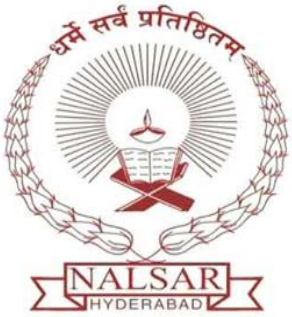


Centre for Aerospace & Defence Laws (CADL)
Directorate of Distance Education
NALSAR University of Law, Hyderabad

Course Material

ADVANCED DIPLOMA IN GIS & REMOTE SENSING LAWS

1.2.6. INFORMATION TECHNOLOGY AND CYBER LAWS

Compiled by:
Prof. (Dr.) V. Balakista Reddy

(For private circulation only)

NALSAR University of Law, Hyderabad

First Edition: 2022 (Reprint 2023)

(For private circulation only)

TABLE OF CONTENTS

MODULE I: INTRODUCTION TO INFORMATION TECHNOLOGY 5-44

1.1. Evolution of Information Technology
1.2. Development of Information Technology
1.3. Advantages of information technology
1.4. Use of Information technology in Education with an emphasis on legal education
1.5. Use of IT in Education during Covid-19 pandemic
1.6. Conclusion

MODULE-II: INTRODUCTION TO INFORMATION TECHNOLOGY LAW: INTERNATIONAL LAWS 45-80

2.1. Legal Aspects of International Information Security
2.2. Key issues and future development of International Cyber-Space Law
2.3. Cyber-Crime and Related Treaties
2.4. Is international Law of Cyber Security in Crisis?
2.5. Cyber-crime Legislation in different countries
2.6. Conclusion

MODULE-III: ROLE OF INTERNATIONAL, REGIONAL, GOVERNMENTAL BODIES AND INGOS COMBATING CYBER CRIMES 81-120

3.1.Different types of organizations
3.2. From Domestic Legislation to International Harmonization: Role of different organisations in prevention of cyber- crimes:
    i. Efforts by INTERPOL
    ii. Efforts by Regional Organisation
    iii. Multi-national Efforts
    iv. Global efforts by the United Nations
3.3. Efforts towards International harmonization
3.4. Organizations and Institutions that address International Cyber-security
    i. Global
    ii. Regional
    iii. International and inter-governmental organizations
    iv. Non-governmental organizations
    v. U.S. Federal Government organization
3.5. Cyber- security industry Associations
3.6. Conclusion

MODULE-IV: CYBER SECURITY IN NEW SPACE 121-158

4.1. Introduction
4.2. Satellite life cycle and space system architectures
4.3.Space segment architectures

4.4.Ground segment architectures
4.5.Threats to space systems and security-related incidents
4.6.Key enabling technologies in New Space
4.7.Cryptography for New Space
4.8.Open challenges for space and satellites
4.9.Conclusion

MODULE-V: INFORMATION TECHNOLOGY (IT) SPECIFIC INTERNATIONAL DISPUTE SETTLEMENT MECHANISM AND ODRs 159-200

5.1.ODR Mechanism: General Overview
5.2.International Scenario
5.3.Different Dispute Settlement Mechanisms
5.4.Indian Position: Dispute Resolution Mechanism using ODR Platforms
5.5.Dispute Resolution Mechanism under the Information Technology Act, 2000
5.6.Conclusion

MODULE- VI: INFORMATION TECHNOLOGY LAW IN INDIA 201-256

6.1.Types of Cyber-crimes
6.2.History of the formation of The Information Technology Act
6.3.Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence
6.4.UNCITRAL model and Impact of Technology Act
6.5.Information Technology Amendment Act, 2008
6.6.Concept of Cyber-security in India
6.7.Reasons for India's increasing number of cyber-crime
6.8.Cyber- crimes in India during Pandemic
6.9.Conclusion

MODULE-VII: INDIAN JUDICIARY AND IT LAW 257-302

7.1.Court's Jurisdiction in Internet Disputes
7.2.Landmark cases under Cyber Law in India
7.3.Cyber-crime related issues in India
7.4.Analysis of Indian Approach to Cyber Jurisdiction
7.5.How to improve response to the cyber-crimes by the judiciary
7.6.Conclusion and recommendations

MODULE - I

INTRODUCTION TO INFORMATION TECHNOLOGY

MODULE I: INTRODUCTION TO INFORMATION TECHNOLOGY

Introduction to Information technology: The rapid growths of information and communication technologies have given rise to the evolution of several new jargons like paperless society, electronic resources, portal / gateway and global digital library. In the day context, all types of libraries viz: academic, public and special are not only providing printed resources to their library users rather they provide printed, electronic as well as other Internet resources like e-books and databases for fulfilling the day to day academic and research requirements of the library users. The challenge, the present society faces in the 21st century is keeping pace with the rapid developments in the information and communication technology, one needs to continuously upgrade their knowledge and skills. It is understood that we live in an information rich society where the amount of information and knowledge in the present world is increasing at a tremendous pace. Information literacy is the ability to evaluate information across the range information needed, locate, synthesize and using the information effectively, using technology, communication networks and electronic resources. Information literacy includes the full range of experience, and the user needs to enable the use of information literacy.

Technology has been defined as "systematic knowledge and action, usually of industrial processes but applicable to any recurrent activity". In providing tools and techniques for action, technology at once adds to and draws from a knowledge base in which theory and practice interact and compact. At its most general level technology may be regarded as definable specifiable way of doing anything. In other words, we may say a technology is a codified, communicable procedure for solving problems. Technology, Manfred Kochen observed impacts in three stages. First, it enables us to do what we are now doing, but better, faster and cheaper; second, it enables us to do what we cannot do now; and third, it changes our life styles. Information technology is a recent and comprehensive term, which describes the whole range of processes for generation, storage, transmission, retrieval and processing of information. In this Unit, an attempt is made to discuss the components of information technology and to identify elements that really matter m the investigation and implementation of new information technologies in information systems and services.

Evolution of Information Technology: Information Technology is study of skills. Modern world is characterized by rapid growth and development of information technology (IT) resulting in more dependence of the society, in a wider sense, on the individual knowledge and competence of a person in the IT area. Although this addiction grows on day after day basis, the human right to education and information is not extended to IT area. IT has great potential to improve excellence, quality, efficiency and effectiveness. Supervision IT, human resources present a demanding task for executives. As organizations jumble up between positions involving in-house employment, to agile employment, and to outsourced support for IT, the need to efficiently obtain, supervise and raise appropriate IT human resources assumes greater significance.

The need to develop, maintain, operate, support a portfolio of information systems never disappears. The past decade has seen the regular appearance of information technology as a new computing discipline in educational institutions. In the past, the time between introducing and using new technologies was somewhat long. The introduction of new Information technologies alters the parameters of the staffing decisions constantly. Despite

economic down streams, down turns and downsizing trends, the demand for new IT professionals is expected to grow over the coming years.

The introduction of new IT in organizations makes the staffing dilemma more demanding, given the lack of acquaintance with the expertise, the education curve connected with its incorporation, the qualified scarcity of experienced human resources. With hurried development of IT and further deepening of information production, more and more enterprises have realized the tactical value of IT and made great reserves in it. However, during IT implementation procedure, decision making, conversion degree, and IT performance is often substandard to the expectation. IT has become full-fledged quickly and gratitude to a tremendously dynamic and tight-knit academic group of people, undergone an evolution unlike any other computing regulation. Information and Communication Technology including issues related to reliability, usability, performance and trust.

The Merriam-Webster Dictionary **defines information technology** as *"the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data."* Merriam-Webster states that the term was first used in 1978.The key point of information technology is that it involves the **processing of data by computers**. Therefore, the construction of computers does not fall within the definition, and the processing of Information by manual or mechanical methods, also does not count. Computers existed before 1978, but they were mainly used to perform complicated calculations. Once computers were applied to indexing and sorting written information, the term "information technology" was invented.

ICT has the potential to "connection the information gap" in terms of civilizing excellence of education, increasing the magnitude of quality educational opportunities, making knowledge building probable through borderless and unlimited accessibility to resources and people, and getting populations in inaccessible areas to satisfy their basic right to education. As various ICTs become increasingly reasonable, reachable, and interactive, their role at all levels of education is likely to be all the more significant in making didactic outcomes relevant to the labour market, in revolutionizing educational pleased and release, and in encouragement "information literacy."

IT is a rapidly evolving field, and anyone choosing a career in information technology should expect to encounter change on a regular basis. IT staff often retrain as new technology arrives and older systems are retired. A brief review of the history of IT will illustrate how much the field has changed in a relatively short period.

The History of Computers: There is much debate over what constitutes a computer. Some claim that an abacus is a computer because it uses counters to store a number, which can then be manipulated. The Jacquard loom, first demonstrated in 1801, is a contender for the title of the first computer because it took punched card patterns as an input and switched yarn according to the given instructions.

Charles Babbage's design for a difference engine, which he produced in 1822, is generally considered to be the first computer design. His analytical engine, which he began to build in 1837 is considered to be the first programmable computer – its intended use was punch cards for the input of instructions. Neither of Babbage's two machines were ever completed.

However, a pupil of his, Ada Lovelace, derived a series of operational instructions for the analytical engine, and this is hailed as the world's first computer program, even though it was never executed.

Some of the basic elements of data processing derive from the work of Jacquard and Babbage. Any modern programmer is familiar with the constructs of the conditional branch (if statements) and loops, and both were present in the analytical engine's instruction set. When the first electromechanical computers were built in the early 1940s, they used punched cards or punched tape for their program input.

The History of Information Technology: The capabilities and design of computers developed rapidly through the forties and fifties, with the first office application appearing in 1951. In the early days of computing, most computer operations were reduced to calculations. The programs that drove them had to communicate directly with elements of the computer. For example, to add one number to another, the programmer would have to write an instruction to fetch one number from an area of storage into a register and then fetch the second number from another named area of storage and add it in the same register .Information technology, as we know it today, could never have happened without the development of natural language programming. Early programming language involved a series of codes, which were numbers. Early computer programmers usually came from a mathematics background.

The industry was born with the first giant calculators digitally processing and manipulating numbers and then expanded to digitize other, mostly transaction-oriented activities, such as airline reservations. But until the 1980s, all computer-related activities revolved around interactions between a person and a computer. That did not change when the first PCs arrived on the scene.

The PC was simply a mainframe on your desk. Of course it unleashed a wonderful stream of personal productivity applications that in turn contributed greatly to the growth of enterprise data and the start of digitizing leisure-related, home-based activities. But I would argue that the major quantitative and qualitative leap occurred only when work PCs were connected to each other via Local Area Networks (LANs)—where Ethernet became the standard—and then long-distance via Wide Area Networks (WANs). With the PC, you could digitally create the memo you previously typed on a typewriter, but to distribute it, you still had to print it and make paper copies. Computer networks (and their "killer app," email) made the entire process digital, ensuring the proliferation of the message, drastically increasing the amount of data created, stored, moved, and consumed.

Connecting people in a vast and distributed network of computers not only increased the amount of data generated but also led to numerous new ways of getting value out of it, unleashing many new enterprise applications and a new passion for "data mining." This in turn changed the nature of competition and gave rise to new "horizontal" players, focused on one IT component as opposed to the vertically integrated, "end-to-end solution" business model that has dominated the industry until then. Intel in semiconductors, Microsoft in operating systems, Oracle in databases, Cisco in networking, Dell in PCs (or rather, build-to-order PCs), and EMC in storage have made the 1990s the decade in which "best-of-breed"

was what many IT buyers believed in, assembling their IT infrastructures from components sold by focused, specialized IT vendors.

The next phase in the evolution of the industry, the next quantitative and qualitative leap in the amount of data generated and how we use networked computers, came with the invention of the World Wide Web (commonly mislabeled as "the Internet"). It led to the proliferation of new applications which were no longer limited to enterprise-related activities but digitized almost any activity in our lives. Most important, it provided us with tools that greatly facilitated the creation and sharing of information by anyone with access to the Internet (the open and almost free wide area network only few people cared or knew about before the invention of the World Wide Web).

While computer networks took IT from the accounting department to all corners of the enterprise, the World Wide Web took IT to all corners of the globe, connecting millions of people. Interactive conversations and sharing of information among these millions replaced and augmented broadcasting and drastically increased (again) the amount of data created, stored, moved, and consumed. And just as in the previous phase, a bunch of new players emerged, all of them born on the Web, all of them regarding "IT" not as specific function responsible for running the infrastructure but as the essence of their business, data and its analysis becoming their competitive edge.

We are probably going to see soon—and maybe already are experiencing—a new phase in the evolution of IT and a new quantitative and qualitative leap in the growth of data. The cloud—a new way to deliver IT, big data—a new attitude towards data and its potential value, and The Internet of Things—connecting billions of monitoring and measurement devices quantifying everything, combine to sketch for us the future of IT.

Just as chemical or metallurgical or electrical technologies enable the processing of raw materials into usable goods, to satisfy man's and societies' needs so does information technology (IT) help the storage, processing, transmission and exploitation of information to satisfy a person's, company's, society's or government's needs for information. The invention of printing was the first big breakthrough in Information Technology. It enabled literacy and education to go up from 10% to over 80% within 50 years by making available vast amount of reading material. That reading also led to the Reformation in Europe. Other break-through for Information Technology were the inventions like telegraphy, telephony, wireless or radio, television, broadcasting, computers (from room size to desk top to lap top to palm top and very soon, wearable ones.)

21st Century information technology revolution: There had been breath-taking inventions in electronics and photonics, micro-miniaturization, super and mega-scale integration; optical fiber and communication satellite transmissions, electronification and digitization of all information, storage and display devices and the transport of electronified information on worldwide telecommunication networks, increasingly under the control of the sender and the receiver. Information covers voice as in telephony, text as in fax, images as in video and data as between computers. The limitation for transmission and reception of information only from instruments connected to wires and therefore only from particular places, has been dramatically overcome by earth-based cellular mobile, radio telecoms and now by satellite based globe wide mobile systems like the Iridium.

Information Technology devices like microprocessors are becoming mass appliances from pace makers for the heart, hearing aids, and efficiency enhancers in automobile engines and devices to steer space vehicles on the moon.

Technology is an enabler for more effectively managing the business, but does not solve the problem unless it is tied directly to business and governance objectives. There is an urgent need for IT in underdeveloped areas where access to even the smallest bits of knowledge can have far-reaching, long term effects. The use of technology has a great many effects; these may be separated into intended effects and unintended effects. The implementation of technology influences the values of a society by changing expectations and realities. Technology, throughout history, has allowed people to complete more tasks in less time and with less energy. However, work has continued to be proportional to the amount of energy expended, rather than the quantitative amount of information or material processed.

In countries like India, which undertook government-centered development since Independence, government has become obstreperous, taking in the largest fraction of the GDP as taxes and the largest amount of their savings as loans. Government is not confined to its primary role of defense, internal security, justice, primary education, primary health, irrigation and roads, but it encompasses production, industries, services and businesses. It is commonly known that most of government's money is spent very inefficiently and much of it, on the salaries and establishment of the Government servants themselves and yet every service is inefficient. And the delays and the non-transparency and controls breed corruption. Talking about IT, Information technology (IT), as defined by the IATA, is, "The study, the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware." IT deals with the use of electronic computer and computer software to convert, store, protect, process, transmit and securely retrieve information.

Technology has had profound effects on lifestyle throughout human history, and as the rate of progress increases, society must deal with both the good and bad implications. Technology often enables organizational and bureaucratic group structures that otherwise and heretofore were simply not possible. Technology enables greater knowledge of international issues, values, and cultures.

Due mostly to mass transportation and mass media, the world seems to be a much smaller place. The effects of technology on the environment are both obvious and subtle. The more obvious effects include the depletion of nonrenewable natural resources (such as petroleum, coal, ores), and the added pollution of air, water, and land. The more subtle effects include debates over long-term effects (e.g., global warming, deforestation, natural habitat destruction, coastal wetland loss.) Each wave of technology creates a set of waste previously unknown by humans. Humanity at the moment may be compared to a colony of bacteria in a Petri dish with a constant food supply: with no way to remove the wastes of their metabolism, the bacteria eventually poison themselves.

Today, the term information technology has ballooned to encompass many aspects of computing and technology and the term is more recognizable than ever before. The information technology umbrella can be quite large, covering many fields. IT performs a variety of duties that range from installing applications to designing complex computer

networks and information databases. A few of the duties that IT professionals perform may include data management, networking and engineering. When computer and communications technologies are combined, the result is information technology, or "InfoTech". Information Technology (IT) is a general term that describes any technology that helps to produce, manipulate, store, communicate, and/or disseminate information. There are mixed consequences of IT on environment. As previously discussed, each wave of technology creates a set of waste previously unknown by humans. Talking of life, about fifty years, back the line, no one was familiar with what is called Cyber Waste, but we are now. So, the point is, despite of higher achievements, there are major drawbacks that IT has failed to rectify during course of its evolution.

Industrial Revolution, Globalization and Information Technology: The spread of the internet and the relatively low cost of digital technology mean that people lucky enough to have access to digital networks are becoming more global and more local at the same time. Small traders in shanties on the outskirts of Nairobi export across east Africa. In China, 'Taobao villages' allow previously cut-off rural populations to sell goods on Alibaba's trading platform.

New industrial technologies – including 3D printing, new forms of factory automation and machine learning – are rapidly enabling the mass personalization of products and local optimization of supply and demand. As a result, the maker movement and the sharing economy are both expanding rapidly. This is increasing the number of people who can use technology to create value. In 2016, GSMA found 314 tech hubs across Africa. Less than two years later, this number had grown almost 50% to 442.

Globalization is, of course, not just about trade in goods. In 1967, in his book The Gutenberg Galaxy, Marshall McLuhan coined the term the Global Village, laying out a remarkably prescient view of the benefits and risks of an increasingly shared global media space. Culturally, those connected to the internet are part of the same village conversations. This brings the opportunity both for enhanced cultural understanding and empathy, as well as the risks of polarizing dynamics.

On everything from domestic and international politics, to gender, race or other social issues, the stories that dominate our societies are no longer shaped by a small group of sources that are considered authoritative and trusted – now everybody has a voice. The cool, assured tones of the BBC World Service or PBS compete with a cacophony of opinion, the 'outrage economy', and a relentless stream of 'Twitter meltdowns'. The expanded space for opinion reduces the relative space for fact. Worse still, these very dynamics can be intentionally used to create discord in the pursuit of discrediting people, ideas or institutions. The race for technological advancement also lays the foundations of geopolitical influence, including the ability to influence the form of globalization. Technologies have always granted those countries and organizations that could master them economic, military and political power to different extents.

Today, countries are aggressively investing in technologies such as artificial intelligence and quantum computing. In fact, successfully harnessing new technologies is likely to be far more consequential than inventing them. In his recent book AI Superpowers, Kai-Fu Lee argues persuasively that China is among the best placed to win the next phase of the AI race,

based on its ability to implement cutting-edge machine learning techniques and leverage its access to massive amounts of data in an AI-friendly regulatory environment. Indeed, a Chinese company, Yitu, won the 2017 Face Recognition Vendor Test, a benchmark organized by the National Institute of Standards and Technology, which serves as the official guideline for US government purchases. Meanwhile, Chinese AI startups received 48% of global AI funding in 2017 – compared to 38% for US AI firms.

The Fourth Industrial Revolution is set to reshape economic power, scientific leadership, and the architecture of value chains as well as future forms of political organization. This has big impacts for how states relate to one another in the next phase of globalization. Global rules and institutions – just like technologies – are far from neutral. They embed our values, assumptions about the world, and desires for what we think the future should look like. Past periods of globalization have been justly criticised for leaving people behind while also being celebrated for generating wealth, spreading technologies and raising living standards around the world. But we can, and should, do better in Globalization 4.0.

The printing press is often cited as an historical precedent for our tech-driven revolution in society. A key milestone in the democratization of information and knowledge, it empowered individuals and permanently altered economic, social and political structures. Literacy, education, scientific progress and political participation became the currency of all, rather than a few – leading to changing values, norms and life expectations. We need to ensure that the technologies driving the next phase of globalization are human-centered and driven by positive values. In particular, as the World Economic Forum's forthcoming report on Digital Futures notes, we should aim for systems and technologies which are inclusive, trustworthy and sustainable.

What does this mean? Well, at the same time as we celebrate the opportunities of AI to make our organizations more productive, we need to be closing the digital divide and making sure algorithms challenge, rather than reinforce, existing prejudices and discrimination. And, as we start to use distributed ledgers to revolutionize global finance, we need to be deploying the blockchain to help refugees prove their identity and to help civil society organizations track commitments to sustainability. Most of all, those of us lucky enough to have the power to develop, invest in or even just use the latest technologies should do everything we can so that those with the least amount of power feel that technology is on their side too. Both the Fourth Industrial Revolution and Globalization 4.0 are opportunities to fix what went wrong in previous eras. And that starts with building a shared commitment to a shared future, based on those values which are truly cross-cultural: striving for the common good, safeguarding human dignity, and acting as stewards for future generations.

Development of Information Technology: Despite the impression often given that information technology has suddenly burst on the scene, its roots could be traced well into the past. Historical Perspective The history of man-made information technology is one of slow evolution dating back to 5,000 years. It has followed the mechanical and later electronic rather than biochemical path, with primitive signs, hieroglyphics, the alphabet writing, the book printing, and computer type-setting - a more or less linear development. More recently, the telephone, radio, television, satellite transmission, transistor, the computer, and the microprocessor represent distinct qualitative changes in the information technology, with the fact that we now have to accept the composite term information technology to include a

whole range of new developments. It has been said that information technology is the science of information handling, particularly by computers used to support the communication of knowledge in scientific technical, economic and social fields.

Definition of Information Technology (IT): The term `Information Technology' (IT) has varying interpretations. Macmillan Dictionary of Information Technology defines IT as "the acquisition, processing, storage and dissemination of vocal, pictorial, textual and numerical information by a micro-electronics-based combination of computing and telecommunications". Two points are worth consideration about this definition:

1) The new information technology is seen as involving the formulating, recording and processing and not just transmitting of, information. These are elements in the communication process which can be separated (both analytically and in practice) but in the context of human communication they tend to be intertwined.
2) Modem information technology deals with a wide variety of ways of representing information. It covers not only the textual (i.e., cognitive, propositional and verbalised forms, we often think under the head information), but also numerical, visual, and auditory representations.

UNESCO defines Information Technology as *"scientific, technological and engineering disciplines and the management techniques used in information handling and processing information, their applications; computers and their interaction with man and machine and associated social, economic and cultural matters".* (Stokes)

Chartrand has defined "Information technology, as the collation, storage, processing, dissemination and use of information. It is not confined to hardware or software but acknowledges the importance of mass and the choices, the assessment criteria used to decide whether he is controlling the technology and is being enriched by it".

According to Zorkoczy (1990) in its restricted sense, "IT is a new science of collecting, storing, processing and transmitting information". while Rayudu (1993) has defined "IT as the acquisition, processing, storage and dissemination of vocal, pictorial, textual and numerical information by a microelectronics based combination of computing and telecommunication ".

In short, information technology is a generic term used to denote all activities connected with computer based processing, storage and transfer of information. It involves computers, electronic media, satellites, telecommunication and storage devices. To be even precise, information technology has its origin in the technologies related to a restricted view of information i.e., the generating, processing, representation and distribution of information.

Information technology, as defined by the Information Technology Association of America (ITAA) is "the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware." Encompassing the computer and information systems industries, information technology is the capability to electronically input, process, store, output, transmit, and receive data and information, including text, graphics, sound, and video, as well as the ability to control machines of all kinds electronically.

Information technology is comprised of computers, network, satellite communication, robotics, video text, cable television, electronic mail, electronic games, and automated office equipment. Information industry consists of computer, communication, and electronics-related organizations, including hardware, software, and services. Another usage of IT is completing tasks using information technology which results in rapid processing and information mobility as well as improved reliability and integrity of processed information.

This definition that was provided by UNESCO, while emphasizing the significant role of computers, appears not to take into its purview the communication systems. It may, however, be stated that communication systems are as essential to information technology as computers. As a consequence, we have a convergence of three strands of technologies: computers, micro-electronics and communications. In other words, a mosaic of technologies, products and techniques has combined to provide new electronic dimensions to information management. This mosaic is known by the name new information technology. It is important to bear in mind that information technology is not just concerned with new pieces of equipment but with much broader spectrum of information activities. Information technology encompasses such different things as book, print; reprography, the telephone network, broadcasting and computers.

Components of Information Technology: Information technology connotes an ensemble of technologies. They particularly cover the computer capability to store and process information, known as information processing and the telecommunication technology, which are capable of transmitting information to distances.

The breakdown of these technologies is presented by James Williams (1982) in his paper "Information Technology - A state of the art." He presents the data in terms of the following six major new technologies that appear to be relevant to modem libraries and information system:

a) Processor, memory and input/output channels;
b) Micro, mini and large scale computers;
c) Mass storage technologies;
d) Data communication, networking and distributed processing;
e) Data entry, display responds technology; and
f) Software.

These technologies can also be grouped into three major areas (1) computer technology (2) communication technology, and (3) reprographic and printing technologies. A number of on-line information services are available today on commercial and institutional level. (which will be discussed later) The reproduction technology has advanced to a considerable extent so that we are having great number of choices for selection and adoption in information work.

Based on the aforementioned definitions, IT developments and areas of applications, the libraries use information technology to:

- Automate housekeeping operations,
- Networking of libraries for sharing and exchange of library resources, and

- Create databases to provide services to the end-users more efficiently than before.

It is experiential that, whenever the utilization of information technology is properly effected, it helps growth and development of libraries in different directions.

A. ***Computer Technology:*** Computer technology (or Science) is the study of operating principles of computers, programming languages and algorithms for solving theoretical as well as practical problems. It involves the development and use of devices for data processing. A computer is a machine that accepts data (in various forms), performs certain operations to process it and presents the results in finished forms according to the instructions provided to it. Computers are used in all aspects of modem living i.e. medicine, education, publishing, business, transport, communication etc and in personal use also. The history of computer technology can be traced back to those years (e.g. 3000 B.C) when the orient civilization used the abacus for calculating the simple arithmetic problems.

However, Blaise Pascal developed the first mechanical adding machine in 1642, which laid the foundation for the modem computing machines. During these years the computers developed from very large in size to very handy in size and their speed of operation from very slow to unimaginable high speed. The most popular computers of today are the personal computers (PCs) manufactured by different companies such as Apple, IBM, Compaq, Hewitt Packard and others.

The widespread use of computer technology has made dramatic developments in the information transmissions process in every field of human endeavor during the past few years. Highly sophisticated information services ranging from elaborate abstracting and indexing services to computerized data bases in almost all scientific disciplines are in wide use all over the world. The current developments in computer technology include mini computers, microcomputers, personal computers, portable computers, super computers, speaking computers, computers with IQs. See the robots, microchip technology, artificial intelligence, software developments, CDROM technology, machine readable data base etc.

Mini and Micro Computers: Miniaturization has been introduced in the 1970s. Although, each minicomputer has restricted capabilities, different machines are built for different functions and between them their range of capabilities equals that of mainframe computers. Moreover they have the advantage of economy and modularity. Microcomputers which are almost as powerful and versatile as minicomputers having a single printed circuit board supplemented with their main component and the microprocessor being no more than $1/4^{th}$ inch square.

Personal Computers (PCs): Personal computer industry has grown as a direct result of the evolution of the microprocessor. They are now available at a cheap rate. These microcomputers are used for the day-to-day personal applications. These computers irrespective of their small size and low cost also provide a wide range of capabilities.

Super Computers: These have extremely large storage capacities and computing speeds, which are at least 10 times faster than the other computers. They are used for large scale

numerical problems in scientific and engineering disciplines. These include applications in electronics, petroleum engineering, weather forecasting, chemistry, physics, medicine etc.

Portable Computers: The industry already developed miniature computers weighing less than one kilogram that can easily fit into a brief case or a coat pocket. The Nippon electronics came out with a portable computer measuring 30 cm by 21.5 cm and weighing 1.7 kg with 48 k byte expandable upto 128-kilo byte. These can be carried and plugged into a special outlet connected to a computer located at some other place.

Speaking Computers: Computers will read the printed matter and speak it about for those who cannot read. Similarly, they will be able to convert speech into written text. This will help the blind to read and deaf to listen. This 'speaking print and printing of speech' is no longer mere imagination. At the Bell Laboratories in the USA, input has been provided to the computer with the description of the tongue, lips, jaws, and vocal cords. The computer is fed with a dictionary of words and grammatical categories. Finally the computer is informed about the complex rules of timing, pitch and stress. It reads the movement of lips and prints the text. In near future we will not need a stenographer. One can go on speaking and the computer gives you the printed text. Similarly, one needs no translator.

Artificial Intelligence: Artificial intelligence is an area of study in which there is an attempt to make mechanics do things. It is currently difficult to make them do especially things that can be done by people. Artificial intelligence has been a sphere of development in computer science. Main topics in artificial intelligence are (1) theorem proving, (2) game theory, (3) scene analysis, (4) pattern recognition, (5) character recognition, (6) knowledge engineering, (7) problem solving, etc.

B. ***Microchip Technology:*** The phenomenal increase in computer capacity and dwindling down of costs are on account of the new and faster development in electronics technology. The invention of transistor in 1947 at Bell Telephone Laboratories made a history in electronics. Within a decade the device consisted of speak of silicon or germanium crystal encased in a pea size metal can, with a complex of electronic switches commonly called as the 'chip'. This integrated circuit technology initiated in 1959 has advanced the technological capacity in quantum jumps.

The race is on to build smaller and denser microchips, the work-hours of the electronics age. Microelectronics has acquired momentum with the advent of mustachio package technology. This dramatically reduces the cost per interconnection by mounting as many as 118 chips on, for example, a single ceramic carrier with upto 704 circuits on each chip.

CD-ROM Technology: Both the print media and its users are becoming obsolete due to exponential growth of information and information sources. The storage media for information are fast changing in a fascinating manner as follows:

a. PRINT MEDIA (papers, metal sheets, other hard materials)
b. FILM MEDIA (Microfilm, microfiche, etc)
c. MAGNETIC MEDIA (Magnetic tapes, drums, etc)
d. ELECTRONIC MEDIA (Floppy, hard disc, microchips, etc.)
e. OPTICAL MEDIA (CD-ROM. Videodisc,

f. CD-WORM, CD-I, etc).

CD-ROM is an acronym that stands for Compact Disc Read only memory. It is an optical disc of 120 mm diameter and a hole of 15 mm at the center with thickness 1.2 mm. Data is recorded in digital form using laser beam. Each disc can store approximately 600 megabytes of information equivalent to 3 lakh pages of text or 1500 floppy disks or an entire text of 20 volumes of encyclopedia.

Advantages of CD-ROM in information storage and retrieval are (1) permanent storage, (2) high density storage, (3) durability, (4) portability, (5) low cost, (6) unlimited use, (7) data protection, (8) personal computer based, (9) no telecommunication, (10) ideal for library storage, (11) networking and data exchange, (12) as mass media, etc.

C. ***Communication Technology:*** Communication or telecommunication technology consists of electromagnetic devices and systems for communicating over long distances. The principal examples are telephone, radio, television, and cable. The history of communication technology can be equated with the history of civilization itself It developed along with human beings communicating to one another. The use of clay tablets, hieroglyphics, alphabets, printing techniques photographic techniques, communications through telegraph, telephone, radio and television: all seemed to develop to facilitate better communication of ideas, expressions etc among human beings. Recently the telecommunication technology developed along three directions to provide i) better communication channels, ii) better networks, and iii) better sending and receiving devices.

The need to communicate more quickly and more efficiently has become a central focus in our technological society. Economy, industry, education and security of the industrial nations are going to depend heavily on the use of the latest means of communication technology and to transmit information. In the form of signals between remote locations, using electrical and electromagnetic media as carriers of signals, Telecommunication has achieved impressive advances in recent years. Channel capacities, reliability and error rates have improved dramatically. The major developments in the area are:

The following are the major modes of communication, which are forms for sharing purpose. i. Telegraph, ii. Telephone, iii. Radio, iv. Cinema, motion picture, v. Television vi. Computers vii. Communication Satellite viii. Online technology, ix. Internet x. E- mail xi. Facsimile Transmission (FAX) xii. Teletext and videotext, xiii. Data system and Network xv. Teleconferencing, xvi. Fiber optics and microwave Networking.

These are Audio-technology, audio visual technology, teletext and video text, fax, on line search, e-mail, satellite technology, fiber optics, ISDN, Networking, teleconference, cellular telephones, voice mail, pagination, communications, etc.

Audio Technology: There have been tremendous improvements and inventions in the field of audio technology. The older gramophone records of T.A. Adison are now dwindling. Much sophisticated cassettes and tape recorders are emerging. Marconi's ancient model of radio set has seen many developments. The outmoded AM (amplitude modulated) radio receivers are being replaced by the modem FM (frequency modulated) receivers. They offer improved world fame. The recent development is the production of compact discs (CDs). These have

very high storage density and can be used for speedy dissemination of information to the needy around the world. The journalists for mass communication of data, information and news can tape the potentiality of this powerful medium. Thus, the new audio technology can be used in libraries and information centers for a wide variety of purposes such as storytelling to children, imparting education, knowledge, recreation, etc.

Audio-Visual Technology: Motion pictures, television, videodisc are the main contributions of this technology. Motion pictures are one of the instruments of mass media communication. They are the dynamic source of information, education and recreation. The recent development in the field is the 3D films. In 3D films, people feel the dimensions of the object as if they come alive on the screen.

John Logic Baird in 1926 invented television. The television industry is undergoing many changes because of changing technology. In its formative period major networks of stations that carry a relatively small selection of programs at any one time dominated it. The spread of cable TV systems and satellite broadcasting in the 80s have resulted in a much wider choice of programs for viewers and in some cities, more than 100 channels are available. Direct Broadcast Satellites (DBS) system was introduced with the launching of satellites for this service. A DBS broadcasts programmes directly to home receivers that are connected to small satellite antennas mounted on roofs.

In stereo TV transmission, two different audio channels are sent with picture. The receiver decodes the two separate channels and produces the audio in two speakers. The sound is more natural than conventional TV with single speaker sound.

High-definition TV (HDTV) has come which uses 1125 scan lines, producing a much smoother and more detailed picture. However, a conventional TV set uses only 525 scan lines to produce a picture. HDTV screen will be bigger and produce high-resolution pictures.

Videodisc is a new medium containing pre-recorded information, which allows the user to reproduce the information in the form of images on the screen of a television receiver at, will. There are three general types: magnetic, capacitive and optical or laser disc is more versatile. It has high storage density for information. The optical disc captures text, photographs and graphics. Both the digital optical disc and the videodisc provide the user with random access within a fraction of a second after the keywords or the page numbers have been typed, the relevant information is presented on the screen. Videodisc uses a special player connected to a television set. The player is far cheaper than high storage magnetic discs. Video-disc technology offers high quality storage, image stability and speed of recall.

Multimedia: This is a unique development in the field of information technology. Multimedia are the technologies that facilitate the integration of two or more types of media such as text, graphics, sound, full motion video, or animation into a computer based application. It is a collection of multi-sensory presentation technologies combined through a common user interface into an information delivery system. The presentation data types can include text, image, graphic, audio, animation and video. The user interface is a computer-based system that might consist of CD-Rom disks and customized graphical display hardware for data compression, decompression, acceleration and transformation.

It allows the user to browse and navigate quickly any type of complex information; it is immensely helpful in the education process and learning and can be used either as a single standalone system or multi-user system for information dissemination.

Videotext and Tele-text: Videotext or view data is an interactive system for transmitting text or graphics stored in computer databases via ordinary telephone line on a television screen. It is a simple to use low cost information system catering to large number of users. Teletext is non-interactive form of videotext.

Teletext is the generic name for three British systems of electronic information delivery, Ceefax, Oracle, and View data. The ceefax and oracle broadcast information continuously for their users and may be received and read by anyone who has a TV receiver and a decoder, whereas. View data operates by means of telephone lines connected to central computer. This direct connection makes it possible to have two-way communication between the home and the information supplier. A ceefax viewer can only see the information that the broadcaster is currently sending. A view data subscriber gets information that is transmitted to his home only when he actually requests it. Telecommunications of British post office is offering such varied services as news, abstracts of publication lists of local restaurants, income tax calculations etc. Similarly in 1984 the P&T Department of India started a system on the lines of tele-text.

Facsimile Transmission: Facsimile has been boosted by the adoption of methods of data compression made possible by compact, reliable and inexpensive electronics. During the initial stages, the average speed of facsimile transmission was found to be 3.4 minutes per page. This technology was slow. It was replaced by micro facsimile satellite communication and fiber optics has increased the potential of facsimile transmission. A Japanese concern developed in March 1990 the first desk top facsimile machine that can transmit full color images with superior quality using digital image processing technology; it can compress or enlarge the image on paper.

Online Information Retrieval: Online means the state of being in direct, immediate communication (on-line-to). With the date base one wishes to interrogate and with the computer on which this database is loaded online searching is the computer on which this database is loaded.

Online searching is the computer-assisted retrieval of the bibliographic citations. It means searching where in the search is processed while the user is connected to the computer, thereby allowing the user to interact with the computer and adapt the search is conducted as a two way conversation between the searcher and the system. The online system is also called as interactive or conversational system. An interactive system is an online system, which allows the user to input instructions, receive a response and then modify or manipulate results.

The advantages are: (1) they provide fast and rapid responses, (2) more accuracy, (3) they permit browsing, (4) can be used as a non-delegated search made, (5) system has the capability of displaying its own controlled vocabulary, (6) search is more wide and exhaustive and (7) helpful in multidisciplinary research areas.

Many commercial and other organizations provide users with online access to databases in machine-readable form. The major search services are DIALOG, ORBIT, NLM (MEDLINE), ESA, BLAISE, RECON, BRS and NASA etc.

Electronic Mail: It is the most used service of the Internet. The messages can be sent to a single person or to a group of persons separately at the same time through this facility. Its speed is high and charges are low in comparison to postal service owing to which it enables one to be in touch with the rest of the world in most technical and efficient way. E-mail programs allow us to save print or reply the messages and also to attach word processing documents, graphics or video images with our reply.

D. ***Internet:*** Simply, the Internet can be defined as the global network of networks. It is a network of interconnected World Wide Webs of different types of organizations like universities, business, defense and science organization. It has emerged not only as an important search device for research and development community but also for political activists, farmers, librarians, journalists, scientists and many others. The various basic facilities that can be availed through Internet may be summarized as follows (Sinha and Dhiman,2001).

i. *List Serves:* This is a discussion group crated to share ideas and knowledge on a particular subject. The discussion groups are created and monitored by someone with an interest in that subject and are monitored by someone with an interest in that subject and are open to anyone. One can join the list simply by sending E-mail request to the list. The programme automatically reads E-mail request to the list. The programme automatically reads E-mail messages and extracts your address and adds this to the circulation list. The message sent to a list is copied and then forwarded to every subscriber of the list. The first message tells you that you have successfully subscribed to the list.

ii. *Usenet/News Groups:* Unlike the list server, the news group servers provide access to thousands of topic-based discussion group services that are open to everyone. The newsreader software allows you to post an article to any group for others to read. A comment to a message can be added to the thread of the article and one can find answer to a specific question.

iii. *File Transfer Protocol (FTP):* This is a mechanism that allows placing and retrieving of files over the Internet. It allows downloading of software, product up gradation and other things. FTP servers also supply a small amount of text information. With the help command one can get online help to know more about any doubts.

iv. *Telnet:* This is used to denote the networking over the telephone. It is a simple programme created by the National Center for Supercomputing Applications (NCSA) that uses transmission control protocol/Internet protocol or TCP/IP to provide connection with another computer. Using telnet you can contact a host machine by typing host name of IP member and can transfer files from the TCP/IP host to your own computer and can access databases.

v. *Gopher:* The Gopher was created by the microcomputer work station center of the University of Minnesota to find information on the Internet in a user friendly way. It is a menu driven programme that allows you to click with information

servers or Gopher holes on the Internet to retrieve the information including text, sound and images.

vi. *World Wide Web (WWW):* The web is a large system of severs and combines/and many of the Internet applications, which offers all kinds of information to any one on net. This is a series of interconnected documents stored on computer sites. If you use your computer and a software program called browser to visit a site on the web, the screen displays a document called a home page. Home page gives the name of the organization or individual sponsoring the web site and it plays a slot of highlight words, buttons or pictures. It is the text and graphical screen display that welcomes the user and explains the organization that has established the page. Information using client server architecture Graphical User Interfaces (GUI) and a hypertext language enable dynamic links to other documents. The Internet can be used to access the information from the remote to read, download and print the electronic books and journals and reference service beside some/ of the housekeeping operations like acquisition and cataloguing.

Categories of Computer technology: Computer technology may conveniently be divided into: processor technology, storage technology and software aspects.

Processor Technology: Computers consist of electronic components assembled in a design or "architecture" that will perform necessary functions of input, output, computation and control (control of both the computer itself and of attached peripheral devices that perform input and output functions and store the files).

In the past, electronic components were expensive, so a minimum number were used in a single processor that alternately performs input, control, processing and output. Besides, the first generation of computers, operated by means of vacuum tubes or valves, were relatively bulky and energy consuming. The first major innovation, leading to microelectronics was the discovery of transistor, a product of solid state physics, which used semiconductor materials. The most important development of these today is based on the non-metallic element `silicon'. Being much smaller than the vacuum tube, the transistor quickly replaced it in all electronic equipment. However, transistors and other equipment had to be wired together and a single piece of equipment might have thousands of such components. The wiring and assembly of such elements were a delicate and costly process. This naturally paved the way for research towards the concept of integrated circuit (IC). At first IC's were simple but, as the technology developed, they rapidly became smaller and more complex. This led to the miniaturization and refinement.

The central feature of micro-electronics is the development of micro-processor, a special form of IC with functions of arithmetic, logic and control - similar to those of Central Processing Unit (CPU) of a computer and contained in a single chip. In addition, the microprocessor includes units to interpret instructions from the stored programme to supply the control memory the information necessary to retrieve instructions and send out data as required. The microprocessor is the building block from which modem computer systems are assembled. The microprocessor uses very, little energy and has few environmental requirements of older machinery. Air conditioning, for example, might not be necessary for a general purpose computer using microprocessor technology. The practical significance of this is that it is now possible to bring the computer to the problem instead of bringing the

problem to the computer. The aspects referred to above form a major hardware component of a computer.

