:

- costs in advance of cyber crime,
- costs as a result of cyber crime, and
- costs in reaction to cyber crime, as previously mentioned.

Individuals and companies typically use costs in advance as a protective mechanism to deter violence. Expenditure on anti-virus applications is one example. As a consequence, costs look at costs that arise as a direct result of a felony, which usually take the form of collateral damage or income wasted. It does, however, contain the mental and physical costs of violence. Individuals had little to little power over these expenses. Costs in action examine the costs incurred as a result of a decision about how to respond to a given crime.

This usually entails reactions from law enforcement and the criminal justice system, all of which are burdened and lose money as a result of cybercrime. There are costs over which you usually have more leverage over what you can do. The costs of cyber crime system is an effort to consolidate all that is known about the costs into a single table, allowing for a clearer view of existing research discrepancies (as of 2016) and promoting further research.The goal was to make it easier for researchers to figure out what the many different component costs of cyber crime are, and how they converge to shape the total cost of cyber crime – a resource that didn't exist in the literature before.

Considering costs in this manner can aid researchers in identifying research gaps and encouraging the creation of coherent research that can be used together in the future to better appreciate the potential cost of cyber crime.

<u>THE COSTS OF CYBER CRIME FRAMEWORK – SUMMARY OF COST TYPES</u>

<u>Technology costs</u>

- Computer security protection software/products (for example, anti-virus, patching)

- Introduction of new/additional technologies Training

- Cybersecurity training/education

- Training for law enforcement investigators and officers

- Training of court and legal personnel

Security practices/behaviours

- Implementing cybersecurity practices

- Usability/user impact as a result of increased security procedures

- Switching internet service providers (ISPs), security providers or products to increase security

- Vetting staff or contractors for security purposes

- Monitoring third parties' security

- Checking credit histories/scores

- Avoidance of the internet and/or other technologies (amongst non-users)

Government activities

- Drafting and creating new legislation

- Efforts to educate public on new legislation

- Implementation of national awareness raising/protection campaigns

Other

- Cyber-insurance administration

- Consumer credit/identity protection services (for example, CIFAS, a fraud protection organisation)

- Fear/worry about cyber crime

- Collection and compilation of cyber crime statistics

3.5 UNDERSTANDING SCALE, TRENDS AND MEASUREMENT OF CYBER DEPENDENT CRIMES

The aim of this study, conducted by David Emm, Professor Steve Furnell and Dr Maria Papadaki, was to provide a better understanding of the range of measures used to assess the prevalence or incidence of cyber-dependent crimes, including:

- viruses and other malware;

- denial of service or distributed denial of service (DDoS); and

- hacking. Such measures are used to help compare the extent of the threats that each poses in terms of volumes and frequency. A better preliminary understanding of these measures is helpful when building the evidence base for the costs of cyber crime. The research involved reviewing various published sources (for example, from security vendors, security surveys and threat reports) to determine the nature and quality of the underlying measures currently (as at 2016) available for cyber-dependent crime.

3.6 THREE STEPS TO UNLOCK CYBER SECURITY VALUE

1. Prioritize protecting people-based attacks: Internal risks are also one of the most difficult obstacles that corporate executives face today. With the rise of phishing, ransomware, and disruptive insider attacks, it's more important than ever to foster a security-first community. Accountability is extremely important. To reinforce healthy practices, both within the company and through the broader industry community, training and education are critical. As a result of doing business online, partners, third parties, and partnerships are growing. To collectively protect and defend their activities, organizations should collaborate with these ecosystem partners. People who are interested are not necessarily those who work for a business.

2. Invest to limit information loss and business disruption:Any organization's lifeblood is information, whether it's information about clients, staff, goods, corporate practices, or facilities. As recent privacy laws, such as GDPR and CCPA, impose significant penalties for non-compliance, companies must take responsibility for their sensitive data. Information security is at the core of ethical corporate practices, and it's essential to avoid business interruption. Using a data-centric approach to security, data loss management systems, and widespread use of cryptographic technology will also help to lower the cost of cybercrime. Enhancing compliance policies around information handling, maintenance, and distribution will help an enterprise transition from harm reduction to secure proprietary procedures when it comes to data loss.

3.7 LET'S SUM UP

In this chapter, we have learned about the cost analysis of cybercrime framework and its various dimensions associated with different stakeholders.

3.8 FURTHER READING

- E. Tyugu, ”Artificial intelligence in cyber defense”, In Proceedings of the 3rd International Congress on Cyber Conflict (ICCC), pp. 1–11,2011.
- X. B. Wang, G. Y. Yang, Y. C. Li and D. Liu, ”Review on the application of Artificial Intelligence in Antivirus Detection System”, In Proceedings of the IEEE Congress on Cybernetics and Intelligent Systems, pp. 506- 509,2008.
- M Rajesh Kanna, D. Hemapriya and C. Divya,” Intelligent Agents For Intrusion Detection System (IAIDS)”, International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 3, January 2013.
- N. Jaisankar, R. Saravanan, K.Durai Swamy, “Intelligent Intrusion Detection System Framework Using Mobile Agents”, International Journal of Network Security & Its Applications (IJNSA), Vol 1, July 2009.
- Yu Chen, “NeuroNet: Towards an Intelligent Internet Infrastructure”, In Proceedings of the 5th IEEE Congress on Consumer Communications and Networking Conference (CCNC), pp. 543 547,2008.
- Iftikhar Ahmad, Azween B Abdullah, and Abdullah S Alghamdi, ”Application of Artificial Neural Network in Detection of Probing Attacks”, In Proceedings of the IEEE Symposium on Industrial Electronics and Applications (ISIEA), 2009

3.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Provide few examples of cost incurred through cyber crime framework**

Government activities

- Drafting and creating new legislation

- Efforts to educate public on new legislation
- Implementation of national awareness raising/protection campaigns

<u>Other</u>

- Cyber-insurance administration
- Consumer credit/identity protection services (for example, CIFAS, a fraud protection organisation)
- Fear/worry about cyber crime
- Collection and compilation of cybercrime statistics

3.10 ACTIVITY

Explain the costs of cybercrime framework and various types of cost.(Word count 2000 to 2500)

Unit 4: CYBER CRIMES: GLOBAL AND INDIAN RESPONSE

4

Unit Structure

4.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- Global perspective of cyber crimes
- Countrywise legal response
- Nature of offences and penalties in India

4.2 GLOBAL PERSPECTIVE OF CYBER CRIMES

One of the most distinguishing characteristics of cybercrime is that it has a significantly broader reach than typical crime. An illegal act committed in one part of the world may have consequences in another. Because of the scope of cybercrime, the whole planet has effectively become a small town. Another characteristic is that the criminalization of cybercrime and the rise in cybercrime is consistent all over the world. It is likely that a crime is committed in one country but not in another. However, if a person commits a felony, even if it is not a crime in his own country, he can be tried under the laws of another country. For example, if an individual in the United Kingdom sends a virus to a machine in India, he could face legal action in India. As a result, cybercrime has omnipotent property, and as a result, it can have victims anywhere on the planet. It is now important for all those who work in the tech world to have a basic understanding of what constitutes cyber crime in numerous countries around the world.

Since the influence of cyber crime is unbounded, any attempt taken at the national level must be international in scope in order to effectively contain cyber crime and defend the interests of society as a whole. Such circumstances necessitate an interpretation of the global legal approach to cybercrime. All around the globe, innovations and technologies, both positive and disruptive, are happening at breakneck speed. Without foreign collaboration, neither country will be able to keep up with the latest developments in the other. A nation that has been a target of recent cybercrime should be able to alert other countries in advance so that it can prepare its security ahead of time. The aim of this page is to provide a brief description of the main features of numerous world statutes.

4.3 COUNTRYWISE LEGAL RESPONSE

The legal approaches to cybercrime in different parts of the world are complex. Such regulation is also in its infancy. There isn't a single regulation that can be said to encompass all of the requirements of current cyber legislation. Unsolicited calls from telemarketers and others, for example, are supposed to be an assault on a person's right to privacy and liberty, but the Indian IT Act and regulations make no allowance for such an act. The United States, on the other hand, adopted a new law for the reason some 13 years ago, and some European countries have followed suit to protect users from telemarketers and mobile phone providers. Some of the representative legislature efforts made by the various countries across the globe are being discussed here.

The United Kingdom, closely followed by Austria, was the first country to enact laws in the area of cyberspace. *The Computer Misuse Act, 1990*, was passed in the United Kingdom, and it includes penal provisions for cyber criminals. Following that, the nation passed the *Regulation of Investigatory Powers Act, 2000.* Following that, Austria took action in the region, amending its current laws with the passage of the *'Cyber Crime Act, 2001'* to combat cybercrime. In November of 2000, Belgium amended its existing laws and made computer forgery, vandalism, computer theft, and hacking criminal offenses. To control internet operations, China passed the *'Computer Information Network and Internet Security Protection and Management Regulations, 1997,'* but the focus was on national security rather than cybercrime prevention. Certain provisions in Estonia's criminal code apply to cybercrime.

Certain provisions of the German Penal Code refer to offences committed with the assistance of computers and data networks. *'The Criminal Damage Act, 1991'* was passed in Ireland, and it provides specific rules on harm caused on or by a computer device or network. *The Computer Crimes Act, 1997* of Malaysia is devoted specifically to computer-related crimes. Malta passed the *'Electronic Commerce Act, 2001'* to regulate electronic commerce, and Part VII of the Act includes amending rules for 'Computer Misuse' to be introduced into the country's criminal code. The Mauritius Penal Code includes specific laws regulating computer-related offences. To fight cybercrime, the nation passed the *'Information Technology (Miscellaneous Provisions) Act, 1998.'* Aside from these rules, there is the *'The Economic Crime and Anti-Money Laundering Act, 2000,'* which deals with money laundering directly.

Romania's legal framework for cybercrime and other associated illegal activity is satisfactory. Title III is the country's title. The anti-corruption law, as well as Laws No. 676 and 196/2003, regulate "the collection of personal data and the security of privacy in the telecommunications industry" and "the prevention of pornography," respectively. 'Singapore's *Computer Misuse Act, 1998,* is devoted specifically to cybercrime. Related clauses can also be found in the UK's *'The Computer Misuse Act, 1990.'* The United States of America (USA) provides the most comprehensive regulatory framework for dealing with cybercrime. It has enacted a number of laws that have regulations pertaining to the device and network abuse. There are several clauses in the Federal Code as well. Individual states have also passed their own regulations on the matter.

4.4 CYBER CRIMES: AN INDIAN RESPONSE

The Indian Act is based on the model law and governs mainly e-commerce. The Act does not focus its attention on the various forms of cybercrimes. The major issue covered under the provisions of the Act are as follows:

- Establish rules which recognize and validate contracts executed through electronic mediums;
- Covers default rules for contract creation and governance of e-contracts performances;
- Provides the definition and characteristic of valid electronic writing and an original document;
- Contains provisions for the recognition of electronic signatures for legal and commercial purposes;
- Recognizes the admission of computer evidences in courts and arbitration proceedings.

Because of the drastic changes in our lives brought on by emerging media and modern communication systems, the legislation was enacted. Company transactions are increasingly being performed using computers and the internet. Instead of conventional paper papers, the general public and business world are gradually using computers to construct, distribute, and preserve information in electronic form. Electronically encoded information is not only less expensive but also faster to store, retrieve, and communicate. While citizens were aware of these benefits, they were nevertheless afraid to perform business and transactions online due to a lack of legal structure. Many regulatory requirements have historically accepted only paper-based records and signature-based papers. Since electronic trading was expected to replace paper-based transactions, regulatory reforms to promote e-commerce were desperately needed. In 1996, the United Nations Committee on International Trade Law introduced a Model Law on Electronic Commerce to resolve this urgent need. India, as a signatory, introduced 'The Information and Technology Bill, 1999' in Parliament with the aim of promoting Electronic Governance and e-commerce in the country by way of suitable amendments in the existing laws of the country.

The Act's goals are specified in the Act's declaration and reasons. The way we work has changed dramatically as a result of new networking technologies and emerging media. A change is taking place in the way people do business. Instead of conventional paper records, companies and customers are gradually using computers to construct, distribute, and store information in electronic form. There are many benefits of storing information in an electronic file. It is less costly, easy to store, retrieve, and connect with, and it is faster. Despite these incentives, citizens are afraid to perform business or complete any transaction in an electronic format due to a lack of adequate legal structure.The conditions for legal approval of writings and signatures are the two main roadblocks to promoting electronic commerce and electronic governance. Many regulatory requirements currently presume the presence of paper-based records and documentation, as well as the expectation that these records carry signatures. Traditionally, the law of evidence was focused on written documents and oral testimony. Since electronic trading removes the need for paper-based purchases, regulatory reforms have become an immediate requirement to promote e-commerce. In the last few years, foreign exchange through the medium of e-commerce has evolved exponentially, and many countries have moved from conventional paper-based commerce to e-commerce.

4.5 NATURE OF OFFENCES AND PENALTIES

Although the Act's primary purpose is to promote e-commerce rather than to restrict cyber criminals, it does specify a range of offences and punishments that deal with actions and omissions that come under the scope of cyber crimes. Offences are dealt with in Chapter XI of the Act, while fines and adjudication are dealt with in Chapter IX. Chapter IX focuses on the following features:

- Regulating conduct in its unique way;
- Civil regulations to be employed by premise rather than criminal;
- The process of adjudication is entrusted to adjudicating officers rather than regular civil courts;
- Such adjudicating officers are required to know the law and IT or must have judicial experience;
- Adjudicating officers are vested with the power of civil court;
- The proceedings to be conducted by such adjudicating officers are to be construed as judicial proceedings;
- The quantum of compensation to be calculated at the market rate for loss or sufferings.

- ***Penalty for Damage of Computer, Computer System or Network***

Section 43 of the Information Technology Act, 2000 stipulates a liability to pay damages in the form of compensation not exceeding Rs. One crore to the persons so affected where any person without the permission of the owner or any other person, who is incharge of a computer, computer system or computer network, does any of the following acts:

- accesses or secures access to any device, computer system, or computer network;
- scans, copies, or extracts any data, computer archive, or information from such computer system or computer network, including information or data retained or stored on any disposable storage medium;
- introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system, or computer network;
- causes any device, computer system, computer network, database, or other programs residing in that computer, computer system, or network to be destroyed or caused to be damaged;
- interferes with or causes interference with any device, computer system, or computer network;

- denies or causes a denial of access to any individual authorized to access any computer, computer system, or computer network by any means;
- extends some help to someone in order to allow access to a device, computer system, or computer network in violation of this Act's provisions, guidelines, or regulations;
- interfering with or modifying any device, computer system, or computer network to charge a person's services to the account of another person.

- ***Penalty for Failure of Return, Information, etc.***

Section 44 of the Act mandates such legal formalities, stating that "any person who is required under this Act or any rules or regulations made thereunder to furnish returns, maintain books, accounts, or otherwise comply with any provision of this Act or any rule or regulation made thereunder to furnish returns, maintain books, accounts, or otherwise comply with any provision of this Act or any rule or regulation made thereunder to furnish returns, maintain books, accounts,

- ***Residuary Penalty***

According to Section 45 of the Act, anyone who violates any of the Act's rules or regulations for which no separate penalty has been established is liable to pay a compensation of not more than twenty-five thousand rupees to the person affected by the violation or a penalty of not more than twenty-five thousand rupees to the person affected by the violation.

- ***Offence Relating to Tampering with Computer Source Documents***

The Act's Chapter XI describes such crimes and outlines the penalty for them. Tampering with machine source documents is specified in Section 65.

- ***Offence of Hacking***

The crime of hacking a computer device is described in Section 66. Under the terms of this act, anybody who hacks a computer resource with the intent to trigger or believing that he is liable to cause wrongful loss or injury to the public, or anyone who damages or changes any information residing in a computer resource, diminishes its worth or utility, or affects it injuriously by any way, commits hacking, and anyone who commits hacking faces a sentence of up to three years in jail, plus a fine.

- ***Offence of Obscene Publication in Electronic Form***

Section 67 of the Act makes the publication of information that is obscene in the electronic form an offence. According to this provision, anyone who publishes or transmits or induces to be published in the electronic form any contentthat is lascious or appeals to the prurient interest or whose effect is such that its appears to deprave and corrupt individuals who are likely, given all applicable circumstances, to read, see or hear the matter contained or embodied in it, shall be punishable on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees. The section covers cyber crimes such as child pornography existing in the cyberspace.

- ***Offence of Non-compliance of Instructions from Controller***

The Controller of Certifying Authorities are appointed by the central government under the provisions of section 17 of the Act. Under section 68 of the Act, the Controller is empowered to direct a certifying authority, or any employee of such authority by order to take steps or cease carrying out of such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules and any regulation made thereunder. Anyone who fails to comply with such an order is guilty of a crime and faces a sentence of imprisonment for not more than three years or a fine of not more than two lakh rupees, or both.

- ***Offence of Misrepresentation or Suppression of Facts***

According to section 71 of the Act, anyone who makes any misrepresentation to, or conceals any material fact from, the Controller or the Certifying Authority for the purpose of acquiring any license or digital signature certificate, as the case may be, is punishable by imprisonment for a period up to two years, a fine up to one lakh rupees, or both.

- ***Offence of Breach of Confidentiality and Privacy***

According to section 72 of the Act, except otherwise specified in this Act or any other legislation currently in effect, whenever any person has secured access to any electronic record, book, register, correspondence, records, paper, or other material without the permission of the person concerned and discloses such electronic record, book, register, correspondence, information, document, or other material in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder,

- ***Offence of Publishing Digital Certificate False in Certain Particulars***

Section 73 (1) states that no one can publish or otherwise make a Digital Signature Certificate accessible to anyone with information that the certifying authority specified in the certificate has not issued it, the subscriber mentioned in the certificate has not authorized it, or the certificate has not been revoked or removed, unless the publication is for the purpose of verifying a transaction.

Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years or with a fine which extends to one lakh rupees or with both.

- ***Offence of Publication for Fraudulent Purpose***

According to Section 74 of the Act, anybody who intentionally produces, publishes, or otherwise makes available a digital signature certificate for some fraudulent or unlawful reason faces a sentence of imprisonment of up to two years, a fine of up to one lakh rupees, or both.

4.6 LET'S SUM UP

In this chapter, we have studied the Indian and Global perspective of cybercrimes along with how each country has viewed the same. In furtherance, we saw the nature of offences and penalties of cybercrimes under the Information Technology Act, 2000.

4.7 FURTHER READING

- Cole, E. Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization. Massachusetts: Syngress Is an Imprint of Elsevier, 2013.
- Wood, P., Editor. Symantec Internet Security Threat Report 2014, vol. 19. Mountain View, CA: Symantec, 2014.

- Greisiger. Cyber Liability and Data Breach Insurance Claims: A Study of Actual Payouts for Covered Data Breaches, 4–5.
- Business Section. “Cyber-Security: White Hats to the Rescue.” In The Economist, New York: Print Edition, 2014.
- Cashell, B., Jackson, W. D., Jickling, M., and Webel, B. The Economic Impact of Cyber-Attacks. CRS Report for Congress; Congressional Research Service: The Library of Congress, Washington, DC, RL32331, 2004.

4.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Which country enacted the first cybercrime law?**

The United Kingdom, closely followed by Austria, was the first country to enact laws in the area of cyberspace.

2. **What does Chapter IX of IT Act, 2000 discuss about?**

Chapter IX focuses on the following features:

- Regulating conduct in its unique way;
- Civil regulations to be employed by premise rather than criminal;
- The process of adjudication is entrusted to adjudicating officers rather than regular civil courts;
- Such adjudicating officers are required to know the law and IT or must have judicial experience;
- Adjudicating officers are vested with the power of civil court;
- The proceedings to be conducted by such adjudicating officers are to be construed as judicial proceedings;
- The quantum of compensation to be calculated at the market rate for loss or sufferings.

3. **What’s the objective of the Information and Technology Bill, 1999?**

India, as a signatory, introduced ‘The Information and Technology Bill, 1999’ in Parliament with the aim of promoting Electronic Governance and ecommerce in the country by way of suitable amendments in the existing laws of the country.

4.9 ACTIVITY

Elaborate on countrywise cybercrime laws across the globe along with a few provisions pertaining to it? (3000-3500 words)

Block-3

TYPES OF CYBER CRIMES

Unit 1: FACETS OF CYBER CRIME

1

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The different kinds of cybercrimes
- Crimes committed through Mobile and wireless technologies

1.2 KINDS OF CYBERCRIMES

a) Cyber Stalking

It is the act of stalking, bullying, or assaulting others by the use of the Internet or a device. This is often done to defame an individual using facebook, social media, instant messenger, web-posting, and other Internet-based mediums that include anonymity. False charges, assaults, sexual harassment of minors, and surveillance are examples of bad behaviour.

b) Child Pornography

It is the possession of a photograph or video of a person (under the age of 18) engaging in sexual activity.

c) Forgery and Counterfeiting

It is the use of a device to forge a document, and counterfeiting is the act of forging a document. With advancements in hardware and software, it is now possible to create a duplicate document that is so similar to the original that the validity of the document cannot be determined without expert judgment.

d) Software Piracy and Crime related IPRs

Software piracy is described as the unauthorized copying and dissemination of software for personal or commercial purposes. It falls in the category of intellectual property theft fraud. Other types of IPR piracy offences include music downloads, video downloads, and so on.

e) Cyber Terrorism

It is described as the use of computer tools to threaten or coerce the government, the civilian community, or any part of the population in order to achieve political or social goals.

f) Phishing

It is a method of obtaining a person's personal and sensitive information via e-mail by impersonating a trustworthy source in electronic correspondence. Identity fraud is the aim of phishing, and sensitive details such as usernames, passwords, and credit card numbers can be used to rob money from a user's account. Vishing is the use of a telephone as a means of committing identity fraud (voice phishing). Sms is a form of phishing in which consumers are enticed by text messages.

g) Computer Vandalism

It is the act of physically damaging computer facilities by the use of coercion or malicious software.

h) Computer Hacking

It is the act of altering computer hardware and software to achieve an objective other than the creator's original purpose. Hacking a computer device can be done for a variety of purposes, ranging from simple displays of technological abilities to locking, altering, or damaging knowledge for social, economic, or political reasons. Now, companies are hiring hackers, or people who specialize in hacking computers, to purposefully break into a company's operating system in order to find and patch security flaws.Hackers can be graded as follows:

- **White Hat:**

White hat hackers are those who break into a system to discover security flaws and warn organizations so that preventative measures can be taken to protect the system from outside hackers. White hat hackers may be paying employees of a company who are hired to discover security flaws, or they can be freelancers who want to prove their worth in this area. Ethical hackers are a common term for them.

- **Black Hat:**

The black hat, in contrast to the white hat, hacks the machine with malicious intent. They could use the mechanism to further social, political, or economic goals. They discover the system's security flaws, retain the files, and manipulate the system for personal or corporate gain until the company whose system has been compromised is aware of the problem and applies security patches. Crackers is a common nickname for them.

- **Grey Hat:**

Grey hat hackers identify vulnerability flaws and flag them to site administrators, offering to patch the problem for a price.

- **Blue Hat:**

A blue hat hacker is someone who works outside of computer technology consultancy companies to bug-test a device before it goes live, searching for exploits to close.

i) Creating and distributing viruses over internet

An organization’s business and financial losses may be caused by the transmission of a virus. The cost of restoring the machine, the cost of lost sales through downtime, and the cost of lost opportunities are all included in the loss. If the hacker is discovered, the company will sue him for an amount greater than or equal to the damage he caused.

j) Spamming

Spamming is the practice of sending unsolicited and advertising bulk messages over the internet.When an e-mail satisfies the following conditions, it is considered spam:

- Mass mailing: The e-mail is not sent to a single user, but rather to a vast group of people.
- Anonymity: The person’s true identity is unknown.
- Unsolicited: The recipient is not expecting or requesting the e-mail.

These spams not only irritate recipients and overburden the network, but they also waste time and take up precious mailbox memory space.

k) Cross site scripting

It is the act of inserting a malicious client-side script into a legitimate website.The malicious script gets access to cookies and other personal information as soon as the browser executes it, and it sends it to remote servers. This knowledge can now be used to obtain monetary gain or physical access to a device for personal gain.

l) Online Action Fraud

There are several reputable websites that have online auction services. Taking advantage of these websites’ reputations, some cybercriminals trick shoppers into online auction scam schemes, which often result in either overpayment of the goods or the item never being shipped after paying is received.

m) Cyber Squatting

It is the act of reserving the domain names of someone else’s trademark with the intention of then selling them to the trademark owner at a higher price.

n) Logic Bombs

Malicious malware has been introduced into legal applications. A particular state sets off the malicious behaviour. If the circumstances remain the same in the future, the malicious operation begins, and depending on the action specified in the malicious code, they either kill or render the device unusable.

o) Web Jacking

A hacker gains access to an organization’s website and then blocks or modifies it to serve political, economic, or social goals. Some educational institutes’ websites were compromised by Pakistani hackers, and animation with Pakistani flags was flashed on the homepage of these websites. On the occasion of India’s Independence Day in 2014, Indian hackers hacked the website of Pakistani railways and blinked the Indian flag on the homepage for several hours.

p) Internet Time Thefts

Hacking an individual’s ISP username and password and browsing the internet at his expense is known as Internet Time Theft.

q) Denial of Service Attack

It is a malware attack in which the network is clogged and, in some cases, collapsed as a result of useless traffic entering the network, obstructing legal network traffic.

r) Salami Attack

It’s a kind of attack that starts with small steps and builds up to a massive assault. The changes are so minor that they go unnoticed. An example of a salami attack is getting access to an individual’s online banking and removing small sums of money that go unnoticed by the owner. Frequently, a default trigger is set in the banking website, and withdrawals below a certain threshold, such as a Rs. 1000 withdrawal, are not registered to the account holders. Withdrawing an amount of Rs. 1000 over a span of time would result in a significant withdrawal.

s) *Data Diddling*

It is a method of altering data before entering it into a database device. Frequently, the original data is kept until the data has been processed. For e.g., a person's DA, or simple wage, is adjusted in his or her payroll data for pay estimation. The total pay is offset by his real salary in the report after the salary is measured and credited to his account.

t) *E-mail Spoofing*

It is the method of altering the header information of an e-mail so that the original source is obscured and the e-mail appears to have come from a source other than the original source to the recipient.

1.3 CRIMES COMMITTED VIA MOBILE AND WIRELESS TECHNOLOGIES

When a thing is created, a new invention is made, or something otherwise unknown to humanity is explored, the thing that is invented was almost always achieved with the intention of benefiting mankind and the world's development and prosperity. However, history shows that almost all created has been used for both positive and negative ends, i.e. for both constructive and destructive purposes.We can use several examples to understand this, such as 'Nuclear Energy,' which was discovered with no knowledge by scientists that its most large-scale use in the future will not be as an alternative source of energy for the sake of mankind, but in the manufacture of nuclear bombs, which will cast doubt on humanity's very existence. We can also use the example of the Internet, which was deregulated after it was discovered with no knowledge by scientists that its most large-scale use in the future will not be as an alternative source of energy.However, we can see that it is now almost similarly used for both helpful and negative practices, such as frauds, pornography, extortion, hacking, stalking, and so on.This is also true of wireless technology and the mobile phone scheme, all of which have been widely misappropriated for illicit and disruptive purposes.[27]

[27] Prof. R.K.Chaubey, "An Introduction to Cyber Crime and Cyber law", Kamal Law House, 2012. p. 569

Mobile phones are at the centre of a quickly spreading crime epidemic, with stolen phones even being used as a form of criminal ‘currency.’ Detection and conviction was often complicated due to the technical complexities of phone theft. As a result, we need additional legislation to address cell phone-related crimes and issues.

a) Phreaking

Phreaking is a slang word for a subculture of people who research, play with, or misuse telephones for the purposes of entertainment or usefulness. The word ‘phreak’ may also refer to the manipulation of a phone device using different audio frequencies. It is often grouped with machine hacking because it is thought to be related. This is referred to as the H/P culture (H for Hacking and P for Phreaking.) The majority of phreakers are between the ages of 12 and 17. Most people stop here, and if the defendant is no longer a juvenile, the sentences will get more serious.

Many Phreaking methods can be applied with small electronic circuits that can be quickly built by hobbyists until the key to their operation is discovered.An early phreak who designed one in a blue enclosure gave it the nickname “blue box” because it was the first circuit to produce the switching tones required to reroute long-distance calls. Other Phreaking circuits were assigned identical names soon after. There have been plenty of other types of ‘boxes’ invented. Modern phreaking often includes making phone calls using a company’s private branch exchange system, especially those accessible via toll-free numbers. Phreakers should not necessarily engage in criminal conduct.In reality, in the programming world, they may be considered a hacker. Phreakers may be more interested in the telecommunications industry, especially the less well-known aspects of telephones.

b) Mobile Phone Theft

Increased rivalry in the mobile telephony market has resulted in competitive tariffs, which has boosted telecom growth and teledensity. At the bottom end of the market, the expense of the phone is most likely the biggest impediment. Despite the fact that this expense has been slowly declining, there is still a price difference between the grey market (which includes stolen/smuggled handsets) and the legal market. Any steps must be taken to curb this crime of smartphone stealing in order to minimize the unregulated grey market and protect consumer interests.[28]

The theft of mobile phone instruments is becoming a major issue in both countries, and it is a major cause of urban crime and robbery. This is regarded as a significant concern worldwide, and the topic is being investigated in order to find a viable solution. In the United Kingdom, a bill (the Mobile Phones Reprogramming Act 2002) was enacted to prevent handsets from being reprogrammed. Reprogramming would allow for re-use but still making it impossible to track down any phone burglary.Other initiatives, such as the development of a Global Central Equipment Identifying Register (CEIR) in Dublin, Ireland, and a “Mobile Industry Crime Action Forum” comprised of operators, manufacturers, and retailers to combat mobile phone fraud and related issues, are also underway.

The United Kingdom is collecting data on cell phone fraud in the European Union via questionnaire answers. These numerous campaigns, including answers to the EU questionnaire, reveal that tackling the issue of mobile phone fraud requires a variety of concerted efforts.Efforts must be made by a variety of groups, relying on a particular database, administrative processes, and collaboration between manufacturers, network operators, and government agencies. In reality, to address this issue, there is a need for even cooperation among governments. It is possible to classify some of the key factors/agents that have arisen as being relevant for combating cell phone fraud based on an analysis of the attempts being made globally.

c) Use of mobile and wireless technology in Terrorist activities

Terrorists’ use of wireless technology and mobile phones, among other things, is one of the most harmful uses of these technologies and phones. Terrorists were able to communicate with their colleagues more quickly than in the past, where connectivity was the most difficult obstacle to overcome in the effective execution of a scheme.Terrorist organizations around the world are now well-equipped with cutting-edge networking devices such as the ‘Satellite Phone,’ which make communication difficult to track. Advanced telecommunications technologies, a collaboration between foreign mobile communications networks and international financial

[28] Preliminary Consultation Paper on Mobile Phone Theft, Telecom Regulatory Authority of India, New Delhi, January, 2004. also available online at http://trai.gov.in/WriteReaddata/ConsultationPaper/Document/mobile%20theft%20rev.1.pdf

institutions, and a lack of legislation allow “m-payments” to be made anywhere, anywhere, by anybody with a mobile phone.Given the global nature of both terrorism and mobile payments, the m-payment service provider, as well as all those tracking terror finance, should have direct real-time access to an interconnected, tightly tracked registry of all people, organizations, companies, and countries accused of having ties to terrorists.[29]

Terrorists can quickly communicate with their masterminds and collect directions via Sim cards given to bogus accounts. After the card is lost, there is no way for investigators to track their whereabouts.

d) SMS spoofing

SMS spoofing is similar to e-mail spoofing in that it seems to come from a familiar number but is actually spoofed and sent by a malicious user. As an illustration, consider the following. Consider a situation in which a woman receives a text message from her husband’s phone in the middle of the night, instructing her to carry cash because he has been in an accident. She’ll almost certainly search the phone number, and if it’s her husband’s, she’ll run out with cash.If this is her answer, she is most likely unaware of the term “mobile spoofing.” A cyber hacker could give someone a message from someone’s cell phone without ever touching it, and no wireless service provider could claim it was spoofed or faked one, thanks to web-based apps.

1.4 LET’S SUM UP

In this chapter, we have studied the different kinds of cybercrimes such as forgery, phishing, hacking, online auction fraud etc. Further, we also have seen the crimes committed through mobile phones and wireless technologies at the present times.

1.5 FURTHER READING

- Gordon, S., & Ford, R. (2003). Cyberterrorism? Onttrek Dec. 20, 2015 uithttp://www.symantec.com/avcenter/reference/cyberterrorism.pdf

[29] The flip Side - Terrorists use mobile payment systems to transfer money, Available at http://www.mgovworld.org/topstory/the-flip-side-terrorists-use-mobile-payment-systems-to-transfer-money/.

- Ranger, S. (2014, June 09). Organized cybercrime groups are now as powerful as nations. Onttrek Dec. 20, 2015 uithttp://www.zdnet.com/organised-cybercrime-groups-are-now-aspowerful-as-nations-7000030323/
- Recognize scam or hoax e-mails and websites. (s.j.). Onttrek Sep. 27, 2015 uit https://www.communications.gov.au:

  https://www.communications.gov.au/what-wedo/internet/stay-smart-online/your-identity/recognise-scam-or-hoax-emails-and-websites available under a Creative Commons Attribution 3.0 International License.
- Swain, B. (2009, July). What are malware, viruses, Spyware, and cookies, and what differentiates them ?Onttrek Dec. 20, 2015 uit http://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookiesand-what-differentiates-them

1.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is spamming?**

Spamming is the practice of sending unsolicited and advertising bulk messages over the internet.

2. **Who are grey hat hackers?**

Grey hat hackers identify vulnerability flaws and flag them to site administrators, offering to patch the problem for a price.

3. **What is the meaning of phishing?**

It is a method of obtaining a person’s personal and sensitive information via e-mail by impersonating a trustworthy source in electronic correspondence.

1.7 ACTIVITY

Explain the different kinds of cybercrimes with examples? (1500 – 2000 words)

Unit 2: CYBER TERRORISM

2

Unit Structure

2.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- What is cyber terrorism and its essential ingredients
- Famous incidents of cyber terrorism
- Provisions under IT Act with respect to cyber terrorism

2.1 INTRODUCTION

In today's world, the problem of terrorism is a very difficult question. Terrorist assaults on humans have risen significantly over the past decade. Terrorism has affected everyone from ordinary citizens to the country's statehood. It has been a global threat since the conclusion of the Cold War. The state institutions are unable to deter or monitor terrorist threats against humanity; terrorists killed a vast number of people around the world. The national and foreign fronts took a variety of counter-measures, but they were unsuccessful in preventing the terrorist attack. However, most of these are built in a common pattern that might be effective in a normal terror attack. We now live in a modern world, where computers and the internet play a role and can be a valuable weapon in the hands of terrorists.

Acts of terror have moved beyond the physical world. The computer, computer system and networks are being engaged to bring well-coordinated attacks against Nation States. Even in cyberspace, Nation States have started drawing imaginary lines of control and indulging in proxy wars. Since the acts of cyber warfare finely mesh with cyber-terrorism – it is thus imperative that a Nation-State have a legal framework, which curbs cyber terrorism and strengthens cyber security. Cyber-terrorism requires intensely focused efforts with the aim of committing terrorism. It is a new vulnerability with the potential to do substantial harm. Although we frequently equate terrorism with the loss of life, we do not ignore the significant implications of cyber-terrorism, such as fear and manipulation.[30]

In the long term, a continuous and focused terrorist program against a nation has the potential to degrade it. Given the broad spectrum of economic, environmental, and even psychological implications that such a campaign might have, cyber-terrorism will continue to be a major threat in the future. Most countries in the world today

[30] Dr. Sirohi M. N., Cyber Terrorism and Information Warfare, Alpha Editions Delhi

depend heavily on technology. An attacker's perfect tactic would be to land a heavy blow on such a crucial backbone. The United Nations' telecommunications department has given an alert that the next world war could well take place in cyberspace. It should come as no surprise that this is the case. Attacks on enemy installations or facilities have commonly been used in wars to deal a crushing blow and gain the upper hand. Given the modern world's absolute reliance on technology, it would theoretically make an excellent target in the event of a war.[31]

Cyber terrorism has arisen as a major threat to the global community, as terrorists use it to distribute fake messages in favour of political and religious agendas. The concept "cyber terrorism" is comparatively new, having been invented by tech genius Barry C. Collin.[32] The term cyber terrorism is a mixture of cyberspace and terrorism, and there is no widely agreed concept of cyber terrorism.When it comes to describing the word cyber terrorism, each academic or theorist in the field has a particular viewpoint. The definition of cyber terrorism in this analysis is split into two categories: intent-based and effect-based.It refers to attacks on the country's servers, networks, and network grids, which rely heavily on networks and cause havoc or terror among its people.

2.3 DEFINITION OF CYBER TERRORISM

The concept of cyber terrorism necessitates a broad description, since the nature of the crime necessitates it. Since the essence of "cyberspace" is such that new forms and tools appear on a daily basis, it is not prudent to confine the concept to a formula or pigeonhole. In fact, the judiciary's first duty should be to define the term as widely as possible in order to prosecute criminals severely, enabling the government to fight the evil of cyber terrorism.[33]

There have been some attempts to define cyber terrorism precisely. In May 2000, Dorothy Denning, a computer science professor, presented an admirably unambiguous definition before the House Armed Services Committee: "Cyber crime is where cyberspace and terrorism intersect. It refers to illegal attacks and threats of

[31] Ibid.

[32] Barry Collin, "The Future of Cyber Terrorism," Proceedings of the 11th Annual International Symposium on Criminal Justice Issues, the University of Illinois at Chicago, 1996.