Storage Technology: In the previous section, the, recent innovations relating to the processing aspects of computer technology were discussed briefly. In considering some of the advances in devices for digital information storage, it may be stated that most of the primary storage in computers is now supplied by semi-conductor circuits. There have been significant developments in memory technology affecting three areas of performance spectrum; the high speed, high performance; the midrange and the low speed bulk memory systems. It is now possible that even a small computer system might have cache memory, a small associative memory retaining most recently referenced information and in a readily available place. In some cases, cache memory may be at the top of a hierarchy of memories having a wide variety of characteristics. Memory management, dynamic memory allocation, and virtual memory schemes, generally found in large computer systems, are now appearing on computers which are small and less costly.

The development of charge coupled devices (CCDs) and bubble memories has filled the gap which previously existed in the continuum of memory devices such as fixed-head magnetic disks and these are slower than other semi-conductor memories. These memories have advantage over magnetic disks in that they contain' no mechanical parts and could be used to store significant amount of information and can be treated as a structured file system. There has been a continuous improvement in recording densities of magnetic media. Floppy disks and microfloppies provide a convenient media to store data. The development of video disk has added a new dimension to the information storage technology. Video disks could' be used to store large volumes of information in digital form. These kind of mass storage devices are believed to be very useful in the development of information storage and retrieval systems. It May be stated that all these innovations in storage technology provide us a variety of alternatives depending on the requirements of speed of operation. These developments add more capabilities to the storage aspects and may be considered advances in the storage technology.

Software Aspects: Software is a generic term covering the concepts, procedures and instructions which enable computer systems to do useful things. Usually, software is conceived in terms of computer programs, discrete units of software which make the computer to carry out specific tasks, and or systems or packages. The importance of software is obvious, since it is the software which applies the power of the computer to solve the users' problems. Many of the users need a clear understanding of the capabilities of software more than hardware aspects. It is known for some years now that the "rapid increase in the capabilities of computer systems has not been matched by corresponding increases in the development and quality of software. This situation has caused much disenchantment with computer systems. The methods by which computer software is produced have changed considerably in recent years with the emergence of "software engineering", which enabled improvements in programming practice, such as structured, or modular programming.

As one of the solutions to the software problem increased production and availability of packaged software is encouraged. Another solution to the problem is the use of fourth generation languages and flexible integrated software to produce prototypes of programmes to meet the user needs. It is hoped that these solutions would be able to meet fairly standard

requirements. For the average user they mean that there will be an increasing number of packages to meet most of his needs.

Communications Technology: The development of communications technology is, in a sense, a symbol of man's effort to communicate rapidly over great distances. Communications technology is older than computer technology. It has grown as rapidly as the computer technology in recent times. These two technologies are now fusing into what Anthony Oettinger has called `compunications'. This newly emergent technology is changing our life styles as few technologies have before. This new technology has probable and important uses in the home, office, factory, community and in information exchange system and holds prospects of immediate relevance to information profession. Some of the significant aspects of information transmission technology are discussed briefly in the following paragraphs.

A communication system can establish paths over which messages can be sent between any two instruments in specified locations at desired times. This type of system is generally known as switched .network.' Communications technology has advanced to the extent that now it is possible to hire services from a commercially operated network. Hence, there is a steady growth of computer-to-computer data traffic. Also, computer manufactures are offering network architectures which together offer multiple operating systems running on families of similar computers. A terminal of a computer network may have access to any of the computers within the network, if it is authorized to do so.

A computer serves as a terminal when connected for providing computation, information retrieval, etc., in accordance with the request of the terminal. A multi-lateral access capability allows the users of the terminal to share these resources. Such networks are characterised by a new technique known as packet switching in which the message is divided into a number of message blocks called packets and are transmitted between nodes in store and forward basis. Among the information resources to be shared are the data bases. A number of information systems have come into operation based on this concept.

Another advancement of great significance in telecommunications from the technological point of view is that of a fundamental and massive shift from analog to digital modes of transmission. This shift is underpinned by new transmission channels of enormous capacity. This shift is massive in that it involves the replacement or upgrading of costly equipment. It also involves types of communications namely voice, facsimile, computer transmissions and television communication, which will all be affected.

For example, every manufacturer of semi-conductor circuits has started to produce a device called Codec-short for `Coderdecoder'. This circuit takes the human voice and transmits by the standard voice-grade telephone channel, samples the signal 8,000 times per second, and encodes it into a digital bit stream. Digitised signals from hundreds of telephone conversations are then bundled, transmitted over a high capacity communication links, decoded at the other end, and reconstituted into a very close approximation of the original voice. While this may appear to be an elaborate and excessively complicated procedure, the switch from analog to digital makes good sense from a number of points of view. *Firstly*, the cost performance of digital circuits continues to improve remarkably. *Secondly*, noise problems inherent in analog devices can be eliminated. This transformation from analog to

digital mode has resulted in the intelligent communication channel and has reduced even the thin line of distinction between communications and computing.

As a result of rapid technological progress, a variety of services, which have traditionally been considered separate, are now becoming increasingly similar. This tendency is generally referred to as convergence of service modes. Telecommunications can now handle not only speech and data but also visual information in a unified manner. Broadcasting is now capable of providing two-way or selective dissemination of audio and visual information by way of a broad-band cables in addition to conventional one way dissemination. With the result, two traditionally separate 'services, telecommunications and broadcasting tend to merge together in their mode of operation and thereby provide users with diversified types of information more efficiently. This innovation could be utilised for the publication of journals through the extensive use of techniques like facsimile text processing and word processing. Library and information services may also be included into the integrated whole. To handle the economy of scale, the concept of Integrated Services Digital Network (ISDN) is evolving very rapidly.

Reprographic and Micrographic Technologies:

Reprography: Reprography, as a term, has gained international recognition in 1963. It includes "photocopying , microcopying, duplicating and in-plant printing and is characterised by the small scale of its operatives". Reprographic techniques include such processes as diffusion transfer, physical transfer, quick stabilisation, diazo, thermography, and electrostatography for copying documents. Reprographic technology has been playing a vital role in the dissemination of recorded information and has now come to stay as one of the means to provide access to document resources geographically located in different places. Document delivery service largely depends on the facilities afforded by reprography.

Micrography: Micrographic technology is an outgrowth of photographic technology. Since this technology is being increasingly used to supplement computer systems, strong electronic and photoelectronic influences make it multi-technology dependent. Micrographic technology finds its application not only as a publishing medium but also, as a communication medium, computer output medium, and storage medium. In the past, the use of microform as a publishing medium was limited because of inherent limitations. It may be stated that the widely known field of use for this technology was in connection with archivation and for file and library compaction, in which microforms replace traditional paper publications. Micropublishing for selective retrieval should be seen as user-oriented application in the context of changing information' transfer needs. It involves two separate, but interlinked distribution processes, (i) publication of full content on microforms, and (ii) distribution of retrieval support information (i.e., index, access to database, etc.). This support information is the key to the retrieval. It can be made available on any medium (such as paper, microfilm, magnetic tape or floppy disk) that provides ease of access to location codes for the full information on microforms.

These micro-publications are resources and often essential tools for certain information workers. Their value for the user depends primarily on the human engineering of the retrieval support hardware and software and relevance of information that can be obtained in response to a particular problem. The production process for a micro-publication reflects a dual information flow. The content is either microfilmed or if it is available in machine-readable

form, converted directly into microfiche by a COM system. The primary information is inexpensively duplicated and distributed to all those who are in need of it. VIicroforms permit (as publication and storage media) compaction, organization for ease of use and partial or full automation of retrieval. Most important, however, are the economic advantages and the potential for up-to-date complete information supply in a decentralized and user-oriented form. As information transfer medium, microforms exhibit many desirable features suitable for use in IRS Systems with automated retrieval and on-demand reproduction. These computer microforms (CMF) systems offer high on-line storage capacity and economic on-demand publishing capabilities, provided special microforms with high reduction ratios are used.

The new technologies are causing rapid changes. The factors which are having impact are computers, microprocessors, lasers, digitisation of information and screen based technology including television and telecommunications. Some of the aspects relevant to information profession are developments in keyboards, OCR, input to photosetting systems, electronic full page composition techniques, and graphic reproduction. Data capture in machine-readable form is becoming easier with the advances in word processing and direct entry photo setters. Increasing digitization of data makes printing a more systems oriented process.

Advantages of Information Technology: A variety of advantages can be derived by the appropriate use of information technology. The advantages can be referred to anything produced with the assistance of technology which allows completing more tasks with greater accuracy and better quality in less time and for lower costs. It could be higher productivity, better quality or it might be less tangible like ensuring users to have better image of the library and improve response time or improving staff morale and motivation, in certain nature of jobs. Hours of manual work are possible for completion within minutes through it. Perhaps, there is a number of operation or service where you cannot apply information technology. The benefits of it are in the following ways:

Information Technology

i. Helps to avoid duplication of effort and work in library operations.
ii. Facilitates cooperation and resource sharing-through library network.
iii. Helps to introduce new services and improve existing services.
iv. Allows integration of various library operations.
v. Executes repetitive nature of works.
vi. Facilitates faster information communication.
vii. Helps to increase the quality and range of services.
viii. Increases morale and motivation of library staff.
ix. Facilitates easy and wider access to all kinds of information, sources.
x. Helps to increase efficiency and effectiveness in library operations. Ultimately helps to save time, space, energy and resources.
xi. Helps to improve productivity and image of the library.

Electronic Resources and Services in Libraries:

A. *Electronic Publishing:* This does everything, which has traditionally been done in the image assembly operation up to paste-up stage. It combines typesetting with the

electronic creation and manipulation of line art and half tones in one system. This term in a broader context includes other communication techniques such as e-mail, videotext, teletext, electronic journal, etc. The trend is towards quick publishing where the document is created using computer and disseminated electronically over networks in the final form.

B. *Desktop Publishing:* The term DTP indicates that entire publishing is done on one desktop. Generally this is used for the production of documents at the working place itself, using computers and publishing softwares such as Ventura and page maker. The author creates the documents on computer, using word-processing software, edits and makes pages, adds graphics, designs cover and pages, on a single desk and the document is produced on laser printer which may then be used as camera ready copy for printing large number of copies through conventional means.

C. *Digital library:* With the rapid development of technology and emergence of Internet, electronic publishing is getting a tremendous impetuous from publishing industry. In fact, digital libraries have brought many changes to the library users, services and functions. The digital revolution is sweeping all aspects of life in civilized world and the libraries have no exception. Digital libraries are able to integrate the freely available information on the web with the more formal literature for which licenses on electronic versions are arranged with publishers. These licenses enhance and replace traditional collection development policies. However, digital libraries facilitate time and place independent information services for students, faculty members and research institution scientists which is indeed very essential in active learning styles. The digital libraries are going to play vital role in the 20^{th} century and they are important component for capturing the explicit knowledge. This has to be supplemented with the implicit knowledge to the digital system, which will eventually get transferred into a knowledge management system.

D. *Virtual library:* Broadly the term virtual library refers to an environment in which component parts combine to provide access to information. Specifically virtual library means a library connected electronically to other libraries or information source. In other words, virtual library means with materials in digital format and telecommunications access to digital catalogues and collections. Frequently virtual libraries are defined as the act of remote access to the contents and services of libraries and other information resources, combining an onsite collection of current and heavily used materials in both print and electronic form with and electronic network that provides access to and delivery from worldwide library and commercial information and knowledge sources.

E. *Online Searching:* Online database retrieval is becoming a major factor in information activity. It is exerting immense influence on the information world on present information services, on formulation of national and international policies. It is enabling information centers and libraries to add a major new dimension of services to their users in many subjects; Engineering, Marine Science, Agriculture, Medicine and even in arts and humanities.

An online search is an interaction between an individual and a database, where the individual states his query in the form of search terms and logical combinations, key words of search terms, to retrieve small sets of very specific information, from large computer-stored databases. The process of searching in an information retrieval system can be manual or

online. An online search means a search of a remotely located database through interactive communication with the help of computer and communication channel. The user can access the database directly information activities. The term online searching can thus be used to indicate search services available from producers of databases or vendors or suppliers of these databases.

F. *E-Collection*: E- collection refers to the digitized documents that are archived and available for retrieval to users. E-collection at IGCAR library consists of the following categories: E-collection states that the libraries planning for e-collecting building should have firm plan for local area network, content creation section, software/hardware procurement. All the efforts should be taken to ensure the copyright of documents being digitized and also their quality. Libraries should adopt a proper method for backing up the e-collections and their recovery in case of any disaster. The appropriate user interface is essential and the option to do search on these e-collections will make the information services to patrons.
G. *E-book formats:* E-books are available in various formats. The most common are Windows executable and PDF, although others include formats for specific computer programs and handheld readers. EXE files are usually HTML files (web pages) compressed into a single file. This file is executable, which means you do not need any extra software to read the e-book, although most require you have Windows 95 or above and Internet Explorer installed. The main problems with this format is the fact that, like a web page, the page may look different on some computers (depending on screen size, resolution, etc.) and also, this format is not compatible with Macintosh systems. PDF stands for Portable Document Format and is widely regarded as the best format for any document designed for Internet transfer due to the small size of the files and the fact that it will look as the writer intended on almost every computer. PDF files are also compatible with Macintosh systems to view PDF files you will need to install the free adobe acrobat reader.
H. *E-Books:* Electronic publishing of books is a major development that is quickly causing changes in the industry. E-publishing has developed rapidly over the past few years. Different companies have launched with different strategies and ideas on how e-books will be delivered. Will people read them on new devices known as electronic readers? Will they read them on the computer screen? Electronic devices such as palm pilots and electronic readers allow people the potential to store hundreds of books at a time. This large potential market has generated a large amount of money being poured into e-publishing to develop both the hardware and the software to make this electronic transition a reality. However, encouraging people to give up their comfortable hardcover and paperback books with dog-eared pages has been no easy measure.

At first it was new upstart technology companies developing the technology and launching new brands. However, recently the traditional publishing houses have also climbed on board and are converting their lines of new releases and backlists into the available electronic delivery formats, including both e-books and print-on-demand technology. Print-on demand (also known as POD) allows publishers to print a single book at a time and avoid costly print runs of thousands of books. A standard for e-books has also been developed by OEBF, an organization of publishers and technology companies. However, Adobe PDF is also a widely

used format for e-books and it competes with the OEB standard. Because e-book technology is faster and can be implemented without the need for expensive print jobs a growing number of publishers and publishing services that produce electronic books have emerged.

These companies aim to compete with the traditional publishers with new product offerings and without the expenses of regular printing. While it is good to see competition in the industry, the e-publishers have been too slow to convert readers to e-books and they face increasing competition from traditional publishers who are entering e-books arena. However, on the plus side for the new e-publishers, technology companies, including microsoft, are working on rapidly developing software and hardware to turn book lovers into e-book readers. Even individual authors have challenged the style of traditional publishing. Horror author Stephen King is publishing a serialized novel solely on web with early success. An e-book or electronic book is essentially a book that has been written in electronic format so that it can be read directly from a computer screen.

An e-book is a text presented in a format which allows it to be read on a computer or handheld device. Many titles which are available in printed versions can be read as e-books, including bestselling fiction, classics and reference texts. E-books are also used to make out-of-print work available, or to bypass print altogether, as with new works by aspiring authors. E-books can consist simply of the electronic text or may also contain extras, such as audio, video or hyperlinks.

I. *E- Journals:* Electronic journal may be defined broadly as any journal, magazine, e-zine, webzine, newsletter or type of e-serial publication, which is available over the Internet, and can be accessed using different technologies such as WWW, gopher, ftp, telnet, e-mail or list serve, etc. E-journals are the periodical, regular or irregular moderated unit made available in an e-format either on a static medium or via computer networks. The University of Glasgow defines the term 'electronic journal' as "any journal that is available over the Internet can be called an 'electronic journal' in some cases, print equivalents exist; in some cases, not. Some electronic journals are freely available; others have charging mechanisms of different types. Established publishers issue some; others are produced from an individual academics office. As with print journals, the quality and relevance of e-journals can vary considerably."

I.1. Types of E-Journals: Electronic journals come in many types. Some of them are traditional paper journals simply made available electronically; others are sample selections or just the table of contents of the paper journal; still others have no equivalent paper copies. They can be broadly grouped into two categories:

- *Online Journals:* Online journals are defined as those journals that are available on 'pay-as-you-go' as cost-per-access basis, via such online hosts as STN internal, using proprietary retrieval software. These e-journals are not considered as part of library collection because in most of the library, users are rarely allowed free to unlimited access to remote online systems. Basically, online journals are the electronic versions of existing printed journals e.g., American Chemical Society. All journals in full text are available through STN International.

- *CD-ROM Journals:* These are full text journals published and distributed in the form of CD-ROM with regular updates, along with search software to access and print. Link online journals, the vast majority of CD-ROM based journals are the electronic versions of printed journals e.g.,
    a) All journals and conference proceedings of IEEE
    b) ADONIS
    c) Applied Science and Technology (AST), Index of Wilson Company.

J. *Electronic resource access types:* The access to e-resources through Internet is prominent because of the inherent advantages of the net over other media such as CD-ROMs and advancement in web technology. The most significant advantage is of wide access and currency of information on the net. However, the types of access are in itself not uniform. The publishers provide the following different types of access mechanism:

a. *Free Access:* On subscribing to the print version of the books, journals, reports, conference proceedings etc., some publishers provide free access to the electronic version of the e-resources.

b. *Fee- based Access:* This is one of the most preferred access mechanisms by both the subscriber and publisher. On the payment of an access fee, which is a certain percentage of the cost of the printed e-resource being subscribed, the publisher provides access to its compete e-holdings. The subscriber will have to maintain the print level subscription throughout the period of agreement. The access fee percentage in such cases depends on the quantum of print level subscription.

c. *Exclusive Subscription:* Institutions can obtain complete access to all the e-journals brought out by the publisher without subscribing to the print counter parts. However, the subscription charges in this case are very high, i.e., approximately 90 percent of the print subscription.

d. *Selective Access:* The subscribers choose a maximum number of e-resources from the publisher and pays for them as per agreed terms and conditions. The publishers because of the difficulties in their administration do not favor this type of access.

e. *Institution v/s Consortium Access:* Institutional access of e-journals is expensive and not many institutions and organizations can afford to subscribe to e-journals, particularly in developing countries. In consortia access, a few institutions that have common interests and requirements can form consortia for e-journal access. This would be an economic model for wider accessibility and develop a stronger information base.

Information Technology in Indian Scenario: India has made remarkable progress in the field of book production and publication, telecommunication, satellite, computer and laser technologies. Promoted by these technological changes and innovations, the scenario has metamorphosed to include a variety of endeavors in the field of library and information science. Information programmes like NISSAT, ENVIS, BTIS NILNET, INDONET, VIKRAM, NMIS INSDOC, BARL, SLET SENDOC, SAIL are being evolved and generated successfully due to advancement in information technology. Besides, the International Information System (IIS), such as ASTINFO /UNESCO, INIS/ IAEA, AGRIS/ FAO. GEMS/UNEP, TIPS/UNDP have their focal points in India.

There are more than 20 organizations in India offering computerized bibliographical information service. Besides information processing packages have been developed by different organizations for (i) SDI and retrospective searches, (ii) current awareness, indexes, catalogues etc. (iii) the source and classers, (iv) online query processing, (v) cataloguing, (vi) acquisition, and (vii) circulation control. In library applications, Tymnet and GTE-Telnet are widely used to access the online bibliographic search services. INDONET is an integrated information management and distributed data processing facility spanning the entire country. Attempts have been made to get databases from various organizations and make them accessible online through INDONET. An international gateway in Bombay is set up with the cooperation of Videsh Sanchar Nigam to enable Indian users to access international databases available from LOCKHEED/DIALOG, SDC/ORBIT and ESANET.

INSDOC has arranged for online access to the ESA/IRS databases from terminal installed in Bombay. The information centre for aeronautics in NAL, Bangalore conducts information searches from the ESA databases. Informatics India limited at Bangalore offers information services, now on a commercial basis. Again we have a programme named INFLIBNET, a computer communication network for linking libraries and information centers in universities, deemed universities, institutions of national importance, UGC information centers, R&D institutions and colleges.

However, in Indian context, only special libraries and information centers are adopting to the new technological changes. But there seems to be very little efforts in the direction of introducing the technological developments in the academic and public libraries. This may be due to (i) lack of motivation and awareness on the part of the library managers; (ii) non availability of skilled personnel; (iii) lack of training opportunities to handle sophisticated tools and machineries; and (iv) financial constraints.

But this state of affairs will be set right if the librarians come forward to adopt themselves to the general and prevailing trend.

Role of Information and Communication Technologies in Transforming Legal Education: Introduction Computers made their entry into education sector in the late 1970s. With computers, other devices like printers, floppy disk drives, scanners and the first digital cameras also made their way in education sector. At that time the term Information Technology (IT) was used to describe computers and these various peripheral devices. Then with arrival of internet and World Wide Web, emails and search engines a complete transformation occurred in almost every field including education. A new term ICT emerged in the language which is short for Information and Communication Technologies. It embraces the many technologies that enable us to receive information and communicate or exchange information with others. According to UNESCO the term “Information and Communication Technologies (ICT) refers to forms of technology that are used to transmit, process, store, create, display, share or exchange information by electronic means.” This broad definition of ICT includes any communication device or application, encompassing: radio, television, cellular phones, computers, satellite systems as well as various services and applications associated with them, such as video conferencing and distance learning. ICT can be used to support the educational content, the educational process as well as the organization and Administration of education.

Importance of ICT in Education: Due to its various characteristics, ICTs are making dynamic changes in society. They are influencing all aspects of life. The influences are felt more and more at schools, colleges and universities. Students and teachers have got more opportunities in adapting learning and teaching to individual needs. ICTs have revolutionized the way people work today and are now transforming education systems. Education policymakers are attracted to the prospect that ICT can improve student achievement, improve access to schooling, increase efficiencies and reduce costs, enhance students' ability to learn and promote their lifelong learning, and prepare them for a globally competitive workforce. Effective ICT integration into the learning process has the potential to engage learners. For instance, using multimedia to present authentic and ill-structured problems in problem-based learning can motivate and challenge students and hence develop their problem-solving skills. The benefits that ICTs can have for teaching and learning include:

1. Using ICT means that information can be obtained almost instantly. The worldwide web, for example, contains a vast amount of easily accessible information. Such information can provide learners with different viewpoints and a wider understanding of issues.
2. ICT helps teachers to adjust teaching materials to suit the needs and ability levels of their students.
3. Computers equipped with internet and other means of ICT provide opportunities to the students to study anytime and anyplace. Now they are not confined to the boundaries of schools and colleges. Use of ICT has extended the scope of offering programme at a distance.
4. ICT promotes multimedia approach of education like, audio-video aid, sounds, motion pictures, television, filmstrips, records, computers and audio tapes etc. The use of audio-video techniques has various advantages in education and learning. It makes learning more interesting. Students can learn more quickly in audio-visual techniques as compared to traditional class room learning. It makes learning more memorable and brings the subject matter to life.
5. It creates environment with multiple tools and materials in which student acquire various skills such as critical thinking, typing, presentation, and research skills. It also facilitates contact between students and teachers, allowing joint activities and sharing of ideas.
6. ICTs enable new ways of teaching and learning rather than simply allow teachers and students to do what they have done before in a better way. ICT has an impact not only on what students should learn, but it also plays a major role on how the students should learn.
7. ICT helps to prepare students for life after school. Proficiency in ICT skills, for example, can improve job prospects.

ICT in Legal Education: In India legal education is regulated by the Advocates Act, 1961. This Act has provided for setting up of the Bar Council of India and State bar councils in the states. Advocates Act, 1961 empowered the Bar Council of India to fix a minimum academic standards as a precondition for the commencement of study in law. Bar Council of India is also empowered to recognise universities whose degree in law shall be taken as qualification for enrolment as an advocate and for that purpose to visit and inspect universities and colleges. The Act thus empowers the Bar Council of India to prescribe standards of legal education and recognition of law degree for enrolment of law graduates as advocates.

Legal education cannot exist in a vacuum, therefore development in legal education is necessary in accordance with the new means of information and communication technologies. Traditional way of teaching is no longer useful in inculcate the practical skills in students required to meet the challenges of competitive world of 21st century. Accordingly Bar Council of India in its Education Rules, 2008, emphasised the importance of ICT in law colleges and made it mandatory for every law college to provide at least 10 internet access points with desktop facilities and one online database in the library for the students.

Application of ICTs in Legal Education: Form the very beginning The Legal Profession is considered as a noble one. Hence, it is necessary to have the best Education System in Law.18 For many years the use of ICTs to teach law has been a minor concern among law schools and colleges. Due to this they face various difficulties such as, decline enrolment, decline job prospects for law graduates, inability of fresh law graduates to present their cases before courts etc. leading to shutting down of many law colleges. Against this backdrops technology offers attractive possibilities of making legal education more efficient and more effective. This is the reason that now a day's every law college is trying to be equipped with ICT facilities as much as possible.19 Some examples of application of ICTs in Legal field are as under:

Electronic Books: E-books are nothing but the digital version of printed books. In addition to textual matters, the e-books consist of hyperlinks, search facilities and multimedia capabilities. E-books compilers compile also the source files into an easy one to distribute life format like HTML, PDF and RTF files. In other words, an e-book has electronic text and that text is showed to the readers visually.

E-Journals: An e-journal is a periodical publication which is published in electronic format, usually on the Internet. Electronic journals have several advantages over traditional printed journals. Student can search the content page of the full text of journal to find article of their choice. They can read it anywhere in their laptops or even on mobiles so they don't have to be in the library. Students can save the journal in their desktops or laptops for future reference.

Electronic Legal Data Bases:

1. *Manupatra Online Legal Database:* Manupatra provides legal, taxation, corporate and business policy database which contain primary documents and analytical content covering commentaries, digests, bare acts, judgments and articles. It is fee based database having different subscription polices for different members of legal fraternity. It provides privileged access to its users and empowers them with in-depth legislative regulatory and procedural information critical for decision making in single online platform. It may be useful for law students for preparing their moot court problems as well as doing legal research as a part of their curriculum.
2. *LexisNexis Database:* LexisNexis® is a worldwide provider of content-enabled workflow solutions designed specifically for professionals in the legal, risk management, corporate, government, law enforcement, accounting, and academic markets. It provides customers with access to billions of searchable documents and records from more than 45,000 legal, news and business sources.

3. *Westlaw:* It is Thompson West's online legal research data base service. It provides quick, easy access to statutes, case law materials, public records, and other legal resources, journals and law reviews published from all around the world. The primary legal materials are available on jurisdictions of UK, USA and Commonwealth countries.
4. *SCC Online Web Edition:* It provides top quality information with an interface which makes legal research a quicker, easier and more effective process for the students or other legal professional. It has a collection of over 380 databases, with more than 3.4 million documents and over 16.7 million pages.
5. *Judgment Information System (JUDIS):* Judgment Information System Consists of the judgments of Supreme Court of India and several other High Courts. All Supreme Court reported judgments which are published in Supreme Court Reporter Journal since its inception i.e. 1950 till date are available.

Effective use of ICTs into teaching-learning process has the potential to engage the students. Various applications of ICTs such as audio-video aid to present practical legal problems can motivate and challenge students and thus enhance their analytical and problem solving skills. But for effective use of ICT in education, there is a need to change the attitude of teachers and students. For this purpose intensive and continues training of teachers regarding the use of ICTs in classroom teachings should be conducted periodically. To motivate the students regarding the use of ICTs in theory as well as in practical training, it should be made part of the curriculum. Computers and internet should be made available for the staff and students so that they can share and communicate with each other important information beyond the four walls of the classroom. Provisions for computer labs, WiFi, emails accounts should be emphasized in the colleges and universities for effective use of ICTs.

Use of IT in Education in times of Covid-19 Pandemic with special focus on Legal education: Online classes, webinars and master classes are a new normal for higher education. Legal education is not untouched with this phenomenon. However, the question is whether these measures are temporary or it would act as a catalyst for much desired reform in Indian legal education. Felix Frankfurter (1927) observed rightly, *"The law is what the lawyers are, and the law and the lawyers are what the law schools make them."* A robust system of legal education is a prerequisite for the "noble" legal profession. The Law Commission in its 266th report has emphasized the dire need for maintenance of standards in legal education, as the seeds of nobility of the profession has to be sown at this stage. Ironically, a large number of committees and commissions have already spilled a lot of ink on suggesting various reform measures with still existing concerns of fake degrees and colleges.

The Bar Council of India (BCI) under the Advocates Act 1961 is tasked with maintenance of standards of legal education which it has been fulfilling through the mechanism of inspection of universities/colleges awarding "degree in law" and prescribing standards for legal education. Historically, the legal profession in India has been rooted in formalism with its own procedures and requirements etched in letters of law. So has been the legal education, being delivered by traditional law colleges within their limited means. If one looks at the timeline of reforms, transformation in legal education in India has been a bit sluggish. The first major reform could be noted as an introduction of the 5-years' integrated law program offered by NLSIU Bangalore in 1986. It took about 10+ years for this reform to seep in,

when the next law school (NALSAR) came into existence. Now over the last decade, we have seen mushrooming of law schools in every state.

A set of private centres of excellence in legal education have also emerged during this period, which shows the way towards making legal education global in India. The lockdown due to Covid-19 has shaken everyone, including the legal profession and the centres of legal education. At this point, agility in quick adaptation of technology and exploring the tools available to transform the systems to function with social distancing is being experimented. Courts have moved to online hearings (only urgent matters as of now), arbitrations and mediations are happening online, clients are being counselled over Zoom.

While some legal professionals, being tech savvy, are enjoying and welcoming this, some are learning new technology and grappling with it, others are posing resistance to the thought of moving online post-Covid. It may be noted that use of technology in legal profession is not new. A transformation through Information and Communication Technology (ICT) enablement of Indian judiciary is being worked out since 2005. While the pace of reform has gained in the last few years with the Digital India campaign, measures like e-courts, national judicial data grid, etc., a full-blown transformation has not yet happened. This Covid situation, acting as a catalyst, now forces us to think upon the pace of this digital transformation in legal profession and, in turn, legal education. Rome was not built in a day, transformation will not happen in a day; however, if one keeps thinking like this, Rome will never be built. One has to begin thinking on future scenarios for using technology in the legal profession.

The seeds of transformation have to be sown in the present generation, which is preparing itself for the profession. Introduction of online learning mechanisms in legal education would be the need of the hour. There were three kinds of responses to the Covid-19 lockdown from legal educational institutions; (A) institutions with agility and reform mindset ramped up their already existing systems to serve students (B) institutions caught unaware by the situation tried to address the issue somehow with free online tools (C) institutions, which could not do anything, due to lack of agility, resources and, mostly, due to lack of reform mindset. I feel proud to be in Category A at UPES with a robust Learning Management System and trained faculty to handle the Hybrid Blended and Online (HBO) learning. We were able to engage students live in the online class rooms as per schedule, mentor them, and conduct their internal assessments and offer online examinations. However, in India, Category A is an exception, most of the institutions fell in Category B and many in Category C. Ramping up some institutions from Category B to A and bringing all institutions from Category C to B should be the focus of legal education reforms. While recommending this, one cannot lose sight of the fact that this country is diverse and there would be some strata of society not having access to resources. However, that should not act as a defence to throw the baby with the bathwater.

Challenges of using Information Technology as a means for Education: One has to think how the situation can be ameliorated and usefulness of digital transformation can be infused in the mindset. This would be the first step. Advantages of online legal education are plenty, not only for the advanced centres for legal education, but even for a law student staying in the remotest part of the country. I think technology has significantly enabled students in remote areas to access resource persons, literature and opportunities of internships online.

Who could have imagined that a student of law in Jharsuguda would be able to hear Harish Salve argue in the International Court of Justice at The Hague, or a student from a village in Darbhanga could do a course from Yale through Coursera or a course from Harvard University through edX. Today, a student can hear the who's who in the comfort of his/her house and even interact with them in many live sessions like Legally Speaking. UGC in its recent guidelines on "Examination and Academic Calendar in view of Covid-19 pandemic and subsequent lockdown" has emphasized the need for promoting online learning and suggests provisioning of virtual classroom and video-conferencing facilities, training of faculty on these platforms, preparation of e-content, and practice by the faculty to complete their 25% teaching through online mode in post-Covid situation as well.

It is a welcome step and should also be embraced by the Legal Education Committee (LEC) of BCI. As Albert Einstein once said, "In the middle of difficulty lies opportunity", this is the right time for the LEC of BCI to introduce reforms recognising the virtues of moving some part of legal education to the online mode and focusing upon legal education with an eye towards the future 5-10 years down the line. In coming days, we need legal professionals in plenty who could handle the situation in tough times and uphold the justice system serving the common man. It would be worth to end by quoting the Law Commission of India, "Legal education in India should be structured in a manner where the BCI, along with legal academics may endeavour to innovate, experiment and compete globally. A balance should be maintained in order to change the entire fabric of legal education system in India, keeping in mind the necessity of globalisation."

While the Technology is being used as a catalyst for change in the education system during this pandemic, it is not free from faults. The Organization for Economic Co-operation and Development (OECD) reports some sobering figures in this regard. 700 million students even have no internet access at home. It is even more sobering to find that half of the students kept out of the classroom by COVID-19 (close to 800 million students) do not have access to a household computer. 43% (some 700 million students) even have no internet access at home. Furthermore, about 56 million students live in locations that are not served by mobile networks.

It clearly shows that challenges in ensuring educational continuity do not stop with the deployment of digital solutions for distance learning. We also need to pay close attention that technology in education will not amplify existing inequalities and not deepen the digital divide. If we don't do that, students from disadvantaged backgrounds will remain shut out if schools shut down, particularly those students who lack the resilience, learning strategies or engagement to learn on their own.

The big challenge is to bridge the digital divide in education. To ensure digital technology provides equitable and inclusive access to education, we have to focus on closing such digital divides. Even where getting online is possible and affordable, extra efforts are needed to empower groups that are excluded. Projects such as Close the Gap that offer high-quality, pre-owned computers to educational projects in developing countries are just one example of how we can achieve this. We will discuss more challenges and opportunities on how to bridge the digital divide in education at the G-STIC conference.

The general challenges are as follows: The major disadvantages of Information Technology (IT) are:

- *Results in lack of interest in studying*- As everything is now accessible or through data saved in a computer or mobile devices, it develops poor study habits and lazy attitude among students through education. Now day's students are more dependent on internet instead of their books and input from the teachers.
- *Discover unusual things in the computer*- Internet do not always help students in search of things that are valuable for them. There are several things found in the internet that are not good for students. As a result student may lead to wrong path.
- *Hindrances academic performance*- Instead of using their laptops and tablets for their studies and online test students more often visit social networking sites which may lower their academic performance.
- *Expensive*- The IT facilities are not available in the schools. Most of the schools are not in a position to afford the purchase, maintenance and other expenditure involved in its use. The cost of laptops, wireless broadband projector for example contributes a large percentage of the school budget.
- *There is a widespread ignorance about the use, applications and advantages of IT* on the part of teachers, head of the institution and educational authorities responsible for bringing improvement in the functioning of the school particularly related to teaching learning and organization of co-curricular activities with the help of such technologies.
- *Today's teachers are not well-equipped with modern use of technology*. There is a great paucity of such competent and skilled teachers who can use and integrate right technology in an appropriate manner for effective integration of IT in dealing with school curriculum bringing desired change in the behaviour of the learners.
- The prescribed curriculum in schools, colleges and university, the examination and evaluation system, the available instructional material and the infrastructure are not in a position to provide desirable support for the use and application of IT in the teaching learning process and other useful activities for the benefit of the pupil.
- Lastly it can be said that lessons delivered online or through digital resources reduce the face-to-face interaction between teacher and student that provides a more personal experience.

Role of information technology in education: Most of the governments have shut down the educational institutes to avoid the infection ofCOVID-19. This nationwide shutdown is affecting around 72% student's population. UNESCO is providing support to many countries in continuing education through remote learning. This is encouraging the use of technology in the field of education. During this pandemic, distance and online education is developing and growing rapidly. There are many organizations who are trying to curate the education such as mEducation Alliance, INEE, UNESCO, Commonwealth of learning etc. Governments are opting for Home-schooling/ Home-education. Initially these changes might have caused inconvenience, but it has also given a new direction to education. Online learning platforms are the boon for education. Even though before COVID outburst too online training was getting used around the world at a large scale, during this shutdown it is being used the most everywhere school, colleges universities etc.

Role of Various Countries To Support Education During Covid-19 Pandemic: Major suffering countries around world are dealing with education during COVID outburst, using different tools and technologies. In china education department is involving the people in developing cloud based online learning platforms.In the same way Hongkong based forum (readtogether.hk) is providing more than 900 educational resources that includebook chapters, videos, assessment tools etc. Education innovation is getting so much attention now a day beyond the government funded projects. There are many private companies which are investing in this field. Google and Microsoft in US, Alibaba in China, Samsung in Korea are awakened to innovate new tools and techniques of education through digital media. Although most of the initiatives are relatively segregated and limited in scope, the COVID-19 pandemic pave a new path for very big scale industry collaborations to be formed around a common educational goal. It is seen by the study that only 60% of the students around the world can join online trainings, remaining were left behind. The major reason behind this is the cost of resources, unless the cost reduced the gapin education quality and socioeconomic equality will be more exacerbated. Many countries are working on Edu-Tech even before covid-19 pandemic because of following reasons1.Costless study material over the internet. Funding agencies supporting schools and connecting them with internet is challenging.

III. The World Bank Group Support to Education Through Ed-Tech : World Bank Group (WBG) works in collaboration with government and performs research work on ICTs (Information and Communication Technologies). It is working a lot to make leaning system robust and to reduce the poverty over the world. WBG provides supports for digital learning, teacher training, educational content development, skill development and R&D activities. During this pandemic, Information and Communication Technologies (ICTs) play very important role in providing innovating form of teaching and learning to the teachers and to the students. Determination of efficient tool to enhance learning and to increase the effectiveness of education system requires critical effort. If implemented properly, use of Information and Communication Technologies (ICT) in education would be very promising. Use of various software in online classroom allow students to learn at their own pace at the same time we have to face many challenges too for e.g. high cost, difficulties in implementation, increased burden of faculty. Also there are some subjects which are little tougher to learn online. Moreover many tools (Hardware and Software) are required with faster speed. Also internet has to be ubiquitous to make ICT successful. Below subsections presents challenges and guidelines provided by World Bank Group A.

Challenges: The World Bank Group is putting a great effort in collaboration with ministries of education of many countries for providing Ed-Tech solutions to the educational organizations while this closure due to pandemic. The guidelines provided World Bank Group presents the standard ways to design and execute remote learning. This learning includes resources such as web learning, learning through TV and Radio, and Mobile learning. Many countries have high quality teachers who can deliver their knowledge to fulfill standard professional expectations. They have pedagogical skills and expertise in their area. They know how to structure lesson planning, and teaching methods to meet individual's expectations. They make use of assessment tools in an effective way. The teachers may be very efficient, remote learning can generate additional challenges and

make teaching process complex as much effort is required to structure and present the contents through web. Teaching contents must be interesting and keep student engaging. While teaching session must be interactive so that students can feel the virtual presence of teacher. And the tools used for assessment should reflect the real learning of the students.

World Bank Group (WBC) Guidelines for Remote Learning: Although there is no standard way available to replace traditional classroom teaching experience, innovative approaches have to be used in respond to COVID-19 and to ensure continuous learning. In many areas of world people are from low income group and there is a lack of accessing high speed internet. There are following principle guidelines for the policy-makers to design remote learning.

i. Designing multipurpose learning model.
ii. Develop an inventory of digital contents that can be deployed through remote learning.
iii. Arrange E-contents in alignment with curriculum of respective university/college to make sure that the contents will meet the objective of the course.
iv. Develop a helpdesk (virtual) to support students and teachers for interaction and to solve the queries
v. Use printed study material at home (if physical distribution of the same is possible), if not then newspaper or social media can be used to provide materials.
vi. Radio education can be a good way of interactive verbal education. This is especially useful in the area where either broadband connectivity is not there or quality of it is very poor
vii. Recorded lectures of good quality teachers can be broadcast on Television. These recordings can be re-run by the students if he/she does not understand any part of lesson.
viii. Enhance the digital infrastructure and bandwidth to promote remote learning.
ix. For a particular syllabus, one portal must be there, where all the contents should be available to the students in a standard way that leads to ease of access.
x. Material should not be bound to one kind of devices. It should be diverse in nature and available through TV, mobile, Laptops and Tablets.
xi. Optimize the learning tools for low bandwidth which will be very helpful in current scenario.
xii. Instead of long lectures, short, crisp and quality lectures should be delivered online to engage all types of students.
xiii. Provide guideline manual to students and faculty to access the material from portal.

Distance learning E-sources:

*A Google Class room:*It is a virtual class room that is being used over all around the world. It allows teachers to structure various topics and then distribute study material under those topics. It saves the time, helps to communicate and keep the work organized. It also allows the students to give comments and ask queries. Teachers can grade students through assignments and quizzes. It has so many features and easy to use for both teacher and students. It is available free.

1. *A Thinkific:* Thinkific is a very famous E-learning platform. It allows the teachers/trainers to create their own courses then they can register the students in those courses freely or on payment basis. It is very user friendly and allows us to create unlimited courses. It provides us one month free trial and charges are taken around 49 Dollar/Month.
2. *Udemy:*This platform is already having more than 20000 subject matters created by the experts. It allows us to create course contents in many ways like PDF, PPT, video, etc. It provides self-paced video learning material. It already has registered more than 12 billion students till date. It takes 50% of the selling of the course from the trainer.
3. *LearnWorlds :*It allows us to create our own online training academy. It is a standalone learning platform. It also provides marketing tools. It allows us to create courses in very user friendly manner. It doesn't require technical skills. Other than study materials ,it also provides tools for assessment such as quizzes, assignments, grade book etc. It charges at least 29 Dollar/ Month fee from instructor.
4. *Skillshare*: It is also very popular learning platform. It contains around 24000 lessons of different subjects.it has more than 4 million students registered with it. It divides classes into four categories i.e. Creative arts, Technology, Business and Lifestyle.
5. *CourseraIt:*It provides great quality e-learning courses. It also provide certifications for various courses. Other than training courses it also provides degree courses. It directly deals with the universities and colleges and provides trainings to their students.
6. *Open-edX:* It is created by the team of Harvard University and MIT. It provides 8000 courses of around 100 universities. The courses are from the streams such as data science, computer science, humanities, business, math and engineering.
7. *G.WizlQ:* It is a self-paced; cloud based E-learning platforms. It allows for on demand webinars live to the users. It gives classroom like feeling to the trainers and to the students. Initially it allows for free trial then applies charges according to number of attendees.
8. *Teachable*: It is a very user friendly and easy online training platform. It provides easy solutions for uploading the E-contents. It also provides quizzes as assessment tools.