[33] http://www.naavi.org/cl_editorial_04/praveen_dalal/pd_cyber_terrorism_oct25_04_02.htm

attacks on computers, networks, and the information stored on them that are carried out to intimidate or coerce a government or its citizens in the pursuit of political or social goals. In addition, for an attack to be classified as cyber terrorism, it must result in violence against people or property, or at the very least cause enough harm to cause fear. Attacks that result in death or bodily injury, explosions, or significant financial loss are examples. Depending on the impact, serious attacks against critical infrastructures could be considered acts of cyber terrorism. Attacks that disrupt non-essential services or are primarily a financial burden would not."[34]

According to FBI "Cyber-terrorism is a criminal act that uses computers and telecommunications capabilities to perpetrate abuse, damage, and/or service interruption in order to instill fear in a community by creating doubt and uncertainty, with the intention of persuading the government or populace to obey a series of laws."[35]

Since the terms cyber crime and cyber terrorism are not synonymous, we cannot assume that any cyber crime is indeed a form of cyber terrorism. To define cybercrime as cyber terrorism, we must first decide if it is motivated by political or ideological motivations. In the current situation, the terrorist organization's objective is to use computers and networks to disrupt the nation's communication, telecommunications, transportation, and financial networks in order to instil fear in the minds of the population, as any country in the world is highly dependent on technology. Terrorists are using computers and networking to carry out illicit activities, as demonstrated by recent attacks in India and across the globe.

2.4 ESSENTIAL INGREDIENTS OF CYBER TERRORISM

Cyber terrorism as an offence exists in three forms. Essential ingredients of these three forms of cyber terrorism are:

Form I:

1. An intention to threaten the unity, integrity, security or sovereignty of India or to strike terror, and

[34] http://www.usip.org/sites/default/files/sr119.pdf

[35] H. M. Hendershot, 'Cybercrime 2003 – Terrorists' Activity in Cyberspace and also at http://www.ijiee.org/papers/126-I149.pdf

2. Causing or likely to cause (i) death or injuries to persons,[36] or (ii) damage or destruction of property, or (iii) damage or disruption of supplies or services essential to the life of the community, or (iv) disruption of or affecting the critical information infrastructure, as specified in Section 70 of the IT Act 2000, by any of the following acts:

a) Denying or causing the denial of access to any person authorized to access computer resource; or
b) Attempting to penetrate or accessing a computer resource without authorization or exceeding authorization or exceeding authorized access; or
c) Introducing or causing to introduce any computer contaminant.

OR

Form II:

1. Knowingly or intentionally penetrating or accessing a computer resource without authorisation or exceeding authorized access, and
2. Obtaining access to restricted information, data or computer database which is restricted for reasons of the security of the State or foreign relations.

OR

Form III:

1. Knowingly or intentionally penetrating or accessing a computer resource without authorization or exceeding authorized access, and
2. Obtaining access to restricted information, data or computer database,
3. With reasons to believe that such restricted information, data or computer database may cause or likely to cause injury to: (i) the interests of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or (ii) in relation to contempt of court, (iii) defamation, or (iv) incitement to an offence, or (v) the advantage of any foreign nation, group of individuals or otherwise.

As evident from the above discussion, the definition of cyber terrorism is to be seen from both State's as well as its subjects' (citizens) perspective. The scope of cyber terrorism has been made very exhaustive. It takes into account both '*cause-and-*

[36] Cyber terror acts may include causing disruption to nuclear reactors, power grids, dams, aviation, railways etc., which may result into death or injuries to a large number of people.

effect' of cyber terrorism (and related activities). Now the question is whether Section 66F could be misused? Answer lies in how the law enforcement agencies and the Courts would view facts and circumstances in a given case and accords it a status of cyber terrorism. For example, the challenge before the Court would be to distinguish whether an offence of defamation could reasonably be covered under Section 499 of IPC or it requires Section 66F of the IT Act? Under Section 499, defamation is with respect to any person, and the word *'person'* does not include a State, whereas Section 66F implies *'defamation of State'*.[37] This section requires strict interpretation and not liberal interpretation.

Moreover, in view of terrorists' activities increasingly being done by foreign mercenaries, it would be obligatory to read Section 66F along with Section 75 of the Act.

2.5 WHETHER THE THREAT IS REAL OR NOT?

The challenges faced by cyber terrorism has piqued the attention of the media, the IT industry, companies, the defence industry, policymakers, and experts from a number of fields, who have popularized a scenario in which cyber terrorists hack into computers that control dams or air traffic control networks, wreaking havoc and endangering not only millions of lives but also national security.[38]

How serious is the danger faced by cyber terrorism? Since the majority of critical infrastructure in today's world is linked via computers, the threat of cyber terrorism is very real. Cyber criminals can obtain access to classified information and the activity of vital resources with the aid of hackers, undermining or at the very least crippling the security, banking, and service sectors of advanced economies.[39]

Our communities' rising dependence on computers and the internet has created a new category of weakness, allowing attackers to approach targets that would normally be impenetrable, such as national security and air traffic control systems. The more technologically advanced a nation is, the more vulnerable its technology is

[37] Krishnan v. Krishnaveni, AIR 1997 SC 987: 1997 AIR SCW 950: 1997 Cr LJ 1519.

[38] Gabriel Weimann, Cyber terrorism: How Real Is the Threat? Special Report No.119, United States Institute of Peace, December, 2004.also at https://thepeacemission2013.files.wordpress.com/2013/03/study-guide-united-nations-counter-terrorism-committee.pdf

[39] Terror on the Internet: The New Arena, the New Challenges USIP Press Books, 2006. also at http://www.usip.org/sites/default/files/sr119.pdf

to cyber threats. As a consequence, there is cause to be worried about the possibility of cyber terrorism.

While cybercrime is on the rise, there has been no cyber terrorist attack on Indian public buildings, highway networks, nuclear power plants, power grids, or other vital national infrastructure machinery. Cyber attacks are common, but they have never been carried out by terrorists or attempted to do the type of harm that can be called cyber terrorism.

2.6 EXAMPLES AND INCIDENTS OF CYBER TERRORISM

The following is a list of events that have caused difficulties for countries or may be identified as terrorist acts by terrorist organisations using information technology around the world:

1. ***Cyber attacks in Middle East***

With tensions between neighbouring countries at an all-time peak, pro-Palestinian and pro-Israel cyber groups have mounted an offensive against websites and postal systems used by political sectors that the opposing groups support. The attacks were confirmed to US officials by the NIPC (National Infrastructure Protection Center) in October of 2000. The threats involved a barrage of e-mail floods, denial-of-service attacks, and Ping flooding against sites belonging to Hamas and Hezbollah, as well as the Israeli Foreign Ministry and Israeli Security Forces.[40]

2. ***India and Pakistan Conflict***

Pro-Pakistan cyber-terrorists and recruited hackers started to threaten India's Internet Population as tensions between the neighbouring regions of India and Pakistan over Kashmir rose. It is suspected that Pakistani sympathizers started distributing lies and attacks against Indian Internet-based populations shortly before and after the September 11thattacks. G-Force and Doctor Nuker have defaced or interrupted service to many big Indian institutions with political links, including the Zee TV Network, the India Institute of Science, and the Bhabha Atomic Research

[40] "Middle East E-mail Flooding and Denial of Service (DoS) Attacks" – National Infrastructure Protection C enter – October 26, 2000 and also at http://www.nipc.gov/warnings/assessments/2000/00-057.htm and https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931

Center. Pakistani Hackerz Club also went so far as to attack the US Air Force Computing Environment and the Department of Energy's website.[41]

3. *Retribution by China*

The bombing of a Chinese embassy in Yugoslavia by American bombers in May 1999 triggered a major website defacement and e-mail bombardment attack on American companies and agencies. The attacks were carried out by pro-China hackers and political parties in order to gain support for the Chinese cause. The White House website, as well as the US Departments of Energy and Interior, and the National Park Service, were all attacked and had their websites defaced. Continuous e-mail bombing took the sites down for three days. Since the attack was sporadic and short, and only a limited number of US pages were infected, the results may have been much worse.[42]

4. *Cyber attack by Tamil Tigers*

With surges of violence in Sri Lanka over many years, cyber-space attacks were the next focus in 1998. The Tamil Tigers, a militant resistance group, sent more than 800 e-mails per day to Sri Lankan embassies. This was done over the course of two weeks. "We are the Internet Black Tigers, and we are doing this to interrupt your communications," said the e-mail address that started the attack. Local Intelligence officials were sent to investigate after the communications caused such extensive damage. The attack was the first recorded attack on a computer device in Sri Lanka by terrorists, according to the authorities.[43]

5. *Yugoslavia Conflict*

NATO web servers[44] were exposed to persistent attacks by hackers hired by the Yugoslav military as NATO air strikes struck the Former Republic of Yugoslavia in Kosovo and Serbia. All of NATO's 100 servers were exposed to "ping overload,"

[41] "Cyber Attacks during the War on Terrorism" India/Pakistan Conflict, Institute for Security Technology Studies - Dartmouth College Vatis, Michael A - September 22, 2001. also at http://www.ists.dartmouth.edu/docs/cyber_a1.pdf

[42] Cyber Protests: The Threat to the U.S. Information Infrastructure, October 2001. Also available at https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931

[43] Cyber Terrorism – "Testimony before the Special Oversight Panel oil Terrorism"- Dorothy E. Denning - May 23, 2000. also at https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931

[44] The North Atlantic Treaty Organization, also called the North Atlantic Alliance, is an intergovernmental military alliance based on the North Atlantic Treaty which was signed on 4 April 1949. The organization constitutes a system of collective defence whereby its member states agree to mutual defense in response to an attack by any external party.

DDoS threats, and a barrage of thousands of e-mails, many of which contained viruses. The attacks on NATO servers were timed to coincide with various website defacements of American military, government, and commercial pages by Yugoslav sympathizers from Serbia, Russia, and China. The NATO communications system is seriously damaged as a result of these attacks.

6. *Cyber attack on Estonia*

Russia conducted a cyber-attack on Estonia, a tiny Baltic republic. Russian indignation has arisen after the Baltic state's government agreed to strip a war memorial to the Red Army from a square in Tallinn's capital. Demonstrations and even protests were organized as a result. But then something unusual happened: the whole world was exposed to a barrage of cyber-warfare, which made government ministries, political parties, banks, and newspapers unavailable. Cybercriminals' tactics, such as vast remotely managed networks of hacked devices, were used to cripple crucial government systems. NATO has dispatched its top cyber-terrorism experts to Tallinn, leaving Western democracies unprepared for the repercussions of such an attack. "We've been blessed to survive this," the Estonian defence ministry said. When a missile strikes an airport, a bank, or state facilities, it is obviously fighting, so what do you call it when the same outcome is obtained by computers? Is that a war situation? There are problems that need to be addressed."Estonia has, unsurprisingly, accused Russia, which, if real, would make this the first cyber attack on another sovereign state. The Estonian attacks were more likely the result of a single angry young Russian hacker than some kind of Kremlin-sponsored blitz. In either case, the consequences are extreme.[45]

7. *Attack on Indian Parliament*

On December 13th, 2001, a cyber-attack was launched against the Indian Parliament. To accomplish their target, the attackers used cutting-edge technologies and committed forgery. They faked the gate pass and downloaded the official Ministry of Home Affairs emblem, other records, and the architecture of the Parliament building in preparation for the attack. Police uncovered a laptop belonging to the key criminals, Mohammed Afzal and Shaukat Hussain Guru. The police found that they had accessed the internet via Internet Service Providers

[45] See "Attack of the cyber terrorists" by MICHAEL HANLON Available at: http://www.dailymail.co.uk/sciencetech/article-457504/Attack-cyber-terrorists.html

located in Pakistan (ISP).In addition, the investigation officers uncovered the incoming and outgoing mobile phone numbers of deceased terrorists, as well as a satellite link with the cell phone of a deceased terrorist.[46]

8. ***Sony PlayStation Network, Microsoft's Xbox Live network case***

In this situation, the workers' and their families' personal details were leaked in 2014. Owing to the leak of film, the corporation has lost sales, confidential staff details such as compensation and social security numbers have been released, and executive e-mails have been made public. The Lizard Squad, a self-described cyber-terrorist group, coordinated the attack. Then they conducted a huge DDoS assault against Sony's PlayStation Network and Microsoft's Xbox Live networks. They followed up these disruptions with an assault on the Tor Project, a network of virtual tunnels that helps individuals and organisations to enhance their privacy and protection on the Internet, and then North Korea targeted the network infrastructure, forcing the network to go offline for nearly ten hours, affecting millions of people. As a consequence, many people assumed it is an act of the US government. However, they succeed in instilling fears in customers' minds about buying goods and in the public's view of multinational corporations. The motive behind these cyber terrorism attacks is the collateral harm that is involved, as well as the apparent diplomatic links that we see in so many attacks. "Cyber-terrorism is probably one of the biggest challenges facing the United States today," according to US President Barack Obama. Unfortunately, the attacks are not only here to linger, but with today's total dependence on the Internet, they are also likely to get even more serious."[47]

2.7 IT ACT & CYBER TERRORISM

In today's world, the fastest way to attack a nation is through a cyber network. Since India now heavily relies on computers and information technology, the effect of a cyber assault on Indian infrastructure and connectivity would be tremendous.

In order to fight cybercrime, a collection of creative laws and global norms is needed. The computer/Internet is shaping the process of information formation and

[46] Sayantan Chakravarty, "Parliament attack well-planned operation of Pakistan-backed terror outfits, evidence shows", India Today, December 31st 2001.

[47] See "Is Cyber-Terrorism the New Normal?" Available at http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/

distribution, as well as redefining the networking process by deeper transmission. With caution and attention, a delicate line between terrorism and law enforcement should be reached. As a result, the Information Technology Act, 2000 was enacted to prosecute cyber criminals.

Previously, there was no clear clause in the IT Act, 2000 that dealt directly with cyber terrorism; as a result, the Information Technology (Amendment) Act, 2008 incorporated a new section 66F. In light of the growing terrorist attacks in India and neighbouring countries, the IT Amendment Act of 2008 is a welcome move.

Section 66F is a combination of Section 66 and Section 70 of the IT Act, 2000.[48] What separates Section 66F from other sections is the degree and nature of the offence. If using a sliding scale approach to measure the gravity of the offence, Section 66 is at one end of this spectrum, whereas Section 66F is at the other end of the spectrum.

Penalty	Section 66	Section 70	Section 66F
Imprisonment Term	May extend to three years	May extend to ten years	May extend to imprisonment for life

The strategy of “Counter strike by offensive Defence” may be used to deter cyber terrorism. The principle of counter-strike by proactive security predicts that information technologies can be implemented and used to achieve acceptable and legalized crippling and relatively disruptive results. Any of the steps introduced totally uninstall the offending device, while others merely disable it for the time being by locking it down or rendering it temporarily non-functional. Not only must the equipment used be secure and efficient, but it must also be “ethical and law-abiding.” A counter-measure that is not very accurate and law-abiding would be a worse treatment than the epidemic, and therefore should be prevented. For example, if a virus is transmitted by the use of a public server, the real and lawful users would be harassed unfairly, and they will be refused facilities to which they are otherwise entitled. As a consequence, the counter-measure must be job-specific and not disproportionate to the accident being discussed.[49]

[48] Section 69 and 69A are preventive sections and hence not included.

[49] Article by Praveen Dalal, Cybercrime and cyber terrorism: Preventive defence for cyberspace violations, Computer Crime Research Center, March 10, 2006.

The threat of cyber attacks remains “imminent,” according to Pavan Duggal, and the country lacks an institutionalized framework to deal with the threat. “The latest DRDO breach was a textbook case of cyber war attack rather than simple hacking,” he added. It was a cyber-attack on India’s vital data networks. The Indian cyber law does not cover cyber warfare as a phenomenon. Clearly, India’s cyber security is out of line with the demands of the real world.”[50]

India has seen an uptick in cyber terrorist attacks in recent years, with government agencies, especially defence institutions, being attacked. In India, the following cases of cyber terrorism have been identified.

1. In revenge for suspected Internet censorship, the hacker collective ‘Anonymous’ initiated a campaign of Distributed Denial of Service (DDoS) attacks against a number of government websites in 2012.
2. Algerian hackers had targeted the DRDO, the Prime Minister’s Office, and a number of other government departments’ websites in 2012.
3. Hackers and militant groups from Pakistan are rising their attacks on Indian websites, introducing a new layer to the continuing war in Jammu and Kashmir. GForce, an online hacker collective whose founders yell slogans critical of India and its claim to Kashmir, has confessed to breaking into high-security data networks run by the Indian government, including the Bhabha Atomic Research Center’s.
4. In March 2016, the Indian Infrastructure was targeted by Al Qaeda, a militant group that reportedly hacked a microsite of the Indian Railways’ Rail net website to display its sinister scope for the first time. The hacked page of the Central Railway’s Personnel Department’s Bhusawal division, which was part of a large intranet created for the department’s administrative needs, was replaced by a message from Al Qaeda’s South Asia leader, Maulana Aasim Umar, urging all Indian Muslims to join Jihad.[51]

In the arsenal of criminals, information technology becomes a basic weapon.They use computers and networks to communicate in secret with their agents all over the world, preventing capture by law enforcement. The main cyber terrorist attacks in India include the Ayodhya incident, the Mumbai attack in 2006, the defacement of

[50] http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274

[51] http://www.ndtv.com/india-news/al-qaeda-hacks-into-indian-railways-website-leaves-message-to-join-jihad-1283023

Indian military sites in India by hackers in July 2005, the attack on the American Center in Kolkata, and the Pathankot Terrorist Attack, among others.

According to Prashant Mali, a cyber law and cyber security specialist, "the threat environment remains very dangerous, and India is now waking to the global threat of cyber warfare." Our data protection remains inadequate due to a lack of or insufficient public knowledge. Despite the fact that NTRO and DRDO have been charged with cyber offensive jobs, only time can say how successful these organizations are."

"The threat environment has changed drastically in the last few years," said Shantanu Ghosh, vice president of India Product Operations at Symantec Corporation, which developed Norton Antivirus. Attackers' motive has changed from popularity to profit, and ransomware has become a profitable illegal business model worth billions of dollars. We've now joined the third big change in the threat environment, which is one of cyber-espionage and cyber-sabotage."

2.8 LET'S SUM UP

In this chapter, we have studied how cyber terrorism has been defined by various research scholars along with its essential ingredients. Furthermore, we saw the famous incidents of cyber terrorism across the globe and ended the discussion with the legal framework of cyber terrorism under IT Act.

2.9 FURTHER READING

- Babak Akhgar, Andrew Staniforth, and Francesca Bosco. 2014.Cyber Crime and Cyber Terrorism Investigator's Handbook (1st. ed.). Syngress Publishing.
- See "Is Cyber-Terrorism the New Normal?" Available athttp://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/
- Robert W. Taylor, Eric J. Fritsch, Michael R. Saylor, and William L. Tafoya. 2018. Cyber Crime and Cyber Terrorism (4th Edition)(4th. ed.). Pearson.
- Joseph F. Gustin. 2004.Cyber Terrorism: A Guide for Facility Managers. The Fairmont Press, Inc., USA.

2.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber terrorism?**

Cyber-terrorism is a criminal act that uses computers and telecommunications capabilities to perpetrate abuse, damage, and/or service interruption in order to instill fear in a community by creating doubt and uncertainty, with the intention of persuading the government or populace to obey a series of laws.

2. **Which provision was introduced under the IT Act to combat cyber terrorism and when?**

Previously, there was no clear clause in the IT Act, 2000 that dealt directly with cyber terrorism; as a result, the Information Technology (Amendment) Act, 2008 incorporated a new section 66F. In light of the growing terrorist attacks in India and neighbouring countries, the IT Amendment Act of 2008 is a welcome move.

3. **Describe the cyber attack by tamil tigers?**

With surges of violence in Sri Lanka over many years, cyber-space attacks were the next focus in 1998. The Tamil Tigers, a militant resistance group, sent more than 800 e-mails per day to Sri Lankan embassies. This was done over the course of two weeks. “We are the Internet Black Tigers, and we are doing this to interrupt your communications,” said the e-mail address that started the attack. Local Intelligence officials were sent to investigate after the communications caused such extensive damage. The attack was the first recorded attack on a computer device in Sri Lanka by terrorists, according to the authorities.

2.11 ACTIVITY

Elaborate on the famous incidents of cyber terrorism across the globe along with provisions enacted in IT Act to combat the same. (1500-2000 words)

Unit 3: CYBER PORNOGRAPHY

3

Unit Structure

3.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- The meaning of cyber and child pornography
- Test of obscenity and pornography
- Obscenity and Freedom of speech and expression

3.2INTRODUCTION

The expression' pornography,' derives from the Greek terms 'porne' and 'graphein,' refers to any piece of art or literature that deals with sex and sexual themes or writing about prostitutes. It is difficult to describe the term pornography, as there is no clear legal meaning since each country has its own customs and practices. Pornography is legal in some countries, but it is immoral and punishable in others.

In simple words, cyber pornography is the act of using the internet to create, view, upload, import, or publish pornography or pornographic materials. Traditional pornographic content has been increasingly replaced by online/digital pornographic content with the rise of cyberspace.There is no legal or clear definition of pornography. The response of culture, traditions, and principles to pornographic material defines the concept of pornography.

The lack of a consistent definition of pornography is due to the fact that there is no common standard of culture and ethics in the world, nor are there universal rules that describe pornography. Obscenity and pornography are described differently in various countries and at different times. The words obscenity and pornography are separate, but they are related. The same content that is forbidden in certain countries may be permissible in others.The word pornography is not specified in Indian law, and it is not dealt with.

The advent of the internet to the world has resulted in a new age in the pornography industry. The pornography industry has learned that the internet is the best tool for disseminating pornographic content around the world. According to a 2010 internet filter analysis survey, there are 4.2 million websites worldwide that sell pornographic content. Every day, 68 million searches are made on search engines, and 72 million people visit adult websites each month around the world.42.7 percent of all internet users watch sexual videos on the internet.[52]

DVDs and videotapes became the most common means of spreading pornography in the early years, or before the internet was readily available.However, after the internet was made accessible to the general public, it soon became the most common avenue for people to view pornography from the privacy of their own homes. A person who may not have access to pornographic content due to social pressure or embarrassment can now freely view pictures or videos on the internet.Greater access to pornography was made possible by the advent of pornography websites that provided images, video clips, and streaming videos, including live web cam access. Over the internet, information technology has made it possible to produce and publish obscene materials; for example, content can be distributed all over the world in seconds, and geographical barriers that historically prohibited international publications from accessing local jurisdictions have vanished.[53]

3.3 TEST OF OBSCENITY AND PORNOGRAPHY

To comprehend the gravity and influence of pornography and obscenity on culture, we must first comprehend these words in their broadest context. The word *'pornography'* has not been legally defined.

The issue of obscenity has always been a complex one as it involves other related issues like decency and morality. It is difficult to judge obscenity in isolation using straitjacket principles. It needs a wider perspective. For example, a depiction of a nude body form is indecent and vulgar for some, but for some, it is an artistic expression to be savoured by one and all. When such a dichotomy exists, it is important that a holistic view should be undertaken as any narrow interpretation of statutes may lead to a miscarriage of justice. It would be more if one were dealing with the vexatious question of *'cyber obscenity'*. Believing and interpreting that *'cyber obscenity'* is an extension of *'physical obscenity'* would be fallacious.

[52] http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html

[53] Gorman, L. and Maclean, D. Media and Society in Twentieth Century, Blackwell publishing, 2003.

In the case of *Regina vs Hicklin*,[54] the test of obscenity was first described as the propensity "to deprave and corrupt those whose minds are open to certain forces and into whose hands a publication of this nature may fall," with the assumption that this test will only extend to anisolated passage of the work.

The Supreme Court of the United States in *Miller vs California*[55] released a seminal opinion that established the fundamental principles and three-point tests for evaluating obscenity in work, namely:

1. That the ordinary individual, following contemporary "cultural norms," will find that the work, as a whole, appeals to the prurient interest.
2. That the work illustrates or portrays sexual activity or excretory activities in an objectionable fashion, as described by relevant state or applicable law.
3. Whether the work has serious literary, cultural, political, or science merit as a whole.

Prior to *Miller vs United States*, the Supreme Court of the United States ruled in a landmark case, *Roth vs United States*,[56] that "obscene content was not covered by the First Amendment and should be governed by the States rather than by a single, Federal standard and also a new judicial standard for determining obscenity that invoked the common person's application of contemporary community standards to judge whether or not the dominant theme of the material taken as a whole appeal to prurient interest."

The Supreme Court went on to state that "to assess if obscenity is derived, we need to consider the following five-part structure:

1. The perspective of the evaluation was from the viewpoint of a man of ordinary prudence.
2. To assess obscenity, societal principles of acceptability were to be included.
3. Obscenity regulations can only extend to works with a particular theme.
4. A work had to be presented in its entirety in order to be judged for obscenity.
5. An obscene work was one that aimed to excited individuals' prurient interest."

[54] Regina vs. Hicklin [1868] LR 3 QB 360

[55] Miller vs. California, 413 US 15(1973)

[56] Roth vs United States, 354 US 476 (1957)

In the leading case of *Ranjeet D. Udeshi vs State of Maharashtra,*[57] the Supreme Court did not use the miller test and instead adopted the Hicklin's Test.The Supreme Court determined several questions related to obscenity. The Supreme Court does not believe obscenity to be a nebulous word, but rather a well-defined term, even though people have different opinions of what is and is not obscene. "In evaluating a work, emphasis should not be put on a word here and a word there, or a passage here and a passage there," the Supreme Court ruled.Though the whole work must be regarded, the pornographic content must be investigated separately to assess if it is so heinous and its obscenity so defined that it is liable to deprave and degrade all whose minds are sensitive to such influences. In this context, it is important not to ignore contemporary society's interests, especially the effect of the contested book on it. When obscenity and art are merged, the art must take precedence over the obscenity, otherwise the obscenity must be so small and trivial that it has little impact and may be ignored.The compromise between "freedom of speech and expression" and "public decency or morals" must be maintained; but, where the latter is significantly abused, the former must surrender."

The Court, on the other hand, warned that treating of sex and nudity in art and literature alone cannot be considered evidence of obscenity. "It is not appropriate to have the angels and saints of Michelangelo wear breeches until they can be viewed," the Court said. If the stringent test of treating sex as the minimum component is adopted, hardly any contemporary writer of fiction can avoid the fate Lawrence did. Part of the bookshops would close, and the other half would specialize in moral and religious literature."

In the said case, the Supreme Court held that "It makes the court the judge of obscenity in relation to an impugned book etc. and lays stress on the potentiality of the impugned item to deprave and corrupt by unethical influences." It will still be a matter for each case to decide, and it does not compel a negative judgment in any case."

The Supreme Court ruled in *Samresh Bose vs Amal Mitra,*[58] that "a lewd writing is not actually obscene." Vulgarity elicits emotions of shame and revulsion, as well as boredom, but it has little effect on the morality of any reader of the books, while obscenity has the power to deprave and degrade those whose minds are sensitive to

[57] Ranjeet D. Udeshi v. State of Maharashtra, AIR 1965 SC 881
[58] Samresh Bose v. Amal Mitra, AIR 1986 SC 967

such unethical influences."The Court differentiated between vulgarity and obscenity in this case, and further noted that when ruling on obscenity, "the Judge should put himself in the role of a reader of any age group into whose hands the book is likely to fall and should try to understand what sort of potential effect the book is likely to have in the minds of the readers."

The Supreme Court of India presently adopts the *Community Standards Test* as a measure of detecting obscene content. In *Aveek Sarkar vs State of West Bengal*[59], the facts of the case revealed that a German magazine published an article about a tennis player picturing him naked with his fiancé as a stand against racism and to show that love champions over everything. The Supreme Court found the respondents innocent of the charges levied against them and held that in a situation like this Hicklin's test cannot be used and the only measure to be implemented is the community standards test; and it further stated that the photograph must be viewed in the context of the message which the photograph appears to convey, and not in isolation. The Supreme Court further instructed that a more adaptive community standards test must be applied for a continuously evolving society like India.

3.4 IT ACT AND PORNOGRAPHY

Section 67 of the IT Act, 2000 deals with obscenity and pornographic content on internet. Similarly, Section 292 of the Indian Penal Code, 1860 deal with the issue of obscenity.

According to Section 67, obscene content in electronic form must be investigated individually to determine if it is so gross and its obscenity so defined that it is likely to deprave and degrade those whose minds are vulnerable to such effects and into whose hands the obscene material in electronic form is likely to fall.

Critically speaking, the said provision, like Section 292(1) of IPC, does not make knowledge of obscenity an ingredient of the offence. Thus to escape criminal charges, one has to prove his lack of knowledge of publication or transmission of obscene information in electronic form. Moreover, though publication or transmission of obscene information may be illegal but mere possession, browsing or surfing through obscene content is not an illegal activity.

[59] (2014) 4 SCC257

It should be noted that under no circumstances any offence related to obscenity in electronic form should be tried under Section 292 of IPC as Section 81 of the IT Act, 2000 states that the Act will have an overriding effect:

‘The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force’.

Moreover, the punishment provision under Section 67 of the Act is far more stringent, i.e., *‘The offender/s shall be sentenced with imprisonment of either description for a period not exceeding three years and a fine not exceeding five lakh rupees on the first arrest, and with imprisonment of either description for a term not exceeding five years and a fine not exceeding ten lakh rupees on the second or subsequent conviction'* at least monetary wise, than what is being given under Section 292 of IPC. Thus any attempt to use Section 292 IPC for publishing or transmitting of information, which is obscene in electronic form instead of Section 67 of the Act would create unnecessary confusion and may also result in miscarriage of justice.

Section 67 of the IT Act of 2000 is identical to Section 292 of IPC.In the case of *Ranjit D. Udeshi v. State of Maharashtra*, the Court ruled that, unlike other clauses that contain terms like “knowingly” or “negligently,” this one does not.As a consequence, mens rea becomes a requirement for maintaining remorse. The offence is not made more egregious by the fact that the perpetrator is aware of obscenity. The Prosecution should not have to assert anything that the statute does not demand.The challenge in collecting legal proof that the defendant was aware of the offence has made the liability strict.The lack of such information can be considered a mitigating cause, but it does not exclude the situation from the clause. If we refer the *Ranjit D. Udeshi case* to Section 67 of the IT Act, 2000, we can infer that the mere publishing and dissemination of indecent content is a crime, regardless of the offender’s mental state.This, though, cannot be a common law that applies to all.[60]

3.5 COMBATING CHILD PORNOGRAPHY

In today’s world, children, especially teenagers, want to explore everything on the knowledge highway. Today’s children have access to the internet and computers at

[60] Prof. R.K.Chaubey, “An Introduction to Cyber Crime and Cyber law”, Kamal Law House, 2012, p. 440

home, and they are expected to use the internet and computers as part of their studies. They are vulnerable to the perceived risks of the internet and they have access to computers and the internet.Children are occasionally involved in sexuality and sexually suggestive content. The parents have little influence over their children, and the children are occupied with exploring the internet and other media in order to satisfy their desires through online access.Children's interests are fulfilled by sex–offenders who take advantage of the situation. At this age, the infant is unable to comprehend or consider the possible risk of these experiences. Abusers use the internet widely to sexually assault minors all around the world.Since the internet has become a household item in India, children have become vulnerable to cyber crime. Paedophiles are committing acts of abuse against children.

In the physical world, parents are mindful of the risks and educate their children about how to prevent or cope with difficulties by following simple instructions. However, when it comes to cybercrime or online-related crime, most parents are unaware of the concerns or risks presented by the different resources provided on the internet. Paedophiles take advantage of these circumstances by luring children and gaining their trust, and manipulating them when their parents or teachers do not warn them of what is wrong or right on the internet.

The Information Technology Act, 2000 does not have any clear rules on child pornography, but later, the Information Technology Amendment Act, 2008 introduced a new Section 67B.

The said provision criminalizes all kinds of online child pornography. The term online refers to publishing or transmitting of material depicting children in the sexually explicit act, etc., in electronic form. Under the said section, five instances of online child pornography have been criminalized:

a) Publishing or transmitting or causing to publish or transmit material in any electronic form which depicts children engaged in sexually explicit act or conduct;
b) Creating text or digital images, collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing material in any electronic form depicting children in obscene or indecent or sexually explicit manner;
c) Cultivating, enticing or inducing children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource;

d) Facilitating abusing children online, and
e) Recording in any electronic form own abuse or that of others pertaining to sexually explicit act with children.

Although under Section 67B, five instances of online child pornography have been criminalized, but it is obligatory to note that clauses (a) and (e) are generic in nature, whereas clauses (b), (c) and (d) are specific.

In the case of *U.S. vs Joseph C. Bledsoe,*[61]the defendant was convicted for knowingly publishing a notice over the Internet offering to exchange child pornography on violation of 18 U.S.C. § 2251(d). The defendant appealed his conviction and sentence. The U.S. Court of Appeals for the Fourth Circuit affirmed the conviction and sentence.

Similarly, in *U.S. vs Philip M. Sebolt,*[62] the accused was convicted for using computer to possess, transmit, advertise child pornography in violation of 12 U.S.C. §§ 2252A(a)(1), 2251(d)(1)(A). Also, in *U.S. vs Michael Shawn McCourt,*[63] the defendant was convicted for attempted distribution and attempted receipt of child pornography over the Internet and possession of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (4).

3.6 OBSCENITY AND FREEDOM OF SPEECH AND EXPRESSION

The Indian Constitution acknowledges freedom of speech and expression as a constitutional right subject to reasonable restriction to uphold law and order, public health, morality, and decency, among other items. Sections 292 and 499 of the Indian Penal Code 1860, however, prohibit freedom of speech and language. It means that one cannot defame others while exercising their constitutional right to free speech and expression, and it bans expression through obscene content, as well as the publishing and dissemination of obscene material.

The facts of the case in *Maqbool Fida Husain vs Raj Kumar Pandey*[64] is that renowned painter MF Husain painted a nude lady in sorrow without giving it a title. In

[61] U.S. v. Joseph C. Bledsoe, 04-4276, 177 Fed. Appx. 311.
[62] U.S. v. Philip M. Sebolt, 04-2588, 460 F.3d 910
[63] U.S. v. Michael Shawn McCourt, 06-1018, 468 F.3d 1088.
[64]Maqbool Fida Husain v Raj Kumar Pandey, Delhi High Court Crl. Revision Petition No. 114/2007

2004, an untitled painting was sold to a private collector. Under the name 'Bharat Mata,' it was used in an online fundraising auction for victims of the Kashmir earthquake in 2006. Husain had no interest or role in this sale. There were massive demonstrations against the artwork, which was used in an auction commercial.Multiple cases were filed under the Indian Penal Code, 1860, sections 292, 294, and 298. The concern was whether the painting's representation of a naked woman as "Bharat Mata" should be deemed obscene under section 292 of the Indian Penal Code. "...the artistic touch to the artwork dwarfs the so-called obscenity in the form of nudity and makes it so picayune and trivial that the nudity in the painting can quickly be overlooked," the Court concluded. The naked woman was not portrayed in any odd poses, nor were her surroundings painted to evoke lewd feelings or desire.The Ashoka Chakra was also not put on any aspect of the woman's body that could be perceived as insulting to the national emblem.

"The literature of India, both religious and secular, is full of sexual allusions, sexual symbolism, and passages of such frank eroticism that are not found anywhere in world literature," the Court observed. "While an artist should have artistic independence, he is not free to do anything he wants," it added. The distinction that must be made is between art as an expression of beauty and art as an expression of an ill mind obsessed by a vulgar manifestation of counter-culture, the latter of which must be kept out of civilian society.""There should be freedom for the thinking we despise," the Court said. If there is no freedom after speech, freedom of speech is pointless. The degree to which democracy spreads equality and accommodation is a test of its reality."

Regarding film censorship, Chief Justice of the Supreme Court M. Hidayatullah held in *K.A. Abbas vs Union of India,*[65] that "our freedom of speech and expression is not absolute, but rather restricted by fair limitations under Article 19 (2) in the interest of upholding public decency and morality." As a result, in the area of cinematograph film, film censorship has total authority to prohibit and regulate obscenity and pornography."

While determining if the film "Satyam Shivam Sundaram" was obscene and indecent, the Supreme Court claimed in *Raj Kapoor and Others v State and Others,*[66] that

[65] K.A. Abbas v. Union of India, (1970) 2 SCC 780

[66] Raj Kapoor and Others vs State and Others, AIR 1980 SC 258

"While a certificate given by the Censor Board is appropriate, it does not prevent the court from deciding if a film is obscene or not."

3.7 LET'S SUM UP

In this chapter, we have studied the meaning and definition of cyber and child pornography and how it is dealt with in the Information Technology Act, 2000, as well as the Indian Penal Code, 1860. Furthermore, we saw the different tests of obscenity observed by the Courts and ended the discussion with obscenity and freedom of speech and expression.

3.8 FURTHER READING

- Wolak J, Finkelhor D, Mitchell K. Internet-initiated sex crimes against minors: Implications for prevention based on findings from a National study. Journal of Adolescent Health 2004; 35:424.e11-424.e20.
- Quayle E, Taylor M. Child pornography and the internet perpetuating a cycle of abuse. Deviant Behavior 2002; 23(4): 331-361.
- Heck, Richard Kimberly (forthcoming). Pornography and Accommodation. _Inquiry: An Interdisciplinary Journal of Philosophy.
- Howitt D, Sheldon K. The role of cognitive distortions pedophilic offending: Internet and contact offenders compared. Psychology, Crime and Law 2007; 13(5):469-486.
- Ost S. Children at Risk: Legal and Societal Perceptions of the Potential Threat that the Possession of Child Pornography Poses to Society. Journal of Law and Society 2002; 29(3): 436-460.

3.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber pornography?**

Cyber Pornography can be defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials.

2. **In which case was the test of obscenity first described?**

In the case of *Regina vs Hicklin*, the test of obscenity was first described as the propensity “to deprave and corrupt those whose minds are open to certain forces and into whose hands a publication of this nature may fall,” with the assumption that this test will only extend to a isolated passage of the work.

3. **Explain Section 67 of IT Act?**

According to Section 67, obscene content in electronic form must be investigated individually to determine if it is so gross and its obscenity so defined that it is likely to deprave and degrade those whose minds are vulnerable to such effects and into whose hands the obscene material in electronic form is likely to fall.