To avoid the educational loss caused by covid-19 lockdown, E-learning platform is the best solution. These E-Learning tools can be accessed through laptop, Mobiles, Tablets, and Smart TVs. Government of various countries encouraging educational institutes to use E-learning platforms so that they can recover from the losses caused by COVID-19outburst. In many developing countries there are poor areas where high quality broadband is not available. The government should make various plans to provide the good quality broadband in such area in this crisis. And make education available to everyone. Teaching trend has been changed; now and onwards digital platform will play very important role in all the teaching institutions.

How the Technology is helping us during pandemic: Epidemics and pandemics have been threatening the human race time and again. SARS, H1N1, Ebola, and more have shown their teeth in the past, but with each such outbreak, we are learning new ways of fighting and managing such unexpected diseases that can potentially kill millions of people. Technology cannot prevent the onset of the pandemics; however, it can help prevent the spread, educate,

warn, and empower those on the ground to be aware of the situation, and noticeably lessen the impact. Today, with converging technologies like mobile, cloud, analytics, robotics, AI/ML, 4G/5G, and high-speed internet, it has become possible to test several innovative approaches to pandemic response. Here, we have listed eight such areas where technology plays a vital role:

A. *Fighting misinformation:* Misinformation about the number of fatalities, diagnosis and treatment options, vaccines, medicines, government policies, etc., creates more panic and anxiety among the population. The result can be widespread chaos, panic buying, hoarding of essential commodities, price rise, violence on the streets, discrimination, conspiracy theories, and so on. In order to reduce false information, companies like Google, Facebook, and YouTube are working tirelessly to guide people to the right, verifiable information such as that published by WHO or local authorities and government. By making accurate information available to everybody, a transparent scenario can be created and the people can be informed about the right steps to take.
B. *Finding Drugs:* When a new pandemic strikes, the first question on everybody's mind is if there's a drug to cure it or a vaccine to prevent it. The world is now desperate to find ways to slow the spread of the coronavirus and to find an effective treatment. Technology is becoming an enabler to make the process faster. AI is playing important role in suggesting components of a vaccine by understanding viral protein structures, and helping medical researchers scour tens of heaps of relevant research papers at an unprecedented pace. Teams at the Allen Institute for AI, Google DeepMind have created AI tools, shared data sets and research results. In January, Google DeepMind introduced AlphaFold, a cutting-edge system that predicts the 3D structure of a protein based on its genetic sequence. The University of Texas at Austin and the National Institutes of Health used a popular biology technique to create the first 3D atomic scale map of the part of the virus that attaches to and infects human cells—the spike protein. AI Can Help Scientists Find a Covid-19 Vaccine.
C. *Increasing traceability and transparency by sharing data:* During a pandemic, clear messaging to the populace is critical to make sure they are informed and reminded to use appropriate precautions. Several groups are using the trending technologies like mobile, AI, ML and more, to provide visibility on the outbreak:
   Microsoft Bing launched an interactive COVID-19 map to provide widespread disease news. Sixfold has published a free live map of border crossing times for trucks to enable all of Europe's supply chains to understand expected delays in receiving shipments. Social platform like TikTok has partnered with WHO on COVID-19 to help keep their users knowledgeable with correct, timely facts, along with a live stream from the WHO where users will be able to ask questions and seek answers. Taiwan CDC central epidemic command centre (CECC) is combining health data with the travel data, to build a monitoring system and provide real-time alerts. Sending automatic alerts during clinical visits if they have travelled to the infected vicinity can serve as an example. In India, telecom operators like Jio, BSNL, Airtel, and more, are using the caller tunes to spread awareness about the pandemic.
D. *Tracking people with facial recognition and big data:* In case of pandemic management, big data analytics can help in quickly identifying infected individuals, connect with them, track who they have come in contact with, and so on. Facial

recognition technologies along with data can accurately identify people even if they are masked. Such technologies can help in monitoring movement and tracking of people who are quarantined. It can also help in keeping a tab on people and ascertaining whether or not they have been in contact with an infected person. CCTV cameras along with facial recognition technologies can help in identifying infected people who break the rules and step out despite being quarantined.

How China is using Big Data & AI to fight the Corona virus? Risk assessment and forecasting through artificial intelligence are now used by China. AI is becoming a vital part of healthcare today. AI-based data analytics and predictive modeling are enabling medical professionals to understand more about a lot of diseases. With the use of AI, more accurate forecasting about disease spread, medication, treatment, etc., could be done. Using AI platforms, it has become easier for researchers to quickly find relevant studies that can potentially lead to new insights or approaches to address the COVID-19 outbreak. AI-based risk assessment tools are being designed by AI research companies to provide clarity amongst the confusion caused by the pandemic. These AI tools are helping in differentiating whether the patients have a common cold, flu, or COVID-19, whether or not the individual needs to be tested, and what tests are required.

Baidu, a Chinese multinational technology company, has built AI-based solutions to effectively screen large populations and detect a change in their body temperature while they are on the move. This system can examine about 200 people per minute without disrupting the flow of people. Such technologies can be implemented in crowded areas, hospitals, train stations, airports, etc., to identify sick people quickly and quarantine them before they infect a larger population.

Contact-less movement and deliveries through autonomous vehicles, drones and robots: Self-driving cars, drones, robots can all help at a time when the need is to avoid human contact. Autonomous vehicles can be used to transport affected people to and from healthcare facilities with ease, without risking the lives of healthy people. Robots can be used for delivering grocery, cooking means, sterilizing hospitals and patrolling the streets. Drones can be used for food deliveries, tracking population, carrying test kits and medicines to quarantine locations, thermal imaging to identify infected people, spraying disinfectant, and more. Many new areas and use cases are coming up where drones, robots and autonomous vehicles are being used.

Drones and Autonomous Robots used to fight Coronavirus in China: Technology supported temperature monitoring. The wireless thermometer guns and other similar infrared body temperature measuring devices have become the most important medical equipment that are being used at checkpoints of offices, airports, hotels, hospitals, train stations, shops, and other public places. These technologies assist in measuring the body temperature from a distance and turn out to be effective in pinpointing the individuals who might need further investigation. Automated thermal monitoring along with facial recognition is making the process faster and more effective.

Remote working technologies to support social distancing and maintain business continuity: As pandemics or other calamities keep threatening the business world, working from home ensures business continuity as well as facilitates social distancing. In such a scenario,

technologies that enable secure access to data, enterprise applications, virtual meetings, cloud conferencing, and virtual/mixed/augmented reality are the forefront leaders to ensure deliverables are not impacted. Remote working is a blessing that comes due to technology and is of one the greatest solution that helps us in social distancing.

Conclusion: It is a recognized fact that the application of Information Technology (IT) in our daily life has changed dramatically over the past couple of years. Information technology is used in every sphere of life like education, communication, business, commerce, treatment and banking etc. Businesses are investing heavily into new technological trends as well as offering businesses the chance to operate more effectively through the application of information technology.

Let's look at the example of communication as it has definitely changed the way of our daily life. Many years ago we used to communicate via writing but now we communicate by using information network like telephone, mobile phone, internet etc. The application IT has changed considerably as we can now communicate via text message, email and communicating via instant messaging on MSN messenger, Facebook and even in the form of Tweets on Twitter. So, it has significantly changed the world's communication over time. IT has changed tremendously over the years especially in the computing field. Nowadays, more or less every household has an iPod or computer or some Apple related product. We know have cloud computing, as well as Virtual servers. Long have the days of needing your own server to run things. You can now involve in online outsourcing. Staying in the east you can work in the west and earn a large amount of dollar.

It has brought a new dimension in the field of education. We can get any type of information staying at home when we need. The famous books of the world are available and easily accessible via internet. Everyday we are now getting new and new information with the help of information technology. IT is now used in E-banking system. We can perform our banking activities via online. At present, IT has also turned a tremendous effect in the field of treatment. Information technology in the modern world has evolved so much that you can enjoy it in all the places. Think about cars with satellite navigation built in, think about climate control, and think about digital displays within your vehicle- these all have been possible by information technology.

It has even changed the way we buy things. Long have the days gone that you needed a cash machine or ATM to withdraw cash and purchase everything with cash. Now, you can purchase using a PDQ machine/ Chip and Pin machine or credit card. It has definitely made our lives so much easier. IT has introduced the internet system and turned a new era in the field of E-commerce. E-commerce is a system of buying and selling goods through online. With extremely busy lifestyles and a lack of time, E-commerce has changed the way we purchase things. It has changed so much that businesses are forever investing in online strategies from online shops to Search Engine Optimization and Search Engine Marketing strategies.

The application of information technology in our daily life has definitely changed the way we live our lives. Long have the days we communicated solely face to face. Long have the days we needed to invest in servers for our business. The application of IT has definitely changed the way communication, commerce, business, education as well as the way we lead

our lives. Not only that, the Information Technology is helping us cope with the '*new normal'* vis-à-vis the Covid-19 Pandemic. It has revolutionized not only the education industry but it has hugely impacted the healthcare facilities, aviation industry, legal industry, E- commerce industry to name a few. As a whole, the IT is helping the economy to restore it back to its former glory.

Today the greatest risk of worldwide catastrophe is pandemic, an enormously infectious virus that's more devastating and may kill many people. The transparency that we have gained through this current COVID-19 situation, we now understand that we were not geared up for this pandemic situation. The next pandemic is not a matter of "if it happens", but "when it happens", would we be prepared in advance against the pandemic at an individual and collective level. What we actually need is preparedness. Indeed, the technology has advanced more and will continue to advance exponentially, but the human institutions and societies need to accelerate in adapting to it and continue investing in building the technology systems for the preparedness. After the COVID-19 outbreak, it is evident that, from AI to robotics, the technology innovations are helping to manage the epidemic and better equip to fight future public health emergency in a timely, systematic, and calm manner.

MODULE-II

INTRODUCTION TO INFORMATION TECHNOLOGY LAW: INTERNATIONAL LAWS

MODULE-II: INTRODUCTION TO INFORMATION TECHNOLOGY LAW: INTERNATIONAL LAWS

International technology law: Information technology law provides the legal framework for collecting, storing, and disseminating electronic information in the global marketplace. Attorneys practicing in this area of the law represent individuals and businesses from all different industries. They help structure information technology transactions in a way that maximizes the client's economic benefit while ensuring regulatory compliance. A great deal of emphasis is also placed on anticipating potential sources of dispute between the parties to a transaction, and crafting agreements that address these concerns, thereby reducing the risk of litigation.

When disputes arise in the field of information technology that cannot be resolved outside of the court system, a lawyer specializing in these types of cases can prove a powerful advocate compared to a general legal practitioner. Information technology law firms tend to hire lawyers with practical experience working in the industry prior to entering the legal profession. With such a background, a lawyer is more effective at explaining technical concepts to a judge or jury, and he or she will likely have contacts within the industry that make finding consultants and expert witnesses less difficult.

In any field of human activity Success leads to crime that needs mechanisms to control it. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe. Recently, many information technology (IT) professionals lacked awareness of an interest in the cyber crime phenomenon.

In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn’t quite fit the crimes being committed, new laws hadn’t quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy—or at the least, distrust— between the two most important players in any effective fight against cyber crime: law enforcement agencies and computer professionals.

Yet close cooperation between the two is crucial if we are to control the cyber crime problem and make the Internet a safe “place” for its users. Information is a resource which has no value until it is extracted, processed and utilized. Information technology deals with information system, data storage, access, retrieval, analysis and intelligent decision making. Information technology refers to the creation, gathering, processing, storage, presentation and dissemination of information and also the processes and devices that enable all this to be done. Information technology is affecting us as individual and as a society. Information technology stands firmly on hardware and software of a computer and telecommunication infrastructure. But this is only one facet of the information Technology, today the other facets are the challenges for the whole world like cyber crimes and more over cyber terrorism.

When Internet was first developed, the founding fathers hardly had any inkling that internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulations. With the emergence of the technology the misuse of the technology has also expanded to its optimum level. The misuse of the technology has created the need of the enactment and implementation of the cyber laws. As the new millennium dawned, the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with the criminal element. According to Donn Parker , *"For the first time in human history, computers and automated processes make it possible to possess, not just commit, a crime. Today, criminals can pass a complete crime in software from one to another, each improving or adapting it to his or her own needs."* but whether this cyber laws are capable to control the cyber-crime activities, the question requires the at most attention.

Until recently, many information technology (IT) professionals lacked awareness of and interest in the cyber-crime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy—or at the least, distrust—between the two most important players in any effective fight against cybercrime: law enforcement agencies and computer professionals. Yet close cooperation between the two is crucial if we are to control the cyber -crime problem and make the Internet a safe "place" for its users.

Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice. IT personnel understand computers and networks, how they work, and how to track down information on them. Each has half of the key to defeating the cybercriminal. IT professionals need good definitions of cyber-crime in order to know when (and what) to report to police, but law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offense. The first step in specifically defining individual cyber-crimes is to sort all the acts that can be considered cyber- crimes into organized categories.

Legal Aspects of International Information Security: The technological progress has led to radical changes in the contemporary world. The system of international relations changed. The development of information and communication technologies (ICT) has affected all the areas of public life including the economy, politics, social issues, and culture, bringing them together in the framework of establishment of an information society. By the present time, the information society concept has been represented in a number of international documents among which are the Declaration of Principles entitled "Building the Information Society: a Global Challenge in the New Millennium" (hereinafter referred to as the 2003 Declaration) and the Plan of Action of the World Summit on the Information Society of December 12, 2003.

Information society is a more general category as compared to the global information society. It can be established within a single state or at the regional or global levels. At the global level, it will be referred to as the global information society.

The global information society can be defined as a system of international relations that are established in the sphere of operation of information systems, which are based on information and communication technologies, in which international information relations affect political, economic, social, and cultural relations. At the same time, the states participate in relations in the global information society as equal subjects of international information relations. The development of ICT is related to the effect on established branches and institutes of international law as well as to the regulation of new relations that arise as a result of ICT development. The most complicated problem is the effect of ICT on established branches and institutes of international law. The mechanism for the development of international law provisions is such that legal regulations tend to "fall behind" the level of ICT development.

Currently, the spreading and use of ICT affect the interests of the entire international community; these technologies can potentially be used for purposes that are incompatible with the objectives of international stability and security and can have an adverse effect on the integrity of the infrastructure of the states, disturbing their security in the civil and military areas. The efforts of individual states are insufficient for ensuring international information security. First of all, the prohibition on the use of information weapons by states must be established in international law. Separate regulation is required for matters of information security of individuals (protection from defamation and privacy).

The forming special principles of international information law include the principle of confidentiality and security in using ICT. Strengthening the trust framework, including information security and network security, authentication, privacy, and consumer protection, is a prerequisite for the development of the information society and for building confidence among users of ICTs. A global culture of cyber security needs to be promoted, developed, and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber security, it is important to enhance security and to ensure the protection of data and privacy while enhancing access and trade. In the 2003 Declaration, the term "cyber security" has a wider meaning that only protection from cybercrimes. In particular, the Declaration notes that the summit participants support activities of the United Nations to prevent the potential use of ICTs for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within states, to the detriment of their security.

These regulations ensure the relation of the developing principle of international information law with the existing principles, namely, the principle that the exercise of freedom of opinion, expression, and information is an essential factor in strengthening peace and international security; the principle that the media should contribute to the strengthening of peace and international understanding and to the struggle against racism, apartheid, and incitement to war; and the principle of the need to publicize the denunciation of information, the spreading of which has caused damage to efforts of strengthening of peace and

international understanding, the development of human rights, and the struggle against racism, apartheid, and incitement to war.

The problems of information security of individuals and legal entities have been examined in fundamental research on the comparative law of information technologies by Bainbridge, Campbell, Rowland and Macdonald , Smedinghoff, and Black.

The issue of privacy protection, primarily using national legal instruments, has been covered in particular chapters in the fundamental research on the law of information technologies by Bell and Ray, Reed , and Angel and special research by Solove and Nouwt, Berend, and Prins .

Technical and organizational aspects of ensuring information security have been covered in the works of Egan and Mather, Hunter , and Volonino and Robinson. The matter of implementation of the concept of ensuring international information security has already been considered in research, although the concept itself has not been stipulated. Lloyd considered the acts of the UN, the Council of Europe, OECD, and the Asia-Pacific Community when addressing the issues of privacy, primarily considering "soft law" acts. In a review of cybercrime problems, this author gives a brief overview of the Council of Europe Convention on Cybercrime, the OECD Guidelines for the Security of Information Systems, and the EU acts.

The contents and significance of the Convention on Cybercrime of November 23, 2001, have been discussed in the studies by Lloyd, Murray, and Koops, Lips, Prins, and Schellekens . But these studies did not cover the problems of using the experience of the Council of Europe at the global level. With regard to the 2001 Convention, Hopkins has noted its excessive broadness and lack of clarity in its basic terms. For example, this Convention defines a computer system as any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. In such case, the term device will include children's toys, Palm Pilots, and cable television devices. Therefore, the scope of the 2001 Convention extends from real computer crimes to interference in any devices where software is used.

The concept of personal data in international acts has been criticized in the legal doctrine. In particular, Berčič and George state that this definition is too broad because any information about a person can be regarded as personal data (e.g., information that an individual is wearing a red shirt). On the other hand, there arise practical complicacies with attributing certain data as personal data (e.g., social security identification numbers). Polcak has pointed out that in various European countries, there are complicacies with attributing IP addresses, personal telephone numbers, data entered anonymously when receiving services via the Internet, and data of deceased persons as personal data.

The absence of unified list of personal data in the national legal systems is the reason of the imperfection of the international legal regulation. The efforts made in the area of harmonization have not been successful enough. This is confirmed by the attempts that are being made at the national level to create an own definition of personal data. In particular, a number of authors have named the Durant v. FSA case in British courts as an example. In this case, the Court of Appeals has defined personal data as information that affects the

privacy of the data subject including their personal and family life and business or professional abilities.

It should be noted that currently, proposals to make global international treaties primarily come from non-state actors. In August 2000, a group of researchers from Stanford University presented the Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (the Stanford Project). Brown drafted a convention regulating the use of information systems in armed conflicts. On November 6, 2009, the International Conference of Data Protection and Privacy Commissioners adopted a resolution entitled "Standards of Privacy and Personal Data," for which it established a work group to develop a draft global treaty and listed the criteria for the drafting of it. It is planned to submit the developed sections of the treaty to the UN. Thus, researchers and international forums are proposing specific projects, but no systemic work is carried out in the framework of the UN, International Telecommunication Union (ITU), or UNESCO.

At the same time, there are no monographic researches of the general concept of international information security that would cover the regional and global levels and the problems of development of its legal basis. The present study, based on the analysis of international acts, reveals the content of the general concept of international information security that would cover the regional and global levels. "Soft law" acts are appropriate for the formulation of the general concept of international information security, but not for its implementation. Therefore, the author proposes a draft convention with the purpose of creating of global network of information security.

Analysis of international acts: The objective of the research is consideration of the international information security concept that has developed at the global and regional levels and formulation proposal for elaboration of legal instruments for its implementation in connection with the concept of the global information society. For this, the analysis of existing international information security system at the global and regional levels shall be made, a description and a generalization of the analysis results. For the analysis of existing international information security system, formal-logical, systemic-structural, and problematic-theoretical methods have been used. At the same time, comparative-legal method is used to analyze the provisions of information security at the global and regional levels.

In order to solve the problems of international security that have arisen with the development of ICT, the UN General Assembly has adopted resolutions entitled "Developments in the field of information and communications in the context of international security" at each of its sessions since 1998. The main idea of these resolutions is that the significant progress, which has been achieved in the development and implementation of the latest information technologies and telecommunications, has caused negative consequences as well as positive ones. At the same time, the positive consequences, namely, new opportunities for the entire mankind, are obvious.

However, the UN General Assembly has expressed concern that new technologies and facilities that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of states to the detriment of their security in

both civil and military fields. The resolutions invite states to inform the UN Secretary-General on the following issues, namely, (1) general assessment of the problems of information security, (2) development of concepts relating to information security, and (3) development of international principles aimed at ensuring information security of global information and telecommunications systems and combating information terrorism and crime.

It should be noted that there exist resolutions which confirm a certain progress in ensuring information security. They contain specific proposals for the development of an information security system that can be used for the draft of relevant international treaties. For example, the UN General Assembly adopted the Resolution No. 58/199 of December 23, 2003, on the creation of a global culture of cybersecurity and the protection of critical information structures, which defines elements for protection of critical information infrastructures, namely, (1) having emergency warning networks regarding cyber-vulnerabilities, threats, and incidents; (2) raising awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them; (3) examining infrastructures and identifying interdependencies among them, thereby enhancing the protection of such infrastructures; and (4) promoting partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures, etc.

The nature of the elements for protection of the most important information structures is such that they can be included in an international treaty if they are specified. Currently, an institutional mechanism for ensuring international information security has been established in the framework of the UN. States submit their assessments of the condition of information security on a regular basis, which are included in the reports of the Secretary-General and have contributed to a better understanding of the essence of problems of international information security and related concepts.

The work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the resulting report (2015) have been quite effective. The Group concluded that international law and, in particular, the Charter of the United Nations are relevant and important for the maintenance of peace and stability and the development of an open, safe, stable, accessible, and peaceful information environment; that voluntary and non-binding standards, rules, and principles of responsible behavior of states in the use of information and communication technologies can mitigate the risk of violation of international peace, security, and stability; and that, subject to the unique features of the information and communication technologies, more standards can be developed over time.

In addition, the EU, OAS, and Caribbean Community (CARICOM) have achieved certain results in the development of regional concepts of the improvement of information security. For example, on February 7, 2013, the Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions entitled "Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace" was adopted. The strategy contains principles for cyber security, strategic priorities, and actions. The principles of cyber security include the principle that the EU's

core values apply as much in the digital as in the physical world; protecting fundamental rights, freedom of expression, personal data and privacy; access for all; democratic and efficient multi-stakeholder governance; and a shared responsibility to ensure security.

In order to support member states in their fight against cybercrime, OAS, through the Inter-American Committee Against Terrorism (CICTE) and the Cyber Security Program, is committed to developing and furthering the cyber security agenda in the Americas. Cooperating with a wide range of national and regional entities from the public and private sectors on both policy and technical issues, the OAS seeks to build and strengthen cyber security capacity in the member states through technical assistance and training, policy roundtables, crisis management exercises, and exchange of best practices related to information and communication technologies.

CARICOM Ministers with responsibility for information and communication technologies met on May 19, 2017, as efforts continue to move on the establishment of the CARICOM Single ICT Space. Several preparatory meetings of officials were held to advance work on the Integrated Work Plan for the Single ICT Space and the draft Terms of Reference for the CARICOM-US Joint Task Force. The Integrated Work Plan will set out the activities that need to be completed for the development of the Single ICT Space. The activities of the work plan will focus on areas such as conducting gap analyses, public awareness, specific telecommunications issues, legal and regulatory reform for cyber security, bringing technology to the people, resource mobilization, as well as forecasting for the CARICOM Digital Agenda 2025. The Single ICT space and the Region's Digital Agenda 2025 will be constructed on the foundation of the Regional Digital Development Strategy (RDDS) which was approved in 2013 and will also have inputs from the Commission on the Economy and the Post-2015 Agenda.

The concept of international information security is developing in the framework of soft law. International treaties in this field are quite scarce. The privacy problem has been represented in the international law. Currently, the privacy provision is contained in many international documents. Of particular importance is Article 12 of the 1948 Universal Declaration of Human Rights, which stipulates that no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. States recognize noninterference in personal and family life as a fundamental human right. It should be noted that the 1948 Universal Declaration is a recommendatory act, but a number of its provisions represent the established international customs. At the same time, the right to protection of private life may be restricted, which makes it impossible to regard it as a right that is recognized unconditionally.

Currently, the protection of privacy has a treaty origin. Provisions for protection of privacy are stipulated in Article 17 of the 1966 International Covenant on Civil and Political Rights, Article 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms, and Article 11 of the 1969 American Convention on Human Rights.

Article 12 of the 1948 Universal Declaration of Human Rights has been incorporated into Article 17 of the 1966 International Covenant on Civil and Political Rights. Everyone has the

right to the protection of the law against such interference or attacks. Similar provisions are stipulated by regional international treaties.

It appears quite reasonable to abolish the unification of the concept of privacy and personal data as a component of privacy in international law. Privacy is an area where individual needs of a person to be left to himself/herself are revealed. Every individual will delineate the limits of his/her privacy to himself/herself. Contemporary international law is limited to the regulation of matters of collection, processing, storage, and transfer of personal data, which are not the only issues of privacy. It appears that the privacy provision in the International Covenant on Civil and Political Rights is quite generalized but does not require specification in the information age, as it enables any individual to protect privacy in every case when the individual so wishes.

The problem of personal data protection in the framework of information security problems is perfectly reasonable to be considered. Information security is a category applicable to all subjects of information relations including states and non-state (legal entities, individuals, TNCs, nongovernmental organizations, etc.) ones. Information security of individuals is related to the respect of their privacy in the information sphere, protection from defamation, libel, insults, psychological pressure, information terrorism, etc. Therefore, the legal problems of privacy in the information sphere are a component of legal regulation of information security of the individual.

If one tries to define the content of privacy in the information area, it will be different for every individual. In the information sphere, the range of data that a person tries to make inaccessible to the public is always different. For example, one person will not hide the fact that they are infected with HIV and may say it in an interview to a journalist, while another person will choose to not even tell close friends about it. Thus, the boundaries of privacy are always individual. Contemporary international law provides limited privacy protection because it cannot adapt to the needs of each individual due to the general nature of the provisions. At the same time, the current international acts do not contain a list of personal data but give a fairly wide definition of such data.

An identical approach to the definition of personal data is characteristic of the OECD Guidelines governing the Protection of Privacy and Trans-border Flows of Personal Data of September 23, 1980, and the 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. In these documents, personal data are defined as any information relating to an identified or identifiable individual. Therefore, protected data include any information about an individual that can be identified. Such a broad range of protected information makes it possible to protect personal data in the situation of changing technologies that are used to collect and process data. In particular, protected data include PIN codes, logins, passwords, etc.

Despite the quite broad definition of personal data in international documents, the concept of personal data is somewhat narrower than privacy in the information area. Based on the provision of the Universal Declaration, the concept of privacy includes not just personal but also family secrets as well as the secret of correspondence. Personal data only relate to data about identified or identifiable individual. Certain provisions are applied only to individual, information on whom is stored in a particular system. For example, the 1981 Convention

stipulates that any individual has the right to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention; etc.

Therefore, the right to access, correct, and destroy personal data is recognized only for the person whose data have been collected. However, family secret is a different term. For example, one may conceal data about a disease of one's child or husband or addictions of deceased relatives. In essence, while personal data relate to one person, family secret is kept in a certain family and affects its collective private interests. Disclosure of family secret can harm both individual and the family as a whole including family breakdown and ruined relationships.

The existing special international acts that protect personal data in the course of their automated processing contribute to protection of not just personal but also family secrets. However, they offer no direct protection of family secrets.

As for the confidentiality of correspondence, certain provisions for telecommunications are contained in the Convention of the International Telecommunication Union. Article 40 of the ITU Convention provides for the secrecy of telecommunication messages. Government telegrams and service telegrams may be expressed in secret language in all relations. Private telegrams in secret language may be admitted between all Member States with the exception of those which have previously notified, through the Secretary-General, that they do not admit this language for that category of correspondence. Member States which do not admit private telegrams in secret language originating in or destined for their own territory must let them pass in transit, except the Constitution. ITU does not have the power to regulate information on the Internet including measures for ensuring its confidentiality. At the regional level, a provision on the confidentiality of electronic communications is stipulated at the EU. The relevant provision is contained in the Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The most progressive in privacy protection is the EU experience. This integration organization has adopted the Regulation No. 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing the Directive 95/46/EC (the General Data Protection Regulation) of April 27, 2016. This act is of direct effect and application in the EU Member States. A feature of the General Regulation is that any processing of personal data in the context of the activity of establishing a controller or data processing entity in the Union must be performed in accordance with the Regulation regardless of whether the data processing is affected within the Union. In order to ensure that individuals are not deprived of the protection provided by the Regulation, processing of personal data of data subjects located in the Union by a controller or data processing entity that have not been

established in the Union must be governed by this Regulation if the data processing relates to the supply of goods or services to such data subjects regardless of payment.

The Regulation establishes a certain legal regime for personal data processing including the conditions for their processing and requirements to their storage and transfer. The processing of personal data by public authorities, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), providers of electronic communication networks and services, and providers of security technologies and services is a legitimate interest of the relevant data controller to the extent that it is necessary and adequate as compared to the objectives of providing network and information security, i.e., the ability of the network or information system to resist (with a given level of confidence) accidental events and illegal or intentional acts that compromise the availability, authenticity, integrity, and confidentiality of stored or transferred personal data as well as the safety of the relevant services transferred via such networks and systems. Protection of privacy within the EU is also supported by the EU Court. In the *Maximillian Schrems v. Data Protection Commissioner case* (complaint No. C362/14), the transfer of personal data by Facebook in the USA was appealed against in the framework of the Principles of Privacy program. The EU Court concluded that the Commission had not stated in its Resolution that the USA had actually provided an adequate level of protection by virtue of their laws or international obligations. Therefore, without having to examine the content of the Principles of Privacy, Resolution 2000/520 did not comply with the EU acts in the field of privacy and is therefore invalid.

However, the EU experience takes account of the patterns of functioning of integration organizations and requires significant adaptation for use at the global level. At the regional level, two conventions have been adopted where computer crimes are regarded as crimes of international nature. These are the Convention on Cybercrime of November 23, 2001 (hereinafter referred to as the 2001 Convention) and the Commonwealth of Independent States Agreement on Cooperation in Combating Offenses related to Computer Information of June 1, 2001 (hereinafter referred to as the CIS Agreement).

The basic ideas of these conventions are the definition of unified elements of computer crimes, which the states should include in their national law, and development of measures for combating such crimes. The CIS agreement has no definition of a computer system whatsoever, which results in an uncertainty with regard to the object of infringement. Both the 2001 Convention and the CIS Agreement contain definitions of computer data. However, the definition in the Agreement is more concise; namely, it is information stored in computer memory, on machine or other device, in a form that is accessible to perception or transfer via communication channels. This definition is incomplete.

The 2001 Convention offers a broader concept; namely, computer data includes any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function. As a result, the CIS Agreement does not cover any software that is inaccessible to human perception but causes computer systems to operate. Interference in such software is dangerous for the public. In this case, the broader approach in the 2001 Convention should be considered justified.

The CIS Agreement contains an attempt to define computer crime, which cannot be regarded as successful. A crime in the field of computer information is described as a criminal offense, the object of infringement in which is computer information. This definition is different from the definition that has been accepted in the doctrine. It is not mentioned that computer information can be both the object and the means of an offense. The 2001 Convention contains a number of terms that are unknown to the CIS Agreement, namely, service provider and data flows. The need to use these terms is due to the fact that the 2001 Convention defines a broader range of measures for combating computer crime than the CIS Agreement.

As for standardized elements of computer crimes, they are different in the 2001 Convention and the CIS Agreement. Some crimes have the same title but different meanings. For example, the 2001 Convention and the CIS Agreement state that illegal access to information is a criminal offense. However, the CIS Agreement is very laconic. It regards illegal access to information that is protected by law as a criminal offense if such act has caused destruction, blocking, modification or copying of information, or disruption of the operation of computers, computer systems, or their networks. The 2001 Convention stipulates that illegal access to a computer system as a whole or a part of it is a crime by itself, without stating any extra qualifying features. Therefore, the 2001 Convention prosecutes any illegal access to computer systems, while the CIS Agreement is limited to access that has led to certain consequences.

The 2001 Convention includes a number of crimes that are not covered by the CIS Agreement. These are illegal data interception, data and system interference, misuse of devices, computer-related forgery, computer-related fraud, and crimes related to child pornography. A special feature of the 2001 Convention is that it covers certain common crimes (forgery, fraud) which become much more dangerous because they are committed using computers.

Therefore, the CIS Agreement uses a narrower approach to the concept of computer crime. These are only the crimes that infringe on the security of computer systems, i.e., the protected object is computer systems as such. The 2001 Convention criminalizes a broader range of acts where computer systems can be the object of or the means for committing the offense. The approach to the definition of computer crime in the 2001 Convention is more correct. The existing contradictions in the content of international treaties on combating computer crime may result in difficulties for the states that are parties to both treaties. Basically, the provisions of the two treaties are mutually exclusive, which complicates their simultaneous application.

It should be noted that the 2001 Convention contains references to a number of international treaties. The issues of the relationship between the 2001 Convention and the CIS Agreement shall be resolved with consideration of clause 2 of Article 39 of the 2001 Convention. If two or more parties have already concluded an agreement or treaty on the matters dealt within this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where parties establish their relations in respect of the matters dealt within the Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention’s objectives and principles. Therefore, in

the case if a state is a party to both of the abovementioned international treaties, the CIS Agreement will apply to the same matter.

Article 13 of the CIS Agreement stipulates that this agreement does not affect the rights and obligations of the parties arising out of other international treaties to which they are parties. Therefore, it allows the application of the 2001 Convention. The existence of various regulations regarding their correlation in the considered international treaties suggests that their practical application may be complicated. For example, the states may experience difficulties in choosing the legal aid procedure. Such issues should be resolved by consultations between the states concerned. However, in view of the harmonization nature of international treaties and the fact that the content of the 2001 Convention is broader, in the case if a state is a party to the two treaties at the same time, such state shall implement the 2001 Convention and, in the part where the provisions of the treaties are different, the CIS Agreement, as this is allowed by the 2001 Convention itself.

Proposal for global network of information security: The concept of developing a comprehensive system of international security is useful because of its systemic nature. This concept is not limited to military security issues but also covers economic, political, humanitarian, and information security. It should be noted that this concept needs to be clarified. Since it concerns the development of a comprehensive system of international security, it should cover the entire system of international relations. The concept of developing a comprehensive system of international security also applies to non-state international relations.

A comprehensive system of international security means a status where the interstate system is protected from the dangers that exist in contemporary world. It implies stable functioning of the system of international relations. Relations between subjects of the interstate system also include information relations. The system of such relations includes interstate and non-state relations.

Information security should be considered in two aspects: If the systemic approach is applied, information security will act as a backbone element. It can be regarded as a status of the international relation system, which is described by stability and security from information weapons and threats. In addition, information security can be regarded as an ideal model. There are conceptual ideas what exactly information security should be like. It is regarded in the sociological (as a certain state of social relations), technical (compliance with standards and other technical requirements), and legal (compliance with prohibitions and restrictions on the spreading of data) aspects. Based on conceptual ideas, information security can be defined as a model for stable functioning of the information relation system.

The comprehensive system of international security and information security has a certain sphere of intersection. Information security of the international system is a component of the comprehensive system of international security. However, international relations are more than just relations between subjects of international public law. The requirement of information security is equally applicable to international non-state and domestic relations.

When one uses the concept of international information security, one may define this concept based on the more general concept of information security. If one distinguishes between

domestic and international information security, the first one relates to domestic information relations and the second one, to international information relations. In each of the systems of relations, information security has common features; namely, it serves as a backbone element and ensures a stable state of the system of information relations. Therefore, international information security is a status of the international information relation system, which is described by stability and security from information weapons and threats.

The development of the concept of international information security has led to the appearance of terms in the legal doctrine that had not previously been known in the practice of states. Currently, researchers use terms such as information weapons, information terrorism or cyberterrorism, and information crime or cybercrime. The state of international legal regulation is such that these new terms have not been stipulated in treaties (save for computer crimes). However, a number of social phenomena evidence that these terms should be regarded as destabilizing factors for the system of international relations.

As for information weapons, they can be described quite generally as any means of affecting the mass and individual consciousness, which can damage, distort, destroy, or conceal data. A special feature of information weapons is that they are not used in the military field alone. Information weapons can be used for committing computer crimes, hacker attacks causing property damage, etc. The use of information weapons has been known in international practice since the second half of the twentieth century. For example, it was used widely in the Palestinian-Israeli conflict.

With the adoption of individual conventions on cybercrime, there appeared a trend in international law to prosecute the consequences of the use of information weapons rather than the weapons as such.

It should be noted that the use of information weapons has various scales. For example, information terrorism can be regarded as one of the most dangerous use of information weapons. Information terrorism can be defined as using information weapons for undermining the constitutional order of other states or the international legal order and international relations in general.

Cyberterrorism comprises both direct terrorist activities with the use of computers, networks and data in networks, and various supplementary operations including coordination, preparation, and organization of terrorist activities using networks and data in networks and spreading knowledge about terrorism and terrorists' skills. Individual examples of cyberterrorism have been known from the second half of the twentieth century. In 1985, a radical leftist group in Japan attacked the united railway management network using computer systems. Fortunately, the computers of the railway had good protection, which could not be hacked. The 2001 Convention takes no account of the special features of cyberterrorism. It only takes account of "ordinary" crimes.

However, in the international law, the term computer crime will always have a special meaning, which is not necessarily the same as the meaning of this term in the national law. Some crimes that are punishable under the laws of one state do not affect the interests of another state or the international community as a whole. While international crimes are threatening for the international peace and security, crimes of an international nature are

common crimes in combating which states cooperate. International crimes can be committed using computers. Global computer networks enable propaganda of war, genocide, apartheid, and racial discrimination. Moreover, the use of computers for military technology can lead to electronic communications becoming a means of aggression.

It should be noted that the existing international treaties on computer crime regard computer crimes primarily as crimes of an international nature. They define the elements of crimes that must be criminalized in national law as well as measures of international cooperation in combating such crimes. The development of legal foundations of the global information society is to a great extent spontaneous. In the framework of the institutional mechanism of cooperation between states, there is not enough systemic vision of what the legal regulation should be like to meet the development of the technological progress. Therefore, the information society concept needs a corresponding integral concept of international legal regulation of information exchange relations in the information society.

Some objectives have existed for a long time and are related to a lack of regulation of certain problems (matters of combating computer crime, protection of privacy at the global level, etc.), while others have appeared relatively recently as a result of technological progress.

What are the objectives that should be addressed at the global level? When determining the range of objectives, one should consider that information technologies have become global and reveal the interdependence of the contemporary world. At the same time, there is the experience of regulation of electronic data exchange relations in the framework of the Council of Europe, which should be recognized as progressive and useful for the global level.

The primary objective for the global level is solving the problems that have already been solved in the framework of the Council of Europe (combating computer crime, protection of personal data). The models of the Council of Europe have already been tested in practice, and in any case they have no significant alternative.

For the prosecution of computer crimes and protection of privacy, the global network of international information security can be created under the Security Council of UN decision by adoption of the international treaty. The global network of international information security shall provide for search in computer networks performed in one state on request of another state, real-time collection of traffic data and real-time collection and interception of content data. Therefore, the general mechanism of legal aid shall be applied, but its content is special.

In the global network of international information security, any state may request another state to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other state.

The global network of international information security stipulates 24–7 access, i.e., each state shall designate a contacting board available on a 24-hour, 7-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data or for the collection of evidence in electronic form of a criminal offense. Basically, this procedure can

take a few minutes. The global network of international information security can also provide the access for non-state actors in privacy violations and defamation cases.

One state may get access to publicly available computer data, regardless of their geographical location, without permission of any other state. This primarily applies to data that are contained on the Internet. If a website has no access codes and the data on it can be accessible to everyone, it can be used by search, investigative, and judicial authorities. It is a general practice of access to data in open computer networks. There exists an international custom, according to which states do not put special restrictions on the spreading of publicly available data in computer networks. Special regulations are established for data, the spreading of which is prohibited or restricted. If any person may have access to information, it would be illogical to deny such access to law enforcement authorities.

In addition, any state can access, through a computer system in its territory, stored computer data, if the state obtains the lawful and voluntary consent of the person or legal entity who has the lawful authority to disclose the data. In this case, the state body of one state must address the provider, which is located in another state, directly.

Therefore, the development of the institute of mutual legal assistance in criminal matters, which is affected by the struggle with computer crimes, is not just about introducing electronic communication technologies in traditional types of legal assistance and not just about specifying legal aid measures in relation to electronic communication technologies but also about radical change in the very content of this institute.

The system of international information security is establishing at the moment. The international information security of the interstate system is a component of the comprehensive system of international security. At the same time, international information security is a stabilizing factor in the system of non-state international relations. However, a number of threats to international information security affect the field of both interstate and international non-state relations. In “soft law” acts, a unified concept of the development of a system of international information security has been elaborated at the global and regional levels. However, “soft law” acts are not suitable for its implementation. They can contribute to development of international customs, but that can take a considerable time. Therefore, global international treaties should be drafted.

The 2001 Convention and the CIS Agreement have become the first international treaties that stipulate a system of measures for combating a specific type of crime in the field of information, namely, computer crimes. Formerly, information crimes had been covered in particular international treaties along with other crimes (such as propaganda of racial discrimination). The treaties considered have a very important role, as they have established the foundations of the jurisdiction of states for criminal cases on the Internet and the rules of international cooperation that ensure coordinated actions of states in combating computer crimes. Despite some shortcomings of the treaties, as a whole they provide for systems of interrelated international and national measures for combating computer crimes and can be the basis for drafting of a global international treaty.

Legislating Cyber Crime: Johnson and Post for example argued that cyberspace should have ‘its own law and legal institutions’, and those state-based governments would generally

have no jurisdiction over online activity. To Johnson and Post, then, the law of cyberspace is, quite literally, the law of another place. It is the law of cyberspace – the same way that we might think of the law of the State of New York or the law of the UK. Lately, there has been recognition of distinctions between the real and virtual but also a merging of the idea of how we think about cyberspace, with the normative question of how cyberspace is or may be regulated. This is most clearly seen where Lessig comments: *"cyberspace presents something new for those of us who think about regulation and freedom. It demands a new understanding of how regulation works and of what regulates life there."*

Many definitions of offence and offender are being forged by the fight, or 'intellectual land grab', that is taking place for control over cyberspace. The increasing political and commercial potential of the Internet is giving rise to a new political economy of information capital. As a consequence, a new set of power relationships is being established within which an increasing level of intolerance is being demonstrated by the new powerful towards various risk groups that the former perceive as a potential threat to their interests. Such intolerance tends to mould broader definitions of deviance. But the definitions of deviance are not simply one-sided. Melossi argued that definitions of crime and deviance arise, not only from the social activity of elite or power groups, but also from 'common members' of society and offenders themselves: 'the struggle around the definition of crime and deviance is located within the field of action that is constituted by plural and even conflicting efforts at producing control'.