3.10 ACTIVITY

Elucidate the test of obscenity and pornography and which test is currently adopted by the Indian Courts and why? (1500-2000 words)

Unit 4: CYBER WARFARE

4

Unit Structure

4.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- How information is being used as a tool of war
- Indicators of cyberwarfare capabilities
- Cyberwarfare and role of India

4.2 INTRODUCTION

The cyber warfare world was created by combining several elements from the experience of human conflict. Certain forerunners developed dispute standards that now extend to the cyber domain well before the advent of the machine and the ability to communicate on the Internet. This chapter looks at the role of intelligence in the history of human war, including both the effort to learn about the adversary and the desire to keep the information safe from enemies. The relentless search for fresh and reliable knowledge has affected every area of conflict across computer networks as cyber operations have become more widespread.

Cyberwarfare is computer or network-based conflict involving politically motivated attacks by a nation-state on another nation-state. In these types of attacks, nation-state actors attempt to disrupt the activities of organizations or nation-states, especially for strategic or military purposes and cyberespionage.

Although cyber warfare generally refers to cyber attacks perpetrated by one nation-state on another, it can also describe attacks by terrorist groups or hacker groups aimed at furthering the goals of particular nations. It can be difficult to definitively attribute cyber attacks to a nation-state when those attacks are carried out by advanced persistent threat (APT) actors, but such attacks can often be linked to specific nations. While there are a number of examples of suspect cyber warfare attacks in recent history, there has been no formal, agreed-upon definition for a cyber "act of war," which experts generally agree would be a cyber attack that directly leads to loss of life.

Cyber warfare can take many forms, including:

- viruses, computer worms and malware that can take down water supplies, transportation systems, power grids, critical infrastructure and military systems;
- denial-of-service (DoS) attacks, cyber security events that occur when attackers take action that prevents legitimate users from accessing targeted computer systems, devices or other network resources;
- hacking and theft of critical data from institutions, governments and businesses; and
- ransomeware that holds computer systems hostage until the victims pay ransom.[67]

4.3 OBJECTIVES OF CYBER WARFARE

According to Cyber security and Infrastructure Security Agency (CISA), the goal of those engaged in cyber warfare is to “weaken, disrupt or destroy the US.” To achieve their goals, “national cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm US interests,” says CISA. These threats range from propaganda to espionage and serious disruption with loss of life and extensive infrastructure disruption. A few examples of threats include:

- Espionage for technology advancement. For example, the National Counterintelligence and Security Center (NCSC) in its 2018 Foreign Economic Espionage in Cyberspace report notes that China’s cyber security law mandates that foreign companies submit their technology to the Chinese government for review and that Russia has increased its demand of source code reviews to approve of foreign technology sold in their country. In 2018, the US Department of Justice charged two Chinese hackers associated with the Ministry of State Security with targeting intellectual property and confidential business information.
- Disruption of infrastructure to attack the US economy or, when attacked by the US, to damage the ability of the US to continue its attacks. For example, by controlling a router between supervisory control and data acquisition (SCADA)

[67] https://searchsecurity.techtarget.com/definition/cyberwarfare#:~:text=Cyberwarfare%20is%20computer%2D%20or%20network,or%20military%20purposes%20and%20cyberespionage.

sensors and controllers in a critical infrastructure, such as the energy sector, an enemy can attempt to destroy or badly damage energy plants or the grid itself.

Cyber attacks are also used to sow discord to destabilize government. For example, according to Report On The Investigation Into Russian Interference In The 2016 Presidential Election, by Special Counsel Robert S. Mueller, III, Russia's Internet Research Agency "used social media accounts and interest groups to sow discord in the U.S. political system through what it termed 'information warfare.' The campaign evolved from a generalized program designed in 2014 and 2015 to undermine the U.S. electoral system, to a targeted operation that by early 2016 favoured candidate Trump and disparaged candidate Clinton."[68]

4.4 TYPES OF CYBER WARFARE ATTACKS

Increasingly, cybercriminals are attacking governments through their critical infrastructure, including transportation systems, banking systems, power grids, water supplies, dams, hospitals and critical manufacturing.

The threat of cyberwarfare attacks grows as a nation's critical systems are increasingly connected to the internet. Even if these systems can be properly secured, they can still be hacked by perpetrators recruited by nation-states to find weaknesses and exploit them.

APT attacks on infrastructure can devastate a country. For example, attacks on a nation's utility systems can wreak havoc by causing widespread power outages, but an attacker with access to hydropower grids could also conceivably cause flooding by opening dams.

Cyberattacks on a government's computer systems can be used to support conventional warfare efforts. Such attacks can prevent government officials from communicating with one another; enable attackers to steal secret communications; or release employee and citizen personal data, such as Social Security numbers and tax information, to the public.

[68] https://searchsecurity.techtarget.com/definition/cyberwarfare#:~:text=Cyberwarfare%20is%20computer%2D%20or%20network,or%20military%20purposes%20and%20cyberespionage.

Nation-state-sponsored or military-sponsored attackers might also hack the military databases of their enemies to get information on troop locations, as well as what kind of weapons and equipment they're using.

DoS attacks, which continue to increase around the world, are expected to be leveraged for waging cyberwarfare. Attackers are using distributed denial of service (DDoS) attack methods to hit government entities with massive sustained bandwidth attacks, and at the same time infecting them with spyware and malware to steal or destroy data. These attacks may inject misinformation into the networks of their targets to create chaos, outages or scandals.[69]

4.5 EXAMPLES OF CYBER WARFARE

Perhaps the earliest instance of a nation waging cyberwar was the Stuxnet worm, which was used to attack Iran's nuclear program in 2010. The malware targeted SCADA (supervisory control and data acquisition) systems, and was spread with infected USB devices; while the United States and Israel have both been linked to the development of Stuxnet, neither nation has formally acknowledged its role.

Nation-state actors are believed to be behind many other cyberwarfare incidents. For example, in March 2014, the Russian government allegedly perpetrated a distributed denial-of-service attack that disrupted the internet in Ukraine, enabling pro-Russian rebels to take control of Crimea.

Then in May 2014, three days before Ukraine's presidential election, a hacking group based in Russia took down Ukraine's election commission's system, including the country's backup system. However, Ukrainian computer experts were able to get the system up and running before the election. The cyberattack was launched to wreak havoc and damage the nationalist candidate while helping the pro-Russian candidate, who ultimately lost the election.

[69] https://searchsecurity.techtarget.com/definition/cyberwarfare#:~:text=Cyberwarfare%20is%20computer%2D%20or%20network,or%20military%20purposes%20and%20cyberespionage.

Hackers associated with the government of North Korea were blamed for the 2014 cyberattack on Sony Pictures after Sony released the film The Interview, which portrayed the North Korean leader Kim Jong-un in a negative light.

During its investigation into the hack, the FBI noted that the code, encryption algorithms, data deletion methods and compromised networks were similar to malware previously used by North Korean hackers. In addition, the hackers used several IP addresses associated with North Korea.

A 2015 attack on the German parliament, suspected to have been carried out by Russian secret services, caused massive disruption when the attack infected 20,000 computers used by German politicians, support staff members and civil servants. Sensitive data was stolen, and the attackers demanded several million euros to clean up the damage.

Although a group of Russian nationalists who wanted the government of Berlin to stop supporting Ukraine claimed responsibility, members of the Russian intelligence were also reported to be involved.

Since then, a Malware Analysis Report (MAR) issued by the Department of Homeland Security (DHS) and the FBI identified two malware codes, HOPLIGHT and ELECTRICFISH, released by North Korea.

Also in 2015, cybercriminals backed by the Chinese state were accused of breaching the website of the U.S. Office of Personnel Management to steal data on approximately 22 million current and former employees of the U.S. government. Chinese cybercriminals have been implicated in the theft of U.S. military aircraft designs, an incident that caused then-president Barack Obama to call for a treaty on cyberarms control.

On a cold winter's day in December 2016, more than 230,000 customers in Ukraine experienced a blackout, the result of remote intrusions at three regional electric power distribution companies. The attack was suspected to originate from Russia. The perpetrators flooded phone lines with a DoS attack and also used malware to attack and destroy data on hard drives at the affected companies. While the power was restored within hours, it took months for the companies to restore full functionality to the control centers that had been attacked.

In 2016, 2017 and again in 2018, variations of malware known as Shamoon struck businesses in the Middle East and Europe. McAfee's Advanced Threat Research concluded that the Iranian hacker group APT33, or a group masquerading as APT33, is likely responsible for these attacks.

On August 2, 2017, President Trump signed into law the Countering America's Adversaries Through Sanctions Act (Public Law 115-44) (CAATSA), imposing new sanctions on Iran, Russia, and North Korea.70

4.6 INFORMATION AS A TOOL OF WAR

Knowledge operations have been used to gain benefits in combat for as long as humans have participated in something that could be defined as "warfare." Attempts to observe enemy troop dispositions or diversion activities to conceal one's own troops in an ambush situation were examples of traditional intelligence campaigns. For gathering intelligence on the enemy's resources and intentions, an effective military leader can depend on a vast network of spies. This kind of spying may be carried out by uniformed scouts or by a camouflaged insider posing as a loyal member of the enemy's military.Of course, information was only valuable if it could be correctly shared in a timely manner, and information delivery posed inherent risks. If an adversary intercepts a messenger, the letter is lost, and the intelligence is sent to the opposing officer. As a result, it could be appropriate to send the message only verbally, in the hopes that the messenger may not leak the information, or in an encrypted script that the enemy may not be able to decipher.Fake communications may be intentionally leaked to the enemy to obstruct decision-making and fog the intelligence available to an adversary.

Since cyber warfare is such a novel phenomenon, it raises much more questions than it answers. The importance of cyber assets in national defence, the feasibility of a cyber policy, and even if the word "warfare" should be used to describe cyber operations are all topics that spark heated discussion. Many cyber operations, such

[70] https://searchsecurity.techtarget.com/definition/cyberwarfare#:~:text=Cyberwarfare%20is%20computer%2D%20or%20network,or%20military%20purposes%20and%20cyberespionage.

as fraud, espionage, and terrorism, have elements of warfare but do not fall within conventional categories.

4.7 INDICATORS OF CYBER WARFARE CAPABILITIES

Because of the technology's existence, the ability to produce and employ nuclear power, whether for peaceful or destructive purposes, was limited to a few developing nations when it was first developed. If a country decided to go nuclear, not only was the equipment difficult to obtain but the selected few powers still assured that ample obstacles were placed in their way. Then there was the threat of nuclear proliferation, which prohibited countries from using nuclear weapons in combat.As a result, the number of countries with nuclear weapons systems remained low. Some countries, such as North Korea and Iran, were quickly identified as attempting to develop a nuclear weapon covertly since there were few countries capable of acquiring the equipment for such a weapon system, and there was also a ban on the transfer of such technologies. Many of these aspects together meant that nuclear power remained a bastion of a chosen few.

This is not the case, though, for cyber technology.Information technology is unlike any other weapon system technology because of its inherent design and accessibility. It's perhaps the first commercial technology that can also be used for military purposes. As a result, the factors determining a nation's ability to fight a cyberwar would vary from those determining traditional or nuclear strength. Although determining a nation's nuclear and conventional warfighting capability is easy, determining a nation's cyber might is more complex.As a result, it's critical to figure out what considerations all go into cyberwar waging capability.

The government sector and the private sector are the two broad types of sources that are indicators of a nation's electronic warfare capability.

4.8 THE GOVERNMENT SECTOR

- ***Available Cyber Warfare Doctrine***

If a nation declares a cyber warfare policy, it is clear that the country has superior cyber capabilities. There is no time to think of a systematic solution during a cyberattack.A Cyber Warfare Doctrine outlines the roles of all players in the event of a cyberattack, provides a clear picture of the national response in the event of such an attack, and helps to prevent possible conflicts by a unified national security strategy. Just a few countries have issued an electronic warfare policy to date.

- ***Active Cyber Warfare Units***

If a nation wants to conduct offensive cyber operations while still protecting its own infrastructure, especially military infrastructure, it must be well prepared. As a result, those countries' military forces will have organizations capable of electronic warfare. A successful cyberwarfare organization will range from a national cyber command to a small unit capable of conducting cyberattacks. Several countries have either raised or are in the process of raising those powers. On the other hand, several countries have clandestine units capable of conducting cyber operations.In May 2013, India's former Defence Minister, Shri AK Antony, announced that the country would soon form a cyber command to deal with the country's online attacks.[71]About the fact that the cyber command is yet to see the light of day, the armed forces remain optimistic that the current government will eventually allot the funds needed to upgrade this strategic asset in India.

- ***Computer Emergency Response Teams (CERT)***

The Computer Emergency Response Team (CERT) is a government-mandated information technology security organization. The mission of the Computer Emergency Response Team (CERT) is to respond to computer security events, report vulnerabilities, and encourage successful IT security practices around the nation. CERT may exist at different levels, ranging from the national level to the level of a single organization. CERTs are now used by a variety of military forces around the world.

- ***Cyber Crime Prevention / Investigation Teams***

Although the aim of such teams is to combat and prosecute cybercrime, the essence of their work allows them to be an important weapon for defensive cyber operations.

- ***Government-run Academic Institutions with Cyber Programs***

Such organizations explicitly demonstrate that the government intends to build a skilled pool of manpower that can be used to conduct both defensive and offensive

[71] Cyber Command for Country Soon: Antony TNN May 26, 2013, 03.09AM IST

cyber operations. Ethical hacking programmes are conducted in a variety of countries, including India, to educate white hat professionals.

- ***Government Sponsored Cyber Projects***

A significant number of countries fund defence-related information infrastructure programmes, such as cyber-training programs. The aim of such programs may be to conduct research and development in the area of cyber technology, which can then be effectively used in strategic and tactical cyber warfare operations. Under the guise of R&D, some countries need such programs to conduct cyber espionage and surveillance.

- ***Intelligence Service Capabilities***

Intelligence is a critical component of cyber operations. When a country's government or security forces invest in cyber intelligence, it's safe to say that the country is indeed investing in cyber warfare capability.

- ***Military Command and Control Communications, Computer and Intelligence (C4I) and Information Warfare Capability***

To be a force multiplier, cyber-warfare must be integrated into a country's overall combat policy. As a result, cyber activities must be blended into the military's overall information warfare and C4ISR policy. If a country's military forces, such as the United States', have well-developed C4ISR capabilities, they will be able to conduct cyber operations with much greater ease than a country with little or limited C4ISR assets.

- ***Military Intelligence Units***

When a nation is attempting to develop aggressive cyber warfare capability, military intelligence teams are almost always tasked with gathering knowledge about the enemy's operating networks and IT processes. It will be difficult to carry out any cyberattacks during a war without this vital piece of intelligence.

- ***Military Units Capabilities***

Military technologies are being updated all over the world to track the rapidly evolving cyberspace, conduct cyberattacks, and protect against them. Armed forces are being trained and prepared to counter the vulnerabilities of the enemy's cyber warfare.The development of such technologies is the most telling sign that a country is attempting to acquire offensive cyber warfare capabilities.

- ***Overall use of IT***

The very presence of networks in a nation’s security forces, as well as its reliance on information technology for day-to-day operations, indicates that the country is prepared for cyber warfare. A well-connected army, navy, or air force would undoubtedly invest in cyber defence. If a force has defensive cyber warfare capability, it is almost assured that it will also have aggressive cyber warfare capabilities.

4.9 THE PRIVATE SECTOR

Although strong-armed forces are needed for a nation to fight a war, this is not the case for cyberwar. Non-state actors, cyber terrorists, and even state-sponsored hackers will engage in aggressive cyberwar/ cyber operations, unlike other means of warfare.A country’s private IT technology is sufficient to ensure that the country is prepared for cyberwar. As a result, the state of growth of the private sector is just as critical as a measure of a country’s cyber warfare capacity. The following are some of the aspects:

- ***Academia***

A well-developed educational infrastructure in computer science and engineering enables the country’s youth to be prepared for a variety of IT-related activities.The same youth can be used to create a solid electronic warfare foundation.

- ***Accessibility of network to the general public***

The greater the infiltration of facilities such as the internet, the more likely the nation would have cyber warfare capability.

- ***Computer security programs***

The nation’s cyber defence would be stronger than most as it is capable of designing or even enforcing sound information security systems.

- ***Expatriate students studying in technologically advanced countries***

China serves as an excellent example of this. According to the Minnesota Daily, between 2009 and 2012, US universities enrolled approximately 100,000 Chinese students, accounting for roughly a quarter of all international students in the country.[72] China now has one of the strongest offensive cyber capabilities.

[72] Department of Homeland Security, Study in the States as available at

- ***Fiber optic cable/copper wiring***

The physical network's size means that voice and data networks can cover even the most distant parts of the world. The wider the scope, the greater the number of users who have access to the internet.

- ***Hackers***

Hackers may be state-sponsored, sanctioned black hats and cybercriminals with clear political objectives. To educate security professionals, several countries run ethical hacking colleges.The more schools there are, the greater the pool of hackers open to the nation.

- ***Hardware production capabilities***

The country's overall development in the field of IT is reflected in its hardware development capability.

- Other considerations may include:
    a) public access to high-speed internet
    b) private sector IT collaboration with other countries
    c) IT networks in the world
    d) presence of IT defence firms in the country
    e) number of ISPs and key nodes
    f) The number of satellite connections that have nationwide network access
    g) Telephone line density
    h) Overall state and IT incorporation
    i) SCADA (supervisory management and data acquisition) systems are examples of process control systems
    j) Skills in software growth
    k) Transnational companies with an interest in or use of information technology

The above metrics indicate that the more mature a country's private IT and telecom industries are, the more likely it is that the country will be able to engage in cyber warfare. In either event, countries with well-developed telecom and IT industries, such as Japan, Taiwan, and India, would need to brace for cyberattacks by rogue

http:// studyinthestates.dhs.gov/2014/01/number-of-chinese-students-studying-inthe-united-states-increases nations and rogue elements. This ensures that defensive cyber capability becomes an inextricable aspect of a country's well-developed IT and telecom industries.

4.10 CYBER WARFARE AND ROLE OF INDIA

Cyberwarfare does not merely involve some countries as perpetrators and some as victims. Cyberwarfare is involved in all social spheres, it is all around us, and we encounter it every day. Every individual has used a fighting technique to gain information at least once in their lives, but this was not necessarily illegal and was mostly of no significance. In the context of cyberwarfare at the national level, among organizations, or by ideological, media and major interest groups, the warfare techniques and their consequences are often socially harmful. The struggle for information includes all countries and their entities. However, some are more aggressive than others because they devote more resources to the development of this field.

Different countries, in terms of their size, economic performance and political orientation, understand the importance and benefits of cyberwarfare and develop its techniques. In fact, it is not clear which entities are more successful in achieving this. The involvement of ICT in government and organizational structures is not necessarily an advantage since it can also represent a weakness in terms of risk. Countries mentioned as the main cyberwarriors (the United States, China and Russia) can be gradually equated with countries that are less dependent on ICT, closed and inaccessible (e.g. North Korea). The United States is certainly the world's leading political, economic and military superpower, which makes it the most popular target for malicious intrusions and attacks on information systems.

In the field of software development, India is an extremely powerful country, but we know little about its activities in cyberwarfare.[73] After the cyberattack India experiences in the summer of 2012, in which officials from the Ministry of External Affairs, the Ministry of Home Affairs, the Defence Research and Development Organization (DRDO), and the Indi-Tibetan Border Police)ITBP) were attacked, and a lot of sensitive information was under threat, it was found that approximately 12,000 computers were affected. At that time, the responsibility for preventing attacks was assigned to the Indian Computer Emergency Response Team (CERT-In), which is a branch of the Department of Information Technology. CERT-In

[73] Taken from Dala [DAL 11], Tiwary [TIW 11] and Kaushik and Fitter [KAU 13].

announced that the number of *'cybersecurity breaches has grown from 23 in 2004 to 13,301 in 2011'*. Because of these breaches, the government divided the CERT-In, in order to better prepare the country for serious threats: *'CERT-In now protects cyber assets in non-critical areas while a new body called the National Critical Information Infrastructure Protection Centre (NCIIPC) protects assets in sensitive sectors such as energy, transport, banking, telecom, defence, and space'.*

The government notes that more attention must be invested in research and development, whereas NCIIPC is preparing the final version of the national cybersecurity policy. In general, India has not suffered any major economic or physical harm due to cyberattacks. However, the government-owned Nuclear Power Corporation of India is at constant risk of security breach, since it continuously detects attacks but is, in its opinion, able to successfully block them. India admits that its cyberwarfare defence strategy was tackled too late and, consequently, it detects attacks on their infrastructure, but is now increasingly preparing adequate strategies and focusing its expertise on the development of this field so that in future India will be able to defend itself from attacks and join other countries that are active in the field of cyberwarfare.

4.11 LET'S SUM UP

In this chapter, we have studied how information can/is being used as a tool of war along with the indicators of cyberwarfare capabilities. Furthermore, we saw the government and private sector indicators and ended the discussion with the role of India in cyberwarfare.

4.12 FURTHER READING

- Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners by Jason Andress and Steve Winterfeld 7. Surviving Cyberwar by Richard Stienno
- Guidelines for Protection of National Critical Information Infrastructure, Version 1.0 (June 2013), issued by National Critical Information Infrastructure Protection Centre 14. Indian Army Doctrine, First edition, October 2004
- Cyber Deterrence and Cyberwar, Rand Corporation monograph by Martin C. Libicki 16. UN Convention on Cybercrime, CETS No.: 185

- Revamping India’s National Security Architecture for Optimum Synergy in the Use of its Instruments of National Power, The 18th Pyara Lal Memorial Lecture, 2014 by Shri Shyam Saran, IFS (Retd) 21. National Cyber Security Framework Manual, Edited by Alexander Klimburg

4.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is CERT?**

The Computer Emergency Response Team (CERT) is a government-mandated information technology security organization. The mission of the Computer Emergency Response Team (CERT) is to respond to computer security events, report vulnerabilities, and encourage successful IT security practices around the nation.

2. **Name 3 indicators in private sector?**

- Computer security programs
- Hackers
- Hardware production capabilities

3. **What is C4ISR policy?**

To be a force multiplier, cyber-warfare must be integrated into a country’s overall combat policy. As a result, cyber activities must be blended into the military’s overall information warfare and C4ISR policy. If a country’s military forces, such as the United States’, have well-developed C4ISR capabilities, they will be able to conduct cyber operations with much greater ease than a country with little or limited C4ISR assets.

4.14 ACTIVITY

Elucidate the Government and Private sector as indicators of cyberwarfare along with a few case studies. (2000-2500 words)

What is cyber warfare? What are its types? Explain cyber warfare with suitable examples. (2000-2500 words)

Block-4

INTERNATIONAL LAW ON CYBER SPACE

Unit 1: INTERNATIONAL LAW ON CYBER SECURITY IN THE AGE OF DIGITAL SOVEREIGNTY

1

Unit Structure

1.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- Existing challenges on international law and governance on cyberspace, and
- International law on cyberspace and digital sovereignty.

1.2 INTRODUCTION

Recent trends in the promotion of digital sovereignty have increasingly deprived us of the complexity and challenges of international law in cyberspace. Digital sovereignty is the ability to control and direct international actors through the use of digital technologies such as the Internet, social media, and other digital media. Although international law is still at an early stage, there is an urgent need for how it is applied in this area, but this is a long game

and is still in its infancy. This article is divided into two parts: a brief overview of the existing challenges for international cyber law and a discussion on the impact of these challenges on the future of cybersecurity.

Thomas Aquinas in his magnum opus Summa Theologica mentioned,"law is an ordinance of reason for the common good, made by those who have care of the community" (Aquinas, 1981). Unfortunately, this adage does not necessarily resonate to international law on cyberspace. The absence of effective international legal instruments on cyberspace has largely been discussed in theoretical and policy-making debates as the complexities in cyberspace render difficult for actors to come into agreements, let alone making agreeable binding law. The contentious academic debates chiefly divide those who believe that states must take more influential roles in formulating international law on cyberspace and those who insist that cyberspace should remain a free and diffused domain. Beyond academic textbooks, more dynamic debates take place by stakeholders and in international institutions (World Economic Forum, 2019; Opinio Juris, 2019). All of these debates reach into one converging point: the absence of international legal regime on cyberspace is derived from actor's complexity and jurisdiction on cyber realm. This is further complicated by the fact that in the past few years several international actors, mostly state actors, promote the idea of digital sovereignty to promote their interest to take back control on information, communication, data, and infrastructure related to the internet (Gueham, 2017). Consequently, this creates harder challenges on possible future international law on cybersecurity. The future of international law on cyberspace would also hardly apply to states' conduct due to the increasing trend of promotion of digital sovereignty norms.

> Sovereignty is one of the non-negotiable policies for ensuring the security of the country. Sovereignty ensures that we as a nation can stand up to pressures from other countries. Sovereignty is critical to ensure our economic independence.
>
> As Information Technology is playing an increasingly important role in India's economy, it becomes imperative to identify the issues of Digital Sovereignty and to formulate appropriate policies to ensure our Digital Sovereignty.
>
> So why is it that India's Digital Sovereignty is threatened? The threat to India's Digital Sovereignty is primarily coming from two areas i.e., the digital standards and the control of the Internet.
>
> Digital Standards are being used extensively to extract undue economic benefit from emerging economies such as India wherein a corporate or a coterie of corporates, typically based in the West, creates a standard and files numerous IPR encumbrances such as patents around the standard. The standard is then taken through one or more international standardization bodies and is turned into an international standard which is then forced unto the users in emerging economies. The users of the standard are then forced to pay disproportionate royalties either directly, or indirectly by paying a higher price for the end products with the manufacturers having to cough up the unfair royalties. The nation-state is helpless in this situation as any intervention will be either a TBT violation (Technical Barrier to Trade) or will be a violation under TRIPS.
>
> A very good example of the devastating effect that such a lack of Digital Sovereignty can have is the case of the DVD manufacturers in China. The DVD manufacturers have to pay royalty charges on each DVD player manufactured in China that is to the tune of 33% of the retail price of the DVD player, for a video format standard that is used as a standard in each DVD

player. This works out to be $20 royalty on a player of $60. As a response, China came out with an alternative video encoding standard called AVS (audio-video standard) so that its manufacturers could use this standard without any undue royalties. However, because of the global technology framework that has evolved, AVS could not significantly help alleviate the situation of the DVD manufacturers in China. China was helpless in preventing such an unfair cess being put on its domestic industry, demonstrating its lack of Digital Sovereignty then.[74]

1.3 DIGITAL SOVEREIGNTY IN INDIA

As India gets more and more dependent on its IT economy, we are going to see more similar issues coming up. The best example of such a situation was the recent case of Microsoft forcing its standards into ISO even though India and a majority of the population of the world voted against it. India again lost its digital sovereignty in this case on a technology that is critical for ensuring digital literacy in the country.

However, India as a nation has only recently woken up to the threat to the nation due to India's lack of control over IT standards and control over the Internet. The Indian government has only in the last half a decade, initiated steps to protect its citizens and businesses from foreign entities imposing their standards on India and Indians. Foreign entities are extracting royalties from the Indian economy without any significant contribution back to the economy.

On the other hand, after China was forced to back down on its aggressive stance on coming out with an alternate wireless LAN standard called WAPI (with the then US Vice President Dick Cheney personally leading the pressure on China), China put together a comprehensive technology standards strategy to protect its Digital Sovereignty.

The second issue which is threatening India's Digital Sovereignty is its ability to protect its interest in the Internet.

[74] https://www.outlookindia.com/website/story/opinion-standards-and-internet-the-cornerstones-for-digital-sovereignty/376498

The visceral of the Internet is primarily controlled by ICANN that determines the allocation of website addresses and machine addresses (IP addresses) through which computers and websites can be identified and accessed. ICANN is a California based company under US legal jurisdiction and it does not come under the jurisdiction of Indian law. Every individual/ business/ government that wants to set up a website on the Internet, has to pay directly or indirectly to ICANN to get the website name and/or the IP address. The lack of our digital sovereignty has ensured that we have very little formal control over how the Internet is governed and that we and our people have to pay unjust amounts to a US company. Also, ICANN has come out with more Top Level Domains (TLD's). What this means is that ICANN can issue a name and we will have no control over it. Or it can come out with unacceptable sites with names of Gods and Goddesses at the end of the name with the Government of India having no control over it while riots break out in India. Of course, ICANN has now moved to a governance format which is termed as “multistakeholderism”.

Loss of Digital Sovereignty makes our IT industry vulnerable and ephemeral as the real control over technology continues to stay with developed economies.

It is the need of the hour for India to come out with a robust Digital Sovereignty policy that protects our IT industry and our consumption of Information Technology. In the absence of such a policy, we stand to get arm-twisted and our businesses will have to give out undue payoffs to non-Indian agencies for using technologies that are fundamental to our economy. It also includes having control over what goes into the building of our IT infrastructure, telecom switches and set-top boxes.[75]

1.4 EXISTING CHALLENGES ON INTERNATIONAL LAW AND GOVERNANCE ON CYBERSPACE

The idea of regulating cyberspace by international law is not something remarkably novel. Since 1996, the efforts of formulating international law on cyberspace have already been continuously proposed (and refuted) by law experts, business actors, and states. There are three dominant ideas on how cyberspace should be regulated by international law: Liberal Institutionalists, Cyberlibertarian, and Statists. Liberal institutionalists like Wu (1997) call for the importance of the

[75] *Ibid.*

international institution and rule-based multilateralism in managing cyberspace. While cyberlibertarians like John Barlow (1996) are proponents of the idea that cyberspace should remain free from tyranny and any oppressive rule that might hinder the internet liberty . Statists, like James Lewis (2010), believe that it is states' responsibility to formulate national and international law to govern cyberspace. These three mainstream ideas echo into the development of international law on cyberspace. Binding and well-functioning international law on cyberspace is still absent due to these ongoing contentious debates. These debates rest on to three major challenges on formulating international law on cyberspace are related to the core of principles and characteristics of international public law: jurisdiction, arbitration, and legal Instruments & jurisprudences.

Jurisdictions in international law according to Basak Cali (2015) relates largely to the subject of international law (or actors in international relations) and territoriality to which law may be formally exercised. The subject of law or actors in cyberspace are widely diverse and diffused as it ranges from state actors, big internet companies, small-medium enterprises (SMEs), hackers, to individuals–not to mention that internet innately also provides anonymity to its users. Those various actors also bear their own different interests and issues on how cyberspace should be regulated. It is still immensely challenging to address which subjects of law are legitimate to make and be affected by international law on cyberspace, as well as what issues should be regulated. This is also increasingly challenging to attribute conducts made by actors and where it is conducted.

Numerous debates either in academic texts or policymaking have been rendered specifically discussing attribution on cyber conduct (Rid & Buchanan, 2014). Yet, there is no single dominant and prevailing voice in that debate except for those attribution of cybercrime from state actors to nonstate actors in which it is relatively agreed and functioning in international regimes, such as exemplified in Interpol, Europol, ASEANAPOL, and UNODC. In terms of domain in cyberspace, international actors have not come into agreement on the status of cyberspace whether it is global commons, belongs to physical states' territory, or based on their national origins (Liaropoulos, 2017). As a result, it creates major challenges to determine jurisdiction of international cyber law until today.

The complexity of actors and issues discussed above render further complications in arbitration. Public international law necessitates clear dispute settlement mechanisms and arbitration to ensure that law is enacted and binding its signatories and subjects (Cali, 2015). In cyberspace law, due to its actors' diversity, there is still no universally agreed legal norm reached on who should get the mandate of dispute settlement mechanisms and arbitration. There is already arbitration on cyberspace conducts but mostly it is related to commerce and crime in which it takes place in the national legal system rather than international court (Kittichaisaree, 2017). Thus, this potentially undermines the impartiality of law since states presumably have greater bargaining power in such a legal system. Nevertheless, it is not impossible to have possible international arbitration in cyberspace. Permanent Court of Arbitration in The Hague, Netherlands might have the potential to be addressed as adjudication party on cyberspace as it already has a mandate on outer space, energy, and environmental cases. However, it needs major approval from state actors to push such mandates and authorities on cyberspace cases.

Related to arbitration, one must take into account the cyberspace challenges of legal instruments and jurisprudence. Both take place in two levels: national and international. Legal frameworks addressing cyberspace are relatively already well-developed in developed countries. In the federal level, U.S. has three fundamental regulations enacted in HIPAA (1996), Gramm-Leach-Billey Act (1999), and Homeland Security Act (2002). In France, the national authority has enacted and developed legal frameworks on cyberspace since 1988. In Russia, the federal authority also adopted the Russian Federal Law on Personal Data no. 152 FZ since 2006 (Kittichaisaree, 2017). However, those countries take a different standpoint on cyber space as Russia controversially stipulates security concern as a priority over privacy rights and the U.S. have a similar problem since Snowden's issue rise into public attention. This disparity will be widened out if we delve into cyber legal frameworks in developing countries such as Malaysia and Indonesia. Malaysia does not have a standalone cyber act or bill in which it creates room for deep state' intervention to citizen's data (ICLG, 2019).

Indonesia is in worse condition–its proposed law on cybersecurity was postponed to be adopted due to massive student demonstrations in the last few months caused by human rights concerns (Jakarta Globe, 2019). These national legal framework disparities show how the absence of effective international law on cyberspace stems from national legal instruments. On the international level, the law on cybersecurity is scarce. Indeed there is Budapest Convention which is claimed to be the only international treaty on cyberspace. But one must not deny the fact that this is a lack of binding dispute settlement mechanism, tends to be state-centered, and focus profoundly on cybercrime. There is also a series of discussions on encouraging international customary law to be the foundation of international law on cyberspace (Brown & Poellet, 2012). Yet, international customary law requires reified practice and solidified legal instruments performed at the national level. As mentioned above, this is still improbable due to disparities of the national legal system on cyberspace in various countries. Efforts to formulate regulation also occur in various institutions, such as ITU, ICANN, and Internet Governance Forum in regard to governing fundamental norms, principles, and operationalities of cyberspace (Deibert & Crete-Nishihata, 2012). Unfortunately, none of those manages to overcome how international law applies effectively to states and addresses various issues in cyberspace beyond cybercrime and technicalities. None of those successfully creates appropriate and binding international legal instruments and jurisprudence. Ergo, international law on cyberspace currently is hardly effective and more difficult to be imposed on state actors.

1.5 INTERNATIONAL LAW ON CYBER SPACE AND DIGITAL SOVEREIGNTY

The complexities and challenges of international law on cyberspace are increasingly deprived by a recent trend on digital sovereignty promotions. Digital sovereignty is the idea to control and govern access, information, communication, network, and infrastructure in digital realm by international actors (Couture & Toupin, 2019). In recent years, this idea has been gaining traction because of three historical conjunctures in cyberspace: China and Russia cyber alliance on digital sovereignty; Snowden and Wikileaks cases; and the rise of GAFA (Google-AppleFacebook-Amazon). China and Russia cyber alliance on digital sovereignty becomes the major precursor of digital sovereignty as both countries actively promote such an idea in order to protect their national interests which mostly are related to economy and security concerns. Both countries demand greater control of their own cyberspace by underpinning the principle of non-interference in multiple global internet governance such as ITU, ICANN, IANA, and Internet Governance Forum (Budnitsky & Jia, 2018). This sparks debate on whether the idea of digital sovereignty is against internet neutrality or not (Mueller, 2012).

However, their efforts influentially shift the paradigm of state control over their cyberspace as that idea is supported by countries like Saudi Arabia and Egypt (Deibert & Crete-Nishihata, 2012). Their efforts also invoked the European Union to reconsider letting internet in laissez-faire mode continue as Snowden-Wikileaks cases rose into public attention. Security and data protection concerns have increasingly become the center of debate gravity on whether the European Union should support (Dworkin, 2015). Later, this concern has broadened up to economic consideration due to the unchecked behavior of rising big internet companies, especially GAFA. The astronomical rise of GAFA made EU consider their digital ecosystem in order to prevent business monopoly and support the innovation and internet capabilities throughout Europe (Stormshield, 2018).

These situations unequivocally set new climate of international law on cyber space in favorable to state actors. These digital sovereignty promotions and advancements would not only potentially undermine particularly non state actors and internet neutrality as the questions of freedom and liberty in cyberspace consequently emerge. These also erode the potential agreeable international law on cyber security. It is because digital sovereignty would potentially create the fragmented cyber space as it will be regulated profoundly by states on territorial basis. The idea of digital sovereignty would disconnect global internet as it is now. As a result, it hardens the possibility of international actors to come into agreement to formulate effective and binding international law on cyber space. It also hardens the possibility to adjudicate cases of cyber violations to state actors since digital sovereignty is engrained with noninterference principles–it is difficult to punish and blame state actors for their conduct in arbitration as we have seen in International Criminal Court. Alternatively, if this idea of digital sovereignty would converge state actors to come into agreement to formulate international cyber law, the law itself would be presumably dominated and determined by state actors interests with their contesting ideas of digital sovereignty at the expense of non-state actors such as business companies, individual citizens, and civil societies.

1.6 CONCLUDING REMARK

The question of does international law apply to states' conduct on cyber space as discussed above denotes that the answer is not effectively. It is derived from the past and current challenges on three aspects of international law: jurisdiction, arbitration, and legal instruments & jurisprudence. In the future, the trend on increasingly promoted digital sovereignty norms potentially drive future international law on cyber space to be hardly effectively imposed on state actors. If, any, the future international law on cyber space would be nuanced by digital sovereignty at the expense of their non-state actors interests. Both scenarios show that international law on cyber space is hardly effective for state actors and need broader calls for formulating rule-based, freedom-based, and inclusive global internet norms in the future.

1.7 LET'S SUM UP

In this chapter, we understood the binding and well-adjudicated international law on cyberspace, which does not effectively apply to states given challenges taken place in public international law related to jurisdiction, arbitration, and legal instruments & jurisprudences.

1.8 FURTHER READING

- Dworkin, Anthony. 2015. "Surveillance, Privacy, and Security: Europe's Confused Response to Snowden",ECFR Policy Memo. Franklin, M.I. 2010.
- "Digital Dilemmas: Transnational Politics in the Twenty-First Century",The Brown Journal of World Affairs, 16(2): 67-85. Gueham, Farid. 2017.
- Digital Sovereignty – Steps Towards a New System of Internet Governance. Paris: Fondapol. Jakarta Globe. 2019.
- Cybersecurity Bill Postponed Until Houses Next Term. https://jakartaglobe.id/context/cybersecurity-bill-postponed-until-houses-next-term/ ICLG. 2019.