Grabosky and Smith identified the following categories of crime emerging in the digital age: illegal telecommunications interception; electronic vandalism or terrorism; theft of communications services; telecommunications and associated intellectual property piracy; electronic distribution of pornography; electronic fraud; electronic funds transfer crime; and money laundering. While many of these categories of crime can be prosecuted under a combination of existing criminal, commercial and intellectual property laws, it is clear that additional legislation is often required in order to deal with certain kinds of computer-related illegalities.

The world's concern about cybercrime intensified after September 11 and is being shared by many international organizations, including the United Nations, the G8, the European Union and the Council of Europe. Highlighting the trans-jurisdictional nature of cybercrimes in turn highlighted the problems of enforcement of law. Typically, policing often boils down to decisions that are made at a very local level over the most efficient expenditure of finite resources. Such decisions become complicated where different jurisdictions cover the location of the offence committed, the offender, victim and impact of the offence. Many legal challenges arise due to the extra-territorial nature of Internet. The problems faced by police and prosecutors in pursuit of cyber-criminals can be illustrated by the brief yet destructive career of the 'Love Bug' virus. The virus destroyed files and stole passwords; it appeared in Hong Kong on 11 May 2000 and spread rapidly throughout the world. The virus affected NASA and the CIA on its two-hour race around the world. The virus is estimated to have ultimately affected over 45 million users in more than 20 countries. The various estimates of the damage caused, ranging from US$2 billion up to US$10 billion, reflect on the inherent difficulty of assessing the harm inflicted by cybercrime.

Virus experts were quick to trace the 'Love Bug' to The Philippines. The Philippines' National Bureau of Investigation and United States FBI agents identified individuals suspected of creating and disseminating the 'Love Bug' using information supplied by an Internet service provider (ISP) but ran into problems with their investigation. Since The Philippines had no cybercrime laws, creating and disseminating the virus was not a crime; since there was no crime, the agents had a hard time convincing a magistrate to issue a warrant to search the suspects' apartment. Getting the warrant took days; sufficient time for them to destroy the evidence. After finally executing the warrant authorities seized evidence indicating that Onel de Guzman, a former computer science student, was responsible for creating and disseminating the 'Love Bug'. As hacking and the distribution of viruses had not been criminalized, officials struggled with whether de Guzman could be prosecuted. After finally charging him with theft and credit card fraud, they watched as the charges were dismissed as inapplicable and unfounded. Because extradition treaties require 'double criminality', that the act for which extradition is sought be a crime by the laws of each involved nation, de Guzman could not be extradited for prosecution by other countries that do have cybercrime laws, such as the USA.

Despite having caused billions of dollars in damage to thousands of victims in numerous nations, de Guzman could not be brought to trial in the matter. Yet, there are also examples where such trans-national nature of crime has provided policing bodies with a flexible tool by which to maximise the potential for gaining a conviction, particularly with regard to 'forum shopping' so that the prospect of achieving the most effective investigation and/or prosecution is achieved. A number of cases from both sides of the Atlantic demonstrate the enabling aspect of the trans-jurisdiction of the Internet. In *United States of America v Robert A. Thomas and Carleen Thomas* the prosecutors 'forum shopped' to seek a site where they felt a conviction would best be secured.

The difficulty lies in properly defining the laws needed to allow for cybercriminals' apprehension and prosecution. While seemingly a straightforward task, difficult issues are raised. First, the definitional scope of cybercrimes, should the definition include only laws that prohibit activities targeting computers or should legislation outlaw crimes against individuals affected through the computer, such as cyber-stalking and cyber-terrorism. Second, whether these laws should be cybercrime-specific, or targeting only crimes committed by exploiting computer technology. Is it, for example, necessary for a country to add a 'computer fraud' offence if it has already outlawed fraud? After it could be argued that crimes such as web site defacement are merely electronic graffiti; password or credit card number stolen off the Internet are simply theft and fraud in a new guise; those involved with Internet pornography and prostitution are simply utilizing a new medium, stalking and harassment will continue to be conducted by mail and telephone as well as via Internet technologies. The authors have however argued elsewhere38 that such an approach is too simplistic and the nature of these crimes is different and as such require separate legislation.

In several ways cybercrime differ from crimes in physical world: 'They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal'. They also pose far greater challenges for law enforcement: Effective law enforcement is complicated by the trans-national nature of cyberspace. Mechanisms of

cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber-crimes.

The first comprehensive inquiry into the criminal law problems of computer crime on the international scale was initiated by the OECD. In 1983, a group of experts met and recommended that the OECD take the initiative in trying to achieve the harmonization of European computer crime legislation. From 1983 to 1985, the OECD carried out a study of the possibility of an international application and harmonization of criminal laws to address cybercrime and abuse. The study resulted in the 1986 report Computer-related Crime: Analysis of Legal Policy, which surveyed existing laws and proposals for reform and recommended a minimum list of abuses that countries should consider criminalizing. It further ensured that instead of unilateral approaches, attempts be made to international harmonization of legal, technical and other solutions.

In this respect OECD along with the Council of Europe, the European Union, the United Nations, and Interpol have played leading and important roles. Ulrich Sieber, author of the cybercrime study commissioned by the European Commission, found a close interrelationship between law reform at the national level and activities on the international and supranational level. As Sieber explained, 'the preparation of the respective initiatives had a considerable impact on national laws by bringing the major national players together'.

Key issues and future development of International Cyber-Space Law:

Setting Rules for Global Cyberspace: With the rapid development of information technology and extensive use of the internet, the issue of how cyberspace should be regulated has increasingly become a serious concern of countries in the world. Admittedly, there is no legal vacuum in the global cyberspace, yet the legal framework for global cyber governance is far from being established. In general, the current rule-making process in the global cyberspace is shaped by three factors, namely, related institutions under the United Nations (UN) framework, legislation by regional and specialized international organizations, and all other efforts made by various stakeholders from different countries.

There are four major institutions under the UN framework dealing with the rule-making process on cyberspace. First is the World Summit on the Information Society (WSIS). On December 21, 2001, the United Nations General Assembly (UNGA) Resolution 56/183 endorsed the convening of the WSIS in two phases including the Geneva phase (December 10 to 12, 2003) and the Tunis phase (November 16 to 18, 2005), which generated four important documents including the *Geneva Declaration of Principles,* the *Geneva Plan of Action*, the *Tunis Commitment, and Tunis Agenda for the Information Society*. According to these documents, *"policy authority for internet-related public policy issues is the sovereign right of states. They have rights and responsibilities for international internet-related public policy issues."*

From December 15 to 16, 2015, a high-level meeting under the auspices of the UNGA was held in New York to review the implementation of the four WSIS documents, and the outcome document of the meeting highlighted the importance of promoting economic development through information and communication technologies, bridging digital divides, complying with the UN Charter and international law, building confidence in the use of information and communications technologies, and improving cyber governance. It also requested the Chair of the United Nations' Commission on Science and Technology for Development, through the *Economic and Social Council (ECOSOC),* to establish a working group to develop recommendations on how to further implement enhanced cooperation as envisioned in the *Tunis Agenda*, taking into consideration the work that had been done on this matter thus far. The UNGA is expected to review the implementation of the outcome document in 2025.

Second is the Groups of Government Experts (GGE) on Information Security under the First Committee of the UNGA. Since 2003, four GGEs have been formed successively to examine the existing and potential threats from the cyber sphere, as well as possible cooperative measures to address them. The third GGE concluded with a report in 2013 that "international law, and in particular the Charter of the United Nations, is applicable" in cyberspace and that *"state sovereignty and international norms and principles that flow from sovereignty apply to the conduct by states of ICT related (Information and Communications Technology) activities and to their jurisdiction over ICT infrastructure within their territory."* The fourth GGE, built upon the work of previous three Groups, further clarified and consolidated the role of state sovereignty in cyberspace by emphasizing that *"states must observe, among other principles of international law, state sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other states."* The 70th UNGA in December 2015 adopted a resolution requesting the establishment of a new GGE "to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them; and how international law applies to the use of information and communications technologies by states, as well as norms, rules and principles of responsible behavior of states.

Another key institution is the United Nations Expert Group on Combating Cybercrime. *The Commission on Crime Prevention and Criminal Justice (CCPCJ)* was established by the Economic and Social Council resolution 1992/1, upon request of UNGA resolution 46/152. The group was set up according to the Salvador Declaration adopted at the 12th United Nations Congress on Crime Prevention and Criminal Justice in April 2010, and it has been functioning as a platform under the CCPCJ for the comprehensive study of cyber-related crimes. Western nations, those from the European Union in particular, have been advocating for the *Budapest Convention on Cybercrime* (entering into force on July 1, 2004) to be accepted by national governments as a universal treaty on crimes committed via the internet and other computer networks. However, many developing countries, including emerging powers like Russia and China, have declined to adopt the convention on the grounds that it is not universally applicable. China insists that any international treaty on combating cybercrime which is intended to be universally applicable should be drafted under the UN framework; this is opposed by many Western nations.

The last one is the International Telecommunication Union (ITU). The ITU convened the World Conference on International Telecommunications (WCIT) in Dubai, United Arab Emirates in December 2012 in order to amend the International Telecommunications Regulations(ITRs), a binding global treaty enacted in 1988. During the conference, developing countries proposed to introduce amendments on internet governance and cyber security to promote equal internet management by national governments, developing and developed alike. However, the United States and other Western countries opposed the ITU's intervention and refused to sign the amended treaty after it was adopted by a large vote. The amended treaty which entered into force in January 2015 includes new provisions on cyber security, broadband connectivity, telecommunication services such as international roaming, energy efficiency and e-waste best practices. At its 2014 Plenipotentiary Conference in Busan, South Korea, the ITU adopted a resolution to set up a working group on international public policy issues pertaining to the internet and the management of internet resources, to organize international and regional consultative meetings with relevant ICT stakeholders on a regular basis.

Besides the institutions under the UN system, the legislation passed by regional and specialized international organizations is also regarded as part of the rule-making process in the global cyberspace. For example, the Shanghai Cooperation Organization (SCO) set up an International Information Security Expert Group to foster consensus on information security among its member states. In January 2015, the SCO submitted the revised version of its 2011 International Code of Conduct for Information Security to the UNGA, an effort involving China's active participation in international cyber-law-making.

Another example is the establishment of the Working Group on Customary International Law under the Asian-African Legal Consultative Organization (AALCO). At the AALCO's 2014 annual session, "international cyberspace law" was put on the agenda upon Chinese proposal. Later, at its 2015 annual session in Beijing, China organized a half-day special meeting on this topic, and a working group on international cyberspace law was set up to explore issues such as state sovereignty, peaceful use of cyberspace, and combating cybercrime. Apart from the ever more active stance China has adopted in agenda-setting on global cyber legislation, some other countries have been seeking to play a bigger role as well. For instance, Turkey included, for the first time, cyber issues into the agenda at the 2015 Group of Twenty (G20) Summit at Antalya, whose communique addressed cyber espionage, applicability of international law in cyberspace, and the United Nations' role in the cyber rule-making process. Meanwhile, such specialized international organizations as the International Committee of the Red Cross and the United Nations Institute for Disarmament Research are also trying to promote legislation concerning cyberspace.

Other stakeholders, especially the global academia, also contribute much to the progress of international legislation on cyberspace. A most prominent example is the Tallinn Manual on the International Law Applicable to Cyber Warfare. Between 2009 and 2012, the Manual was written at the invitation of the Tallinn-based NATO Cooperative Cyber Defense Center of Excellence by an international group of 19 experts. Other famous manuals completed by scholars include the San Remo Manual on International Law Applicable to Armed Conflicts at Sea prepared during the period of 1988 to 1994 by a group of legal and naval experts participating in their personal capacity in a series of roundtables convened by the

International Institute of Humanitarian Law, the 2008 Draft Manual on International Humanitarian Law in Air and Missile Warfare prepared by Harvard University's Program of Humanitarian Policy and Conflict Research (HPCR), and a manual on armed conflicts in outer space being prepared by McGill University in Canada.

These academic researches mainly build upon theories of international law and therefore are not legally binding, although the Tallinn Manual has aroused heated debate around the world. Some argue that the manual has exaggerated the threat emanating from armed conflicts in cyberspace because the majority of existing cyber-attacks do not qualify as armed conflicts, and thus more attention should be paid to the rule-making in cyberspace during peacetime. As a result, Tallinn 2.0, the updated version of the original Tallinn Manual, is now being drafted to reflect prevailing ideas about international rules and regulations in the cyber context, such as state sovereignty, state responsibility, international human rights law, and cyber operations during peacetime.

In addition to these manuals, there exist other initiatives including the London Process, Brazil's NetMudial process, and China's World Internet Conference in Wuzhen, etc., all of which are based on a multi-stakeholder approach involving nation-states, international governmental and nongovernmental organizations, academia, and civil society. In short, there are numerous parties involved in the global cyber rulemaking process, while no single party or institution is able to play an overarching and integrating role in the process, thus adding much uncertainty to the future trends of international cyber legislation.

Key Issues in Shaping International Cyberspace Law: While an international legal system on cyberspace is slowly taking shape, some key issues such as global cyber governance model, state sovereignty in cyberspace, online freedom, application of the law of armed conflict to cyberspace, and international cooperation on combating cybercrime have emerged as the most salient topics for discussion during the global legislation process. Below is the author's view on these important issues.

First and foremost, the UN-centric approach ought to serve as the core governance model in the global cyberspace. Cyberspace is a sui generis domain, with dual characteristics of reality and virtuality and also dual attributes of sovereignty and global commons. On one hand, as an interconnected and indivisible global information channel, cyberspace is shared by all internet users on the planet. Unlike outer space, the high seas, the Antarctic or other global commons, cyberspace per se does not have any territory or boundary, it is a man-made virtual space based on the interaction and intertwinement of human cyber activities supported by cyber infrastructures. The orderly functioning of cyberspace concerns the interests of all states, and so cyberspace should not be controlled or dominated by any single country. On the other hand, cyberspace also has elements of sovereignty. Each state is entitled to the exercise of sovereignty over cyber infrastructures, online data, cyber activities and cyber governance within its own territory. Each state may also exercise extra-territorial jurisdiction over cyber activities pursuant to international law. Therefore, cyberspace should be governed by both sovereign states and the international community.

When it comes to cyber issues related to the common interests of the international community, we should make full use of existing mechanisms under the UN framework. The UN system is the core architecture for global governance, playing a leading role in

international peace and security. In global cyber governance, the UN should also take the central position. While maintaining the various global cyber governance platforms, we may consider the option of establishing a special committee on cyber governance under the UNGA, which will take into account the interests of multi-stakeholders, including those of nation-states, private sectors, technology community and civil society, and coordinate various responsibilities and functions of different mechanisms on cyber governance, so as to build a harmonious, rule-based order for cyberspace.

We should welcome and encourage all parties to actively participate in cyber governance and assume their respective responsibilities and roles, with a view to foster a multi-stakeholder approach of cyber governance. Internet companies, NGOs and the technology community should continue to play an important role in application innovation, industrial development and self-discipline, standard formulation and operation support. Yet the multi-stakeholder approach must not focus only on companies and NGOs while marginalizing the role of national governments. As administrators of state affairs and the major participants in international cooperation, national governments undertake great responsibilities in cyber affairs and have every reason to play a leading role in the cyber policy making process and try to accommodate the views of various parties.

In recent years, the internationalization of the Internet Corporation for Assigned Names and Numbers (ICANN) has been promoted and the U.S. government also made an announcement in 2014 of its intention to transfer its stewardship of the ICANN. All these steps can be regarded as initial progress in the long-lasting joint efforts by the international community. In December 2015, the UNGA high level meeting was held at the UN Headquarters in New York to have an overall review of the implementation of the WSIS outcomes. It provided an opportunity for in-depth discussions on important issues in the implementation of the WSIS outcomes, including the progress, gaps and challenges, as well as areas for future actions, which marked a new stage of development of global cyber governance. In this light, all parties should jointly promote the multiple cyber governance mechanisms under the UN framework, such as the International Code of Conduct on Information Security in the UNGA, the UN Group of Governmental Expert on Information Security (UNGGE), the UN open-ended Inter-Governmental Expert Group on Cybercrime, the WSIS process, and relevant ITU mechanisms.

Second, state sovereignty and the fundamental freedom of speech and expression in cyberspace should be treated as basic principles in international cyberspace law. The principle of state sovereignty, which is the cornerstone of contemporary international relations and international law, should apply to cyberspace. In this regard, the report put forward by the UNGGE in 2013 affirms that state sovereignty and derived international norms and principles should be applied to relevant activities conducted by states on the technology of information and communications, and are also applicable in the jurisdiction of countries over the infrastructure of technology of information and communications. The 2015 UNGGE report not only reaffirms the above arguments, but further develops the substance of state sovereignty in cyberspace as well. The above-mentioned consensus indicates that important progress has been made on the application of the principle of state sovereignty in cyberspace.

State sovereignty is the combination of rights and obligations, which means that the application of state sovereignty in cyberspace implies both the enjoyment of rights and the assumption of obligations. States are entitled to, where applicable, the rights of sovereignty in cyberspace, including but not confined to the following: sovereignty rights over cyber infrastructure, online data, cyber activities and public cyber management in its territory; extra-territorial jurisdiction under international law over cyber activities outside its territory; the right of self-defense against armed attacks; the right to invoke counter-measures against international wrongful acts; and the right to equally participate in global cyber governance and the international law-making process.

State sovereignty in cyberspace also implies that a state is to fulfill its obligations accordingly, which include but are not limited to the following: respect for the sovereignty of other states, ensuring that it shall not knowingly allow cyber infrastructure located in its territories to be used for acts that adversely and unlawfully affect other states; maintaining peaceful use of cyberspace and refraining from the threat or use of force; non-intervention of internal affairs of other states by cyber means; and finally, respect and protection of basic human rights and freedoms including the freedom of speech and expression.

Freedom of speech and expression is a fundamental right enshrined in international human rights instruments, such as the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights. Yet in accordance with relevant international rules, it forbids citizens, in exercising such rights, to endanger national security, public order or the lawful rights and freedom of others, including the rights of privacy and intellectual property.10 The freedom of speech and restrictions thereupon is equally applied to cyberspace. State sovereignty on cyberspace does not exempt states from their obligations. Meanwhile, there is no absolute freedom of speech and expression in cyberspace. What we should do is strike a balance between national security, public order, as well as the freedom of speech and expression of individuals in accordance with international and domestic laws.

Third, the application of existing laws of armed conflict to cyberspace requires further scrutiny. For sure, existing international laws, including The Charter of the United Nations, apply to cyberspace in principle, which has been explicitly presented in the UNGGE's statements both in 2013 and in 2015. Considering the increasing prominence of cyber-attacks targeted at a few major countries like the U.S. and China, some scholars tend to categorically describe these attacks as acts of cyber warfare, thereby invoking the provisions of The Charter of the United Nations on the threat or actual use of force, and advocating the application of *jus ad bellum* ("right to war"), *jus in bello* ("law of war"), and the law of state responsibility to all cyber-attacks. However, this "military paradigm" in response to cyber-attacks may indeed aggravate the arms race and militarization in cyberspace. "Cyber warfare" is the most serious confrontation between states in cyberspace, yet in reality, few cyber-attacks, if any, are launched by a state targeting other states. As a matter of fact, most cyber-attacks are committed by individuals or other non-state actors, which are generally viewed as cybercrime or infringement of cyber rights that should be regulated by domestic criminal law or the law of torts.

Even if some of these attacks are conducted by states or may be attributable to states, most of them fall far below the threshold of "threat or use of force" or "armed attack." Instead, they are only cyber-attacks of minimal levels of intensity, which are comparable to other

internationally wrongful acts such as interference with the internal affairs of other states. These attacks should and can be addressed by peaceful means such as resorting to the UN Security Council, rather than employing military forces. Under certain circumstances, even if cyber-attacks are suspected of constituting "threat or use of force" or "armed attack," due to the extreme difficulties in identifying the actual culprits, substantial uncertainties still exist with respect to the source and motivation of the attacks, as well as the extent to which the victim state's territorial integrity is violated by such attacks. To date, state practice concerning cyber warfare has been scarce, and whether relevant rules can generally be applied to the so-called "cyber warfare" demands cautious exploration. With regard to the use of force, *lex lata* (the "current law"), including *jus ad bellum* and *jus in bello*, apply in principle to cyberspace. In the meantime, however, it is of urgent necessity for international society to set new rules concerning cyberspace.

Fourth, international cooperation on combating cybercrime should be enhanced. Despite the lack of a global legal instrument, the international community can still do much in dealing with the common challenge posed by rapidly increasing cybercrime.

As the most comprehensive multilateral treaty to cope with cybercrime, the Budapest Convention on Cybercrime first adopted in 2001 by the Council of Europe has played an important role in promoting regional cooperation in fighting against cybercrime. However, this Convention also has some drawbacks. Mainly formulated by Western countries, the Convention has largely failed to take into consideration the concerns of developing countries, and its Provisions that a state may conduct cross-border investigations without the consent of another state risk jeopardizing the judicial sovereignty of other states. Besides, as the Convention focuses on crimes against the security of computer information systems, it can no longer keep up with the new development of cybercrime which has integrated traditional crimes, internet technologies and the expansion of criminal interest networks. The deficiency of the Convention also lies in its lack of openness and inclusiveness in terms of country representation. For instance, at present, only eight among its 47 formal members are non-members of the Council of Europe.

In order to develop global legal standards that can meet the demand of most countries in the world, and follow the new developments of information technology, it is necessary to establish an international legal instrument on combating cybercrime under the UN framework. The above Convention can be used as a good reference for this endeavor. At the same time, the international community should also render full support to the UN Inter-Governmental Expert Group on Cybercrime, so as to lay a solid foundation for the establishment of effective international legal instruments

Ways to Strengthen the International Cyberspace Legal Framework: Given the distinct features of cyberspace and past experience of international society, two major principles should be closely observed in the future development of the international cyberspace legal framework. Above all, such a legal framework must be based on The Charter of United Nations, which enjoys a paramount legal status over other international law and is of crucial importance to building global consensus on cyber legislation. The fundamental principles of modern international law provided for in the Charter, such as equality among state sovereignties, non-interference in internal affairs of any state, non-use of force, and peaceful settlement of international disputes, should also serve as the guiding principles for

establishing a global order in cyberspace. Meanwhile, considering the unique features of cyberspace and the common interests of all nations in cyberspace, new legal principles with regard to sustainable development, shared benefits and co-governance should be followed as well.

The second principle is that the legal regime for cyberspace should be based on a balance between various elements:

1. Balance between general international law and special law for cyberspace. Existing international law, especially The Charter of the United Nations, certainly applies to cyberspace. Yet a lot of unique problems without ready solutions in the existing legal framework are emerging in cyberspace, and it is necessary to formulate new laws to tackle them. For example, we need to develop and improve international rules and regulations on e-commerce, which has become an important economic phenomenon. States also need to strengthen the legal framework for international judicial cooperation so as to combat cybercrime and cyber terrorism effectively. Naturally, for the matters that are not regulated by cyberspace law, general international law should be applied in principle.
2. Balance between international law and domestic law. Most countries have enacted domestic laws to regulate cyberspace, in large part to criminalize and punish illegal cyber acts which seriously threaten their national interests. Meanwhile, due to the inconsistency among, or even lack of, national laws in some areas, many countries are also calling for enhancement of international legislation to coordinate national laws or to make uniform international rules. Careful consideration is still expected, in order to decide which problems in cyberspace should be regulated by international law or by domestic law, and which problems should be regulated by both of them through proper coordination and mutual reinforcement.
3. Balance between peaceful and coercive means in enacting international law. Non-use of force and peaceful settlement of international disputes are two fundamental principles of modern international law, and they are also the fundamental principles that states should abide by in cyberspace. Given the shortage of state practice on cyber warfare, international society should be very cautious about the application of existing laws of war to cyberspace. Instead, peaceful legal measures are to be further explored and applied by all nations to address their common threats such as cybercrime and cyber terrorism.
4. Balance among interests of all parties in using cyberspace. To promote the sustainable development of cyberspace, the international legislation process needs to take into consideration the interests of governments, non-state actors such as individuals and companies, as well as the whole international society, the key to success being to remain open to the views of all these parties during the legislation process.

Based on these principles, a brief roadmap can be drawn for the formulation of international cyberspace law in the future. Here, the establishment of the legal regime on outer space, which developed from a joint declaration to a convention on the general legal framework, then culminated in treaties in specific areas, serves as a good example. Similarly, three steps can be taken to set up the legal regime on cyberspace.

The first step is to formulate a general declaration for activities in cyberspace, which should define the fundamental principles of cyber activities and be applied to all cyber areas, thus providing important guidelines for all stakeholders in cyberspace. Such a declaration may include the following principles: application of general international law including the UN Charter to cyberspace; state sovereignty and jurisdiction over cyber infrastructure, online data and cyber activities; peaceful use of cyberspace and prevention of cyberspace militarization; promotion of the legal rights and interests of all countries, especially those of developing nations given their lack of experience and capabilities in using cyberspace; international cooperation in cyberspace; protection of cyber freedom, cyber intellectual property rights and privacy rights; protection of cyber infrastructure, information and cyber environment; prevention and punishment of cybercrime in accordance with international and domestic law; and finally, multilateral, democratic and transparent cyber governance.

Following the above-mentioned declaration, the second step is to draft a convention which serves as a *Magna Carta* for cyberspace activities. It should clearly identify the rights, obligations and responsibilities of all stakeholders in cyberspace and lay down a basic framework for future legislation.

The final step is, under the guidance of the Magna Carta, to further develop related principles and institutions in specific areas, such as rules and regulations on internet traffic, safety of online information, protection and management of cyber infrastructure, and prevention of international cybercrime, among other issues. Only by this step-by-step approach can a legal framework for cyberspace be built with incremental global efforts, which will be shared by, and beneficial to, all nations of the world.

Cyber-crime and related treaties: There are international and regional treaties on cybercrime. A case in point is the Council of Europe's Convention on Cybercrime of 2001. This Convention seeks to harmonize national laws, improve cybercrime investigation techniques, and improve international cooperation. It also provides guidance to signatories on the measures needed at the national level to deal with cybercrime, including amendments and additions to substantive law (i.e., to establish cybercrime offences in criminal law) and criminal procedural law (i.e., to establish the procedures for criminal investigations and prosecutions). The Convention further provides signatories with guidance on mutual assistance and acts as a *mutual legal assistance treaty* (i.e., an agreement between countries to cooperate on investigations and prosecutions of certain and/or all offences proscribed by both parties under national law; Maras, 2016) for countries that do not have one with the country requesting assistance.

There are several cybercrime and cybercrime-related treaties that are region-specific:

i. *The Commonwealth of Independent States' Agreement on Cooperation in Combating Offences related to Computer Information of 2001*. This agreement calls on states to adopt national laws to implement the Agreement's provisions and to harmonize national cybercrime laws.
ii. *The Arab League's (formerly known as the League of Arab States) Arab Convention on Combating Information Technology Offences of 2010*. This convention's primary aim is to strengthen cooperation between states to enable

them to defend against and protect their property, people, and interests from cybercrime.

iii. *The Shanghai Cooperation Organization's Agreement on Cooperation in the Field of International Information Security of 2010.* This agreement's focus extended beyond cybercrime and cybersecurity to include information security (INFOSEC) of member states as one of its primary objectives, as well as national control over systems and content.

iv. *African Union Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa (Draft African Union Convention) of 2012.* This convention promotes the provision and maintenance of human, financial, and technical resources needed to facilitate cybercrime investigations.

v. *African Union Convention on Cyber Security and Personal Data Protection of 2014.* This convention includes, among other things, a call to African Union states to create and/or amend national laws to adequately combat cybercrime, harmonize national laws, create mutual legal assistance treaties (MLATs) where they do not exist, facilitate information sharing between states, facilitate regional, intergovernmental, and international cooperation and utilize existing means available to cooperate with other states, and even the private sector.

Cybercrime laws and directives have also been developed and implemented by regional organizations and/or regional intergovernmental organizations. Examples include:

- *Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime of 2012*. This law serves as a guideline for states in the SADC to develop substantive and procedural cybercrime laws. Because it is a model law, it does not pose any legal cooperation obligations on states. The states that have and/or create cybercrime laws can utilize the SADC Protocol on Mutual Legal Assistance in Criminal Matters and the SADC Protocol on Extradition to facilitate cooperation and coordination in international cybercrime investigations.
- *The Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime of 2011.* This directive requires member states to criminalize cybercrime in national law and facilitate mutual legal assistance, cooperation, and extradition in cybercrime and cybersecurity-related matters. ECOWAS has a Convention on Mutual Assistance in Criminal Matters and a Convention on Extradition to facilitate cooperation in cybercrime investigations and extradite cybercriminals.

Is International Law of Cyber- Security in Crisis? None of the global challenges facing the modern international community can be adequately addressed by any single international actor, irrespective of how powerful that actor may be. Whether one thinks of climate change, international terrorism, or cyber threats, all such challenging contemporary phenomena necessitate a framework for international co-operation. It is international law that ‘affords [such] a framework, a pattern, a fabric for international society’. By establishing a framework of constraints, the law simultaneously guarantees a sphere of autonomy for its subjects. In the context of international law, legal norms lay down shared boundaries of acceptable conduct in international relations, while preserving important space for manoeuvre, discretion and negotiation.

This is the idea at the root of the famous '*Lotus presumption'*, according to which states may generally act freely unless prevented by a contrary rule of international law. In order to delineate this zone of freedom for states and other international actors with respect to a new phenomenon of international significance, it is necessary to identify, interpret and apply relevant legal rules to it.

Cyberspace, broadly understood, is precisely such a phenomenon. Crucially, the uses and abuses of this complex borderless virtual space impinge on vital state interests in the physical world, including national security, public safety, or economic development. As such, cyberspace extends far beyond the domain of internal affairs of any state.

Yet, with respect to the management of cyberspace, it may appear that international law fails to deliver. Although the main building blocks of the Internet's architecture were laid over two decades ago, it took until 2013 for state representatives to agree on the rudimentary threshold assumption that international law actually applies to cyberspace.

Crisis indicators: Three indicators of the apparent crisis of international law stand out. First, the area of cyber security appears resistant to codification of the applicable rules in a comprehensive multilateral binding treaty. This is not for want of trying by the leading international stakeholders. Already in 1996, France put forward the earliest proposal with the lofty title *Charter for International Cooperation on the Internet*. Later, a *joint Russo-Chinese initiative resulted in two proposals for a Code of Conduct for Information Security*, submitted to the UN General Assembly in 2011 and 2015, respectively. However, none of these proposals was met with much enthusiasm by other states and scholars describe the prospects of an 'omnibus' treaty being adopted in the near future as slim to negligible.

Second, states have shown extreme reluctance to contribute towards the development of cyber specific customary international rules. In addition to state practice in this area being inevitably shrouded in secrecy, states have been reluctant to offer clear expressions of *opinio juris* on matters related to cyber security. At times, this approach may certainly be understandable, being the consequence of a domestic political gridlock or even a deliberate waiting strategy. On the whole, however, it adds to the pervasive ambiguity as far as the specific applicability of international law is concerned. This trend is visible even in the most recent developments. A representative example of another missed opportunity to steer the development of cyber custom is provided by the new *United States (US) Law of War Manual* adopted in July 2015.

Although it does contain a chapter on cyber operations, the Manual skirts virtually all of the unsettled issues, including standards of attribution, rules of targeting or the requirement to review cyber weapons. While the first two indicators relate to states' reluctance to act in ways meaningful for the generation of new rules, the third concerns their actual conduct in relation to cyber governance. It would be inaccurate to claim that states have entirely given up on standard-setting. However, instead of interpreting or developing rules of international law, state representatives have sought refuge in the vacuous term 'norms'. We can see this trend most clearly in the context of the work of the UN GGE. In its latest report, the group touted the advantages of 'voluntary, nonbinding norms of responsible state behaviour'. The report claimed that such norms prevent conflict in cyberspace, foster international development, and reduce risks to international peace and security. The report further

recommended 11 such norms for consideration by states, while making it clear that these norms operate on a decidedly non-legal plane.

Despite their minimalistic nature, the norms have thus far received very limited endorsement by their addressees. For example, at a US-China summit in September 2015, the two participating heads of state 'welcomed' the report but refrained from committing themselves to any of the proposed norms.

Together, these three indicators signify a trend of moving away from the creation of legal rules of international law in the classical sense. Instead of developing binding treaty or customary rules, states resort to normative activity outside the scope of traditional international law. Although this trend appears to be especially prominent in the area of cyber security, it is by no means limited to it. In legal theory, this phenomenon has been described as 'the pluralization of international norm-making', characterised by the observation that 'only a limited part of the exercise of public authority at the international level nowadays materializes itself in the creation of norms which can be considered international legal rules according to a classical understanding of international law'. In order to understand the impact this situation has on the international legal regulation of cyber security, we must zoom out slightly to take in the broader context of existing international law.

Existing Legal Landscape: The absence of a cyber-specific system of rules of international law does not mean that there are no legal rules that would apply to cyber activities. As we have seen, states accept that generally applicable rules of international law apply to states' conduct in cyberspace, too. This is undoubtedly correct. If international law is to be an efficient governance structure, it must be adaptable to new phenomena without the need to reinvent an entire regulation framework on each occasion.

By way of an example, the UN Charter was finalised when the invention of nuclear weapons was still a closely guarded secret and this instrument thus understandably did not refer to this type of weapons in its provisions on the use of force. Still, the International Court of Justice (ICJ) had little difficulty in holding, in the Nuclear Weapons Advisory Opinion issued decades later, that those provisions 'apply to any use of force, regardless of the weapons employed',38 notwithstanding the fact that a particular type of weapons might not yet have been generally known or even invented when the Charter was adopted. Following the same logic, cyber operations must equally be subject to the international law regulation of the use of force.

In addition to these generally applicable rules of international law, certain sectoral and regional treaties taken together provide a 'patchwork of regulations' for cyber activities. These include, in particular, the 1992 Constitution of the International Telecommunication Union; the 2001 Budapest Convention on Cybercrime and its 2006 Protocol on Xenophobia and Racism; the 2009 Shanghai Cooperation Organisation's Information Security Agreement; and the 2014 African Union's Cyber Security Convention. Although important in their own right, these international agreements govern only a small slice of cyber-related activities (such as criminal offences committed by means of computer systems or operations interfering with existing telecommunications networks), or have a very limited membership (six states in the case of the Shanghai Cooperation Organisation's agreement and none yet in that of the African Union's convention).

Therefore, although cyberspace is certainly not a lawless territory beyond the reach of international law, for now there is no complex regulatory mechanism governing state cyber activities. Moreover, states seem reluctant to engage themselves in the development and interpretation of international law applicable to cyber security. This voluntary retreat has generated a power vacuum, enabling non-state actors to move into the space vacated by states and pursue various forms of 'norm entrepreneurship'.

Power Vacuum: Vectors of power and law do not overlap perfectly. State power is certainly influenced by many other factors, which may include military might, wealth, and moral authority. Nonetheless, it needs little emphasis that the powerful normally seek to use legal regulation to consolidate and project their power. If we understand power simply as 'the ability to alter others' behaviour to produce preferred outcomes', then setting legal obligations is one way how to exercise this ability. Everything else being equal, it is more likely than not that these 'others' will act in accordance with a certain standard of behaviour when it is required by law than when it is not.

Yet, legal uncertainty may at times be deemed desirable by even the most powerful states. For example, during the early days of space exploration, only two states were capable of acting in outer space: the US and the Soviet Union. Yet these two states resisted, for a significant time, to commit themselves to any binding rules that would govern outer space. Both believed that the adoption of such rules would only serve to constrain their activities in space. In that vein, 'legal uncertainty was useful to those with the power to act in space, on either side of the cold war.

However, cyberspace and outer space – albeit frequently lumped together as so-called 'global commons' – are decidedly different from one another. This is not only because many states are challenging the very idea of cyberspace as commons by seeking to assert greater control online. More importantly, cyberspace is already a much more crowded domain than outer space could ever be. To wit, the US and the Soviet Union were not just the only states engaged in space exploration for several decades, they were also the only actors capable of space flight as such. In contrast, cyberspace is populated primarily by non-state actors, which include individuals, corporations, and other more loosely organised groups. The possibility of anonymity online combined with the corresponding difficulty of attribution of cyber operations have resulted in the 'dramatic amplification' of power in the hands of these non-state actors at the expense of their state counterparts.

The effect of legal uncertainty is thus much more complex than what we saw in relation to outer space, as it affects a far more populous spectrum of actors, state and non-state alike. Accordingly, non-state actors have now moved into the vacated norm-creating territory previously occupied exclusively by states. These developments have been primarily driven by the private sector and by the academia, as epitomised by Microsoft's cyber norms proposal and by the so-called *Tallinn Manual project.*

Non State Driven Initiative:

The more recent of the two, Microsoft's proposal entitled International Cybersecurity Norms: *Reducing Conflict in an Internet-Dependent World* was published in December 2014. Interestingly, this was not the first private-sector initiative of this kind. Exactly 15 years

earlier, *Steve Case,* then the CEO of AOL, urged states to revise their 'country-centric' laws and adopt instead 'international standards' governing crucial aspects of conduct online, including security, privacy, and taxation. Still, Microsoft's text is the first comprehensive proposal of specific standards of behaviour online, which, despite its private origin, proposes norms purporting to regulate solely the conduct of states. The openly proclaimed central aim of this white paper was to reduce the possibility that ICT products and services would be 'used, abused or exploited by nation states as part of military operations'. To that end, the paper put forward six cyber security norms, which collectively called on states to improve their cyber defences and limit their engagement in offensive operations.

In 2013, an international group of experts led by Professor Michael Schmitt published the *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Although the project was undertaken under the auspices of the Estonia-based NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), the Manual makes it clear that its text should be seen as reflecting the views of the experts themselves and not the states or institutions from which they originated. As apparent from its title, the Manual maintains a clear military paradigm throughout, focusing on the law on the use of force (*jus ad bellum)* and the law of armed *conflict (jus in bello*). Its text identifies 95 rules adopted by consensus among the group of experts who were guided by the ambition to 'replicate customary international law'.68 Early reviews of the Manual criticised its almost exclusive focus on activities occurring above the level of the use of force, whereas in reality, most (if not all) cyber operations fall below that threshold.69 However, the ongoing *'Tallinn 2.0' project,* scheduled for completion in 2016, should dispel some of these objections by turning its attention to 'below-the-threshold' operations and by addressing issues of state responsibility, the law of the sea, international telecommunications law, and even human rights law. Like the Microsoft paper, both iterations of the *Tallinn Manual* project put forward standards of state behaviour and are avowedly state-centric in their approach. Understandably, the two initiatives differ in important ways. The 'norms' proposed by Microsoft are clearly meant as broad suggestions only, meaning that states need to transform them into more specific commitments.

For instance, norm 2 stipulates that 'states should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them'. As recognised in the paper itself, such policies need to be developed by each individual state and tailored to the needs of the concerned state.

By contrast, the *Tallinn Manual* 'rules' take on the more restrictive and specific form of purported customary legal obligations, which should simply be observed by states as binding without the need for their further endorsement or adaptation. In other words, the Manual aims to interpret how 'extant legal norms' apply to conduct in cyberspace, and not to '*set forth lex ferenda'*. Yet, given that the Manual frequently puts forward detailed and novel positions, it does not always succeed in maintaining a bright line between norm interpretation and norm development. Nevertheless, the purported rules it contains are much more specific than Microsoft's cybersecurity norms. For example, rule 37 sets out the prohibition of cyber-attacks against civilian objects in the context of an armed conflict. Both crucial terms – 'cyber attacks' as well as 'civilian objects' – are precisely defined by the Manual. Although some disagreements may persist about the application of the rule in particular circumstances,

the content of the norm is sufficiently clear and precise to generate legal rights and obligations.

However, what initiatives like Microsoft's white paper or the Tallinn Manual project share is their non-state origin and expressly non-binding nature. Microsoft was keenly aware of its proposal's limitations in this respect and noted that it merely 'encouraged' states to set the proposed norms on the trajectory towards making them first 'politically' and then 'legally' binding. Similarly, the Manual noted in its opening pages that it was meant to be 'a non-binding document'. As the texts in question are in their entirety the products of non-state initiatives, they could hardly amount to anything else. After all, with potential minor qualifications in the area of collective security, it is still true that only 'the states are the legislators of the international legal system.

If these texts are non-binding, one might question their relevance from the perspective of international law altogether. True, their normativity (in the sense of the strength of their claim to authority) is lower than that of international legal rules. But that does not mean that these efforts are wholly irrelevant for the formation of rules of international law, and even less do they document any supposed irrelevance of international law to the area of cyber security. On the contrary, non-state-driven initiatives of this kind potentially amount to 'a vital intermediate stage towards a more rigorously binding system, permitting experiment and rapid modification'. Moreover, they render the law-making process more multilateral and inclusive than the traditional state-driven norm-making can ever be. Therefore, the crucial question is whether states decide to pick up the gauntlet thrown at them by their non-state counterparts and reclaim their role as principal lawmakers.

States at a critical Juncture: The current situation is certainly not without prior historical parallels. Cyberspace is not the first novel phenomenon to have resisted the development of global governance structures for some time after its emergence. A degree of waiting or stalling may even reflect states' desire to obtain a better understanding of the new phenomenon's strategic potential. Yet with states' improved comprehension of the new situation, their willingness to subject themselves to binding rules usually increases, too. Even the domain of outer space has been eventually subjected to a binding legal regime, despite the strong initial reluctance of the dominant spacefaring states.

Other domains with a higher number of participants may provide more appropriate analogies. For instance, in the context of Antarctica, many non-binding norms were put forward in the 1960s and 1970s with the aim to conserve living and non-living resources of the Antarctic environment. These norms gradually evolved into the 1991 Antarctic Environmental Protection Protocol, a complex binding instrument that has since been ratified by all key stakeholders.

Similarly, it took over three decades since the 1954 launch of the first nuclear power plant in the world in Obninsk, Soviet Union, until the first international conventions on nuclear safety were adopted. In the meantime, states were guided by non-binding safety standards and criteria, most of which were issued by the *International Atomic Energy Agency (IAEA).* Afterwards, nuclear safety conventions consolidated this emerging body of non-binding norms and made many of the relevant standards mandatory for all member states.

As these examples demonstrate, instead of lamenting over a supposed crisis of international law, it is more appropriate to view the current situation as an intermediate stage on the way towards the generation of cyber 'hard law'. Non-state-driven initiatives provide opportunities for states to identify overlaps with their strategic interests and they may serve as norm-making laboratories. Their usefulness in this sense is confirmed by a recent report of the East West Institute, which helpfully maps out areas of convergence across various proposals of norms of state behaviour in cyberspace including those analysed here.

A final point to consider is the so-called attribution problem (understood as the difficulty in determining the identity or location of a cyber-attacker or their intermediary). For some time, it was rightly seen as an impediment to the development of effective legal regulation of cyber activities. It was argued that the prevailing anonymity online 'makes it difficult – if not impossible – for rules on either cybercrime or cyber war to regulate or deter.' However, recent technological progress has translated into increased confidence of states with respect to attribution of cyber activities. For instance, the US has claimed that it now has the capacity to locate its cyber adversaries and hold them accountable. In a similar statement, Canada noted that it has robust systems in place allowing it to localise cyber intrusions, including those orchestrated by state-sponsored actors. Significant progress has also been made in the understanding of the legal standards of attribution as applied to online conduct. Although it is probably correct that the attribution problem can at most be managed but not solved, these developments show that time may be ripe for states to endorse the regulatory and deterrent potential of international legal rules.

Building on the emerging normative convergence identified above, states should be able to reclaim their central role in international law-making. In the more immediate future, they should become more forthcoming in expressing their opinion as to the interpretation of existing international law to cyber issues. This will in time enable the applicable *opinio juris* to consolidate, thus facilitating the process of transformation of state power into obligations of customary law. Additionally, states should gradually overcome their current aversion to treaty commitments. Reports from late 2015 that the US and China started negotiating a binding arms control treaty for cyberspace are possible early signs that this process is already underway. Finally, this iterative process of state-appropriated norm-making could in the long run quite plausibly result in the adoption of one or several comprehensive multilateral undertakings, possibly commencing with definitional matters to pave the way towards future consensus-building over more substantive issues.

Cyber/Computer Crime Legislations in Various Countries

United States of America: The Computer Fraud and Abuse Act was enacted by Congress of USA in 1986 and the same was amended in 1989, 1994, 1996, 2001 by the USA Patriot Act, in 2002 and 2008 by the Identity Theft Enforcement and Restitution Act. The USA has also passed other enactments, which contains some or other aspects of fighting cyber-crimes.

The United Kingdom: The United Kingdom has passed various legislations to deal with cyber- crimes and to regulate the transactions on cyber space. In the context of combating cyber-crimes, the important Acts are: 1) The Computer Misuse Act, 1990 and 2) Regulation of Investigatory Powers Act, 2000.

*Ireland:*Ireland has passed Criminal Damages Act, 1991 to deal with damages caused to or by a computer system or network.

People's Republic of China: In order to strengthen the security and the protection of computer information networks and of the internet, and to preserve the social stability, Computer Information Network and Internet Security, Protection and Management Regulations were adopted by China and it came into effect on 30th February 1997.

Singapore: Singapore is one of those countries wherein a conscious effort was undertaken to demarcate the cybercrimes and subject them to specialized treatment. It passed the Computer Misuse Act, 1998 based on UK.

Australia: Australia has adopted the Cyber Crime Act, 2001 to amend the law relating to computer offences and other related purposes. This was amended in 2002.

Conclusion: The new legislation which can cover all the aspects of the Cyber Crimes should be passed so the grey areas of the law can be removed. The recent blasts in Ahmedabad, Bangalore and Delhi reflects the threat to the mankind by the cyber space activities against this I personally believes that only the technology and its wide expansion can give strong fight to the problems. The software's are easily available for download should be restricted by the Government by appropriate actions. The jurisdiction problem is there in the implementation part which should be removed because the cyber criminals does not have any jurisdiction limit then why do the laws have, after all they laws are there, to punish the criminal but present scenario gives them the chance to escape Today in the present era there is a need to evolve a 'cyber-jurisprudence' based on which 'cyber-ethics' can be evaluated and criticized. Further there is a dire need for evolving a code of Ethics on the Cyber-Space and discipline.

Following Frank William Abagnale & Robert Morris, many other hackers are intending to make use of their skills for better purposes. This trend continues even now where companies as their security analysts hire the brilliant hackers. Also, there is a dire need for evolving a code of Ethics on the Cyber-Space and discipline. In the cyberspace, following traditional principles of criminal law to fix liability is not possible. Since most of the cyber criminals are those who are under the age of majority, some other legal framework has to be evolved to deal with them. Since cyber world has no boundaries, it is a Herculean task to frame laws to cover each and every aspect. But, however a balance has to be maintained and laws be evolved so as to keep a check on cybercrimes.

MODULE-III

ROLE OF INTERNATIONAL, INTRANATIONAL, REGIONAL, GOVERNMENTAL BODIES AND INGOS COMBATING CYBER CRIMES

MODULE-III: ROLE OF INTERNATIONAL, INTRANATIONAL, REGIONAL, GOVERNMENTAL BODIES AND INGOS COMBATING CYBER CRIMES

Role of International, Intranational, Regional, Governmental Bodies And Ingos In Prevention Of Cyber Crimes: Traditionally, crime and punishment are largely local, regional, or national. Today, many differences confronting us are associated with the transnational character of cybercrimes. It is therefore important to have international legal instruments ready to serve anti-crime efforts. This chapter looks at international harmonizing efforts to fortify the legal battle against cybercrime, categorizing the actions into four aspects: professional law-enforcement efforts, regional efforts, multi-national efforts, and global international efforts. Subsequently, the article also categorizes the international actions according to the subject-matters into additional aspects, including the promotion of security awareness at both international and national levels, the harmonization of legislation, coordination and cooperation between law-enforcement agencies, and direct anti-cybercrime actions. The article will also examine the nations' attitudes toward the Convention on Cybercrime. Based on the analysis, this module will briefly evaluate the effectiveness of previous attempt at international harmonization.

Different types of organizations:

International organizations: Talking about the differences between international and supranational organizations, an international organization can be defined, following the International Law Commission, as an "*organization established by a treaty or other instrument governed by international law and possessing its own international legal personality*". International organizations generally have States as members, but often other entities can also apply for membership. They both make international law and are governed by it. Yet, the decision-making process of international organizations is often "*less a question of law than one of political judgement*". International organization, institution drawing membership from at least three states, having activities in several states, and whose members are held together by a formal agreement. The two main types of international organizations are intergovernmental organizations and international nongovernmental organizations.

Inter-governmental organisations: Concerning the differences between international and supranational organizations, an intergovernmental organization or *international governmental organisation* (IGO) is an organization composed primarily of sovereign states (referred to as member states), or of other intergovernmental organizations. Intergovernmental organizations are called international organizations, although that term may also include international non-governmental organization such as international non-profit organizations or multinational corporations. Intergovernmental organizations are an important aspect of Public International Law. IGOs are established by a *treaty* that acts as a charter creating the group. Treaties are formed when lawful representatives (governments) of several states go through a ratification process, providing the IGO with an international legal personality. Intergovernmental organizations in a legal sense should be distinguished from simple groupings or coalitions of states; such groups or associations have not been founded by a constituent document and exist only as task groups.

Intergovernmental organizations must also be distinguished from treaties. Many treaties do not establish an organization and instead, rely purely on the parties for their administration becoming legally recognised as an *ad hoc* commission. Other treaties have established an administrative apparatus which was not deemed to have been granted international legal personality.

The first and oldest intergovernmental organization is the International Telecommunication Union, founded in 1865, which served as a model for later organizations such as the League of Nations. The role of international intergovernmental organizations is helping to set the international agenda, mediating political bargaining, and providing a place for political initiatives.

Regional organization: Regional organizations (ROs) are, in a sense, international organizations (IOs), as they incorporate international membership and encompass geopolitical entities that operationally transcend a single nation state. However, their membership is characterized by boundaries and demarcations characteristic to a defined and unique geography, such as continents, or geopolitics, such as economic blocs. They have been established to foster cooperation and political and economic integration or dialogue among states or entities within a restrictive geographical or geopolitical boundary. They both reflect common patterns of development and history that have been fostered since the end of World War II as well as the fragmentation inherent in globalization, which is why their institutional characteristics vary from loose cooperation to formal regional integration. Most ROs tend to work alongside well-established multilateral organizations such as the United Nations.

While in many instances a regional organization is simply referred to as an international organization, in many others it makes sense to use the term regional organization to stress the more limited scope of a particular membership. Examples of ROs include, a.o., the African Union (AU), Association of Southeast Asian Nations (ASEAN), Arab League (AL), Caribbean Community (CARICOM), Council of Europe (CoE), Eurasian Economic Union (EEU), European Union (EU), South Asian Association for Regional Cooperation (SAARC), Asian-African Legal Consultative Organization (AALCO), Union for the Mediterranean (UfM), Union of South American Nations (USAN).

From domestic legislation to international harmonization: Role of different organisations in prevention of cybercrime: People usually are impressed by the illusory overlap between Internet space and international space. Notwithstanding the fact that information systems are linking continents, islands, residents and communities into a giant virtual network, states and areas preserve their traditional sovereignty. McConnell International's metaphor (2000, p. 8) said that: "In the networked world, no island is an island." At this turning point, the globally connected Internet has made cybercrime a trans-border problem. The "international dimension" (Wasik, 1991, pp. 187-201), "trans-national dimension" (Sofaer & Goodman, 2005) or "global dimension" (Grabosky, 2004, pp. 146-157) of cybercrime is universally perceived. While law is always territory-based, the tool, the scene, the target, and the subject of cybercrime are all boundary-independent. Domestic measures will certainly be of critical importance but not sufficient for meeting this

worldwide challenge. International coordination and cooperation are necessary in fighting offences commonly prohibited by every country.

Many international organizations have been making efforts to harmonize actions within their forums. Many authors have also been pursuing research on international harmonization from different standpoints and for different goals; for example, Sieber (1996, 1998), United Nations Crime and Justice Information Network (UNCJIN, 1999), Police Commissioners' Conference Electronic Crime Working Party (2000), Sofaer et al. (2000), Putnam and Elliott (2001), Schjølberg & Hubbard (2005), and so on. Although information about the basic facts of international harmonization that these research studies deal with is the same, different knowledge can be drawn from different thinking. For the purpose of convenient summarization within this article, we categorize the international harmonization actions into the following groups: professional organizations, regional organizations, multi-national organizations, and global organizations. Many other valuable international actions have simply not been considered due to the limit of this study (it is hardly possible to assume that studies on cybercrime can cover all useful international actions of international organizations at all levels).

Professional efforts of International Criminal Police Organization (Interpol: Many international organizations qualify for professional organizations, because their goals and activities are focused on certain specific issues; these organizations include Interpol, the International Telecommunications Union, etc. However, professional efforts here primarily mean substantial actions in the field of cyber-security protection and cybercrime prevention. Although some other organizations also greatly contribute to coordinating cybersecurity protection, their emphasis is not necessarily on the law. By this standard, this section only analyzes the actions of the International Criminal Police Organization (Interpol).

As an international law-enforcement organization with 184 members, Interpol started to tackle computer crime very early, coordinating law-enforcement agencies and legislations, in regard to which Interpol made efforts to improve counter-cybercrime capacity at the international level. A 1981 survey of members on cybercriminal law recognized dilemmas in application of existing legislation (Schjølberg & Tingrett, 2004). Based on the recognition of the legal gaps between countries, and gaps between the legal framework and criminal phenomena, Interpol expanded its task to both law enforcement and legal harmonization.

Currently, there are four working parties within the framework of Interpol, comprising African, American, Asia-South Pacific and European Working Parties on Information Technology Crime. Besides these groups, a Steering Committee for Information Technology Crime was established in order to harmonize the different regional working-party initiatives. Considering the already-harmonized legislation as the prerequisite for the coordinated law enforcement, the African Working Party agreed upon "the project on legislation and comparative law existing in the Africa with a view to having more African states co-signing and/or ratifying the Council of Europe Cybercrime Convention." Apparently, legal harmonization is one of Interpol's important tasks in working towards an effective law-enforcement environment.

In regard to law enforcement, Interpol has provided a technical guidance in cybercrime detection, investigation and evidence collection. The Interpol Information Technology Crime Investigation Manual was compiled by the European Working Party on Information Technology Crime. Compared with the substantive and procedural law harmonization of today's Convention on Cybercrime, the Manual developed a technological law-enforcement model to improve the efficiency of combating cybercrime.

Along with efforts in law enforcement on cybercrime, Interpol also takes distinct actions to prevent cybercrime, cooperating with credit-card companies to combat payment fraud by building a database on Interpol's web site (Police Commissioners' Conference Electronic Crime Working Party, 2000, p. 64). As one of the necessary cooperation projects at the international level of law-enforcement, cybercrime and other trans-border crimes are specially dealt with by Interpol in gathering and sharing information. In addition, Interpol is making efforts to establish a network to for harvesting information relating to activities on the Internet.

Regional efforts: There are many regional international organizations, with a narrow or broad coverage of states, more or less making efforts to maintain cybersecurity and harmonize international measures to combat cybercrime. This section will introduce only four of these organizations, which have taken typical actions in combating cybercrime.

i. The Asia-Pacific Economic Cooperation (APEC)

In the Asia-Pacific region, the APEC coordinates its 21 member economies to promote cyber-security and to tackle the risks brought about by cybercrime (APEC, 2003). The APEC has conducted a capacity-building project on cybercrime for member economies in relation to legal structures and investigative abilities, where the advanced APEC economies support other member-economies in training legislative and investigative personnel.

After the 9/11 attacks on the U. S., the APEC Leaders issued a Statement on Counter-Terrorism, condemning terrorist attacks and considering it urgent to reinforce collaboration at different layers to fight against terrorism. The Leaders called for reinforcing APEC activities to protect critical infrastructure.

The Telecommunications and Information Ministers of the APEC economies issued the Statement on the Security of Information and Communications Infrastructures and a Programme of Action in 2002, supporting measures taken by members to fight against misuse of information. The Senior Officials' Meeting has made a recommendation which designates six areas that can serve as the foundation for the APEC's endeavor for cybercrime prevention, comprising legal development, information sharing and cooperation, security and technical guidelines, public awareness, training and education, and wireless security. The Ministers and Leaders of APEC have made a commitment to "endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including the UN General Assembly Resolution 55/63 and Convention on Cybercrime by October 2003."

In response to this call from the leaders, a survey of laws was carried out and a summary was made of the responses from member economies received in 2003 (E-Security Task Group, 2003). The economies proposed corresponding projects in information-security task groups. For example, the U.S. proposed a project in the E-Security Task Group of the Telecommunications and Information Working Group. The first phase of this project was a meeting of cybercrime experts from around the region. The meeting was held from 21-25 July, 2003 in Bangkok, Thailand, and was attended by over 120 delegates from 17 economies. The objectives of the meeting were to assist the economies to develop the necessary legal frameworks; to promote the development of law-enforcement capacity; and to strengthen cooperation between private and public sectors in addressing the threat of cybercrime In the conference, the experts present agreed that every economy needed a legal framework including one for substantive and procedural law, and for the law and policies of inter-economies cooperation. They confirmed the role of international instruments, particularly the Convention on Cybercrime. They also emphasized jurisdictional cooperation, law-enforcement construction, and the capacity building of the investigators.

In 2005, The sixth APEC Ministerial Meeting on the Telecommunications and Information Industry passed the Lima Declaration, "encouraging all economies to study the Convention on Cybercrime (2001) and to endeavor to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with international legal instruments, including UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001)." However, due to the great difference between member economies within the APEC, the development toward unified legal instruments has not been too satisfactory. Although some economies have claimed that their laws have been completely consistent with the Convention, and some other economies were taking actions to implement provisions similar to the Convention, many other countries have quite different legal systems or have no law criminalizing cybercrime.

Efforts are still to be made in the forum of the APEC to address cybercrime. The U.S. proposed the Judge and Prosecutor Cybercrime Capacity Building Project in 2006 in order to develop a curriculum devised by government and private sector experts; to translate the curriculum into domestic languages; and to train the trainer (judges and prosecutors).

ii. The Council of Europe (COE)

The Council of Europe has been working to tackle rising international anxiety over the risks brought about by the automatic processing of personal data since the early 1980s. In 1981, the Council of Europe implemented the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108, 26 January 1981), which was revised according to the Amendment to Convention ETS No. 108 Allowing the European Community to Accede, 15 June 1999, and the Additional Protocol to Convention ETS No. 108 on Supervisory Authorities and Trans-border Data Flows, 8 June 2000. The Convention recognized the desirability "to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing," and the necessity "to reconcile the fundamental values of the respect to privacy and the free flow

of information between peoples" (Preamble). The Convention covers the protection of personal data in both the public and private sectors.

Chapter II of the Convention established basic principles for data protection, one of which is data security (Article 7), covering the prohibition of accidental or unauthorized access, alteration and dissemination.

The expert committee appointed in 1985 published Recommendations of 1989 and 1995, addressing the issues of substantive laws and procedural law in this area respectively (See Recommendation No. R. (95) 13). Recommendation R. No. (89) 9 recognized the importance of an adequate and quick response to the new challenge of computer-related crime, which often has a trans-border character, and recommended the governments to consider the Report on Computer-Related Crime drawn up by the European Committee on Crime Problems.

Then there is Recommendation No. (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology. The Recommendation recognized that information systems may also be used for committing criminal offences, evidence of criminal offences may be stored and transferred by these systems, while the criminal procedure law of member states often do not provide for appropriate powers to search and collect evidence in these systems during a criminal investigation. The appendix to the Recommendation lays down the principles for criminal procedure laws on search and seizes, technical surveillance, obligations to co-operate with the investigating authorities, electronic evidence, use of encryption in research, statistics and training, and international cooperation.

In 1997, the Council of Europe began drafting the Convention on Cybercrime, which was open for signature in 2001 and took effect in 2004. In 2003, the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer System (ETS NO. 189) was implemented. The Convention addresses substantive law, procedural law, jurisdiction, and international law in the field of cybercrime. The Convention is a historic landmark in the combat against cybercrime. It is expected that the Convention will have a deep impact on the legal reform relating to cybercrime in its 46 member states and one candidate state.

In the 2004 Conference on Cybercrime, the Council of Europe called for "wide and rapid" access to and "effective implementation" of the Convention on Cybercrime, raising awareness in the highest political level, and encouraging cooperation between public and private sectors.

In the 2005 Conference on Cybercrime, the Council of Europe expressed concern about the fast-increasing threats and serious social and economic results of cybercrime including terrorist activity on the Internet, noting that most cybercrime is international cybercrime, recognized the need for effective and compatible laws and tools to enable efficient cooperation to combat cybercrime, calling upon public and private cooperation, and encouraging access to the Convention on Cybercrime.

In 2006, the Council of Europe launched a Project against Cybercrime, intended to grant assistance to the development of national legislation in line with the provision of the Convention, training of judges, prosecutors and law-enforcement officers, and training of criminal justice officials and 24/5 contact points in international cooperation.

iii. The European Union

The EU took a series of actions to tackle cybercrime through impelling a coordinated law enforcement and legal harmonization policy. Civil liberty has also been a focus in the anti-cybercrime field.

In 1995, the European Parliament and the Council endorsed Directive 95/46/EC of 24 October 1995 on the protection of Individuals with regard to the Processing of Personal Data and on the Movement of Such Data. Section VIII of the Directive specifically deals with confidentiality and security of processing of personal data. The Directive applied to protection of natural persons (Article 2(a)). The scope of the Directive was limited to the processing of personal data entirely or partially by automatic means (Article 3-1). The Directive required that appropriate technical and organizational measures have to be implemented to protect personal data against illegal destruction, alteration, access and other illegal forms of processing (Article 17-1).

The Directive required the Member States to provide administrative and judicial remedies for the victim (Article 22), and provided for the compensation liability of (Article 23) and sanctions on (Article 24) the transgressor.

In 1997, the European Parliament and the Council endorsed Directive 97/66/EC of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. The Directive was aimed at furthering the protection implemented in Directive 95/46/EC, and providing for the harmonization of the member states' provision to attain an equivalent level of protection (Article 1-1). The Directive extended the protection of legitimate interests to legal persons (Article 1-2).

The application scope of the Directive was limited to the processing of personal data relating to the provision of publicly available telecommunications services in the public telecommunications networks; particularly via the ISDN (Integrated Services Digital Network), and public digital mobile networks (Article 3-1). As the Directive 95/46/EC is concerned with automatic processing systems, Directive 97/66/EC has emphasized the linkage with the telecommunications network. The Directive provides requirements directly targeted at the service providers (but not member states) "to take appropriate technical and organizational measures to safeguard the security of its services." (Article 4-1). The Directive requires the Member States to implement the regulations ensuring the confidentiality of communications, prohibiting listening, tapping, storage or other kinds of interception or surveillance of communications by unauthorized natural and legal persons (Article 5). The Directive limited unsolicited communications (Article 12), which covers automatic calling systems or facsimile machines, but not e-mails. On 27 November 2001, a plenary session

took place in Brussels of the EU Forum on Cybercrime, organized by the EC and where the primary discussion was about the retention of traffic data (EU Forum on Cybercrime, 2001).

In April 2002, the Commission of the European Communities presented a proposal for a Council Framework Decision on Attacks against information systems, and this proposal constitutes the case of the Decision of 24 February 2005. The Framework Decision criminalized the offences of illegal access to information systems (Article 2), illegal system interference (Article 3), illegal data interference (Article 4), and instigation, aiding and abetting of these offences or attempt at them (Article 5). The Framework Decision only dealt with attacks through unauthorized access to or interference with information systems or data. According to the Decision, illegal access can only be constituted when the illegal activities are targeted intentionally against an "information system with specific protection measures in place and [the attacks] must be for economic gain." (Article 2)

The Commission further considered the future possibility of "specific protection measures" (Proposal for a Council Framework Decision on Attacks against information systems) to broadband networks, saying that, "it is necessary that criminal law covers unauthorized access to their systems even though there may not be adequate technical protection for their systems." (ibid.) Thus, concerning the interference with information systems, it is constituted by serious "hindering" or "interrupting" of the functioning of information systems by "inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data" (Article 3).

This Framework Decision does not specify penalties for illegal access to information systems and instigation, aiding and abetting and attempting of these offences, but requires member states to take the necessary measures to ensure that they are punishable by effective, proportional and dissuasive criminal penalties (Framework Decision, Article 6.1). The Decision specifies the penalties for illegal system interference and illegal data interference as punishable by criminal penalties to a maximum of at least one to three years of imprisonment (Article 6.2). As for the "aggravating circumstances", the criminal draws a maximum of at least two to five years imprisonment (Article 7.1). These aggravating circumstances include an organized attack, and an attack that has "caused serious damages or has affected essential interests" (Article 7.2). Criminal organization is defined as a "structured association, established over a period of time, of two or more persons, acting in a concerted manner with a view to committing offences."

It is worth noting that the matters mentioned in the Framework Decision can also be found in the Convention on Cybercrime. After revision of the legislation required by the Convention, the national law (of Finland) will also meet the demand of the Framework Decision. Today, comprised of 27 member states and three candidate countries, the EU remains active in addressing cybercrime.

iv. The Organization of American States (OAS)

As other regional organizations, the Organization of American States (OAS) with 35 member states is also highly concerned about the issue of cybercrime. Through its forum for the

Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA), the OAS has long recognized the central role that a sound legal framework plays in combating cybercrime and protecting the Internet. Such recognition has prompted the REMJA to recommend the creation of the Group of Governmental Experts on Cybercrime (The Group of Experts) in March 1999. The Group of Experts has been devoted to analyzing cybercrimes, to inspecting the domestic cybercrime law, and to finding ways of cooperating in the Inter-American system of combating cybercrime. The Group of Experts has held four meetings. The Meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA III) has urged member states to take steps to endorse cybercrime law; harmonize cybercrime laws to make international cooperation possible. The Meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA V) has recommended that member states evaluate the advisability of implementing the principles of the Convention on Cybercrime, and consider the possibility of acceding to that Convention.

In 2004, the Fourth Plenary Session of the Organization of American States General Assembly passed the resolution on "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity," proposing that "An effective cybersecurity strategy must recognize that the security of the network of information systems that comprise the Internet requires a partnership between government and industry."

Multi-national efforts

Unlike professional organizations that are limited to a more specific field of concern, and unlike regional organizations that are limited to a more specific location of states, the multi-national international organizations care for affairs of a broader range and take actions in a broader territorial environment. This section recounts the efforts of three of the multi-national organizations.

i. The Commonwealth of Nations

The Commonwealth of Nations took a direct and timely action in the harmonizing laws of its member states. In October 2002, the Commonwealth Secretariat prepared the "Model Law on Computer and Computer Related Crime" (Bourne, 2002, p. 17). Within the Commonwealth's 53 member countries, the "Model Law" has had a wide influence on domestic legislation. Through this model law, the Convention on Cybercrime has become one of the legislative choices in substantive criminal law, covering the offences of illegal access, interfering with data, interfering with computer systems, illegal interception of data, illegal data, and child pornography.

Compared with the Convention on Cybercrime, the Model Law expanded criminal liability - so as to include reckless liability- for the offences of interfering with data, interfering with computer systems, and using illegal devices. The Model Law also covered the problem of dual criminality by stating that the act applied to an act done or an omission made by a national of a state outside its territory, if the person's conduct would also constitute an

offence under a law of the country where the offence was committed. This may lead to prosecution or extradition based on dual criminality, but not extradition as it is provided in the Convention on Cybercrime.

Some of the member countries of the Commonwealth have made efforts to draft domestic law according to the model law, such as Bahamas and St. Lucia. In Barbados, Belize, and Guyana, the Model Law is being considered as a guide to the enactment of similar legislation. However, in many other countries of the Commonwealth, there is still no special legislation for cybercrime.

Besides impelling legislation within the forum, another focus of the Commonwealth is on mutual assistance in law enforcement between Commonwealth member states and between Commonwealth member states and Non-commonwealth States. In the 2005 Meeting of Commonwealth Law Ministers and Senior Officials, the Expert Working Group proposed 10 recommendations for member states to adopt suitable measures for improving domestic law enforcement and trans-national assistance, and encouraged member states to sign, ratify, accede to and implement the Convention on Cybercrime as a basis for mutual legal assistance between Commonwealth member states and non-Commonwealth states.

ii. The Group of Eight (G8)

Since the mid-1990s, the Group of Eight (G8) has created working groups and issued a series of communiqués from the leaders and actions plans from justice ministers. At the Halifax Summit 1995, the Group of Seven recognized "that ultimate success requires all governments to provide for effective measures to prevent the laundering of proceeds from serious crimes, to implement commitments in the fight against trans-national organized crime." The group released 40-point set of "recommendations to combat Trans-national Organized Crime efficiently" at the G7/P8 Lyon Summit. The recommendations urged the states to increase the level of criminalization, prosecution, investigation, and international cooperation, while acknowledging in their entirety human-rights protection.

At the Denver Summit 1997, the Group of Eight proposed to strengthen their efforts to realize the Lyon recommendations, by concentrating on punishing high-tech criminals, and promoting the governments' technical and legal abilities to react to trans-territorial computer crimes. The Group of Eight Meeting of the Justice and Interior Ministers of December 1997 responded to the increased international movement of criminals, organized crime, and terrorists and their use of the ICT. Ministers noted, in a Statement of Principles Concerning Electronic Crime, that, while criminal legislation was a national responsibility, the character of the information networks obstructed countries from operating traditional power over this problem. Domestic legislations have to be complemented by international cooperation to criminalize the abuse of the networks and harmonize the investigative action.

At the subsequent summits, the Group of Eight repeatedly expressed their concern about cyber-criminality. At the Okinawa Summit, the Okinawa Charter on Global Information Society adopted the principle of international collaboration and harmonization of cybercrime. "In order to maximize the social and economic benefits of the information society", the

Group of Eight agreed on principles and approaches for the protection of privacy, the free flow of information, and the security of transactions. The Charter recognized that the security of the information society necessitated coordinated action and effective policy responses.

iii. The Organization for Economic Cooperation and Development (OECD)

With its 30 member countries, the OECD addressed computer security for several decades. In 1983, an expert committee was appointed by the OECD to discuss computer crime phenomena and criminal-law reform (Schjolberg & Hubbard, 2005). Offences against confidentiality, integrity or availability listed in the 1985 OECD document included unauthorized access, damage to computer data or computer programmes, computer sabotage, unauthorized interception, and computer espionage. In December 1999, the OECD officially approved the *Guidelines for Consumer Protection in the Context of Electronic Commerce* (Department of Justice, 2000, p. 27), representing member states' consensus in the area of consumer protection for e-commerce: consumers should be protected in e-commerce not less than the protection they enjoyed within traditional commerce (Department of Justice, 2000, p. 27). The OECD adopted Guidelines for the Security of Information Systems and Networks in July 2002, calling on member governments to "establish a heightened priority for security planning and management", and to "promote a culture of security among all participants as a means of protecting information systems and networks" (OECD, 2002a, Part I).

The guidelines established nine principles, including awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment (OECD, 2002a, Part III). Because of the nature of the guidelines and the distance from the legal actions, practical endeavors were left to the member countries to make.

Global international efforts by the United Nations (UN): There are numerous global organizations. Nevertheless, the UN is capable of being identified as the only global organization that forms a forum of its 191 member states with fuller functions. Compared with professional organizations, the UN does not limit its activities to certain domains. Compared with regional organizations, the UN does not limit its activities to certain states (in the field of cyber-security protection and cybercrime prevention). The actions of the UN have unique advantages in coordinating international positions.

In 1985, General Assembly Resolution 40/71 of 11 December called upon governments and international organizations to take action in conformity with the recommendation of the commission on the legal value of computer records of 1985, in order to ensure legal security in the background of the broadest possible use of information processing in international transactions. In 1990, the General Assembly of the UN adopted the Guidelines Concerning Computerized Personal Data Files. It proposed to take appropriate measures to protect the files against both natural and artificial dangers. The guidelines extended the protection of governmental international organizations (Part B).

"*The International Review of Criminal Policy: United Nations Manual on the Prevention and Control of Computer-related Crime*" called for further international work and presented a proper statement of the problem. It stated that at the international level, further activities could be undertaken, including harmonizing substantive law, and establishing a jurisdictional base.

The Background Paper for the Workshop on Crimes Relating to the Computer Network at the Tenth UN Congress on Prevention of Crime and Treatment of Offenders proposed two levels of definition of cybercrime: In the narrow sense, that is, the strict computer crime, had to refer to "any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them." In the broad sense, that is, computer-related crime denoted "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distribution information by means of a computer system or network."

The UN General Assembly has endorsed several resolutions dealing with its desire to witness progress regarding this issue. According to information provided by Schjølberg and Hubbard(2005), checking Resolutions 55/63 (2000) and 56/121 (2001) on Combating the Criminal Misuse of Information Technology, the value of the Group of Eight Principles was noted, and states were urged to consider these principles; checking Resolutions 53/70 (1998), 54/79 (1999), 55/28 (2000), 56/19 (2001), 57/53 (2002), 57/239 (2002), 58/32 (2003), and 58/199 (2003), all calling on member states "to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats." These resolutions have the same motive to improve the cybersecurity awareness at both the international and the national levels.

In Resolution 55/63, the General Assembly noted the value of the following measures to combat computer misuse:

a. To ensure the elimination of safe havens for cybercriminals;
b. To coordinate cooperation in the investigation and prosecution of cybercrime;
c. To exchange information for fighting cybercrime;
d. To train and equip law-enforcement personnel to address cybercrime;
e. To protect the security of data and computer systems from cybercrime;
f. To permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;
g. To ensure mutual assistance regimes for the timely investigation of cybercrime and the timely gathering and exchange of evidence;
h. To remind the general public of the requirement to prevent and combat cybercrime;
i. To design information technologies to help to prevent and detect cybercrime;
j. To take into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight cybercrime.

The General Assembly invited states to consider the measures in their endeavor to fight the criminal misuse of information systems, and decided to maintain the question of the criminal misuse of information technologies on the agenda of its future session. In Resolution 56/121,

the General Assembly invited states to consider the work and achievements of the Commission on Crime Prevention and Criminal Justice and of their international and regional organizations when developing national law, policy and practice to prevent cybercrime. The resolution emphasized the value of the measures set forth in Resolution 55/63, and again invited states to take them into account in their efforts to combat the criminal misuse of information technologies. However, the General Assembly decided to postpone consideration of this subject, pending work considered in the plan of action against high-technology crime of the Commission on Crime Prevention and Criminal Justice.

It is necessary to mention that, besides the advantages, the disadvantages of the UN's actions are also striking. The UN is a multifunctional international organization, which in some sense has malfunctioned over the years. Focusing on the current topic, it can be said that the consensus on cybercrime in this forum remains a preliminary one. The diversified legal systems of members of this gigantic organization hinder the conclusion of a fruitful agreement.

The focuses of international harmonization: From the above presentation on international actions in anti-cybercrime areas, we can further summarize the major themes of these international organizations. These aspects mainly include the promotion of security awareness at both the international and national levels, the harmonization of legislation, coordination and cooperation in law enforcement, and direct anti-cybercrime actions.

i. Promotion of security awareness at the international level

The typical actions in this aspect have been taken by the UN. The UN's two Resolutions (55/63 (2000) and 56/121 (2001)) on Combating the Criminal Misuse of Information Technology recalled the importance of the Group of Eight principles, and urged states to take these principles into account. Some other resolutions also called on member states to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as promising measures to limit these threats. Other international organizations also made efforts to promote security awareness at the international level. For example, after the 9/11 incidents, the APEC Leaders called for a reinforcing of APEC activities to protect critical infrastructure.

ii. Promotion of security awareness at the state level

All international organizations have made efforts to promote security awareness at the domestic level. For example, the APEC guided its member states and regions to promote cyber-security and tackle the threats of cybercrime. The APEC also conducted a project for developed states to support other states in training personnel. The Shanghai Declaration of 2002 supported measures to fight against misuse of information.

iii. Harmonization of legislation

Legal harmonization has been a major emphasis on the work of various international organizations. Harmonization in Europe started in the 1980s and a recent achievement was

the Convention on Cybercrime. Other international organizations have also endeavored to attain legal harmonization. Early in 1981, Interpol surveyed the criminal laws of member states so as to explore defects in the existing legislation, and made efforts to harmonize the laws. Today, Interpol's African Working Party on Information Technology Crime Projects is trying to persuade the African states to sign and ratify the Convention on Cybercrime. APEC also took steps to survey the laws and to encourage economies to enact comprehensive laws consistent with the Convention on Cybercrime and the pertinent UN resolutions.

The EU Framework Decision of 2002 specifically granted the member states the responsibility of criminalizing the offences of illegal access to and illegal interference with information systems. The REMJA urged states to criminalize cybercrime and harmonize the member states' laws, and consider the possibility of joining the Convention on Cybercrime. The Commonwealth Model Law on Computer and Computer Related Crime expanded the criminal liability of the Convention on Cybercrime so as to include reckless liability. Through this Model Law, the Commonwealth made efforts to criminalize cybercrime in the member countries. The Group of Eight Paris Conference discussed the public and private interact with the objective of implementing an international penal code for fighting cyber-criminality. The Okinawa Charter on Global Information Society further consented to international collaboration and harmonization concerning cybercrime.

iv. Coordination and cooperation in law enforcement

Interpol's European Working Party on Information Technology Crime compiled the Computer Crime manual to provide technical guidance in law enforcement. The Convention on Cybercrime also covers cooperative mechanisms in law enforcement against cybercrime. The EU discussed about the retention of traffic data in 2001. The Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA)'s Group of Experts on Cybercrime have been devoted to discover cooperation ways in the Inter-American system to combat cybercrime. The Group of Eight reviewed existing cooperation mechanisms and gaps, and made attempt to discover ways to fill these gaps. The Group urged the states to increase criminalization, prosecution, investigation, and international cooperation. The Denver Summit proposed to promote governments' technical as well as legal abilities to act in response to trans-territorial computer crimes. The Birmingham Summit called for agreement on a legal framework for evidence preservation and protection of privacy, and for agreements on the international sharing of evidence so as to struggle more effectively against a broad scope of crimes, including cybercrime.

v. Direct anti-cybercrime actions

The direct international anti-cybercrime actions comprise two fundamental aspects: cybercrime prevention and cybercrime investigation. They have been more valuable before international harmonization in legislation could come into being. Different organizations have taken individual measures with specific emphases. For example, Interpol directly cooperated with credit-card companies to fight against payment fraud. The OECD's *Guidelines for Consumer Protection in the Context of Electronic Commerce* 1999 emphasized the protection of consumers in e-commerce as well as that in traditional

commerce. Guidelines for the Security of Information Systems and Networks 2002 called on member governments to "establish a heightened priority for security planning and management", and to "promote a culture of security among all participants as a means of protecting information systems and networks".

From conversation to the European Convention

As one of the most outstanding achievements, international actions bred a comparatively effective implementation: the Convention on Cybercrime and its Protocol. The general purpose of the Convention is laid down in the Preamble as to deter crimes against the confidentiality, integrity and availability of information systems and the misuse of such systems. The purpose of the Protocol is to supplement the provisions of the Convention on cybercrime on the criminalization of acts of a racist and xenophobic nature committed through information systems (Protocol, Article 1). The Convention has been widely accepted as a landmark, providing for both the substantive and procedural legal frameworks, both the domestic and international level of countermeasures, so as to achieve higher effectiveness in fighting against cybercrimes.

Articles 2-12 of the Convention have required nations to criminalize the activities of illegal access to data and computer systems; illegal interception; data and systems interference; misuse of devices that can be used to enact the aforementioned crimes; computer-related forgery and fraud; content-related offences including child pornography; copyright crimes; and attempt, aiding or abetting. Article 13 of the Convention also establishes corporate liability, and sanctions and measures for these offences. Articles 3-7 of the Protocol require nations to criminalize the activities of disseminating racist and xenophobic information through information systems. Also to be criminalized is racist and xenophobic motivated threat, racist and xenophobic insult, and in respect of genocide or crimes against humanity, denial of their existence, gross criminalistic approval or justification of them, and the behavior of aiding and abetting them.

The Convention provides two constituent elements for cybercrimes. First, the Convention establishes criminal liability on the subjective element of intent. Sometimes, the constitution of certain offences requires elements such as intent to procure "economic benefit" in computer-related fraud provided by Article 8. Second, the Convention establishes criminal liability on the objective element on act "without right" in all offence provisions. The problems of what is an act committed intentionally, what is an act with right and without right, are all left to national law interpretation.

The Convention allows domestic laws to provide additional constituent elements, and provides the possibility of a reservation. Apparently, the Convention fully respects the decision-making of member states on the matter of criminal policy. As a result, we have good reason to worry that this diversified implementation will decrease the consensus on the harmfulness of conducts and increase the possible obstacles to international actions. The negative effect of this kind of provision is expected to diminish the effectiveness of prolonged expensive international negotiation for an agreement, although the provision itself is exactly one of the contents negotiated and agreed upon.

The Convention has also been criticized by civil liberties groups concerned that it will undermine individual privacy rights and that it expands too greatly surveillance powers, and is fundamentally unbalanced. As Taylor (2004) pointed out, the Convention contains comprehensive, far-reaching powers of surveillance, search, and seizure, while lacking a criterion for the protection of privacy and limitation of power. The basic concerns in the field of human rights are the over-expansion of the states' power of surveillance, and over-criminalization of citizens' behavior. Before information systems have been completely developed, the states would strictly take this borderless system under control; those who use information systems would voluntarily enter the tight legal encirclement. For those who use information systems before these legal instruments, they are to accept externally imposed constraints; while for those who use information systems after these provisions, they are born into an inherent limitation. Both these two groups of users may feel a loss of freedom of information.

Despite the anxiety mentioned above, the Convention has unquestionably had some influence on the worldwide consensus in relation to the predicament of cybercrime. We are capable of seeing that the Convention will become one of the important steps towards a broader international accomplishment.

Firstly, some countries have taken practical measures to ratify the Convention. The total number of ratifications and accessions is 19 countries, including one non-member state of the Council of Europe, the U. S., with 24 countries (including three non-member states of the European Council, Canada, Japan and South Africa) having signed the Convention, not followed by ratifications. The treaty has entered into force in only a small number of countries, representing a small proportion in terms of land area and population. However, it is still an important step towards a broader consensus: "A little is better than none."

Secondly, besides successful endeavors, countries, including most signatory countries, are still on their way to ratifying the treaty. The Council of Europe Conference on "Cybercrime: a Global Challenge, a Global Response" in 2005 "strongly encourage states to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level and on behalf of international co-operation." The treaty has come into force in some of the Nordic countries, including Denmark, Iceland, and Norway, but Finland and Sweden are still seeking ratification though they were both countries of signature on the date opening for signature in 2001.

However, this process has proved hard without the expected number of countries ratifying in the five-year period after the Convention was open to signature. The pressure against not ratifying the treaty coming from inside the countries seems to be a greater obstacle than the differences over the drafting of the document. A significant obstacle comes from the difference of legislative styles between the Convention and the individual countries. Many of the valid provisions in current Finnish law do not need revision. Whether the original Finnish Penal Code (which includes quite a few revisions concerning offences relating to data processing) is capable of dealing with *all* of the offences provided by the Convention has not been tested in judicial practice. But the Finnish legislature will have to add some new

provisions to the Penal Code, if it wants to cope with the Convention. Expressly, provisions concerning the offence of interference with and gross interference with the information processing systems, the offence of possession of instruments for cybercrime (covering the computer viruses), the liability for inchoate cybercrime, and for corporate liability, and so forth must be taken in.

The critical challenge of the Convention on Cybercrime to conventional international legal cooperation lies in the absence of a demand for the double criminality criterion. Since this criterion is in decline, individual countries are far from implementing it in domestic law, either. In accepting the Convention, individual countries will therefore have to revise domestic laws in the relevant area.