- Cybersecurity Laws and Regulations: Malaysia. https://iclg.com/practice-areas/cybersecurity-laws-andregulations/malaysia Kittichaisaree, Kriangsak. 2017.
- Public International Law of Cyberspace. New York: Springer. Lewis, James A. 2010.
- “Sovereignty and the Role of Government in Cyberspace”, Brown Journal of World Affairs, 16(2): 55-65. Liaropoulos, Andrew. 2017.
- “Cyberspace Governance and State Sovereignty”, in Democracy and an OpenEconomy World Order, ed. George Bitros & Nicholas Kyriazis. Cham: Springer.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are major challenges on formulating international law on cyberspace?**

There are three major challenges on formulating international law on cyberspace are related to the core of principles and characteristics of international public law: jurisdiction, arbitration, and legal Instruments & jurisprudences.

1.10 ACTIVITY

Explain the legal framework of cyberspace under international law along with its jurisprudential perspective. (Word count 2000 to 2500)

Unit 2: THE CUSTOMARY INTERNATIONAL LAW OF CYBERSPACE

2

Unit Structure

2.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- Historical background of customary practice and how it has affected the cyberspace regulation.
- The international norms which governs cyber laws in various jurisdictions.

2.2 INTRODUCTION

International law's applicability to cyberspace and cyber activities has been a source of debate. The highly contested topic was whether cyberspace provides a new "Wild West" in which current international law standards, if not international law itself, would be inapplicable and therefore would not govern actions taking place in this "space." Both scholarly research and state practice have agreed that international law extends to cyberspace and cyber operations. This was acknowledged in the UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) reports in 2013 and 2015, and several States confirmed this position in their comments to the UN Secretary-General and in their national cyber defense and cybe security plans. As a result, the focus shifted to deciding how international law principles could be interpreted and applied to cyberspace and cyber operations. This does not, however, imply that applying international law norms is straightforward. On the opposite, there are significant concerns over how to perceive and enforce a number of standards. In this regard, there are two key challenges: on the one hand, due to the special characteristics of cyberspace, interpreting the application of international law to cyber operations may necessitate any adaptation. In the other hand, international law topics, especially States, may have differing, if not divergent, views of basic international law norms.

The first thing to understand about international law is that it bears just a passing similarity to the law that most people are familiar with. In most nations, domestic laws are enacted by a sovereign body (such as Congress) after careful thought. Statutes are meticulously designed to ensure that the legislation has a specific effect. This is not the case for international law. Treaties are not the principal means of defining international law, contrary to common opinion. International law is a jumble of historical experience and history, as well as negotiated treaties between countries. Under this patchwork of rules, customary international law—rather than laws or conventions—takes precedence in emerging areas of the law.

When states adopt their general and compatible practices out of a sense of moral responsibility, customary international law evolves. When this happens, nation-states deem customary law to be legally binding. Nations can take measures they consider necessary in situations where there is no existing consensus on what constitutes lawful conduct. The Lotus philosophy, so named after the International Court of Justice decision in which it was created, is based on this. Just a few acts are called peremptory conventions of international law, meaning they are generally considered to be wrong and illegal. Piracy, child trafficking, and hijacking are examples of exemplary regions. The international legal system's very existence is one of the reasons there are so few widely recognized standards.

It is determined by what nations do and feel they are obligated to do, which makes reaching a consensus impossible. Except in seemingly simple situations like torture, there is no rule without agreement. Many states regard “torture or unfair, inhuman, or degrading treatment or punishment” as a violation of human rights norms that have become customary international law. Nonetheless, acts resembling torture occur, and states that support them are rarely condemned, so it is impossible to claim that there is full international consensus on the subject.Although the few prohibitions accepted as peremptory norms do not apply to war, this does not mean that armed conflict is unregulated.

There is a body of customary law reflecting the extensive and virtually uniform conduct of nation-states during traditional warfare that is widely accepted and well understood—the law of war. Unfortunately, the application of the law of war to cyberspace is problematic because the actions and effects available to nations and non-state actors in cyberspace do not necessarily match up neatly with the principles governing armed conflict. Cyberspace gives nation-states new options, enabling them to take non-kinetic actions that may not have been available previously. Actions that may have required the use of military force in previous conflicts now can be done with cyber techniques without the use of force. States can also take actions in cyberspace that would be consistent with the use of armed force but more easily avoid taking responsibility for the actions—they can take cyber action “without attribution.” In the absence of a specific legal regime for cyberspace, the logical approach is to take what guidance exists to govern more conventional warfare and determine whether it can be applied to cyberspace activities. The subsequent brief discussion is a general examination of how national practices become customs binding on the body of nations as customary international law. Following the general discussion is a more detailed discussion of how customary international law might apply to nation-state cyber actions.

Countries' diplomatic affairs are gradually taking place in cyberspace. State and non-state players established policies and moral conceptions that may be considered international customary law in statu nascendi, ranging from questions regarding data protection and Internet monitoring to privacy and malicious expression. The aim of this contribution is to raise evidence in favour of the idea that international law analysis should be expanded to cover cyberspace. Due to the absence of treaty law in this field, one must turn to a secondary source of international law, namely tradition, as noted by one eminent researcher: 'customary law still regulates various branches of international law, and, more importantly, new rules of that law are emerging.'

2.3 DEVELOPMENT OF LAW THROUGH CUSTOM OF CYBER

The increasing use of computers and computer networks through the 1970s and 1980s was followed swiftly by the rise of the "network of networks" known as the Internet in the mid-1990s. Ultimately, the Internet spawned an entirely new domain of operations referred to as cyberspace. It is in and through this virtual space that cyber activities occur. So, not only are the activities in cyber new, where cyber actions take place is a unique location. Because it has existed for such a short time, there is not a robust body of law governing state conduct in cyberspace. There are documented instances of state cyber practice, however, and these have begun to lay a pattern for establishing customary cyber law.

As noted above, customary law does not instantly appear but is developed through state practice and rationale. The cyber practices of states and the thought behind those actions over the past 30 years must be examined to determine if there is customary law in cyberspace. If no principles have developed, as earlier discussed, cyberspace remains unconstrained under the default customary international regime. Although opinio juris is a critical element, it is easiest to analyze the development of custom beginning with an examination of state action, which is more visible and easily documented than motivation. Complicating the analysis is the secrecy surrounding most cyber operations. The US Department of Defense (DoD), for example, claims it suffers millions of scans and thousands of probes into its networks each day. With rare exceptions, no states or individuals come forward to take credit for these actions, so assessing the motivation of these unknown cyber actors is difficult. Albeit complicated and difficult, a few examples of state practice in cyber are available for examination.

Arguably, the first cyber attack occurred in the Soviet Union. In 1982, a trans-Siberian pipeline exploded. The explosion was recorded by US satellites, and it was referred to by one US official as “the most monumental nonnuclear explosion and fire ever seen from space.”It has been reported the explosion was caused by computer malware the Central Intelligence Agency implanted in Canadian software, apparently knowing the software would be illegally acquired by Soviet agents. Because the explosion happened in remote Siberia, it resulted in no casualties. It also embarrassed the Russian Committee for State Security (the KGB), who thought they had stolen the most recent software technology from the United States. As a result, the facts behind the explosion were concealed, and the USSR never publicly accused the United States of causing the incident.

Multiple “soft” computer attacks occurred against US systems as the Internet grew exponentially over the next 25 years. Many of these involved attempts to copy sensitive information or relatively simple but potentially devastating denial of service attacks.22 Some of the more infamous include Moonlight Maze (1998–2001), which probed government and academic computer systems in the United States; Code Red (2001), which launched a worm intended to conduct a denial of service attack against White House computers; and Mountain View (2001), a number of intrusions into US municipal computer systems to collect information on utilities, government offices, and emergency systems.

Although there was speculation about the origins, none of these incidents could be definitively attributed to a state actor. In contrast to the, until recently, little-known Siberian incident, it was a very public series of cyber events considered by many to have heralded the advent of cyber warfare. In April 2007, following the removal of a Russian statue in Estonia's capital of Tallinn, a widespread denial of service attack affected its websites. As a result Estonia, one of the world's most wired countries, was forced to cut off international Internet access. Russia denied involvement in the incident, but experts speculate the Russian Federal Security Service (FSB) was behind the distributed denial of service event.

The following year, Russian troops invaded the Republic of Georgia during a dispute over territory in South Ossetia. In August 2008, prior to Russian forces crossing the border, Georgian government websites were subjected to denial of service attacks and defacement. While there is widespread belief the incident was "coordinated and instructed" by elements of the Russian government, no one has been able to attribute these actions definitively to Russia.

The wakeup call for the US military occurred in 2008, although the details did not become public until two years later. Operation Buckshot Yankee was the DoD's response to a computer worm known as "agent.btz" infiltrating the US military's classified computer networks. The worm was placed on a flash drive by a foreign intelligence agency, from where it ultimately made its way to a classified network. The purpose of the malware was to transfer sensitive US defense information to foreign computer servers. In what qualifies as bureaucratic lightning speed, US Cyber Command was established less than two years later, with a mission to, among other things, direct the operations and defense of DoD computer networks.

In addition to unmasking the extent of network vulnerabilities, the event highlighted the lack of clarity in international law as it relates to cyber events. Two recent incidents merit attention before discussing the law in depth. In 2010, Google reported Chinese hackers had infiltrated its systems and stolen intellectual property. Through its investigation, Google learned the exfiltration of its information was not the only nefarious activity; at least 20 other companies had been targeted by Chinese hackers as well. These companies covered a wide range of Google users, including the computer, finance, media, and chemical sectors. The Chinese had also attempted to hack into G-mail accounts of human rights activists and were successful in accessing some accounts through malware and phishing scams. Google released a statement explaining what it discovered through its investigation and what steps it was taking in response to China's action, including limiting its business in and with China.

Also in 2010, a computer worm named Stuxnet was detected on computer systems worldwide. Stuxnet resided on and replicated from computers using Microsoft's Windows operating system but targeted a supervisory control and data acquisition (SCADA) system manufactured by Siemens. Cyber experts determined the worm was designed to affect the automated processes of industrial control systems and speculated that either Iran's Bushehr nuclear power plant or its uranium enrichment facility at Natanz was the intended target. After Stuxnet became public, Iran issued a statement that the delay in the Bushehr plant becoming operational was based on "technical reasons" but did not indicate it was because of Stuxnet. The deputy director of the Atomic Energy Organization of Iran stated, "Most of the claims made by [foreign] media outlets about Stuxnet are efforts meant to cause concern among Iranians and people of the region and delay the launch of the Bushehr nuclear power plant."32 Iranian president Ahmadinejad stated at a news conference that malicious software code damaged the centrifuge facilities, although he did not specifically state it was Stuxnet or the Natanz facility.

2.4 LET'S SUM UP

In this chapter, we have learned the formal international agreements, cyber custom which is beginning to develop through the practice of states. Besides, we have also learned the serious actions against major financial institutions.

2.5 FURTHER READING

- "The analysis of the practice of states before the conclusion of the 1967 Outer Space Treaty shows that historically, custom was the first source of the international law of outer space." Vladelen S. Vereshchetin and Gennady M.

Danilenko, “Custom as a Source of International Law of Outer Space,” Journal of Space Law 13, no. 1 (1985): 22, 25.

- Malanczuk, Akehurst’s Modern Introduction to International Law, 43, n. 10. See I. C. MacGibbon, “The Scope of Acquiescence in International Law,” 1954 British Yearbook of International Law, 143, 145–46; and MacGibbon, “Customary International Law and Acquiescence,” 1957 British Yearbook of International Law, 115, 138.
- Harry Newton, Newton’s Telecom Dictionary, 23rd ed. (New York: Flatiron Publishing, 2007), 502–3.

2.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the difficulty in application of customary cyber laws?**

There is a body of customary law reflecting the extensive and virtually uniform conduct of nation-states during traditional warfare that is widely accepted and well understood—the law of war. Unfortunately, the application of the law of war to cyberspace is problematic because the actions and effects available to nations and non-state actors in cyberspace do not necessarily match up neatly with the principles governing armed conflict.

2.7 ACTIVITY

Explain the detailed account of rise of customary practice in the sphere of cyberspace. (Word count 2000 to 2500)

3

Unit 3:CYBERWARFARE AND INTERNATIONAL LAW

Unit Structure

3.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- Historical background of cyberwarfareand its treatment in international law.
- The international norms and United Nations strategy on cyberspace.
- Various governing treaties on cyber-attack across the globe.

3.2INTRODUCTION

Cyber warfare is a hot topic for politicians and military officials all over the world. At all levels of government, including the armed forces, new divisions to ensure cyber security are being established. However, in armed conflict environments, cyber operations may have very significant implications, particularly if their impact is not limited to the data of the targeted information system or computer. Indeed, cyber operations are often meant to have a real-world effect. Manipulation of an enemy's air traffic control controls, oil pipeline flow systems, or nuclear reactors, for example, can be accomplished by tampering with supporting computer systems.Any cyber operations have the potential to have a huge humanitarian effect on civilians. Since one of the key purposes of this body of law is to shield civilians from the consequences of conflict, it is critical to address the principles of international humanitarian law (IHL) that regulate those operations. This essay aims to answer some of the issues that emerge when applying IHL to cyber security. IHL is a body of legislation that was drafted with conventional kinetic warfare in mind. Policymakers and military officials all over the world are concerned about cyber security.The United Nations Institute for Disarmament Research (UNIDIR) recently released a report that explains the actions taken by thirty-three states that have directly used electronic warfare in their military strategy and organization, as well as an analysis of thirty-six other states' cyber defense approaches.

For the purposes of this discussion, “cyberwarfare” refers to warfare carried out in cyberspace using cyber means and methods. Where “warfare” is widely interpreted to refer to the use of military force in times of armed conflict, “cyberspace” can be described as a globally integrated network of digital information and communications infrastructures, which includes the Internet, telephone networks, computer systems, and the data they contain. Infecting a belligerent adversary's data network with a malicious virus, for example, would be called cyberwarfare, but aerial bombing of a strategic cyber command would not.The fact that cyberwarfare is performed in cyberspace does not rule out the likelihood of physical or other non-electronic consequences happening outside the cyber realm, and the perpetrator may also wish for this to happen. Persons whose lives, or artifacts whose operation is dependent on computer networks, such as certain power stations, modes of transportation, or people attached to different types of medical, military, or technical life-support systems, are examples of cyberwarfare goals.

3.3 HOW IS CYBERWARFARE UNIQUE?

When defining and adapting current international law to cyberwarfare, the unique features of cyberspace must be taken into account. Most importantly, cyberspace is the only fully man-made domain. It is jointly developed, maintained, managed, and run by public and private partners all over the world, and it is continuously changing in response to technical advancement. Since cyberspace has no geopolitical or natural borders, information and electronic payloads can be transmitted from any point of origin to any point of destination through the electromagnetic spectrum.These are transported in the form of numerous digitalized fragments through volatile routes before being reassembled at their destination. Although states, non-state organisations, private businesses, and individuals all have access to cyberspace, IP spoofing and botnets, for example, make it possible to hide the root of an activity, making accurate detection and attribution of cyber attacks especially difficult.

3.4 CYBER WARFARE AND INTERNATIONAL HUMANITARIAN LAW

There is no unanimously agreed definition of cyber warfare, however there are a few authoritative drafts. The Tallinn Manual 2.0 distinguishes between (a) the means, and (b) the methods of cyber warfare as being: a) cyber weapons and their associated cyber systems; b) cyber tactics, techniques, and procedures by which hostilities are conducted (Tallinn Manual, p. 452). This definition notes that the ‘means of cyber warfare’ include cyber weapons and cyber weapon systems. In this context, a weapon is the part of the system which causes damage or injury. This broad definition allows for cyber warfare to encompass cyber devices, equipment, or software used, designed, or intended to be used to conduct a cyber attack. Subsequently, it defines cyber weapons as "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack" (ibid). It states that this definition is applicable to International Armed Conflicts and Non-International Armed Conflicts.

Academics such as Rid and McBurney define cyber weapons as a "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things" (Ridd, Cyber Weapons p. 7). A third definition is provided by the US Air Force which interprets weapons as "devices designed to kill, injure, disable or temporarily incapacitate people, or destroy, damage or temporarily incapacitate property or material" (US Air Force Instructions, Legal Review of Weapons and Cyber Capabilities, p. 6). All three definitions have one primary aspect in common: they all agree that cyber weapons are the tools of harm. Consequently, there are a few things which can be deduced about cyber warfare from the above definitions. Firstly, a vast multitude of cyber weapons exists ranging from highly advanced to much more basic. Gone are the days when the worst thing on the Internet to be afraid of was a pesky virus. The current highly sophisticated malware looks for software vulnerabilities which can result in fatal damage to the opponent's entire computer network. The most advanced cyber weapons are capable of entering networks which are off the grid, causing total damage. Such stateof- the-art weapons are expensive to make as there are not many individuals capable of writing them to such a high standard. On the other hand, a basic cyber weapon is easier to detect as it focuses on denying service to an opponent's computer rather than targeting the computer directly. Such an attack was conducted by a pro-Kremlin youth group against Estonia in 2007. Secondly, cyber weapons result in different effects. The initial stage affects the targeted computer networks. This results in destruction of the system and impacts persons by for example cutting power to a power plant or locking exit doors. The main difference between cyber weapons and traditional weapons is the sequence of events:

traditional weapons usually cause immediate damage to people, whereas cyber warfare affects people at a later stage.

Indiscriminate cyber weapons

Having provided an explanation of cyber weapons above, it is important to determine whether a weapon is inherently indiscriminate as per the review of a weapon under international humanitarian law (IHL). Indiscriminate cyber weapons are defined as being: a) directed at a specific military objective, or b) limited in the effects as required by law of armed conflict. Consequently, they strike military objectives and civilians or civilian objectives without distinction (Tallinn Manual, p. 455). Criterion (a) highlights the primary principle of IHL to respect the delicate balance between humanitarian considerations and military necessity. IHL focuses on protecting civilians from attacks. Therefore, the weapons need to be as accurate as possible to limit the risk of harm. From what can be gathered, powerful States are meeting or have met the requirement in (a) in terms of their cyber warfare. As technology advances, an increasing number of States will be able to fully fulfil this requirement. On the contrary, criterion (b) involves effects that are not limited. As per the Manual, here is a sequence of events which breach (b) as the effects cannot be limited: 1. A State uses malware against another State in an armed conflict; 2. The malware is targeting military computer networks; 3. Even though the intended target is military, the malware will unavoidably spread into the civilian networks (Cyber Weapons Reviews under International Humanitarian Law 'Tallinn Paper no 11', p. 19). The above scenario demonstrates the unintentional simplicity in breaching (b). Therefore, there are two subparts to (b) to make it fit in the IHL framework. Firstly, the effects need to be harmful and cause injury to persons or damage to property. Secondly, the indiscriminate effects must be foreseeable.