Some other countries are seeking to remodel the Convention so as to provide a prohibition on the types of conducts and to create procedural and international mechanisms for serving successful investigations and prosecutions of crimes. The flexibilities of the Convention may have a positive effect in leaving to member states the alternative of using different methods and languages in their domestic law. This may actually lead to a wider application of the Convention so as to cover more and diversified legal systems. While the U.S. has asserted that its own domestic law does not need revision, South Africa has implemented substantial criminal provisions in line with the Convention. Japan is considering filling the gap between its domestic law and the Convention. At least, among the APEC economies, Taiwan, the Philippines, and Hong Kong are considering taking the Convention as the basis on which they will carry out their own legislative amendments.

Some international organizations are propelling cooperation in promoting the member states' access to the Convention. As mentioned above, in the framework of Interpol, the African Working Party on Information Technology Crimes is working to promote domestic legislation and adherence to the Convention. APEC, the EU, and the REMJA V of the OAS have also taken measures to spread the Convention to its member states. There are also efforts to develop cybercrime legislation beyond the Convention. As mentioned above, the Commonwealth's model law represents a breakthrough in extending criminal liability to the *mens rea* of offences of interfering with data, interfering with computer systems, and illegal devices so as to include reckless liability. Some of the Commonwealth's member states are also on their way towards legislation that will model the Convention and model domestic law.

Finally, in fact, most countries, particularly countries where cybercriminals are usually left at large, have taken no action in spite of the importance of the Convention. These countries have very specific interests in maintaining what may be considered "criminal" in other countries but are "legal" in their own countries, as far as web sites, services, or even sales of goods online are concerned. The potential cybercrime perpetrators, regardless of whichever nationality they belong to, also seek asylum in such countries in order to escape punishment by countries that are seeking to extend their judicial arms to deal with cases committed inside their sovereign territory and committed by their citizens outside their territory.

Although the Convention on Cybercrime has been attracting increasing attention at both the domestic and international levels, it is necessary to point out that, once the Convention was in documentary form, the enthusiasm and efforts of other international entities towards a higher degree of international harmonization of legislation have been to some extent weakened. This situation reflects neither the purpose, nor the intended side effect of the Convention. However, a ready instrument must have its negative influence on the otherwise unsettled disputes of the problems of cybercrime deterrence. Regrettably, both the advantages and disadvantages of the Convention will bring about a more cautious discussion and a better plan will be discouraged from being implemented. At least, the similar but different schedules for international treaties, in either broader or narrower scope, have seen an interruption with the passing of the Convention. The Convention thus becomes not only a mutual compromise of member states, but also a turning-point in the knowledge and experiences of cybercrime punishment and prevention.

Traditionally, new legal instruments have usually been the subject of academic annotation immediately after its implementation, while the legislature is usually reluctant to change existing legal instruments. These two factors further determine the unfortunate fate of the better and newer proposals, particularly proposals having more or less better elements than the implemented one. In a word, we can say that classics were good, but classics hinder better classics; consensus is good, but consensus always hinders better consensus: and the Convention is good, but it potentially hinders a better convention.

Although the Convention was also appraised by politicians, such as the U. S. President George W. Bush, as "providing for broad international cooperation in the form of extradition and mutual legal assistance", and containing "safeguards that protect civil liberties and other legitimate interests" (Bush, 2003), the effectiveness of the Convention's cooperative framework is subject to reasonable doubt without a majority of countries' access to the agreement (Goldsmith, 2005, p. 4). Authors such as Archick (2004) have proposed that the Convention's arm would not be long enough to reach the countries that are regarded as a "haven" for cybercriminals: attacks are launched from those countries, but the countries do not join the agreement. Consequently, the countries with law and without law, or being the member and being non-member of the Convention, have to encounter mutual conflicts. The situation confronting international society is obviously still one of the tardiness of the acceptance of existing instruments and the lack of a universal agreement.

The limited progress in the international harmonization: Over the years, the international co-operation on cybercrime has been very active and comprehensive (Pihlajamäki, 2004, p. 286). The international level of consensus on criminal law has, however, not been achieved. Previously, the criminalization of war crimes, crime against peace, crimes against humanity, genocide, torture, and other crimes have been the successful examples. The application of pertinent agreements in specific courts has demonstrated that an international forum can acquire certain achievements prior to legislation at the national level. Traditional international criminal law has aimed at harmonizing substantive law and coordinating procedural law on offences that have existed in society since the coming into being of humankind.

Presently, what the countries are eager to realize is an international agreement on offences with a history of only several decades. The anxiety for success, the absence of trial practice, the lack of an accumulation of experience and knowledge, the alienation between the legislature and general public, and the different interests between the various countries, all deliver an international consensus in its lowest form. It is inevitable that during the drafting stage and particularly after the Convention on Cybercrime has been opened for signature; many commentators have published their evaluation and criticism. Combined with other progress made in international harmonization, the most important unsolved problem may be the limited participation and the limited consensus.

Firstly, international harmonization has hitherto been primarily the forum of the developed countries. The working mechanism of an effective international treaty is for all of the signatory countries to take effective action and preserve a common theatre of operation. The treaty is not aimed at any third party and thus the third party is not restrained by it. The participating countries of the Convention on Cybercrime are limited, representing only a limited population. Along with the development of the Internet globally, the number of cybercrimes will be correlated with the population base of Internet penetration, and the global population base. Most of the present international harmonization measures have not been incorporating the countries with the largest population. This will make the measures less effective. Considering the characteristics of cybercrime, the "safe haven for criminals" can only be eliminated when almost all the sovereign states have access to one agreement and almost all the online users are subject to the power of law enforcement. Although an international document can be modeled by member states when making domestic laws, the expectations should not be raised too high in respect of a timely update at a similar pace when it comes to international measures.

Secondly, another limitation is that a lower level of consensus has been reached. Unlike traditional offences in international criminal law, which have rarely been penalized in domestic law, cybercrime was initially devised in the legislation at the national level. In many countries, domestic legislation on offences such as genocide, crime against peace and similar types of crime did not happen before the countries were subject to the obligation of international treaties. The situation of cybercrime is that countries that have already enacted laws assisted or forced the countries that have not enacted laws to enter a consensus. As a whole, international cooperation in preventing cybercrime is more sluggish than domestic legislation; its impact on domestic legislation is, nonetheless, undeniable. Domestic laws should be amended according to international instruments so that the measures provided in the international instruments can be effectively carried out. An agreement on a wider scope of issues in cybercrime is also necessary so as to ensure effective law enforcement. However, such an agreement is still lacking. The efforts of various international organizations should be integrated into a more unified action.

Thirdly, there is, strangely, a tendency towards pluralization on the international harmonization. In regulating or deregulating the information community, different interest groups stay at different standpoints. In criminalizing and decriminalizing the online activities, different players hold different opinions. Different organizations propose countermeasures for the benefit of a certain number of their member states. Yet other

organizations oppose any kinds of plans for imposing constraints on the free use of information systems. The mechanism is that while one interest group is anxious about the misuse of information systems, another group may concentrate on the side-effect of anti-misuse actions. Various international harmonization measures are full of a trade-off of interests and a contrast of powers. This marathon process of negotiation has inherited the inherent style of international actions.

Fourthly, another tendency is the regularization of international harmonization. The effect of international harmonization is less significant compared with the efforts. The role of the UN as a universal international organization seems limited to arranging an international treaty in this area. If the United Nation's frequent "call" does not motivate member states to legislate on cybercrime, a universal agreement would be a better alternative in promoting consensus. The UN may have the opportunity to incorporate the consensus reached in other fields into the above-mentioned unified action.

Globalization does not mean globalized welfare at all. Globalized information systems accommodate an increasing number of trans-national offences. The network context of cybercrime makes it one of the most globalized offences of the present and the most modernized threats of the future. We can take actions in two different ways to resolve this problem. One is to divide information systems into segments bordered by state boundaries. The other is to incorporate the legal system into an integrated entity obliterating these state boundaries. Apparently, the first way is unrealistic. Although all ancient empires including Roman, Greece, and Mongolia became historical remnants, and giant empires are not prevalent in current world, the partition of information systems cannot be an imagined practice. Information systems become the unique empire without tangible territory.

Offences occurring in information systems are not likely to receive punishment from this system. Rather, they are punishable by the territory-based states that they cross. It is increasingly stringent and necessary to establish an international cooperation system for punishing cybercrime. Various international organizations have taken actions to resolve the problem in different forums and at different levels.

The Convention on Cybercrime is acknowledged as a landmark in the sphere of the international harmonization of cybercrime law. However, apart from the fact that it represents a significant step forward, more states will have to sign the Convention and abide by its mandates in order to serve as a deterrent. International harmonization centered on the convention is obviously limited and must necessarily be extended to more participating member states with an even wider scope of issues. The final effect should be achieved only through a universal agreement on combating cybercrime. The UN may have higher potential to implement such universal measures. However, we should not expect an instantaneous reaction from any of the international organizations, because not too much attention and interests of these international organizations are concentrated on the problem of crime or precisely, on cybercrime.

While these organizations are devoted to dealing with the more important international affairs, threats against a critical information infrastructure will become more serious, until

they are listed at the top of these organizations' schedule. Consequently, the development of an international level of consciousness and an international level call for a national level of consciousness are still the grounds for effective actions.

Organizations and Institutions that Address International Cyber-security:

A. *Global*:

a. United Nations Internet Governance Forum:

The IGF initiatives are expected to follow the principles and practices of being open and transparent, inclusive and non-commercial. They work in accordance with the bottom up consensus process of the IGF and need to have a multi-stakeholder participation (at least three stakeholder groups initially, and evolve toward inclusion of all stakeholder groups), in both formation of the Initiative and in any other Initiative related events. The IGF Best Practice Forum on Cyber-security is a multi-stakeholder group focusing on identifying best practices in Cyber-security.

Last year, in 2019, the BPF published research to identify best practices related to the implementation, operationalization, and support of different principles, norms, and policy approaches contained in these international agreements and initiatives by individual signatories and stakeholders. Amongst others, these agreements include the Paris Call for Trust and Cybersecurity in Cyberspace, the Tech Accord, the Agreement on cooperation in ensuring the International Information Security between the Member States of the Shanghai Cooperation Organization and the 2015 UNGGE proposed norms. In 2020, the BPF Cyber-security is building on its 2019 report by focusing on identifying additional international agreements and initiatives on cybersecurity, and performing a deeper analysis of a narrower set of agreements. In this deeper analysis, we're looking specifically at whether the agreement includes any of the UN-GGE consensus norms; and whether any additional norms are specifically called out. The narrower set of agreements is focused on those that are specifically normative, rather than having directly enforceable commitments.

b. United Nations Group of Governmental Experts:

The United Nations Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security (formerly: on Developments in the Field of Information and Telecommunications in the Context of International Security) is a UN-mandated working group in the field of information security. Six working groups have been established since 2004, including the GGE 2019-2021. The UN GGE can be credited with two major achievements outlining the global agenda and introducing the principle that international law applies to the digital space.

In 2018, another UN-mandated working group – the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG) – was established in parallel with the GGE, involving 'all interested states'.

c. Cyber security & Infrastructure security Agency:

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more

secure and resilient infrastructure for the future. CISA builds the national capacity to defend against cyber-attacks and works with the federal government to provide cyber-security tools, incident response services and assessment capabilities to safeguard the 'government' networks that support the essential operations of partner departments and agencies.

CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and deliver technical assistance and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide. CISA also delivers insights on these assessments related to current capabilities to identify gaps, which—along with an examination of emerging technologies—help determine the demand for future capabilities (both near- and long-term). CISA enhances public safety interoperable communications at all levels of government to help partners across the country develop their emergency communications capabilities.

Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of a natural disaster, act of terrorism, or other man-made disaster.

The National Risk Management Center (NRMC) is housed within the Cyber-security and Infrastructure Security Agency (CISA). NRMC is a planning, analysis, and collaboration center working to identify and address the most significant risks to our nation's critical infrastructure.

NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: Identify; Analyze; Prioritize; and Manage the most strategic risks to our National Critical Functions—the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination.

d. Anti-Abuse Working Group

As the Internet has evolved, so has the scope and scale of network abuse. Unsolicited bulk email (spam) is often merely a symptom of deeper abuse such as viruses or botnets. Consequently, the Anti-Abuse Working Group has a wide scope, to include all relevant kinds of abuse.

The technical details of spam and other abuse constantly vary, in terms of application channel and technique. Channel examples include SMTP, SIP, XMPP and HTTP. Examples of techniques range from buffer overrun to social engineering.

Within scope are all systems and mechanisms, both technical and non-technical, that are used to create, control, and make money from such abuse.While areas such as hosting illegal content or copyright infringement are not seen as a central part of the working group's remit, they are unquestionably bound up in other aspects of network abuse and, as such, may be areas of interest.

The working group considers both technical and non-technical aspects of abuse, with the following goals:

- Produce and continue to update a BCP (Best Common Practice) document for ISPs similar in nature to RIPE-409 but covering a wider range of possible abusive behaviours.
- Provide advice (beyond that of the BCP) to relevant parties within the RIPE region such as ISPs, governments and law enforcement agencies on strategic and operational matters.
- Discuss and disseminate information on technical and non-technical methods of preventing or reducing network abuse.

e. Forum for Incident Response Security Teams (FIRST):

FIRST is the Forum of Incident Response and Security Teams. The idea of FIRST goes back until 1989, only one year after the CERT(r) Coordination Center was created after the infamous Internet worm. Back then incidents already were impacting not only one closed user group or organization, but any number of networks interconnected by the Internet. FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

f. Network Operators Groups:

(NOGs)Network Operator Groups (NOGs) are informal forums that bring together network operators, network engineers and other technical professionals to discuss matters relating to routing, network security, peering and interconnection, and other operational Internet issues. While the forums are generally structured around sharing relevant technical information, they also provide training and other skills development opportunities to the region’s operators.

NOGs promote Internet infrastructure stability, security, and network coherence, and facilitate better Internet accessibility for the community. They are open to all, including students, and are attended by various stakeholders including representatives of ISPs, telcos, mobile operators, CDNs, academia, governments, and cloud, enterprise, and financial organizations.

g. Security and Stability Advisory Committee (SSAC):

In accordance with Section 12.2 (b) of the ICANN Bylaws, the Security and Stability Advisory Committee advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services such as WHOIS). The SSAC engages in ongoing threat assessment and risk

analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly.

The SSAC produces Reports, Correspondence, and Comments on a range of topics. Reports are focused on providing information, recommendations and advice on technical Security Stability and Reliability (SSR) issues to the ICANN Board, the ICANN community, and/or the broader internet community. Correspondence comprises letters, comments and other documents on administrative, community and other non-SSR issues. Comments are prepared in response to explicit questions posed to or requests made to the SSAC, or as a response to ICANN's public comment forum.

h. United States Technology Training Institute (USTTI):

In preparation for the 1982 ITU Plenipotentiary Conference in Nairobi, Ambassador Michael Gardner asked leaders of major, often competing, U.S. ICT corporations to join together with senior U.S. government officials to provide diverse tuition-free training for qualified communications professionals, regulators, and entrepreneurs from the developing world. The affirmative response was overwhelming and, as a result, the USTTI was launched at the Nairobi ITU conference as a public-private, non-profit partnership dedicated to aggressively sharing ICT knowledge with women and men dedicated to making modern communications a reality throughout the developing world.

B. Regional:

a. Asia Pacific Computer Emergency Response Team:

In March 2002, the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) invited the leading CSIRTs and CERTs from Asia Pacific economies to attend the Asia Pacific Security Incident Response Coordination Conference (APSIRC). The aim of APSIRC was to improve working relationships among CSIRTs and CERTs in the region. The key outcome of the APSIRC meeting was the decision to form the APCERT, consisting of 15 CSIRTs and CERTs from 12 Asia Pacific economies, as the vehicle for regional cross border cooperation and information sharing in mitigating cyber threats. In February 2003, the members of the APSIRC meeting accepted the APCERT agreement and elections were held for the positions of Chair and Secretariat, and the membership of the Steering Committee (SC). In February 2005, during the APCERT Annual General Meeting (AGM) in Kyoto, Japan, the position of Deputy Chair was created and elected. The APSIRC set out the initial goals and objectives upon which the APCERT was established. The APCERT vision was revised in 2011 to reflect the broadened perspective of the group and its members.

The APCERT will maintain a trusted contact network of cyber security experts in the Asia Pacific region to improve the region’s awareness and competency in relation to cyber security incidents through:

a) enhancing Asia Pacific regional and international cooperation on cyber-security
b) jointly developing measures to mitigate large-scale or regional network security incidents;
c) facilitating information sharing and technology exchange on cyber security and threats among its members;

d) promoting collaborative research and development on subjects of interest to its members;
e) assisting other CSIRTs and CERTs in the region to conduct efficient and effective computer emergency response.

b. The European Union Agency for Cyber-security:

The European Union Agency for Cyber-security, ENISA, is the Union's agency dedicated to achieving a high common level of cyber-security across Europe. Established in 2004 and strengthened by the EU Cyber-security Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cyber-security certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

The mission of the European Union Agency for Cyber-security (ENISA) is to achieve a high common level of cyber-security across the Union in cooperation with the wider community.

In a world that has become hyper-connected, cybercriminals pose a significant threat to the internal security of the European Union and security of its citizens online. The COVID-19 pandemic has highlighted the need for more security in the digital world. People have increased their presence online to maintain personal and professional relations, while cybercriminals have taken advantage of this situation, targeting in particular e-commerce and e-payment businesses, as well as the healthcare system.

c. Regional Internet Registries (RIRs):

A regional Internet registry (RIR) is an organization that manages the allocation and registration of Internet number resources within a region of the world. Internet number resources include IP addresses and autonomous system (AS) numbers.

The regional Internet registry system evolved over time, eventually dividing the responsibility for management to a registry for each of five regions of the world. The regional Internet registries are informally liaised through the unincorporated Number Resource Organization (NRO), which is a coordinating body to act on matters of global importance.

There are 5 regional registries and they are as follows-

The African Network Information Center (AFRINIC) serves Africa. The American Registry for Internet Numbers (ARIN) serves Antarctica, Canada, parts of the Caribbean, and the United States. The Asia-Pacific Network Information Centre (APNIC) serves East Asia, Oceania, South Asia, and Southeast Asia.[4] The Latin America and Caribbean Network Information Centre (LACNIC) serves most of the Caribbean and all of Latin America. The Réseaux IP Européens Network Coordination Centre (RIPE NCC) serves Europe, Central Asia, Russia, and West Asia.

The Internet Assigned Numbers Authority (IANA) delegates Internet resources to the RIRs who, in turn, follow their regional policies to delegate resources to their customers, which include Internet service providers and end-user organizations. Collectively, the RIRs participate in the Number Resource Organization (NRO), formed as a body to represent their collective interests, undertake joint activities, and coordinate their activities globally. The NRO has entered into an agreement with ICANN for the establishment of the Address Supporting Organisation (ASO), which undertakes coordination of global IP addressing policies within the ICANN framework.

d. Cooperative Cyber Defense and Center of Excellence (CCDCOE)

The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. The heart of the Centre is a diverse group of experts from 28 nations: Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, the United Kingdom and the United States. We bring together researchers, analysts and educators from the military, government, academia and industry.

Their mission is to support our member nations and NATO with unique interdisciplinary expertise in the field of cyber defence research, training and exercises covering the focus areas of technology, strategy and law and to foster cooperation of like-minded nations. We bring together NATO Allies and partners beyond the Alliance.

e. Inter-American Cooperation Portal on Cyber-Crime:

The Inter-American Cooperation Portal on Cyber-Crime and the Working Group are two of the major outcomes of the process of Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA) aimed at strengthening hemispheric cooperation in the investigation and prosecution of these crimes.

Meanwhile, the Working Group was established by the REMJA in 1999 as the principal hemispheric forum to strengthen international cooperation in the prevention, investigation and prosecution of cybercrime; facilitate the exchange of information and experiences among its members; and make necessary recommendations to enhance and strengthen cooperation among the OAS member states and with international organizations and mechanisms.

f. North Atlantic Treaty Organization (NATO):

Cyber threats to the security of the Alliance are becoming more frequent, complex, destructive and coercive. NATO will continue to adapt to the evolving cyber threat landscape. NATO and its Allies rely on strong and resilient cyber defences to fulfill the Alliance's core tasks of collective defence, crisis management and cooperative security. The Alliance needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces.

NATO Policy on Cyber Defence: To keep pace with the rapidly changing threat landscape and maintain robust cyber defences, NATO adopted an enhanced policy and action plan, which were endorsed by Allies at the Wales Summit in September 2014. An updated action

plan has since been endorsed by Allies in February 2017. The policy establishes that cyber defence is part of the Alliance's core task of collective defence, confirms that international law applies in cyberspace, seeks to further develop NATO's and Allies' capabilities, and intensifies NATO's cooperation with industry. The top priority is the protection of the networks owned and operated by the Alliance.

The policy also reflects Allied decisions on issues such as streamlined cyber defence governance, procedures for assistance to Allied countries, and the integration of cyber defence into operational planning (including civil preparedness). In addition, the policy defines ways to take forward awareness, education, training and exercise activities, and encourages further progress in various cooperation initiatives, including those with partner countries and international organisations. It also foresees boosting NATO's cooperation with industry, including on information-sharing and the exchange of best practices. Allies have also committed to enhancing information-sharing and mutual assistance in preventing, mitigating and recovering from cyber- attacks.

NATO's cyber defence policy is complemented by an action plan with concrete objectives and implementation timelines on a range of topics from capability development, education, training and exercises, and partnerships.

At the Warsaw Summit in 2016, Allies reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. As most crises and conflicts today have a cyber-dimension, treating cyberspace as a domain enables NATO to better protect and conduct its missions and operations.

At Warsaw, Allies also pledged to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority. Together with the continuous adaptation of NATO's cyber defence capabilities, as part of NATO's long-term adaptation, this will reinforce the cyber defence and overall resilience of the Alliance.

Developing the NATO cyber defence capability: The NATO Computer Incident Response Capability (NCIRC) based at SHAPE in Mons, Belgium, protects NATO's own networks by providing centralised and round-the-clock cyber defence support. This capability is expected to evolve on a continual basis and maintain pace with the rapidly changing threat and technology environment. To facilitate an Alliance-wide and common approach to cyber defence capability development, NATO also defines targets for Allied countries' implementation of national cyber defence capabilities via the NATO Defence Planning Process.

Cyber defence has also been integrated into NATO's Smart Defence initiatives. Smart Defence enables countries to work together to develop and maintain capabilities they could not afford to develop or procure alone, and to free resources for developing other capabilities. The Smart Defence projects in cyber defence include the Malware Information Sharing Platform (MISP) and the Smart Defence Multinational Cyber Defence Capability Development (MN CD2) project. The Multinational Cyber Defence Education and Training (MN CD E&T) project recently concluded its work.

NATO is also helping its Allies by sharing information and best practices, and by conducting cyber defence exercises to help develop national expertise. Similarly, individual Allied countries may, on a voluntary basis and facilitated by NATO, assist other Allies to develop their national cyber defence capabilities. NATO has established a Cyberspace Operations Centre in Mons, Belgium. The Centre supports military commanders with situational awareness to inform the Alliance's operations and missions. It also coordinates NATO's operational activity in cyberspace, ensuring freedom to act in this domain and making operations more resilient to cyber threats.

Increasing NATO cyber defence capacity: Recognizing that cyber defence both about people as it is about technology, NATO continues to improve the state of its cyber defence education, training and exercises. NATO conducts regular exercises, such as the annual Cyber Coalition Exercise, and aims to integrate cyber defence elements and considerations into the entire range of Alliance exercises, including the Crisis Management Exercise (CMX). NATO is also enhancing its capabilities for cyber education, training and exercises, including the NATO Cyber Range, which is based at a facility provided by Estonia. To enhance situational awareness, an updated Memorandum of Understanding (MOU) on Cyber Defence was developed in 2015. This updated MOU is being concluded between NATO and the national cyber defence authorities of all Allies. It sets out arrangements for the exchange of a variety of cyber defence-related information and assistance to improve cyber incident prevention, resilience and response capabilities.

The NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia is a NATO-accredited research and training facility dealing with cyber defence education, consultation, lessons learned, research and development. Although it is not part of the NATO Command Structure, the CCD CoE offers recognised expertise and experience. The NATO Communications and Information Systems School (NCISS) in Oeiras, Portugal provide training to personnel from Allied (as well as non-NATO) nations relating to the operation and maintenance of NATO communications and information systems. NCISS also offers cyber defence training and education.

The NATO School in Oberammergau, Germany conducts cyber defence-related education and training to support Alliance operations, strategy, policy, doctrine and procedures. The NATO Defense College in Rome, Italy fosters strategic thinking on political-military matters, including on cyber defence issues.

Cooperating with partners: Because cyber threats defy state borders and organisational boundaries, NATO engages with a number of partner countries and other international organisations to enhance international security. Engagement with partner countries is based on shared values and common approaches to cyber defence. Requests for cooperation with the Alliance are handled on a case-by-case basis founded on mutual interest. NATO also works with, among others, the European Union (EU), the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE).

Cyber defence is one of the areas of strengthened cooperation between NATO and the EU, as part of the two organisations' increasingly coordinated efforts to counter hybrid threats. NATO and the EU share information between cyber crisis response teams and exchange best practices. Cooperation is also being enhanced on training, research and exercises.

Cooperating with industry: The private sector is a key player in cyberspace, and technological innovations and expertise from the private sector are crucial to enable NATO and Allied countries to effectively respond to cyber threats.

Through the NATO Industry Cyber Partnership (NICP), NATO and its Allies are working to reinforce their relationships with industry. This partnership includes NATO entities, national Computer Emergency Response Teams (CERTs) and NATO member countries' industry representatives. Information-sharing activities, exercises, training and education, and multinational Smart Defence projects are just a few examples of areas in which NATO and industry have been working together.

C. International & Inter-Governmental Organizations

a. United Nations Office on Drugs and Crime:

For two decades, the United Nations Office on Drugs and Crime (UNODC) has been helping make the world safer from drugs, organized crime, corruption and terrorism. We are committed to achieving health, security and justice for all by tackling these threats and promoting peace and sustainable well-being as deterrents to them. Because the scale of these problems is often too great for states to confront alone, UNODC offers practical assistance and encourages transnational approaches to action. We do this in all regions of the world through our global programmes and network of field offices.

The Office is committed to supporting Member States in implementing the 2030 Agenda for Sustainable Development and the 17 Sustainable Development Goals (SDGs) at its core. The 2030 Agenda clearly recognizes that the rule of law and fair, effective and humane justice systems, as well as health-oriented responses to drug use, are both enablers for and part of sustainable development. This office spearheads the UN's efforts to combat transnational crime, including cybercrime. In 2011 UNODC established an Open-Ended Inter-Governmental Expert Group to study cybercrime and the international community's response to it. Visit this page for summaries of the Inter-Governmental Expert Group's meetings. UNODC also maintains the Cybercrime Repository, a database of national legislation and case law on cybercrime, and SHERLOC, a larger database of national legislation and case law on transnational crime.

b. International Telecommunications Union (ITU)

A fundamental role of ITU, based on the guidance of the World Summit on the Information Society (WSIS) and the ITU Plenipotentiary Conference, is to build confidence and security in the use of Information and Communication Technologies (ICTs). At WSIS, Heads of States and world leaders entrusted ITU to be the Facilitator of Action Line C5, "Building confidence and security in the use of ICTs", in response to which ITU launched, in 2007, the Global Cybersecurity Agenda (GCA), as a framework for international cooperation in this area.

The ITU is a specialized agency of the United Nations that promotes the harmonization of technical standards for information and telecommunications technologies. It is also fosters international cooperation to improve cyber-security through its Global Cyber-security

Agenda and through its partnership with UNODC, the UN Office on Drugs and Crime. In addition, the ITU has partnered with UNICEF to publish Guides for Child Online Protection.

c. United Nations Institute for Disarmament Research (UNIDIR) Cyber Policy Portal

This autonomous UN institute assists the international community in finding solutions to disarmament and security challenges. It also strives to anticipate new security threats before they become critical. UNIDIR's Cyber Policy Portal provides access to the following information:

- IGO Directory -- This directory provides links to the websites of inter-governmental organizations that are active in promoting cyber security and preventing cyber attacks. For each IGO, you will find a selection of policy documents, model laws, and related documentation.
- Directory of Multilateral Framework (Treaties) -- This directory includes multilateral and regional treaties (conventions), model laws, and soft law instruments related to cyber security.
- Comparison Tool -- Use this tool to compare cyber security measures and policies in different countries and among various inter-governmental organizations. Begin by selecting two or more countries or two or more IGOs from the respective menus. Points of comparison include national policies/strategies, legal frameworks (national legislation), and international cooperation (ratification of multilateral and regional treaties).

D. Non-Governmental Organizations:

a. Anti-Phishing Working Group (APWG)

The APWG established in 2003 as the anti-phishing working group, is an industry association focused on unifying the global response to cybercrime. the organization provides a forum for responders and managers of cybercrime to discuss phishing and cybercrime issues, to consider potential technology solutions, to access data logistics resources for cybersecurity applications, to cultivate the university research community dedicated to cybercrime, and to advise government, industry, law enforcement and treaty organizations on the nature of cybercrime.

This international industry association combats phishing and email spoofing through the development of data standards and model response systems and protocols.

b. Spamhaus

This international non-profit organization, based in London and Geneva, tracks cyber threats (spam, phishing, malware, and botnets) and provides real time, actionable threat intelligence to network operators, corporations, and security vendors. It also works with law enforcement agencies worldwide to identify spam and malware sources. The Spamhaus Project is an international nonprofit organization that tracks spam and related cyber threats such as phishing, malware and botnets, provides realtime actionable and highly accurate threat intelligence to the Internet's major networks, corporations and security vendors, and works with law enforcement agencies to identify and pursue spam and malware sources worldwide.

Founded in 1998, Spamhaus is based in Geneva, Switzerland, and Andorra la Vella, Andorra, and is run by a dedicated staff of 38 investigators, forensics specialists and network engineers located in 10 nations.

Spamhaus realtime threat and reputation blocklists currently protect over 3 Billion user mailboxes and are responsible for blocking the vast majority of spam and malware sent out on the Internet. Spamhaus data is today used by the majority of the Internet's ISPs, email service providers, corporations, universities, governments and military networks.

As well as DNS-based Blocklists (DNSBLs) Spamhaus produces special data for use with Internet firewall and routing equipment, such as the Spamhaus DROP lists, Botnet C&C data, and the Spamhaus Response Policy Zone (RPZ) data for DNS resolvers which prevents millions of Internet users from clicking on malicious links in phishing and malware emails. To meet public demand for its DNSBLs, Spamhaus has built one of the largest DNS infrastructures in the world. The Spamhaus network of over 80 public DNSBL servers spread across 18 countries serves many billions of DNSBL queries to the public every day, free of charge.

c. European NGO Alliance for Child Safety Online (eNACSO)

Funded by the European Commission, the executive arm of the EU, eNACSO provides a platform for child protection NGOS throughout Europe to share expertise and best practices on policy matters related to child safety online.

The European NGO Alliance for Child Safety Online is a network consisting of 22 children's rights NGOs from across the EU working for a safer online environment for children. Our mission is to promote and support actions at national, European and international level aimed at protecting children and promoting their rights in relation to the Internet and new technologies. Our work is based on the 1989 UN Convention on the Rights of the Child (UNCRC) and the Optional Protocol to the UNCRC on the sale of children, child prostitution and child pornography. eNACSO is funded by the European Commission's Safer Internet Programme.

d. International Association of Internet Hotlines (INHOPE)

INHOPE is a collaborative global network of non-profit organizations working to combat the online distribution of child pornography through the establishment of hotlines for reporting illegal content. INHOPE is made up of 46 hotlines around the world that operate in all EU member states, Russia, South Africa, North & South America, Asia, Australia and New Zealand. INHOPE's vision is a world free of Child Sexual Abuse Material online. The mission of INHOPE is to support the network of hotlines in combating online Child Sexual Abuse Material (CSAM). In a borderless digital world CSAM has global consequences and as CSAM increases so do our efforts and those of our partners to combat it. They advocate for legislative and policy changes with the support and funding from the European Commission.

e. Internet Watch Foundation (IWF)

The IWF is a UK-based, industry-funded non-profit that works to identify, locate, and remove online images and videos of child sexual abuse in cooperation with law enforcement agencies worldwide. minimise the availability of online sexual abuse content. Specifically:

a. Child sexual abuse content hosted anywhere in the world.
b. Non-photographic child sexual abuse images hosted in the UK.

IWF focuses on the removal of child sexual abuse images and videos. IWF works internationally to make the internet a safer place and helps victims of child sexual abuse worldwide by identifying and removing online images and videos of their abuse. They are a not-for-profit organisation and are supported by the global internet industry and the European Commission.

f. The Rand Corporation

This independent think tank, which is known for the quality and rigor of its work product, is a good source for credible research and informed commentary.

g. International Committee for the Red Cross (ICRC)

The ICRC's website is the best online resource for researching international humanitarian law (IHL). In addition to its searchable databases of primary law, the website includes the following secondary source content:

- New Technologies and IHL -- This page aggregates all ICRC content concerning the novel humanitarian and legal challenges posed by emerging technologies, including cyber weapons and cyber warfare.
- Terrorism and IHL -- This page aggregates all ICRC content on the application of IHL to acts of terrorism.
- Resource Centre -- Search by keyword for articles and other ICRC publications.
- IHL Bibliography -- Every three months, the ICRC compiles a comprehensive list of books and articles published in English and in French on topics related to IHL.

E. U.S. Federal Government Agencies

a. Department of Justice -- Division of Computer Crime & Intellectual Property Section (CCIPS)

The CCIPS works with other federal agencies, the private sector, and foreign law enforcement agencies to prevent, investigate, and prosecute computer and intellectual property crimes. Visit the Documents and Reports page to access annual reports, topical white papers, testimony before congressional committees, and blog posts.

b. Department of Homeland Security

The following agencies, which fall under the DHS umbrella, also play a key role in combating cyber-crime.

- *U.S. Secret Service*

The Secret Service maintains an Electronic Crimes Task Force (ECTF) to investigate identify theft, network intrusions, attacks on business email systems, ransomware, and related matters.

- *U.S. Immigration & Customs Enforcement (ICE)*

ICE operates the Cyber Crimes Center (C3), which provides technical support to domestic and international law enforcement agencies investigating cross-border crime. The Center is comprised of the Cyber Crimes Unit, the Child Exploitation Investigations Unit, and the Computer Forensics Unit.

c. Department of Defense (DoD) Cyber Command

Cyber Command has developed a strategy for defending the U.S. and its national interests against cyber-attacks, as well as a strategy for defending its own computer network systems and formulating contingency plans to maintain military operations in the event of a cyber-attack.

Cyber-security Industry associations:

a. WiCyS - Women in Cyber-security:

WiCyS is the only non-profit membership organization with national reach that is dedicated to bringing together women in cybersecurity from academia, research and industry to share knowledge, experience, networking and mentoring. The initiative was created through an NSF grant (Award #1303441) by Dr. Ambareen Siraj at Tennessee Tech University six years ago, and has grown into a wonderful alliance among academia, government and industry.

b. The SANS Institute:

SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center.

c. OWASP - The Open Web Application Security Project:

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

d. Information Systems Security Association (ISSA)

Developing and Connecting Cybersecurity Leaders Globally - ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure.

e. *Center for Internet Security*

The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization focused on enhancing the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration. CIS provides resources that help partners achieve security goals through expert guidance and cost-effective solutions.

f. Information Security Forum (ISF)

The ISF is the world's leading authority on information risk management. A not-for-profit organisation, we supply authoritative opinion and guidance on all aspects of information security. We deliver practical solutions to overcome the wide-ranging security challenges that impact business information today.

g. National Association of ISACs:

The mission of the National Council of ISACs (NCI) is to advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. Members of the Council are the individual Information Sharing and Analysis Centers (ISAC) that represent their respective sectors.

h. Internet Security Alliance:

ISA was founded in 2000 in collaboration with Carnegie Mellon University. ISA membership is open to public and privately held entities and currently has substantial participation from the aviation, banking, communications, defense, education, financial services, health care, insurance, manufacturing, security and technology industries.

i. International Association of Privacy Professionals (IAPP)

The IAPP is the largest and most comprehensive global information privacy community and resource. Founded in 2000, the IAPP is a not-for-profit organization that helps define, support and improve the privacy profession globally.

j. International Consortium of Minority Cybersecurity Professionals (ICMCP):

The International Consortium of Minority Cyber Professionals (ICMCP) was created as a 501(c) 3 non-profit association dedicated to the academic and professional success of minority cyber-security students and professionals. Our mission is to achieve the consistent representation of women and minorities in the cybersecurity industry through programs designed to foster recruitment, inclusion and retention – one person at a time.

k. National Cyber Security Alliance (NCSA):

NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individual’s use, the networks they connect to, and our shared digital assets.

l. Federal Information Systems Security Educators' Association (FISSEA):

The Federal Information Systems Security Educators' Association (FISSEA), founded in 1987, is an organization run by and for information systems security professionals to assist federal agencies in meeting their information systems security awareness, training, education, and certification responsibilities.

m. The Association for Executives in Healthcare Information Security (AEHIS):

The Association for Executives in Healthcare Information Security (AEHIS) launched in 2014 as the first professional organization serving healthcare's senior IT security leaders. AEHIS offers CSO's and other top-ranking information security leaders the professional development and networking opportunities critical for their success. Members have access to the educational resources and support for addressing key industry specific privacy and security issues.

n. International Association for Cryptologic Research (IACR):

The International Association for Cryptologic Research (IACR) is a non-profit scientific organization whose purpose is to further research in cryptology and related fields. Cryptology is the science and practice of designing computation and communication systems which are secure in the presence of adversaries.

o. The Institute of Internal Auditors (IIA):

The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

p. The Credit Union Information Security Professionals Association CUISPA:

CIUSPA is a national association of credit union information technology professionals focused on improving security and risk management through cooperation.

q. Information Security Research Association (ISRA):

The Information Security Research Association (commonly known as ISRA) is a registered non-profit organization focused on various aspects of Information Security including security research and cyber security awareness activities.

r. Association of Information Security Professionals (AISP)

To promote, develop, support and enhance the integrity, technical competence, management expertise, status and interests of information security professionals in Singapore.

s. Australian Information Security Association (AISA):

The Australian Information Security Association (AISA) is an Australian representative industry body for the information security profession. Formed in 1999, AISA is focussed on

individual membership. AISA aims to foster and promote the development of the information security industry and encourage the professional development of our members.

t. International Association of Security Awareness Professionals (IASAP):

Formed in 2012, the International Association of Security Awareness Professionals is an independent 501(c)6 non-profit association comprised of corporate members. Member participants are professionals who manage information security awareness programs for their organizations, and are responsible for everyday awareness operations.

u. Executive Women's Forum on Information Security, Risk Management & Privacy (EWF):

The Executive Women's Forum is the largest member organization serving emerging leaders as well as the most prominent and influential female executives in the Information Security, Risk Management and Privacy industries.

v. Information Security & Forensics Society (ISFS):

Information Security and Forensics Society (ISFS) was registered under the Hong Kong Societies Ordinance in May 2000. Our mission is to advocate and enforce professionalism, integrity and innovation in Information Security and Computer Forensics in Hong Kong and the surrounding region.

w. Cyber, Space & Intelligence Association:

Cyber, Space, & Intelligence Association was founded in early 2011 to provide an environment for a vital flow of ideas between national security thought leaders in Government, Industry, and Congress focused Cyber, Space, and Intelligence challenges and opportunities.

x. Cloud Security Alliance (CSA):

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

Conclusion:

While a relatively small number of organizations produce reliable data, sufficient information exists to develop a model that maps degree of vulnerability versus the effectiveness of organizational response. For instance, international data on cybercrime legislation and awareness can be correlated with arrest rates in individual countries. When combined with stocktaking databases, this method allows one to determine the rate of progress in individual nations versus cybercrime issues. Similarly, quantitative data provided by national CERTs can be used to obtain insights about their performance in their respective national contexts

and constituencies. An example of these kinds of analysis, along with a Data Dashboard tool, can be found in the report (Madnick, Li, et al., 2009b).

Over time, we anticipate the possibility of pairing international and national statistics with information from the private sector. Security and monitoring companies such as Symantec, Arbor Networks, Microsoft, and McAfee provide quantitative data that address the global spread of Internet vulnerabilities. In many cases, the volume and quality of data released by these organizations far outpaces the information released by international and national organizations; however, the true value of this information lies not in an isolated analysis, but in the intersection of private data with the national and international sphere. For instance, statistics concerning the originating country of cyber-attacks or the absolute volume of attacks can potentially be paired with national CERT data to determine the degree of national vulnerabilities and traffic that each CERT is capable of handling.

These metrics, and others that can potentially be derived, may provide a powerful method of simultaneously evaluating data quality and organizational performance. An important next step in our inquiry is to examine additional data providers and explore ways of pairing this data with national and international organizations to form evaluative statistical models. While doing so, it is important to remain cognizant of the institutional context that that enables or constrains the provision of information.

The need is to reassess and renew as necessary the present international legal frameworks, offering a forum for broader international discussion expressing an outlook towards increasing and advancing international law-enforcement cooperation among the national authorities. This development should consider the influences of the novel and emerging issues in respect of international law-enforcement cooperation, with recommendations on capacity-building, which should show an equal concern for the situation in countries at different stages of development so as to avoid a futureless future of information chaos.

MODULE-IV

CYBER SECURITY IN NEW SPACE

Introduction

The space industry is a complex system of moving parts, changing dynamics and developing ideas. Emerging through the Cold War era, it was dominated by a handful of nations and state-level activity, developing large and expensive satellites with long operational lifetimes. Information was strictly on a need-to-know basis which aimed to hinder the military capabilities of enemies, laying a groundwork of obscurity in developmental practices. The practices surfacing during this time are typical of what is known as “Old Space”.

Since this time, the boom of the consumer microelectronics industry, more rapid research and development practices and the lower costs of launch means that space is viewed now as a highly valued resource for business. This private sector interest has expanded the space market globally (estimated to be worth $269 billion as of 2017) and brought different players and projects to the table. The change in the economics of space to one which is profit-driven has prompted R&D to have a quicker turnaround with smaller agile teams, mirroring the IT industry rather than traditional aerospace or military outfits.

This agility pattern born from incorporating standard modules and components whilst making space travel cheaper and more widespread across industries is characterized by the term “New Space”. This ecosystem, as Paikowsky calls it, is also moving towards other trends such as large satellite constellations of the orders of hundreds and thousands, and small satellite (weighing 600kg or less) production. In 2018, 328 small satellites were launched, six times as many as in 2012, with and half of them for commercial purposes. Commercial-off-the-shelf (COTS) components are now commonplace in satellites and ground control systems, decreasing construction times and costs. Companies are taking more risks with their satellites, leading to more innovative applications and technologies.