IHL will only be applicable to a cyber warfare occurrence if the attack occurs during or triggers an armed conflict. It is questionable whether a cyber attack can constitute the 'use of force' or an 'armed attack' in order for IHL to apply. Furthermore, attributing the attack to a State or an armed group poses questions which take time to be answered, whilst on the other hand IHL cannot wait until it is determined whether the cyber attack qualifies as such or not. There is a need for more adherent rules which encompass non-physical armed attacks to reflect the changing weaponry of the 21st century. The Tallinn Manual makes useful suggestions, but still has a long way to go to place cyber warfare in the IHL framework.[76]

3.5 CYBER OPERATIONS, ATTACKS, EXPLOITATION AND DEFENCE

The reduction of information to electronic format and the subsequent transfer of that information between physical elements of cyber infrastructure is referred to as “cyber activity” or “computer network operation” (CNO). “Computer network attack,” “computer network exploitation,” and “computer network defense” are the three types of cyber operations.Computer network attacks (CNA) refer to any cyber operations aimed at “disrupting, denying, degrading, or destroying information resident in computers and computer networks, or the computers and networks themselves,” while computer network exploitation (CNE) refers to “enabling operations and intelligence gathering to gather data from target or adversary automated information systems or networks.” Computer network defence CND, on the other hand, refers to “measures taken to secure, track, analyze, identify, and respond to unauthorized activity within... information systems and computer networks,” or, in other words, the prevention of CNA and CNE using surveillance, counterintelligence, law enforcement, and military resources. This vocabulary, which is unique to cyberspace activities, must be distinguished from other technical words used in international law, such as “force,” “armed attack,” and “attack.”

3.6 CYBER OPERATIONS AND JUS AD BELLUM

The jus ad bellum is the body of law governing the use of force by states in international relations. The UN Charter is the most important source of jus ad bellum today. Such facets of the rule, such as the particular modalities regulating the use of force in self-defense, are not covered by the UN Charter and must be drawn from customary law as expressed in state procedure and opinio juris, as well as defined in international jurisprudence.In this case, it would be appropriate to determine if cyber operations constitute (1) a globally wrongful threat or usage of “force,” (2) a “armed assault” justifying the use of necessary and proportionate force

[76] https://leidenlawblog.nl/articles/cyber-warfare-the-definition-challenge

in self-defense, or (3) a “threat to the peace,” “breach of the peace,” or “act of aggression” requiring UN Security Council action.

In fact, the first issue is important because state-sponsored cyber operations that count as a use of “force” against another state would not only violate the UN Charter's general prohibition of “force,” but would also likely lead to a foreign military conflict. In the other hand, cyber operations below the threshold of “force,” even if otherwise forbidden under the customary principle of non-intervention, can constitute lawful counter-measures in response to foreign wrongful actions that do not meet the threshold of “armed attack” by another state.The second issue is important because the existence of cyber operations that constitute a “armed assault” allows the targeted state to exercise its inherent right to self-defense by means that are otherwise forbidden by the Charter, such as the use of force.

Finally, assessing that cyber operations are a “danger to the peace,” “breach of the peace,” or “act of aggression” requires the UN Security Council to take punitive action, including military force, to preserve or restore internal peace and security, regardless of whether the cyber operations in question are categorized as “force” or “aggression.”

3.7 CYBER OPERATIONS AND THE PROHIBITION OF INTERSTATE FORCE

Cyber Operations as “Force”

“All Members [of the United Nations] shall refrain in their foreign affairs from the threat or use of force against the territorial integrity or political freedom of any entity, or in any other manner inconsistent with the United Nations Purposes,” according to article 2(4) of the UN Charter. As a result, the issue of whether cyber operations count as “force” under the scope of this prohibition emerges.

In the absence of a treaty formulation, the principle of “power” must be understood in good conscience in terms of the Charter's object and intention and the ordinary interpretation to be assigned to the word in its sense. Despite the fact that the ordinary sense of “force” is obviously broad enough to encompass both armed and unarmed means of coercion,18 the vast majority of observers today regard the word “force” in UN Charter article 2(4) as literally interchangeable with “armed” or “military” force. This does not imply that the ban against the use of kinetic, toxic, biochemical, or nuclear weapons is exclusive to such weapons.The ban extends “to all use of force, regardless of the weapons used,” according to the International Court of Justice.

Indeed, once the results of cyber operations are equal to those likely to arise from kinetic, toxic, biochemical, or nuclear weaponry, they come under the prohibition of article 2(4) of the UN Charter. This will undoubtedly entail the use of cyber operations as an offensive or defensive weapon to inflict death or injuries to people, as well as the destruction of artifacts and facilities, whether the destruction be caused by physical damage, technical harm, or a combination of the two.

Cyber operations manipulating target computers systems to trigger a meltdown in a nuclear power plant, or opening the floodgates of a dam over a densely populated area, or disabling a busy airport's air traffic control during bad weather conditions, are both obvious examples of a use of “force” within the meaning of article 2(4) of the UN Charter. The main issue is determining whether cyber operations that do not, or do not explicitly, cause death, damage, or destruction qualify as a use of “force.”The UN Charter's preparatory works explicitly demonstrate that the prohibition of “power” did not apply to economic exploitation or political pressures. Furthermore, article 41 of the UN Charter defines “interruption of... communication” as a “measure not requiring military force,” implying that any denial of service attacks (DOS) will be exempt from article 2's prohibition (4). This does not, however, imply that all cyber activities fall short of military force in the absence of violent consequences.

Although one early commentator suggested a complicated set of indicative criteria for distinguishing between military force and economic or political exploitation in the cyber domain, others have recently pointed out qualitative, quantitative, and temporal flaws in these criteria, highlighting rather than removing the ongoing lack of clarification in this region.From a teleological standpoint, it is arguable that the Charter can only achieve its overarching goals of maintaining international peace and security (article 1) and “saving succeeding generations from the scourges of war” (preamble) if it prohibits the use of any forcible measure likely to provoke military counter-force and, ultimately, the outbreak of international armed conflict.

The Charter cannot, by logic, authorize the ban of interstate force to be circumvented by the use of nonviolent means and approaches that are, for all intents and purposes, equal to a violation of the peace between the parties. Consider the debilitating impact of cyber operations causing the failure of large cities' electrical power supplies, the incapacitation of networks regulating factory activity, or the penetration of malware intended to “blind” a whole air defense infrastructure. In this sense, it's worth noting that UN Charter article 2(4) forbids the use of force between states, regardless of its extent or size.Also small acts of interstate force, as the International Court of Justice (ICJ) explained in the Nicaragua Case, come under the general prohibition of article 2(4) of the UN Charter, regardless of whether they count as acts of “aggression” or “violent assaults,” allowing the threatened state to use force in self-defense. This view is supported by the position taken in International Humanitarian Law, which holds that even small acts of military action between states are necessary to initiate an international armed conflict.Indeed, it would be illogical for article 2(4) of the UN Charter, as the primary standard aimed at ensuring international peace and stability, not to routinely ban all kinds of interstate behavior necessary to trigger an international military conflict within the scope of article 2 of the Geneva Conventions, as the primary norm aimed at ensuring international peace and security. In fact, the UN Charter goes even further, prohibiting not just the direct use of force in interstate affairs, but also the threat of force.

3.8 LET’S SUM UP

In this chapter, we have learned the formal international agreements, cyberwar fare and its essentials. Additionally, we have also learned how UN has tried to formulate the strategies to curb cybercrime.

3.9 FURTHER READING

- For the ICRC’s position on this issue see Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under IHL, ICRC, 2009, § II.

See also Prosecutor v. Martić, judgement of 8 October 2008, ICTY, §§ 300–302.

- Jean-Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law, vol. I, 2005, p. 19.
- Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under IHL, ICRC, 2009, p. 22.
- Marco Roscini, "World Wide Warfare—Jus ad bellum and the Use of Cyber Force", in Armin Bogdany and Rüdiger Wolfrum (eds.), Max Planck Yearbook of United Nations Law, vol. 14, 2010, p. 96.
- Michael Schmitt, "Cyber Operations and the Jus in Bello: Key Issues", Naval War College International Law Studies, 2011, p. 8; Michael Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello", International Review of the Red Cross, vol. 84, no. 846, 2002, p. 381.

3.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber operation?**

The reduction of information to electronic format and the subsequent transfer of that information between physical elements of cyber infrastructure is referred to as "cyber activity" or "computer network operation" (CNO). "Computer network attack," "computer network exploitation," and "computer network defense" are the three types of cyber operations.

3.11 ACTIVITY

Explain the detailed account on UN strategies and related provisions on cyber-attack and security. (Word count 2000 to 2500)

4

Unit 4: INTERNATIONAL COURTS FOR CYBERSPACE

4.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- Various international courts handling the matters related to cybercrime and related matters.
- Provisions governing the jurisdictions of these courts.
- Role of judges in these courts.

4.2 EXISTING INTERNATIONAL COURTS

4.2.1 The International Court of Justice

The Court was established in the early 1900s, based on the 1899 and 1907 Hague Peace Conventions. In 1913, it was renamed the Permanent Court of Arbitration and relocated to The Hague's Peace Palace, which was funded by Andrew Carnegie's contributions. The Permanent Court of International Justice was created by the League of Nations after World War I, but it was never a member of the League. The Court ceased to exist after World War II broke out, but convened for the last time in October 1945. The International Court of Justice was created by the United Nations Charter, which stipulates that all UN members be parties to the Courts Statute.The Court, which began operations in 1946, is the United Nations' primary judiciary body. The International Court of Justice serves as a global tribunal. The Court is made up of 15 judges who are chosen for a nine-year term by the United Nations General Assembly and the Security Council, who sit separately. No country may have more than one judge, and one-third of the judges are elected every three years. A State party to the case can select an ad hoc judge for the case's purposes.The Court's authority is as follows: The Court resolves legal cases that are referred to it by consensus with the parties to the lawsuit, in compliance with international law. Only the United Nations' organs and 16 specialist organizations with the authority to make such a request will request advisory opinions on legal issues from the Court. If there are any questions regarding the authority, the Court will rule. The decisions are final and irreversible.

4.2.2 The International Criminal Court

The promise of universal justice lies in the prospect of an international criminal court. 1 Many serious cyberattacks will go unpunished without an international court or tribunal to deal with the most serious cybercrimes of global concern. The most extreme global cyberattacks of the last year have shown that virtually no one has been investigated, convicted, or punished for their actions. Such crimes must be covered by a worldwide convention or series of treaties, and they must be investigated and tried by an international criminal court or tribunal.After ground, sea, air, and outer space, cyberspace is the fifth shared space in need of international collaboration, cooperation, and legal steps. The international community must be made aware of the need for a global solution to the immediate and growing cyberthreats. International law shall protect peace, justice, and stability in cyberspace by a treaty or series of treaties under the United Nations. The rapid evolution of global cyberattacks, such as large and orchestrated attacks against sovereign states' sensitive intelligence infrastructures, necessitates an immediate response in the form of a global treaty.

The United Nations has launched a thorough investigation into the issue of cybercrime. The 12th United Nations Congress on Criminal Prevention and Criminal Justice, held in Salvador, Brazil in April 2010, requested that the UN Commission on Crime Prevention and Criminal Justice convene an open-ended intergovernmental advisory committee to conduct a thorough report on the issue of cybercrime and its solution in Article 42 of the Salvador Declaration. The Commission and the United Nations General Assembly both approved the recommendation in resolution 65/230.The aim of this systematic report is to look at the issues “in order to explore options for strengthening existing and proposing new national and international legal or other solutions to cybercrime.”

The Court was founded in 1998 at a conference in Rome by 120 countries. The International Criminal Court's Rome Statute was introduced and went into effect on July 1, 2002. 111 countries have ratified or acceded to the Rome Statute. While the Court is not affiliated with the United Nations, it has historical, legal, and organizational links to the organization. The Rome Statute and other contract arrangements control the relationship. The International Criminal Court (ICC) is the world's first permanent, treaty-based, entirely autonomous international criminal court, established to promote the rule of law and ensuring that the world's worst criminals are not forgotten.The Court's authority is just a supplement to national criminal authorities, not a replacement for them. If a State party to the Rome Statute refuses or is reluctant to sue, it may investigate and prosecute. Anyone who violates any of the Statute's provisions will face legal action by the Court. The International Criminal Court's authority is limited to States that become Parties to the Rome Statute, but certain States are expected to completely participate in the investigation and trial. Article 5 restricts the scope of the court's jurisdiction to the most serious offences that affect the international community as a whole. The article explains the jurisdiction, which includes genocide, crimes against humanity, war crimes, and violence. Individual states may refuse to are unable to exercise authority in a particular case.

According to article 17, a State is unable to report or prosecute a crime if there seems to be a real lack of will to do so. When a state's justice system tends to be in complete or significant failure, or when it is unable to procure the accused or the requisite proof and witnesses for any reason, or when it is otherwise unable to carry out its prosecutions due to its unavailability, the state is unable. Other extreme crimes, such as terrorist attacks, were debated at the final diplomatic conference in Rome, but the conference regretted that no universally accepted concept could be reached.Terrorism attacks are serious offences that concern the international community, and the conference agreed that a study conference convened under Article 123 of the Statute of the International Criminal Court deem them for inclusion in the list of offenses subject to the Court's jurisdiction. In 2010, the Court was summoned in five instances. Uganda, the Democratic Republic of Congo, the Central African Republic, Sudan's Darfur, and Kenya are all affected. Furthermore, the lawyer is pursuing preliminary inquiries in a variety of other countries around the world.

Also in the new authority, the International Criminal Court may have a part to play in the war against terrorism. The Court can, upon request, “cooperate with and provide assistance to, a State Party undertaking an investigation into or prosecution in respect of conduct that constitutes a crime under the jurisdiction of the Court, or that constitutes a serious crime under the national law of the requesting State.”

Terrorism is unquestionably a “violent crime.” Massive and organized cyber attacks on information infrastructures can still be deemed a “violent crime,” even though they aren't considered terrorism.The Kampala Review Conference took place from May 31 to June 11, 2010. The Conference drew about 4600 delegates from states, intergovernmental bodies, and non-governmental organizations. The International Criminal Court was now fully functioning as a legal organ, and the Meeting was formally opened by the Secretary-General of the United Nations. The Rome Statute was amended, with the addition of a description of the crime of violence. The Kampala Declaration was also adopted, with section 12 reading, “Decide to observe 17 July, the day of the adoption of the Rome Statute in 1998, as the Day of International Criminal Justice from now on.”

- ***The rule of law on the most serious crimes in cyberspace***

The institutional convergence of procedural and court cases on terrorism and other serious offences in cyberspace may be strengthened by a binding global legislative instrument like the International Criminal Court's Rome Statute. The Rome Statute may provide a global judicial system to ensure that certain actions are not excluded from effective sanctions. If criminal actions or terrorist use of the Internet, as well as huge and coordinated multinational activities in cyberspace, the Rome Statute has Articles on investigation, indictment, and three branches of Courts for regular and structured prosecutions.However, the Prosecutor, as an impartial arm of the Court, can, after evaluating the evidence provided, launch an investigation on a case-by-case basis. (Articles 18 and 53) Under Article 18 on provisional decisions on admissibility, the Prosecutor can “seek permission from the Pre-Trial Chamber to take appropriate investigative action for the purpose of maintaining evidence where there is a one-of-a-kind opportunity to acquire critical evidence or where there is a serious risk that such evidence will not be available later.”Such a unique procedure could be used in the investigation of terrorist threats and large-scale, coordinated cyberattacks. That is also the Pre-Trial Chamber that issues an arrest warrant later on. The Court can exercise its duties and powers on the territories of all States Parties to the Rome Statute, with a maximum penalty of 30 years in prison and the possibility of a life sentence.

4.2.3 The International Criminal Tribunal for the former Yugoslavia (ICTY)

The Tribunal is a United Nations court of law, established under the United Nations Charter's Chapter VII. On May 25, 1993, the Security Council passed Resolution 827, which created the Tribunal.The Tribunal's mandate is to try crimes committed in the former Yugoslavia since 1991, and it has jurisdiction over the following issues:

- Grave violations of the 1949 Geneva Conventions
- War crimes
- Genocide
- Crimes against humanity

In contrast to national courts, the Tribunal has concurrent power, but it has the authority to assume primacy and take over inquiries and prosecutions at any time. The Chambers are made up of 16 permanent judges and up to nine ad hoc judges, all of whom are appointed by the UN General Assembly. Three Trial Chambers and one Appeals Chamber include the judges. The judges are chosen for a four-year term.

The courts have guaranteed a fair and open hearing by weighing the facts in order to assess the accused's guilt or innocence. The Tribunal has demonstrated that effective and transparent international justice is possible, as well as setting significant international criminal and humanitarian law precedents. The Appeal Chamber is made up of seven permanent judges, five from the International Criminal Tribunal for the Former Yugoslavia and two from the International Criminal Tribunal for Rwanda (ICTR).The ICTR's Appael Chamber is made up of the same seven judges, but each appeal is heard and determined by five judges. Since the Nuremberg and Tokyo tribunals, the Tribunal becomes the first major war crimes tribunal.

In the disputes, the Tribunal has prosecuted and filed complaints against people of all ethnic backgrounds. The Prosecutor's Office is independent of the Security Council, every State or foreign body, and the ICTY's other organs. On the basis of evidence obtained, the Prosecutor initiates investigations at his or her discretion. Before an indictment may take effect, it must be approved by a magistrate. The convicted are being detained in The Hague's ICTY Detention Unit.The maximum sentence that may be imposed is life imprisonment. Sentences are carried out in one of the countries that has concluded a deal with the UN. The judges also have regulatory responsibilities, such as drafting and adopting legislative documents that govern the Tribunal's operations.

4.3 THE ROLE OF JUDGES IN INTERNATIONAL COURTS

The role of judges in upholding the rule of law and human rights in cyberspace must be driven by the fundamental principles for judges outlined in the Consultative Council of European Judges' (CCJE) Magna Carta of Judges, which was adopted on November 17, 2010. The basic principles relating to judges and the legal system are contained in this Magna Carta of Judges, which is strongly recommended as global principles incorporated in a global Treaty.In a national and international context, these fundamental principles include criteria for the rule of law, judicial independence, access to justice, and ethical and responsibility principles. According to section 23 of the Magna Carta, these rules extend mutatis mutandis to judges of both European and foreign courts.The following is the description of the rule of law and justice in section 1:

Any democratic state's judiciary is one of the three branches of government. Its mission is to guarantee the Rule of Law's very survival and, as a result, the law's correct enforcement in an objective, just, equitable, and effective manner. Section 2 explains the main precept of judicial independence: “Judicial independence and impartiality are basic prerequisites for the administration of justice.”

4.4 LET’S SUM UP

In this chapter, we have learned the jurisdiction and limitations of international courts in matters related to cyber security and related aspects.

4.5 FURTHER READING

- Wilson, Clay: Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for US Congress (November 2007).
- Sofaer and Goodman: Cyber Crime and Security - The Transnational Dimension of Cyber Crime and Security (2008).

- Sieber and Brunst: Cyber terrorism and Other Use of the Internet for Terrorism Purposes – Threat Analysis and Evaluation of International Conventions (2007).

4.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Explain Article 5 of ICJ.

Article 5 restricts the scope of the court's jurisdiction to the most serious offences that affect the international community as a whole. The essay explains the jurisdiction, which includes genocide, crimes against humanity, war crimes, and violence. Individual states may refuse to are unable to exercise authority in a particular case.

4.7 ACTIVITY

Provide a detailed account on role of International court of justice on cyber crimes.(Word count 2000 to 2500)

BAOU
Education
for All

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

○

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in