Major applications of New Space The academic sector is striving to push the innovative boundaries of New Space by exhibiting new technologies in space. Missions such as STRaND-11 demonstrated the feasibility of using smart-phone electronics in satellites.

A surge of investment in the Earth observation market has been powered by the applications of satellite imagery and signals intelligence, namely business intelligence products, as well as environmental conservation efforts. Companies such as Planet and HawkEye 3603 are operating constellations of small satellites in low Earth orbit (LEO).

Global broadband services, another major applications emerging in New Space, aim to bring connectivity to rural and remote areas and provide fault-tolerant networks for critical services. Satellite broadband revenue has shown steady growth in the last five years, with more rapid growth predicted as proposed satellite constellations of the order of hundreds and thousands become operational, such as Starlink, OneWeb, Telesat and LeoSat.

Satellite geolocation services, providing precise time and position data to dedicated receivers, have been a steady addition to several industries, enabling applications including route planning, fleet management and time-critical purposes used in the financial and energy sectors. Many sectors to which Global Navigation Satellite Systems (GNSS) can be applied have developed the global ground equipment market. In 2016, GNSS equipment revenue

made $84.6 billion of the total ground equipment revenue of $113.4 billion, which has been on a steady incline since 2012.

The use of satellites in warfare has a leading role to play in the modern era, with 68% of munitions being guided by satellites in the 2004 Iraq war. These systems have stricter security requirements and to employ features such as encryption, anti-jamming techniques and frequency hopping. The US military's use of commercial satellites has increased in recent conflicts and pushed further with legislation passed in the Bush era. Small satellites are being increasingly used to support military functions, with USA, Russia and China launching 39, 20 and 17 small satellites, respectively, between 2012 and 2018.

This part therefore aims to provide an analysis of the New Space era in terms of the previous security threats, emerging security challenges and key technologies which are advancing and innovating the space and satellite industry.

Security challenge Being able to manipulate such remote objects as satellites provides a new challenge to the hacking community. Scarce documentation and source code provide the ultimate "black box" challenge. Combined with the "security through obscurity" mentality with which vendors develop these products, major vulnerabilities in satellite systems are being discovered. The security analysis of satellite user terminals in brought to light numerous vendor's use of hard-coded credentials, insecure protocols and weak authentication mechanisms. This ageing mentality is not suitable for systems making use of cyber technologies, especially those which support critical infrastructure which are piquing the interest of the hacking community.

Security is now no longer an afterthought for terrestrial enterprises; standards, regulations and organizational security-driven mindsets have prompted the integration security practices both retrospectively and from a foundation level. An attack may not succeed using terrestrial methods and may be easier or more beneficial to target a satellite- based system which the organization uses.

For instance, to negatively impact an economy may be more easily achieved by targeting satellites providing point-of-sale card services for many commercial entities.

Organization Section 2 provides an overview of satellite architectures of the space and ground segments. Section 3 presents security threats relevant to space systems, partly based on the analysis of previous satellite security incidents. Technologies which are enabling and enhancing the New Space industry are outlined in Sect. 4, and outstanding challenges for space and satellite security are identified in Sect. 5.

2. Satellite life cycle and space system architectures

This section presents an overview of the main life cycle phases for satellites and details the different space architectures.

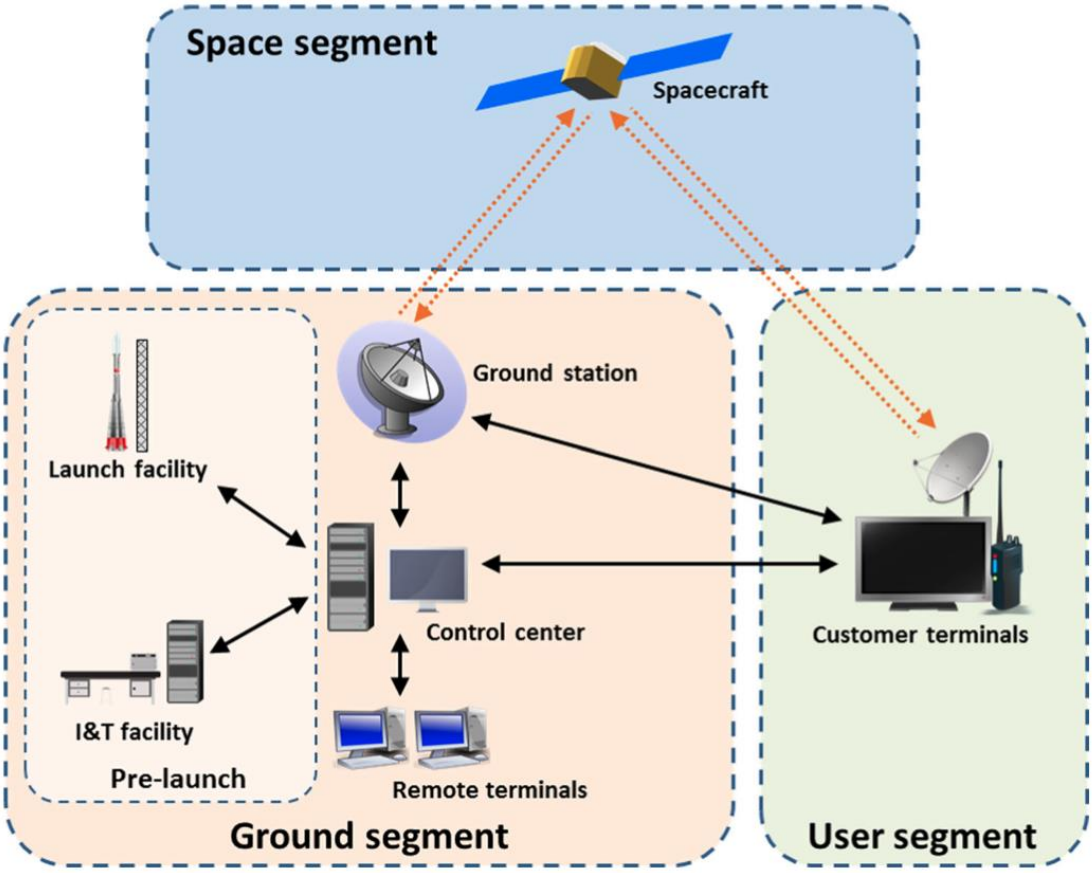


Fig. 1 Typical satellite architecture. Dotted orange arrows denote radio links; solid black arrows denote ground network links.

2.1 Satellite life cycle

The duration of a satellite's operation is primarily mission-specific, but the life cycle of a satellite after its manufacture follows a standard structure of launch, commissioning, in-service and end of life.

Launch After stacking a launch vehicle with the satellites and launched into space from a designated facility. After reaching the intended position, the launch vehicle will deploy the satellites, which several operators may have shared.

Commissioning The satellite is positioned on its specific orbit in order for normal operations to occur called commissioning. The ground segment begins to monitor and control the satellite using Telemetry, Tracking and Command (TT&C) systems, and the health of satellite subsystems is validated to prepare for in-orbit operations, typically over a two-month period.

In-service The satellite begins its designated mission until it is disposed of. The majority of the satellite's lifetime will be spent in routine operations, with the ground stations monitoring TT&C to maintain the satellite and operate the payload.

End of life At the end of its operation, commands to shut down the satellite are issued from the ground. The satellite is commanded to enter either into a higher "graveyard" orbit, or into a lower orbit for the satellite to burn up in the atmosphere.

2.2 Space and satellite systems

Space systems have a typical structure, consisting of a space segment and a ground segment, which communicate with each other via radio frequency (RF) signals (see Fig. 1). The space segment comprises the satellites or groups of satellites in orbit (as well as launch vehicles designed to release satellites into space). A satellite contains a payload, the equipment designed to carry out the satellite's function, and a bus, which houses the payload and remaining satellites systems. The main satellite systems include TT&C, command and data handling (C&DH) and attitude determination and control (ADCS). These systems are responsible for receiving and processing uplink and downlink signals, validating, decoding and sending commands to other subsystems, and controlling the stabilization and orientation of the satellite, respectively. Communications with the satellites are achieved through RF waves, usually sent with frequencies in the MHz and GHz range. The communication channel from the Earth to the satellite is the uplink and, similarly, from the satellite to the Earth is the downlink. Table 1 lists the common RF frequency bands used in satellite communications. The ground segment encompasses all the terrestrial systems which receive or send RF signals, monitor and command satellites, and distribute payload and telemetry data to stakeholders. The principal ground segment elements include ground stations with corresponding TT&C capabilities, centres to manage mission operations and the payload, and the terrestrial networks which connect the various ground systems to each other and disseminate data collected from the payload.

Another element of the satellite architecture is the user segment, which can be seen as an extension of the ground segment for the end-users of a satellite-based service. This is the device or interface which can interact with satellite signals directly or with other ground segment systems or applications.

2.3 Space segment architectures

The shape of the space segment varies greatly depending on the purpose of the mission, the simplest being a single satellite, characteristic of university, scientific or research missions.

A mission may make use of multiple orbiting satellites, clusters and constellations being the two main scenarios (see Figs. 2 and 3). A cluster usually contains a small number of satellites orbiting in close proximity to each other in some sort of formation. Satellite constellations usually consist of a large number of satellites in different orbital planes. Likely be controlled and coordinated by the same operator, the constellation will synchronize orbits and commands to create complimentary ground coverage to complete the mission objective.

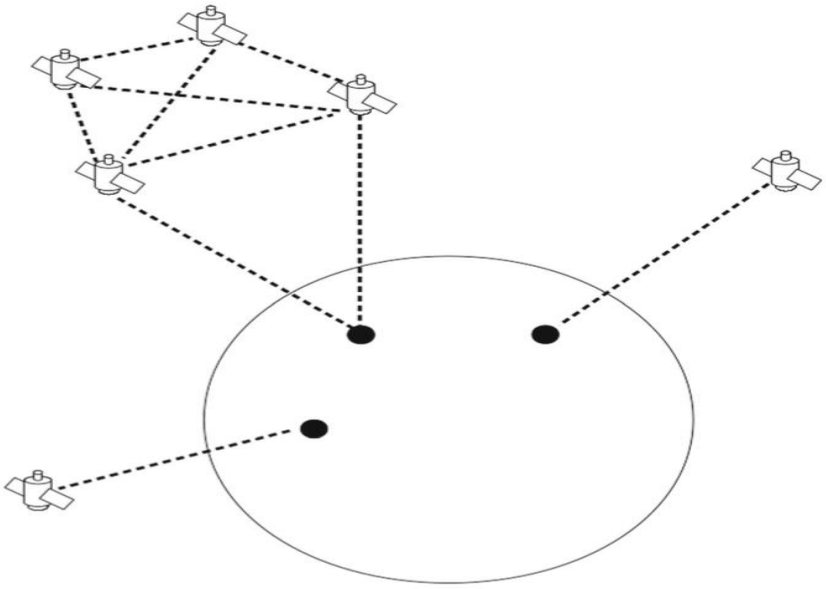


Fig. 2 Single satellite and satellite cluster orbiting Earth. Dotted lines represent communication links between satellites and between satellites and designated ground sites on Earth

Table 1 Satellite frequency bands

Name	Band
VHF	30–300 MHz
UHF	300–1000 MHz
L	1–2 GHz
S	2–4 GHz
C	4–8 GHz
X	8–12 GHz
Ku	12–18 GHz
K	18–27 GHz
Ka	27–40 GHz
V	40–75 GHz
W	75–110 GHz

Satellites can communicate solely with the ground segment and can also pass data through inter-satellite links between satellites in the constellation or cluster.

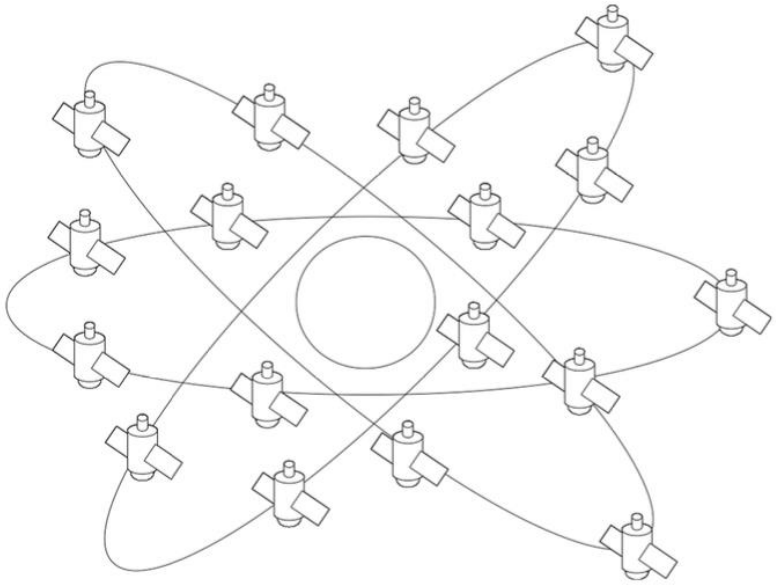


Fig. 3 Satellite constellation orbiting Earth. Solid lines represent satellite orbits

2.3.1 Satellite constellations

Several new satellite constellations are operating in space. This section provides an overview of some current and pro- posed constellations. Information relating to constellation size, satellite mass and expected lifetime, and communication implementations is given in Table 2.

Planet Planet own and operate an earth-imaging constellation with the company mission to image the entire Earth's surface every 24 hours. Their 3U CubeSats known as "Doves" make use of the Ubuntu OS, Debian packages and Python modules and host a 90-mm aperture optical payload.

A ground station network of 11 sites supports Planet's flock of Doves. These ground stations, designed to be of a standard and reproducible COTS component build, are located across the globe. After a successful pass, imaging data and telemetry logs are uploaded to servers hosted in Amazon Web Services (AWS), a managed cloud provider, and their mission control software is also written in Python.

Imagery data are formatted with Digital Video Broadcasting—Satellite—Second Generation (DVB-S2) encoding scheme as the physical layer. Generic stream encapsulation (GSE) is applied to the data link layer, prior to being formatted as IP packets. This link is apparently encrypted and is used to downlink pictures and logs.

HawkEye 360 HawkEye 360 has a constellation of three satellites which fly in a cluster formation, named its Pathfinder mission, the primary purpose of which is to provide high-precision radio frequency interference (RFI) geolocation services. The Pathfinder mission serves as a proof-of- concept, laying the foundation for larger eighteen-satellite (six-cluster) constellation.

HawkEye 360 also make use of COTS components onboard their satellites, specifically using Linux operating systems, GNU radio+ software4 and COTS software-defined radios (SDRs). They revealed that its satellite's SDR payload is based on the XilinxZynq 7045 SoC and uses analog devices 9361 transceivers. Commercial ground station operator KSAT5 was chosen by HawkEye 360 to provide primary ground segment support, with UHF/S-band TT&C stations located at HawkEye 360 headquarters in Virginia, USA.

Starlink SpaceX has plans to build an almost 12,000-satellite constellation to provide high-speed global broadband. Starlink satellites can perform orbit manoeuvres with krypton-powered Hall thrusters. Two prototype satellites, Tintin A & B, were launched in 2018, and a further 60 test satellites were launched in May 2019.

Limited details have been released about the hardware and software designs of the satellites and ground segment systems, and communication protocols used. Starlink is also proposed to make use of optical inter-satellite links; however, these have not been demonstrated with the 60 test satellites.

OneWeb Another player in the satellite broadband market is OneWeb. An initial test constellation of six satellites was launched in 2018, featuring an electronic propulsion system consisting of Hall thrusters powered by Xenon and the use of AES-256 encryption. Unlike Starlink's vertically integrated approach, OneWeb has partnered with Airbus, Hughes and GMV for manufacturing, ground segment support and constellation management.

Table 2 Satellite constellations

Company	Constellation Size	Satellite mass (kg)	Expected lifetime	Communication bands	Protocols
Planet	140	5	1–5 years	X-band	DVB-S2
				S-band u	GSE
				UHF TT&C	IP
HawkEye 360	3 (present)	12.75	2–7 years	S-band	Unknown
	18 (future)			X-band	
				UHF TT&C	
				S-band TT&C	
				S-band ISL	
Starlink	12,000	227	5–7 years	Ka-band	Unknown
				Ku-band	
				V-band	
				Optical ISL	
OneWeb	648	150	5 + years	Ka-band	Unknown
				Ka-band	
				V-band	
Leosat	108	1250	Unknown	Ka-band	DVB-S2
				Optical ISL	DVB-S2X

LeoSat LeoSat's constellation also aims to provide a high- speed data network with global coverage, targeted towards the business-to-business market. The constellation, to be developed by Thales Alenia Space, will be operated from two distributed ground operation centres. Each satellite will have four optical inter-satellite links, acting as routers in space, in an attempt to remove the dependence on ground gateways to relay data.

2.4 Ground segment architectures

The ground segment architecture varies greatly depending on the mission purpose, the service to be provided and the types of communication interfaces required. The user segment, whilst separate from the main ground segment, also influences its design.

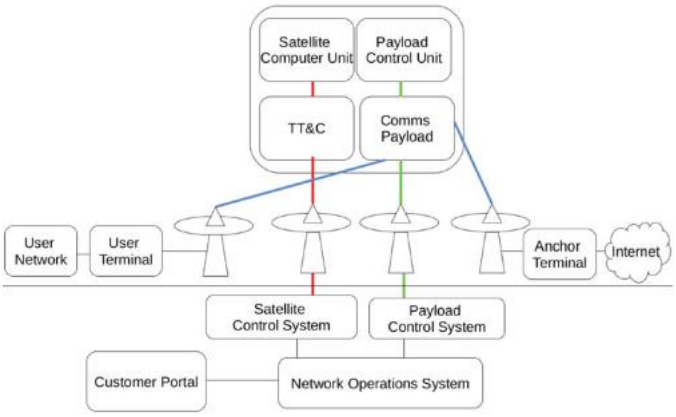
TT&C and network operations can be separated from communications related to the service the satellite provides. Users can obtain data through a direct connection between a satellite and dedicated receiver device, or through a gateway ground station forwarding on data from its connection with a satellite to a user interface via terrestrial networks. Alternatively, data can be exchanged with the service provider through feeder or hub stations, as discussed in the following examples.

Communications satellites Communication satellites are typically placed in geostationary orbits (GEO) which orbit at the same rate as the Earth at the same fixed point, but can also operate in LEO. They act as a relay between two parties wishing to communicate, commonly known as bent pipe architecture. The sending ground station transmits a message to the satellite on one frequency, which the satellite then passes onto the destination ground station at a different frequency which is then sent through the user's network (see Fig. 4a). These types of satellites enable communication between remote areas with limited terrestrial infrastructure.

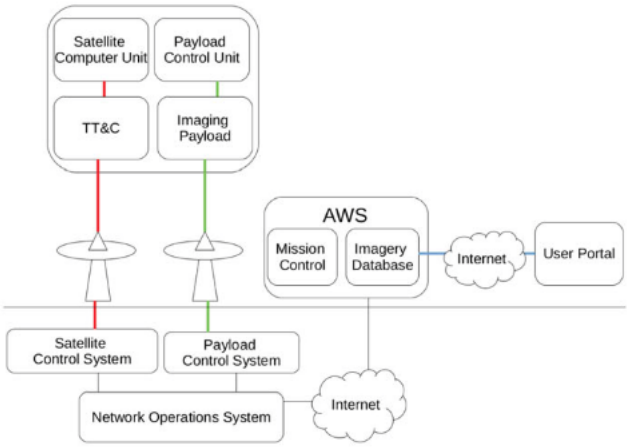
Broadcast-only satellites For particular markets, the space and ground segment are constructed to offer broadcast-only services to users. Services such as direct-to-home (DTH) satellite television and GNSS rely on specific hardware for users to receive and use signals broadcast over a large area. In DTH broadcasting, TV programmes are uplinked to a satellite from an Earth station and then broadcasted over a wide region to be received by a user's personal dish at their home. In the case of radio navigation, GNSS satellites transmit positioning and timing information to dedicated GNSS receivers.

Web-based access Other architectures exist in which the satellite operator regulates the distribution of payload data from their satellites. In this case, users have no requirement for dedicated equipment to receive satellite signals, as the satellite operators release data themselves to their users through terrestrial capabilities (see Fig. 4b). Planet's Earth Observation (EO) imagery uses 11 ground stations built to a standard specification, all of which can command and control satellites and receive imagery data. These data are centrally processed by systems in the cloud, and access to imagery data is regulated by Planet and distributed through web application program interfaces (APIs) and browser-based applications.

Fig. 4 Ground segment architectures. Red lines represent satellite TT&C communications, green lines represent payload control communications, and blue lines represent the link between two users of the communication service. Black lines represent terrestrial networking links



(a) Ground segment for communications satellites.



(b) Ground segment architecture for web-based access e.g. Planet [ ]

3. Threats to space systems and security-related incidents

The space industry has been the victim of several attacks since its inception from a wide range of adversaries and for a multitude of reasons. This section explores the types of attacks which the space industry has faced, the motivation behind them and the sectors most at risk. An analysis of past security incidents on the space industry is also presented. The Consultative Committee for Space Data Systems (CCSDS) report titled "Security Threats against Space Missions" presents an overview of threats against space missions, including illustrative examples of threats against various classes of missions. However, it is difficult to present a detailed threat model as it is strongly tied with the goals and security requirements of the target mission. In this section, hence, we explore the critical security threats and their feasibility of exploitation in New Space.

3.1 Ground segment

Compromising the ground station is ultimately the easiest way to control a satellite as it provides the equipment and software required to legitimately control and track it, and it uses existing and established terrestrial systems and attack vectors. The types of threats are generally the same during a satellite's life cycle. Types of attacks can include:

– Physical attacks, including compromising physical security measures, e.g. gaining unauthorized access to a ground station and other physical IT assets. A successful exploitation of a vulnerability through a physical attack might disable the ground station and directly affect the operation of the mission and the services provided. It might also aim to overtake the facility in order to take control of the spacecraft without technically attacking the systems. A NASA report, detailed the theft of an unencrypted notebook computer and the consequent loss of International Space Station command and control algorithms.

– Computer network exploitation (CNE) is where an attacker is able to compromise the network to which a ground station is connected to. In the same vein as attacks on enterprise IT networks, attacks could feature exploitation of poorly configured or vulnerable technologies as well as phishing to again gain unauthorized access to ground control stations.

– Cloud infrastructure, presently, powers majority of the computing framework in the ground station. From data storage to data processing, the entire platform is pipelined to cloud solutions. For example, AWS ground station is a fully managed service that lets you control satellite communications, process data and scale your operations without having to worry about building or managing your own ground station infrastructure. Failure of the cloud infrastructure could have catastrophic effect on the ground station including denial of service (DoS) for the satellite receiver. Major cloud service providers including AWS and Google Cloud Platform (GCP) are known to have regular outages or disruptions among their networks due to both internal and external attacks. These instances could hinder operations of satellite-based real-time systems.

– Data corruption/modification refers to the intentional or non-intentional alteration of data, whether being communicated or at rest. It can result in software failures or bugs, hardware

failures, use of unauthorized software, or active attempts to change/modify data to deny its use. A corrupted spacecraft command could result in catastrophic loss if either no action occurred (e.g. command is discarded) or the wrong action was taken onboard a spacecraft.

– Supply chain attacks including leaking of software/tools/ data sheets, open source research and use of common components, resulting in vulnerabilities and exploits which are incorporated into the supply chain.

– Unpatched/Outdated/Legacy COTS software deployed among the platform is a known attack surface. CVE (Common Vulnerabilities and Exposures) is an actively maintained list of publicly disclosed vulnerabilities against COTS or open-sourced software. However, the deployed software needs to be continuously updated with the latest version which contains the fixes for the discovered vulnerabilities. Unpatched versions of the software expose the application with openly documented attack vectors available for exploitation.

3.2 Communications

Communications to and from the satellite are achieved through RF waves, usually sent with frequencies in the GHz range. TT&C and data communications can be compromised at any point in the satellite's life cycle, which may require the attacker to gather additional information and conduct attacks on the ground segment. The main attack methods to disrupt data communications are listed below.

Jamming: Jamming is the act of overpowering a RF signal of a particular frequency with a higher power one of the same frequency, in order to disrupt communications between the ground station and satellite, or vice versa. Requiring an antenna, knowledge of the signal frequency and the appropriate power level to transmit, an attacker can transmit a continuous signal to deny legitimate communications. Alternative methods for jamming can be achieved through software vulnerabilities, discussed in Sect. 3.3. Key advances in the field can be seen through the Boeing EA-18G Growler air platform, an actively developed jamming infrastructure for electronic warfare. It is equipped with special payload—jamming pods, which are carried in the place of conventional weapons, in under-wing pylons. One of the systems that may be carried by EA-18G is AN/ALQ-218, supplied by Northrop Grumman. It is a Tactical Jamming System (TJS) applicable at the beginning of the radio- electronic communication.

The jammer consists of two independent groups of receivers, primary and auxiliary. The primary receiver group consists of four channelized and four cued receivers, which operate in tandem to provide immediate signal acquisition, accurate parameter measurement, immediate updates and precision geolocation, employing geolocation techniques by means of GPS tracking, or the IP address of a given device. In turn, the auxiliary receiver group provides an extended range of frequencies, substitutes the primary receiver in long-term measurements, helps in the recognition of intra- pulse modulation and updating estimates for geolocation. The AN/ALQ-218 engages a unique combination of short, medium and long baseline interferometer techniques, i.e. a device responsible for measuring the interference of electro-magnetic waves, with a patented passive algorithm to provide geolocation of emitters for

cueing jammers and other built-in equipment such as electro-optical sensors, infrared radiation (IR) technology and on-board radar stations.

Eavesdropping Eavesdropping is the interception of data over a communication channel. For satellite and ground systems, this channel is an RF signal sent over the air, meaning that all communications are susceptible to interception. Data sent over RF signals are sometimes not encrypted or use low-grade encryption which can be overcome to retrieve the cleartext information.

The ELectronic INTelligence (ELINT) satellites are one of the tools used by military and security services in several countries to eavesdrop on the information being transmitted through the air. Galactic Radiation and Background (GRAB), a US 80-kg satellite launched in 1962, was the first ELINT satellite launched and provided unprecedented information about the signals emitted by Soviet radars at a time when those two superpowers were Cold War adversaries and when information about activities inside the Soviet Union was almost impossible to obtain at that time. The ELINT satellites need enormous antennas to pick up radio signals, since they are located 36,000 km above the equator. The antenna on the US military communications satellite Mobile User Objective System (MUOS) is 28.6m diameter when unfurled in orbit—the largest known publicly. But the secret eavesdropping satellites are reported in the media to have already had 50-m-wide antennas by 1994 and 90-m ones by 2006.

Hijacking Many instances of satellite hijacking, reusing a satellite for another purpose, have been noted in recent history. This could be altering the legitimate signals or changing them completely. COTS products can also be used for this purpose.

Broadcast signal intrusion is a form communication hijacking, where broadcast signals of radio, television or satellite are hijacked. The mode of hijacking can be done, either by overpowering the original signal at the same frequency or directly breaking into the transmitter and replacing the signal. The Max Headroom Broadcast Signal Intrusion Incident is one of the most known instances, where the attacker smothered the TV station's broadcast by sending a more powerful signal to the antenna atop their broadcast tower and distributed it over their satellite link and land-based microwave links.

Spoofing Spoofing is the art of transmitting a signal, appear- ing to be legitimate, but sending erroneous data for your own purposes. The spoofing of location data in global navigation satellite systems can have a significant impact. For instance, Global Positioning System (GPS) signals which provide accurate location and timing services can be spoofed with COTS components. In fact, GPS systems aboard several ships reported that the ships were on land when in fact they were still in the Black Sea.

Extensive research has been carried out to find the parameters values required for a successful GPS spoofing. The identified ranges provide benchmarks to successively avoid spoofing attacks. Cryptographic techniques designed to protect GPS spoofing are further discussed in Sect. 4.5. Other techniques that have been developed to tackle spoofing include utilizing other self-contained sensors, namely inertial measurement units (IMUs) and vehicle odometer output. To detect a spoofing attack, the technique analyses GNSS and IMU or

odometer measurements independently during a preselected observation window and cross-checks the solutions provided by GNSS and inertial navigation solution (INS)/odometer mechanization.

The legacy GPS signals include an encrypted binary code known as Y-code that is transmitted, with these signals only intended for military use. Without the encryption keys, it is virtually impossible for an adversary to generate the Y- code and, hence, virtually impossible to spoof a GPS receiver set to track Y-code. The Selective Availability Anti-spoofing Module (SAASM) can track Y-code only when loaded with the currently valid decryption key, and the modules are tamper-proof to prevent reverse engineering by adversaries. SAASM receivers such as the NovAtel OEM625 are only available to government-authorized customers. By using the encrypted signal, the device provides greater signal accuracy in the event of GPS interference. Furthermore, the government is capable of disabling civilian satellite navigation signal so that the only remaining signal is reserved for users with the SAASM module.

3.3 Space segment

Once in orbit, a satellite has limited physical contact with humans, although that does not mean security threats are not present. Vulnerabilities in the software and hardware in use on the satellite can occur and can impact the satellite's operation and robustness of security controls. In the case of using SDRs and digital signal processing software to provide radio functionality, insufficient checks in radio frame processing and sending malformed data packets could lead to buffer overflows and create denial-of-service conditions to jam communications. This type of jamming is significantly more stealthy as it is triggered by sending only a small number of packets and also does not require sending a continuous RF jamming signal. Since satellites are deployed on missions requiring high dependability, they are equipped with embedded reliable operating systems (cf. Sect. 4.1), which provide significant security guarantees against memory-abuse attacks.

Depending on the complexity of the satellite and ground control systems and the security measures (or lack thereof) in place, taking control of a satellite to manipulate its system and/or orientation of orbit can be a difficult task. Requiring significant skill and knowledge to breach the TT&C links, and chaining several of the previously mentioned satellite attacks, other areas such as software vulnerabilities and replaying of recorded transmissions can contribute to achieving control. Even agencies such as NASA and government organizations are not immune to threats such as these, with several examples of satellites being under the control of attackers.

3.4 Regulatory requirements

Guidelines established by the Committee on National Security System (CNSS) have been used for years to regulate security protections on satellite communications used in national security missions. The CNSS Policy 12 (CNSSP-12) strives to implement security practices into the ground and space systems at the design phase, rather than attempting to fit security in afterwards. It enforces the use of techniques such as authentication, NSA-approved end-to-

end encryption and pseudorandom bit streams to achieve confidentiality and integrity and to remove predictability in messages.

Although commercial satellite systems used in national security missions and interfacing with government systems must also adhere to CNSSP-12, commercial and private spacecraft falling outside of this are not required to gain a formal accreditation of cyber security. However, some enterprises are using the principles of CNSSP-12 to prioritize security requirements. As examples, the LeoSat constellation is trying to be "as close to CNSSP-12-compliant as possible" by incorporating encryption over all data sent over its network and the Starlink constellation will feature "End- to-end encryption encoded at firmware level".

3.5 Review and analysis of satellite incidents

For our analysis, we have prepared a timeline of incidents involving the space industry from various sources including academic literature, governmental agencies and news articles from the public domain between 1977 and 2019. These incidents were categorized in terms of:

– The segment under attack or exploited

– The type of target, i.e. government, commercial, civilian and military

– The type of incident, e.g. jamming, spoofing, CNE, hijacking, etc.

– The motivation for the incident, e.g. state espionage, hack and leak, criminal activity, etc.

It should be noted that since these incidents are from public domain sources, certain limitations are placed on this analysis. Incidents may have been under- or miss-reported as incidents may have not been detected, or over confusion about what has happened, or for national security concerns in sectors such as military or government.

Table 3 shows a breakdown of the number of incidents with respect to the sector and segment which were targeted, and the type of technique used. The ground segment is the most targeted sector from the incidents examined, followed by RF data communications. This is anticipated due to the familiarity of tried and tested techniques on the ground segment by attackers and the exposure of RF communications across the world. The space segment, whilst having a smaller frequency of reported incidents, is still being targeted despite having several difficulties to conduct attacks.

The majority of reported incidents were focused on governmental assets. Twenty-eight incidents targeted commercial organizations, over twice as many as the civilian or military sectors. Due to the secrecy of military operations, incidents may not have been reported publicly, and the frequency of military incidents may in fact be higher.

Table 3 Segment and sector analysis of satellite security incidents

	Category	Frequency
Segment	Ground	83
	Space	8
	Data communications	38
	Unknown	2
Sector	Government	91
	Commercial	28
	Civilian	11
	Military	11
Incident type	Jamming	19
	Eavesdropping	3
	Spoofing	3
	Control	4
	CNE	30
	Hijacking	16
	Phishing	3
	Internet hijacking	1
	Denial of service	3
	Theft/loss	48
	ASAT incident	3

Incidents concerning the theft or loss of space industry- related assets and CNE activities were among the highest reported, expected due to the terrestrial-based nature of these techniques. Jamming and hijacking incident frequency follow behind and were the most popular to abuse and disrupt the RF communications segment. Other types of incidences were reported, such as eavesdropping, control, spoofing and phishing, but occurrences were limited to between 1 and 4 times.

The motivation of space and satellite incidents was also explored, and Fig. 5 shows the number of incidents for each type of motivation or intent. State espionage incidences made primary use of ground segment techniques. Common mistakes are being made in this segment as CNE activities hold a significant lead over data communications and space segment techniques. CNE and phishing techniques were also dominant in incidents motivated by corporate espionage and hack and leak attacks.

Politically motivated incidents were usually carried out through RF jamming or signal hijacking, aiming to either stop or alter satellite TV and radio broadcasts with political messages. Signal jamming and hijacking were also noted to be accidental and from personal use, e.g. GPS jamming to avoid employer asset tracking, or in some cases for unknown motivations. Some instances of signal hijacking were used to convey warnings to the public over satellite TV, and jamming was also used in attempts to stop criminal operations using satellite phones.

Three anti-satellite (ASAT) incidents (two tests and one planned mission) were intended to destroy a state's own orbiting satellites.

Criminal organizations exploit the ground and data communication segments, using CNE to gather information to sell onto other states. Another incident did not attack satellite systems directly, rather it used satellite Internet connections to find valid subscriber IP addresses to infect other servers. As the ingenuity and innovation of the New Space era increase, so does that of adversaries.

A number of space and satellite industry incidents were also grouped in ten-year period in Fig. 6, which also shows the number of operational satellites between 1958 and 2018 from[1]. This figure shows an increase in the number of incidents reported in this ten-year period since 1977 and an increasing rate of satellites in operation. Both of these data sets show a substantial leap since the widespread adoption of the Internet in organizational IT practices in the early 2000s and beginning of the New Space age. Whilst there are competing factors to determine the success of malicious incidents, e.g. increases in computing power, new attack techniques and tools and the adoption of consistent security cultures, this increasing trend could be carried on in future decades if the space industry does not make security a priority.

4. Key enabling technologies in New Space

For decades, the designs of military, government and commercial satellite systems from space-capable nations have been on the most part, proprietary. This is in part due to the nature of the tasks these satellites were performing, those related to national security and sending sensitive data, or to protect satellite operator's intellectual property, although academic institutions generally detail the hardware and software in use in their satellite experiments. This section analyses key technologies of the New Space era.

[1] JSR: Number of active satellites from 1957 to 2018. Statista Inc., https://www.statista.com/statistics/897719/number- of-active-satellites-by-year/.

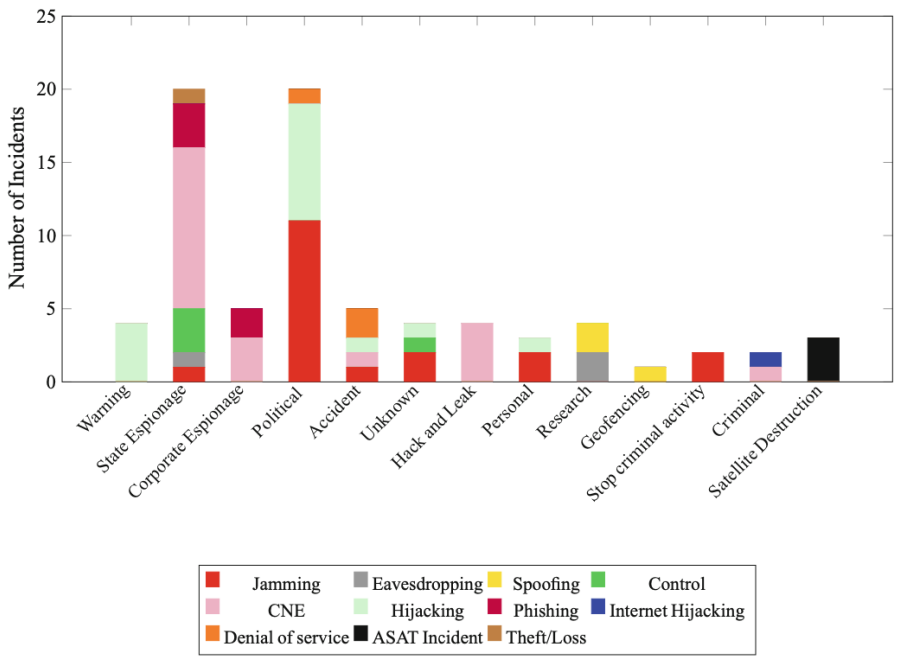


Fig. 5 Motivation of satellite incidents and a breakdown of the techniques used

CubeSats are steadily becoming a part of global computing infrastructure, where components need to be protected from adversarial physical access. Sensitive computation often has to be performed in a trusted execution environment (TEE), which, in turn, requires tamper-proof hardware. If the computational fabric can be tampered with, the correctness of the computation cannot be trusted. A recent study has demonstrated this approach, providing a practical hardware security module solution for space and using them as a root of trust for a certificate authority (CA). CubeSats have also been used to demonstrate quantum key distribution (QKD), a series of post-quantum secure cryptographic techniques for sharing a secret key among two parties (cf. Sect. 4.5).

COTS components, open source and GPL-licensed products

The space industry has taken advantage of the global boom of affordable and powerful commercial electronics. The use of COTS components in academic endeavours is commonplace due to the limited budgets of research projects, but it has also provided a platform to examine and exhibit these technologies in-orbit. It seems a likely conclusion that satellite start-ups originating from university students will continue COTS practices to build upon their academic experience. In addition, the time and cost savings are a strong driver for COTS use across the entire commercial sector.

Details of satellites designed and constructed by academic institutions with COTS components in mind are prevalent. Many of these constructions utilize field programmable gate arrays (FPGAs), system-on-chip (SoC) components and microcontrollers. These satellites also make use of the open- source real-time operating system such as “XilKernel”, FreeRTOS. Other open-source software and hardware designs specifically for space and ground systems include KubOS10 , UPSat and EQUiSat .

Table 4 Small satellite classifications

Classification	Mass (kg)
Minisatellite	100–500
Microsatellite	10–100
Nanosatellite	1–10
Picosatellite	0.1–1
Femtosatellite	0.01–0.1

In recent years, some companies have been more forth- coming about their satellite architectures, mainly those which implement COTS technologies. Section 2.3.1 details the information known about the construction of Planet and HawkEye 360's satellites. Planet also released an open-source radio solution which has been deployed in each of its satellites, providing both hardware and software tools.

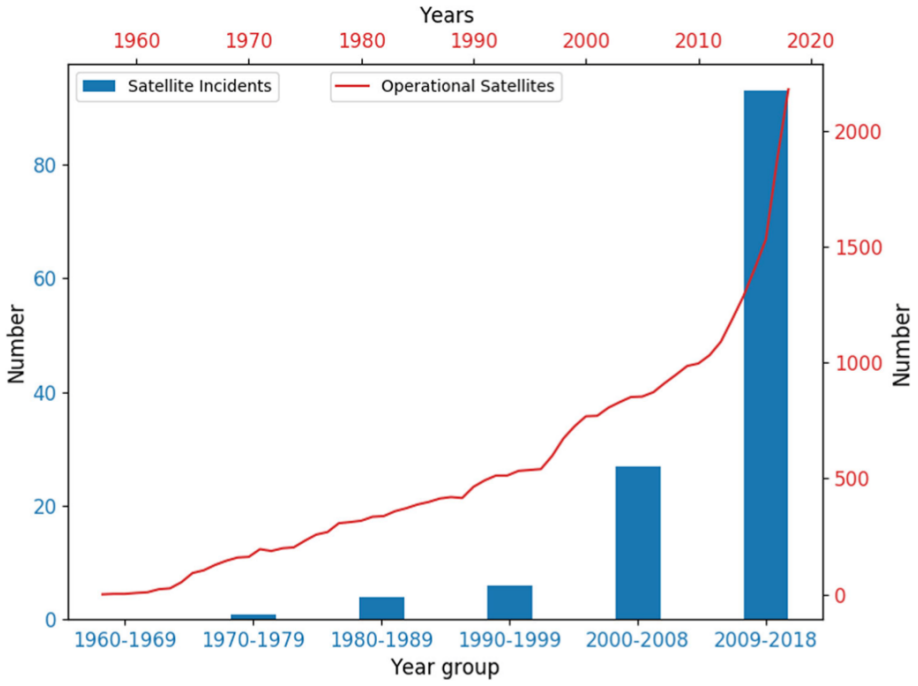


Fig. 6 Number of satellites attacks per year group is plotted on the bottom and left axes, and the number of operational satellites between 1958 and 2018 is plotted on the top and right axes

The trend towards use of COTS software and hardware is driven by several factors, including significantly lower procurement cost. COTS products are often highly complex, some of them involving tens of millions of lines of code, so that no one knows their content and behaviour in detail. Legacy systems make up the vast bulk of the code base, and all new systems become legacy when they come on line. With this complex system, COTS products are essentially a black box to their users. The US government provides a list of risks associated with employing COTS software and mitigation techniques to avoid them. The

usage of COTS products, thus, needs to be met with vigorous security analysis through black-box testing mechanisms (e.g. fuzzing, boundary value analysis, equivalence partitioning) using COTS tools or be checked for compliance with known security guidelines like STIG (Security Technical Implementation Guides) and OWASP Top Ten for software and FIPS 140-3 for hardware before being deployed in use.

Software-defined radios (SDRs) One of the major technology advancements made in the New Space era is SDRs, which "represent a radio that has software control over some functions, and still being partly implemented in analog electronics". Functionality traditionally implemented in hardware—filters, modulators, mixers—is now moving to software. This technology affords space systems with flexibility and reconfigurability, whilst also removing the need for dedicated hardware to save space on satellite buses. SDRs such as RTL-SDR, USRP and LimeSDR are commonly available for purchase.

This move to SDRs shows a shift between the technologies in Old Space and New Space. For Old Space, radio communications were achieved through traditional dedicated radio hardware. The relationship between satellite hardware, software and the Open Systems Interconnection (OSI) model, which abstracts communications into seven separate layers, typically falls into the one shown on the left side of Fig. 7. Hardware is used for the physical and data link layers, with software covering the other five layers and optionally the data link layer. SDRs implement functions that originally resided in hardware, but now in software, encapsulating the physical, data link and network layers, demonstrated in the right side of Fig. 7. More parts of the communications stack consist of software instead of hardware, reducing satellite reliance on hardware but opening the system to software threats. Traditional radio components have in-built limitations, such as specific frequencies and filter ranges. Trusted hardware functions are now in software, so future implementations must consider how to trust software to behave as intended and in a secure manner.

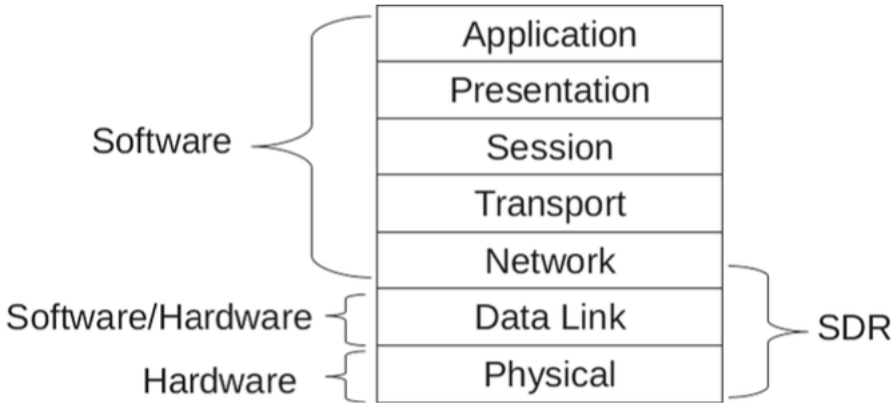


Fig. 7 OSI communication model for satellites showing relationship to SDR technology

Authentication of signals is a critical aspect of secure communication. Most mechanisms of authentication (e.g. digital signatures and certificates) exist above the physical layer, though some (e.g. spread-spectrum communications) exist at the physical layer often with an additional cost in bandwidth. The use of SDRs at physical layer has provided low-cost authentication solutions using various software techniques like fingerprint embedding where a low-power secret modulation is superimposed over the message waveform which serves as an authentication tag.

Although SDRs provide significant advantages over hardware techniques, they introduce protocol-independent software vulnerabilities into the system. In the process of securing SDRs, several integrated components have been proposed. A survey paper on the security of SDRs discusses the threat model SDR faces and architectures proposed to mitigate them. Notably, a secure SDR architecture proposed is composed of an automatic and calibration unit (ACU), a radio security module (RSM) and a location component based on a GNSS receiver (cf. Fig. 8). The ACU controls the output spectrum to be compliant with the local spectrum regulations. The SDR stores the information (e.g. spectrum configuration files) on the spectrum regulations in various spectrum jurisdictions in the world. The GNSS receiver in-built provides the location of the SDR at any given time; the ACU uses the location and the spectrum configuration files to determine the correct spectrum regulations.

The ACU represents a protection technique against security threat if the SDR services are related to transmission and communication of signals. Even if a malicious waveform is activated in the SDR node, the ACU can prevent it from transmitting in unauthorized bands. The RSM is responsible for download, activation and execution of the software modules. With the potential harm that malicious SDR code could cause, the veracity of the RSM functions is critical; therefore, these functions must be implemented with a suitable level of trust.

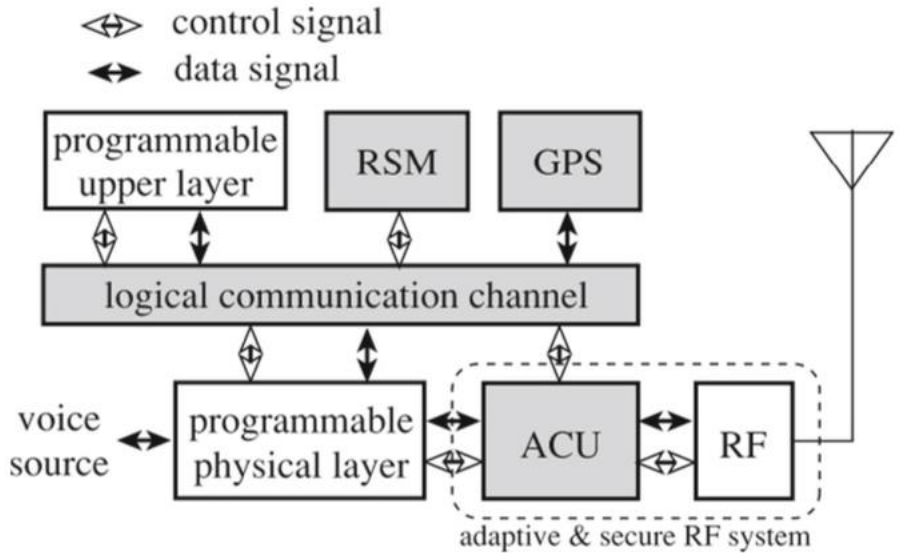


Fig. 8 ACU- and RSM-based SDR hardware architecture [

A popular digital signal processing software used with SDRs is GNU radio, which provides standardized signal processing blocks to implement radio communications with SDRs, either with real RF hardware or in a simulated environment. It has been used widely in academic circles with some confirmed usage in the commercial sector.

SDR usage is becoming more widespread with significant numbers of "How To" guides on satellite eavesdropping with SDRs available on the Internet, e.g. [2] [3] detail how to obtain weather satellite imagery using SDRs, provides commentary on using an SDR to listen on transmissions from spacecraft travelling to the International Space Station (ISS), and a tutorial for decoding messages from the satellite communications provider Inmarsat is available from[4].

4.2 Ground segment

Automation and autonomy Autonomy has made great strides in the past few decades with autonomous vehicle prototypes in action and great leaps made in robotics. Autonomous operations are those in which a system performs self-regulating and self-controlling actions and have been attempted to be implemented in the ground segment since the late 1980s. Strides have been taken to provide autonomy in space rovers—NASA's Curiosity rover employed autonomy in areas such as navigation and sample selection.

The ability of a ground station and mission control centre to command, control and receive payload transmissions for satellites without the need for human interaction is a desirable one. Automation helps to reduce costs but also enable scalable and complete management of potentially large numbers of satellites belonging to a constellation.

Experimentation of autonomous ground station and on- orbit operations has been developing, with examples provided, reporting successful demonstrations of autonomous operations. Autonomy has also expanded to commercial interests with SpaceX releasing Starlink constellation information which states that satellites are "capable of tracking on-orbit debris and autonomously avoiding collision".

Commercial interests, such as Planet, have already incorporated automated procedures in both their software and firmware development and in the satellite commissioning stages, which are expanded upon in[5]. Initially, a ground-based software process, Planet, moved to on-board commissioning software due to the unscalability of their original process for an

[2] Dillon, H.: Receiving weather satellite images with Softrock. http://www.alternet.us.com/?p=1398

[3] Baguley, R.: Full Earth Disc Images From GOES-17 Harvested By 2019 SDR (2019). https://hackaday.com/2019/05/03/full-earth-disc- images-from-goes-17-harvested-by-sdr/.

[4] rtl-sdr.com: RTL-SDR Tutorial: decoding Inmarsat STD-C EGC Messages (Aug 2015). https://www.rtl-sdr.com/rtl-sdr-tutorial- decoding-inmarsat-std-c-egc-messages/.

[5] Zimmerman, R., Doan, D., Leung, L., Mason, J., Parsons, N., Shahid, K.: Commissioning the world s biggest satellite con- stellation. In: 31st Annual AIAA/USU Conference on Small Satellites. No. SSC17-X-03 in Year in Review (2017). https:// digitalcommons.usu.edu/smallsat/2017/all2017/.

entire constellation. Forty-seven out of 88 of its satellites were able to complete the commissioning process completely automated. Out of the 150 calibration manoeuvres for ADCS across all satellites, 110 were fully automated. Whilst not a perfect run, these automated operations allowed satellites to be commissioned by teams of 1–2 operators, reducing their involvement and increasing the efficiency of the entire process.

Cloud computing Cloud computing is a strong candidate to provide part of ground segment infrastructure, moving processing and storage away from personal computers to large data centres, accessed over the Internet. Cloud computing affords greater flexibility and availability with multiple sites for redundancy and provides an independence from location or device-type restrictions. Planet's imagery data and mission control software are hosted in the cloud and customer's access imagery through web-based protocols.

From an education and amateur standpoint, networks such as the Satellite Network Open Ground Stations (SatNOGS) and Global Educational Network for Satellite Operations (GENSO) (no longer actively maintained), provide software and hardware details to begin tracking satellites with the use of cloud computing architecture. These implementations use client software to operate the ground station after receiving instructions through their network, with telemetry data available for access over the Internet.

Some ground station operators such as KSAT, who provide these capabilities for Earth-i and HawkEye 360, have already adopted cloud-based technologies to manage customer's scheduling needs through browser-based applications. RBC signals, a satellite ground station network operator, confirmed that it had plans to implement cloud-based mission control software developed by KubOS.

Even Amazon is transitioning into the space arena after success in e-commerce and cloud platforms, providing ground stations as a service. Space sector companies such as DigitalGlobe, BlackSky, Spire Global, Capella Space and Open Cosmos are reported to be its first customers.

Whilst cloud providers can guarantee some measurable non-functional performance metrics, e.g. service availability or throughput, there is lack of adequate mechanisms for guaranteeing certifiable and auditable security, trust and privacy of the applications and the data they process. For example, there exists a fragile transparency in the trustworthiness of remote satellite imagery from cloud providers because of conflicting policies between them and governments on grounds of international security. Object Management Group provides a list of cloud security standards and certification to be expected from the providers before moving to a service. In addition to the general standards and frameworks, there are others that operate at country or regional levels or that apply to specific industries (e.g. PCI DSS) or to specific types of data (e.g. HIPAA, GDPR). It is impertinent that cloud customers continually review service provider security controls and standards to ensure they are properly defined and enforced as this is the sole security guarantee from a cloud provider.

Edge computing An abstraction of cloud computing, edge computing, leverages processing within a closer local network to perform operations typically performed in cloud services.

This brings applications and data to a closer location to the user, reducing latency in networks.

Edge computing has been used with Internet of things (IoT) devices, especially sensors which provide readings for processing to nearby edge devices. System decisions can then be made based upon readings and then data sent to the cloud afterwards. An example of this is smart cities where sensors readings across cities provide edge devices the data to make decisions to influence transportation, energy and crime.

IoT devices, edge computing and satellites have already become intertwined. The Australian-based company Fleet provides a gateway device containing an edge server, satellite modem and antenna which connects to IoT devices. This gateway collects, processes and analyses sensor data and uses their satellite communications network to send only the relevant information to a business's central cloud infrastructure.

4.3 Space protocols and their security

Satellite communication links often suffer from higher error rates and latencies than terrestrial cabled networks and, in the case of LEO satellites, only have a small window of time to communicate whilst in range of a ground station. Communication protocols have often been lightweight to lower the resource requirements of satellites.

The CCSDS has created a set of protocols for telemetry, telecommand and OSI model layers (application, transport, etc.). Adapted to support protocols from the IP suite, CCSDS is making data communications more accessible and familiar for new enterprises in the space industry. The implementation and demonstration of these protocols have been noted in over a thousand missions listed on the CCSDS website[6], with several commercial telecommunication satellites using CCSDS command and control capabilities.

Surveys on satellite communication protocols are presented in[7] which summarize current protocols in use. This section aims to provide a more extensive overview into their security.

Physical One of the most widely used satellite services is satellite TV. The majority of satellite TV broadcasts is achieved using DVB protocols, i.e. DVB-S, DVB-S2, DVB-SH. These physical (and data link) layer protocols standardize methods to broadcast television signals globally, and encryption can be applied on top of these transmissions. The conditional access system (DVB-CA) defines a common scrambling algorithm (DVB-CSA) and a physical common interface (DVB-CI) for accessing encrypted content. DVB-CA providers

[6] The Consultative Committee for Space Data Systems: CCSDS Missions. https://public.ccsds.org/implementations/missions. aspx.

[7] Davoli, F., Kourogiorgas, C., Marchese, M., Panagopoulos, A., Patrone, F.: Small satellites and CubeSats: survey of structures, architectures, and protocols. Int. J. Sate. Commun. Netw. (09 2018)

Burleigh, S.C., Cola, T.D., Morosi, S., Jayousi, S., Cianca, E., Fuchs, C.: from connectivity to advanced internet services: a comprehensive review of small satellites communications and net- works. Wirele. Commun. Mob. Comput. 20192019, 1–17 (2019)

develop their wholly proprietary conditional access systems with reference to these specifications. Cryptanalysis of the common scrambling algorithm provides intuition for the vulnerability of the algorithm to several generic attacks. However, no feasible attack against the protocol with considerable advantage has been published yet. Constellation companies Planet and LeoSat propose to use DVB protocols for imagery downlinks[8] and "both earth-to-satellite and satellite-to-earth links"[9] respectively.

Optical communications A recent development in satellite communications is the use of optical communication payloads using visible light communications (VLCs). These can provide higher data rates whilst steering clear of radio frequency electronic warfare activities such as jamming and avoiding exhausting the RF spectrum. Whilst affected by cloud coverage, making them less fitting for ground to space links, they are suitable for inter-satellite links.

Already large optical payloads have been demonstrated in satellites such as Artemis, Spot-4, Envisat Adeos-II, OICETS, Kodama, DAICHI and SDS-1 at extremely high wireless data rates. NASA's Laser Communication relay aims to discover whether optical communication transceivers can be built with similar mass and power requirements to a traditional RF system. Broadband constellation plans such as Starlink and LeoSat aim to use laser communications for inter-satellite links to reduce latencies in their networks.

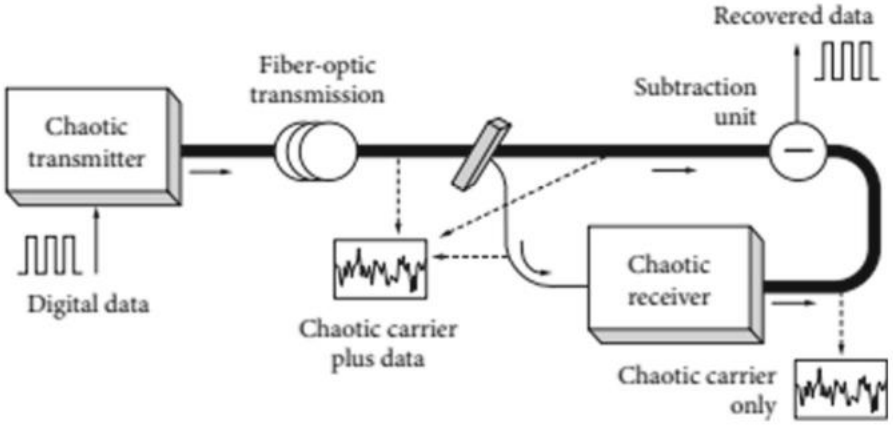


Fig. 9 An optical communication system based on chaos encryption

[8] Zimmerman, R., Doan, D., Leung, L., Mason, J., Parsons, N., Shahid, K.: Commissioning the world s biggest satellite con- stellation. In: 31st Annual AIAA/USU Conference on Small Satellites. No. SSC17-X-03 in Year in Review (2017). https://digitalcommons.usu.edu/smallsat/2017/all2017/.

[9] LeoSat: LeoSat Non-Geostationary Satel-lite System—Attachment A. licens-ing.fcc.gov/myibfs/download.do?attachment_key=1158225.

Optical communication can be secured by quantum cryptographic techniques using QKD (cf. Sect. 4.5). A less secure but significantly studied in the literature method of securing communication is chaotic encryption. It can be realized by encoding the message using chaotic carriers. The objective of chaos hardware encryption is to encode the information signal within a chaotic carrier generated by components whose physical, structural and operating parameters form the secret key. Once the information encoding has been carried out, the chaotic carrier is sent by conventional means to a receiver. Decoding of the message is then achieved directly in real time through a so-called chaos synchronization process. However, chaotic cryptosystems have proven to be insecure because of the inadequacy of logistic maps used for encryption(Fig. 9).

Data link Educational and small satellites have been noted to use various simplistic data link protocols, some of which were originally designed for amateur packet radio such as AX.2521, offering data frame processing and fault detection, but not error correction. Other data link protocols such as the unified space link protocol (USLP), new satellite data link protocol (NSLP), low-altitude multiple satellite data link control (LAMS-DLC), Proximity-1 and Nanolink, detailed in [10], provide similar data framing services and varying degrees of error correction and reliability procedures, but no built-in security.

Low-impact educational missions do not immediately prompt for more complex and security-driven protocols; however, commercial enterprises such as Planet also reported using the AX.25 protocol. These organizations often have greater needs for confidentiality and privacy, for which these types of lightweight protocols may not be suitable.

The CCSDS Space Data Link Security (SDLS) protocol extends its data link protocols to incorporate confidentiality services through encryption of the frame data, authentication and integrity through authenticated and non-authenticated message authentication codes (MACs), respectively, and anti-replay protection through the use of sequence numbers. The scheme is designed and analysed in adherence to the security concerns mentioned in ISO 7498-2[11]. The protocol, overall, attempts to offer confidentiality, integrity and/or authenticity of the transmitted data. However, it fails to provide guarantee against DDoS by jamming, traffic flow analysis and data substitution attack if the encryption does not use authentication.

Networking and transport Network protocols such as the Space Packet Protocol (SPP) and Delay Tolerant Network Bundle Protocol (DTN BP) allow for asynchronous data transfers, suitable for data transmission delays found in satellite communications. Broadband services commonly use IP protocols. Reliability services emerge through transport protocols. The space communications protocol specification- transport protocol (SCPS-TP) based upon TCP and Licklider Transmission Protocol (LTP) which can run over UDP or the data link offer such services. The TP stack was actually designed as a part of SCPS protocol suite, with an SP security layer, FP file transfer and NP network protocol intended to replace IPSec, FTP and IP, respectively. However, with the evolution of the Internet and supporting protocols,

[10] Davoli, F., Kourogiorgas, C., Marchese, M., Panagopoulos, A., Patrone, F.: Small satellites and CubeSats: survey of structures, architectures, and protocols. Int. J. Sate. Commun. Netw. (09 2018)
[11] Iso 7498-2:1989 (2000). https://www.iso.org/standard/14256. html

these other SCPS layers have become irrelevant. TCP has historically been deemed ill-fitting for space due to its bad performance; however, these newer space-related protocols are designed to balance the high error rates and latency issues which lower TCP performance. Alternatively, TCP performance enhancing proxies (PEPs) are widely used to overcome the limitations of TCP over satellite links. This is known as TCP splitting, where each overlay hop between each PEP is considered as a new TCP connection.

IPSec provides authentication and encryption of data packets to provide secure encrypted communication between two computers over an IP network. However, TCP PEPs are not compatible with IPSec as PEPs need to analyze the headers of TCP segments and IP packets between two ends to route the packets through suitable PEPs. Since IPSec tunnels mask the content of the IP packets, in particular the source and destination of data, it is impossible to implement a PEP through a IPSec tunnel. Several solutions have been proposed to circumvent this issue by either adding additional information to the packet or selective usage of the IPSec protocol.

The CubeSat Space Protocol (CSP) provides a simple design to achieve networking and transport services, which also compatible with several different physical and data link protocols. CSP includes encryption and integrity features with the use of the XTEA algorithm for encryption of packets and HMAC-SHA1 for message authentication. Although these algorithms have known cryptographic weaknesses that undermine these security features, they are preferred for their lightweight operation on CubeSat's embedded systems.

For securing communications for the CCSDS Space Packet protocol, the use of encryption and digital signatures is prescribed to increase security. The encryption lies solely on the application data and not the header of packets, and the digital signature or an integrity check value (ICV) is appended to the end of the encrypted data. Some drawbacks appear with this implementation namely that the header remains in cleartext; this solution offers no anti-replay protection, and it may be possible to differentiate between encrypted and unencrypted packets from the header.

Application Whilst application layer protocols are usually mission dependent, we note some file transfer protocols that are currently in use: CFDP developed by CCSDS and Saratoga developed by SSTL. Whilst Saratoga is designed to operate over IP and is suitable for short LEO satellite passes, CFDP combines functionalities from both the application and transport layers to ensure reliable file delivery over multiple types of link with minimal resource consumption.

Application layer security controls can be applied to the communication stack; however, security considerations provided at lower protocols, at the network, data link or physical layers, may be sufficient for some missions. [12] lists the transport layer security protocol and X.509 certificates as a way to implement encryption and authentication controls, though the verification of certification chains renders this protocol unsuitable for space owing to long latency times whilst handshaking.

[12] The Consultative Committee for Space Data Systems: The Application of Security to CCSDS Protocols. Technical Report CCSDS 350.0-G-3 (2019)

4.4 User segment

The user segment deals with the applications of satellite systems. Applications such as navigation, TV and communications often require dedicated hardware. Other systems use the data that these dedicated receivers collect to serve a specific product or application. For satellite TV transmissions, a dish and set-top box must be installed to receive the particular channels provided and perform subsequent tuning and decoding of transmissions for viewing. For navigation purposes, a GNSS receiver acquires signals from a constellation to determine the location of the receiver. Applications use data from GNSS receivers in mobile phones or satellite navigation devices to plan routes, e.g. Waze.

Alternatively, instead of consumers having the ability to receive satellite signals themselves, a satellite operator may collect all data themselves and then distribute it via terrestrial networks. Earth observation, signal intelligence, metrological and scientific applications typically make use of this. This way, customers do not need to install or buy hardware to get access to the data. Access to the data is managed by the opera- tor, and key technologies include web APIs and customer web portals, often cloud-based, or dedicated installable software. Planet and HawkEye 360 provide various apps and APIs to access imagery and signal mapping data for customers. Scientific data may be free to access and download from the web, e.g. datasets from the International Satellite Cloud Climatology Project (ISCCP) are accessible from their website[13].

4.5 Cryptography for New Space

Novel cryptographic mechanisms are emerging in the satellite industry. Navigation message authentication (NMA) is an authentication mechanism to provide authenticity and integrity of the navigation data to the receiver. NMA can use both or either of the symmetric/asymmetric key encryption approaches to achieve this goal.

The Chips Message Robust Authentication (CHIMERA) is a hybrid NMA and spreading code authentication mechanism proposed for GPS signals. It achieves NMA using asymmetric elliptic curve digital signature algorithm (ECDSA) P-224, a well-established standard. However, CHIMERA requires receivers to have occasional access, via- non-GPS channels, to provide authenticated GPS public keys and a public key infrastructure (PKI) to verify the authenticity of the key provided.

The Galileo GNSS, as part of message authentication of its public open service, will incorporate the established Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol with a novel single one-way chain of crypto- graphic keys shared by all satellites. The TESLA protocol has low computational and communication overhead and can also support one-to-many transmissions, making it a suitable choice for GNSS. The TESLA protocol uses MAC to prove the origin and identity of a message. The key to compute the MAC, belonging to a chain generated by a one-way function, is sent some time after the message and the MAC.

[13] International Satellite Cloud Climatology Project: ISCCP Data Access. https://www.ncdc.noaa.gov/isccp/isccp-data-access.

In the Galileo Open Service implementation, different keys are transmitted to user receivers from different satellites, but the keys are still from the same chain. The keys are transmitted in the reverse order of their computation from the chain. Hence, using the one-way function, the receiver can verify that each chain key is from the same chain as the root key by recomputing the chain. However, it is impossible to predict future keys by adversaries as it is computationally hard to invert an one-way function. Cryptanalysis of the architecture shows that with current proposed parameters, combined with the use of efficient hashing hardware, it can lead to a feasible attack with significant collision probability. Whilst increasing robustness of transmissions against data losses and in difficult visibility conditions, it also allows cross-authentication of neighbouring satellites.

The symmetric key encryption style of TESLA eliminates the PKI requirement posted by CHIMERA. However, the main disadvantage of the scheme arises from their security condition; it requires a coarse time synchronization between the sender and the receiver. Without this assurance, the receiver cannot be certain that the navigation message has not been generated by a spoofer who received the valid sign- ing key from the satellite signal.

Variants of TESL A protocol include μTESL A, infTESL A and multi-level μTESL A which have been proposed for wireless sensor networks to overcome the disadvantages of the TESLA protocol. Still, performance analysis has not been performed for them with respect to GNSS satellite links.

QKD allows two parties to establish a secret key with unconditional post-quantum security by making use of the fundamental laws of quantum mechanics. QKD occurs in two phases, namely the quantum phase, where quantum superimposed signals are exchanged between the two parties establishing the raw key for each party. The second phase is the classical phase, where interactive key exchange protocols are used to distil two identical strings from the raw key.

Optical communication networks provide ideal channels for exchange of quantum photons. However, glass in the optic fibres tends to absorb the photons, increasing the error rate of the transmitted signals. Since security bound for quantum security provides a maximum error rate of 11% for transmission, the use of optic fibres is limited to a distance of few hundred kilometres for appreciable security.

On the other hand, by using satellites equipped with high-quality optical links, satellite-QKD can achieve ultra- long-distance quantum communication in the 1000 km range. Hence, optical free space links are currently the most promising channel for large-scale quantum communication by use of satellites and ground stations. The usage of a satellite terminal in space makes it possible to develop quantum communication networks on a global scale. Significant experimental efforts have been devoted to investigating the feasibility of satellite-based quantum communications. NanoBob, QEYSSat and NanoQEY are some key advances in quantum research to establish a practical satellite QKD system.

5 Open challenges for space and satellites

In this section, the challenges for satellite and ground segments are discussed. The security and usability of a system are often a delicate balance and require careful consideration to achieve a desired level of service for the end user. These open challenges have been categorized into two streams, security and privacy related, and data throughput and energy consumption, to reflect these conflicting needs.

Lightweight authentication and secure communications

– Most of the satellite communication protocols are designed to be lightweight to reduce power and memory requirements and increase the speed of transmissions. Broadband constellations are aiming to provide services with high data rates and low latencies. Adding security into protocols introduces an overhead into the communication stack, increasing power consumption and memory usage. Depending on the mission, this overhead may not be tolerable, so security and missions needs must be weighed in the design and decision-making process to create an acceptable risk level for the mission.

– The use of security controls also facilitates another risk factor. An attack which aims to drain a satellite's power, e.g. creating lots of resource consumption, may lead to the satellite to turn off security controls to prioritize power-saving efforts. This makes the satellite more vulnerable to other attacks such as gaining unauthorized access or eavesdropping on cleartext communications.

– Protocols for space missions are largely mission dependent. Whilst there has been attempts to document and recommend certain communication protocols, there is no consensus in the space industry in how to best implement secure communications and authentication, or which missions warrant the need for higher or lower security requirements. Security is often added as an afterthought in the protocols used in space, and some current options utilizing existing terrestrial techniques are not suitable for satellites. Even in satellite systems which use encryption, maintaining unencrypted connection for emergency situations such as satellite tumbling is important. However, communications would be in cleartext, able to be retrieved by eavesdropping on the connection.

– Physical layer security achieved through information- theoretic models provides computationally unbounded security as opposed to cryptographic protocols with computational security. Reusing the physical layer features can decrease additional energy cost for security as embedded systems like CubeSats cannot afford the additional silicon area, power consumption and code space needed to perform the expensive mathematical calculations of cryptographic methodologies. Physical transmission techniques achieve security by exploiting the unpredictable features of wireless channel through artificial noise, jamming, beamforming, etc. However, performance analysis methods for satellite links are needed that consider realistic legitimate and eavesdropper system assumptions and non-asymptotic coding lengths before practical consumption.

Key management

– Scalability—Whilst it may be a straightforward task to manage the keys of a single or small cluster of satellites, large satellite constellations require a large number of keys, making scalable key management an open issue. Constellations aiming to provide high data rates, such as broadband services, will also encompass a large network of ground stations, each with their own keys. presented that to provide maximum throughput for the Telesat, OneWeb and Starlink constellations, there would need to be 42, 71 and 123 ground station locations, respectively, with a varying number of antennas per station for their proposed constellation size. Whilst maximum throughput may not be the desired level, these projects will still require vast ground segment support, presenting a larger attack surface and demanding scaled and consistent security controls over all ground segment interfaces. Satellite TT&C and payload systems may require separate keys for when the user segment communicates directly with the satellite. Separate keys for TT&C, payload management and user interactions with a payload may be required. If a separate key for the pay- load is compromised, the TT&C keys remain unknown and this command and control link is not compromised. Inter-satellite links also add more complexity to the situation. To provide confidentiality of each inter-satellite link (ISL), a satellite requires to have another set of keys to communicate with each of its neighbours, separate from ground-to-Earth and Earth-to-ground links. All these competing key requirements compound the issue of scalable key management further.
– Group dynamics—another challenge relates to the dynamics of satellites entering and leaving a constellation. For the satellites entering and leaving the constellations, keys must be issued and revoked respectively for TT&C, payload management and for user interactions. ISLs also complicate this as it is necessary for satellite neighbours to update their keys when changes in the constellations occur. Keys will have to be issued and revoked in a flexible manner to allow for changes in constellation group dynamics.
– Key protection—transportation, satellite stacking and delayed launches provide ample opportunities to com- promise satellites and their keys, as it is not possible to keep eyes on the satellite constantly. Launch failures may scatter components over a large area, which may not have been destroyed due to their radiation hardening. Sensitive information, such as cryptographic keys, may be recoverable from these components. Reliability of hardware keys under active security threats leads to the development of physical unclonable functions (PUFs) and true random number generators (TRNGs) to generate cryptographic keys and IDs used for device authentication, cloning prevention, generating session keys, etc. Trusted Platform Module (TPM) is an international standard to design secure hardware with integrated cryptographic keys. Device Identifier Composition Engine (DICE) and SpaceTEE are hardware security designs for embedded systems which offer key protection through tamper-proof hardware.

– Quantum key distribution—whilst significant advances have been made in satellite-based quantum key derivation, there are still various technical challenges which need to be addressed. Reducing quantum signal capable satellite size without compromising accuracy, higher orbit for satellites processing quantum signal for increased global coverage and analysis of discrete variable and continuous variable QKD using metrics such as relative secret key rates, communication overheads and computing resource requirements for error

correction codes are some key areas which need to be addressed to enhance an accurate signal transmission and continuous global quantum network.

Software/firmware updates Satellites manufactured in Old Space usually had long development times to guarantee that these systems would not fail. Satellites were launched which had antiquated technology aboard, which could be vulnerable to serious threats. Hardware upgrades or replacements were rarely made, and high operational quality verification of software and firmware changes delayed their installation on the space segment.

New Space has brought agile development and operational processes. The use of FGPAs and SDRs makes it possible to re-program hardware and software in orbit easily. However, updates to software, firmware, hardware, cryptographic keys and insecure algorithms may introduce vulnerabilities, either inadvertently through a legitimate transmission of the update, or through an attacker using this circumstance to purposefully inject flaws into the satellite. In the case of the space probe Phobos 2, a software update inadvertently caused the space-craft to lose its lock on the Sun which drained power and ceased communications. Being able to use techniques such as software attestation, where software is able to prove its identity and that a system is trustworthy, may be one way to resolve this issue.

Reliable software Real-time On-board Dependable Operating System (RODOS) is a real-time operating system for embedded systems and was designed for application domains demanding high dependability. A reliable secure operating system must offer trusted or reliable execution of software components, memory safety, fault tolerance against both hardware and software failures and to perform in nominal mode with respect to external and internal perturbations. FreeRTOS achieves memory safety through an inbuilt software model checker called CBMC. The pro- gram effectively reasons every execution path through a program on every input searching for assertion or memory violation. MINIX3 and Kaspersky OS achieves reliability through microkernel architecture, where only a minimal set of abstractions run at the highest privilege level and reincarnation servers, which replaces a fresh copies of non- responsive or crashed drivers at user space. However, critical features like live updates, crash recovery of stateful services and virtualization are still being developed and the operating systems must be repurposed and analysed for space-based mission and threats before practical use.

Secure positioning of satellites In addition to command and control of a satellite, TT&C operations also include satellite ranging where the distance between the Earth and satellite is measured. These measurements help to verify a satellite is on the correct orbit and is in the expected position, and if not, commands to alter this can be sent. In the case of a mega-constellation, due to its size, this process happens on a much larger scale and it be may be easier for an attacker to place a malicious satellite into the constellation unnoticed.

Satellites are becoming more interconnected and making use of Internet protocols similar to IoT devices. Being able to measure the position of IoT devices compliments several IoT applications, but also offers assurances that you are communicating with the correct device. This idea is important for satellite constellations as well—you want to make sure the satellite you are communicating with is the one you think it is. A rogue satellite attempting to appear

legitimate, whilst communicating with the ground or other satellites correctly, cannot occupy the same physical space of another legitimate satellite, so satellite ranging and positioning can be included as part of verifying a satellite's identity.

Distance bounding mechanisms have been proposed as a way to achieve secure positioning in wireless networks, and satellite ranging from TT&C makes use of similar concepts. Satellite constellations could potentially make use of not only measurements from ground stations, but also from other constellation satellites through the use of their ISLs, but also maybe satellites in higher orbits such as GEO; however, further work is required to explore this issue.

Routing in ISLs The use of ISLs provides communication routes which do not rely solely on ground infrastructure, but also give rise to questions over when, where and how routes are calculated. A constellation operator must decide whether routes are static or dynamic, be calculated on-demand or pre- computed, and implemented on a centralized, decentralized or distributed platform. Each of these options has operational advantages and limitations and which also impact security requirements. Centralized static routes offer fixed communication paths administered by a single authority which may provide more control over the routes but is a single point of failure with fault tolerance and network congestion issues. Distributed on-demand routing splits computations among different nodes when required which increases fault tolerance. However, it also increases the attack surface of the routing procedure as more nodes are required and an attack may be easier to propagate through a network. Several protocols for ISL routing are discussed in[14] which may offer suitable implementations for both single- and multi-layer constellations. However, more work is required to address aspects such as network resilience after satellite destruction, flexible space networking mechanisms and optimal ground segment coverage.

Distributed control As mentioned earlier, when it comes to large constellations, scalability is an ongoing challenge, not only for the space segment but also for the ground. Large constellations will likely not be able to be managed from one single site. Operations may have to be distributed over several sites, requiring coordination between sites and handover from one to the next. In addition to these aspects, establishing standardized ground station builds and security practices also compounds this issue.

Fault tolerance The space environment is a harsh one with severe thermal, radiation and vibration extremes which can affect satellite components. Radiation in particular can have a devastating effect on satellites and is why many components are radiation-hardened. Single-event upsets (SEUs), where ionizing radiation causes a change of state in a components, can cause bits to be flipped, damaging data stored on the satellite. Keys stored on the satellite may be altered due to flipped bits and render satellites unable to communicate with the ground using encryption. If cost is a factor, then regular COTS components may be favoured

[14] Qi, X., Ma, J., Wu, D., Liu, L., Hu, S.: A survey of routing techniques for satellite networks. J. Commun. Inf. Netw. 1(4), 66–85 (2016)

over their radiation-hardened counterparts. New fault-tolerant crypto- graphic mechanisms, e.g. [15], will be required to account for these types of challenges in the space environment.

Intelligence gathering Deducing information concerning a satellite or constellation's operation may be possible with- out having to view the payload data. A satellite's power consumption and orbit, as well as observations from tele- scopes and sensors, may be used to determine mission objectives. This may be of concern to satellites attempting to remain as covert as possible and impacts the privacy of satellite operations. For example, powering on a payload when in the vicinity of a particular region could indicate imaging or signals intelligence purposes.

Companies must register the frequencies on which their satellites operate and their orbital slots with the International Telecommunications Union (ITU), United Nations organizations which has jurisdiction over global space activities. National organizations such as the Federal Communications Commission (FCC) in the USA also regulate spectrum usage in a national capacity. This publicly available information provides ample opportunity to listen and record RF signals in the hopes of reverse-engineering message formats. An integral part of the state sector space industry is information gathering about other nations and the physical nature of RF means this challenge is not going away.

Ground segment Attacks on the ground segment are prolific throughout the space industry's history, as seen in Sect. 3. It remains one of the easiest segments to attack, owing to the use of commonplace technologies across several industries and in consumer electronics, and to tried and tested CNE attacks which are successful in all sectors.

Network and application security, user awareness and organizational security culture are ongoing problems. Phishing campaign which installed backdoor Trojan programs is a common attack vector to gain a foothold into a network and may have played a part in other satellite compromises.

Details on open-source components are publicly avail- able which is an advantage to an attacker in finding security vulnerabilities. Global manufacturing capabilities for COTS components provide increasing opportunities for malicious actors to alter components in the supply chain. It is therefore paramount to establish confidence in the supply chain and trust overall to ensure that satellites, ground stations and user devices are designed, built and managed by parties who are held to high security standards.

Several New Space organizations are start-ups, founded by groups of graduates with experience of developing small satellites in academic institutions. Companies such as Kepler Communications, IceEye and Astrocast hoping to tackle the New Space market are university spin-offs. University missions are a starting point for many future start-ups and are typically not designed with security in mind due to the low impact of the satellite being in- orbit. There is a risk that start-ups may continue under this same mindset, with- out security ingrained into design and operating practices, which could become a bigger issue

[15] Banu, R., Vladimirova, T.: On-board encryption in earth observation small satellites. In: 40th international carnahan conference on security technology, pp. 203–208. IEEE (2006)

government and military contracts are won.
Signal Manipulation As discussed in Sect. 3, RF communication can be manipulated. Devices and techniques such as GPS jammers and spoofers, and broadcast TV/radio signal hijacking have made signal disruption an easier undertaking. The rise in COTS and SDR products available at affordable prices and the reduction of necessary specialist knowledge have increased the ease of such attacks. Also, optical communications, whilst providing an alternate means of communication to RF, are vulnerable to manipulation through optical dazzling, where a target is rendered blind from a more intense source direct radiation. This is the equivalent to jamming and prevents the transmission of legitimate signals, but is reversible and temporary.

Techniques and technologies aiming to prevent these types of signal manipulation have been used in the military and government sectors and are now moving to commercial satellite systems. They include techniques such as spread-spectrum and frequency hopping, which are applied at the physical layer to make signals appear noisy or switch their frequency usage with pseudo-random sequences.

Intrusion detection and prevention Terrestrial-based net- works employ intrusion detection and prevention systems (IDS/IPS) to monitor and respond to threats. In the New Space era, a new, similar technology will be required for satellites to observe and tackle potential attacks on-board satellites such as data protocol and RF-based attacks. This brings up questions over competing power and memory requirements and scalability issues and introduces more hardware and software, which could be vulnerable. An IDS or IPS may appear to be an easy and cheaper way to implement security for satellite operators but should not be a replacement for secure design and development of satellite systems.

User segment interface Applications of New Space satellite systems provide new ways for users to interact with these services. Whether interacting directly with a receiver or accessing a service through software or web portals, several challenges arise on how to deliver these services in a secure manner. Authorization and access control play a large part in securing a system. For dedicated receivers, e.g. satellite phones, access to the service or data should not rely solely on access to the device itself. Similarly for software or web- based solutions, just because a system expects a particular format for a user to interact with it does not mean that it cannot be abused, especially if these types of systems support on-demand services to reconfigure payloads or direct satellites. Verification of a user's identity and their level of access do not always go hand-in-hand when designing any system and a major challenge is ensuring robust enough authentication and authorization controls whilst minimally impacting usability.

6 Conclusion

Key advancements are being made in the space and satellite industry. Private sector investment in existing companies and new start-ups is driving innovation and ingenuity, in technology and also the applications of satellites. Satellite applications have a diverse nature and cross boundaries of state, military, commercial and civilian sectors. A review of past attacks on the space industry revealed attacks mainly focused on the ground segment or electronic warfare activities, for espionage and political activities. However, constellations of

thousands of satellites are planned for launch in the upcoming years, making commercial satellites a much more attractive target by adversaries with a multitude of motivations and capabilities.

Advancements in technologies such as COTS components, SDRs and cloud computing were discussed, and their resulting impact on security of the industry. Many challenges and open design problems relating to both security and operational requirements are still to be resolved. An overview of issues facing secure communication practices, privacy, sup- porting terrestrial systems and the user segment is provided.

MODULE-V

IT SPECIFIC INTERNATIONAL DISPUTE SETTLEMENT MECHANISM AND ODR

MODULE-V: IT SPECIFIC INTERNATIONAL DISPUTE SETTLEMENT MECHANISM AND ODR

Dispute Resolution Mechanism in Cyber Related Crimes: If the world could be crystallized into one space-it is the virtual world of 'cyberspace', devoid of territorial boundaries where conventional offline laws may have little or no application! With the growth of Internet & e-commerce, disputes of diverse nature have surfaced including social, commercial, intellectual property related and cultural or political conflicts, often involving entities/individuals from multiple territorial jurisdictions. The parties to a dispute, who may belong to different jurisdictions, are wary of submitting to the courts of another jurisdiction to adjudicate upon the dispute(s) in question. In such a scenario, 'Online Dispute Resolution', automated by software or by appointing a neutral third party/panel and conducted exclusively online seems to be the most viable and practicable solution. In case of online disputes, few subject areas such as domain name disputes, B2B, B2C transactions have already been identified wherein online dispute resolution has been efficient in resolving e-disputes with minimal time and cost.

This module is broadly divided into 3 parts- the 1st part will give an overview of what ODR (other dispute resolution) mechanism means and the scope of it and also will briefly discuss the ODR system in different countries. The 2nd part talks about the international ODR mechanism, ADR and cyberspace: the role of alternative dispute resolution in online commerce, intellectual property and defamation, current and future implementation of ADR processes for cyberspace disputes and the 3rd part is specific to India and the existing ODR mechanism in India and the challenges of implementing the ODR mechanism.

ODR mechanism: General Overview

Meaning of ODR: The virtual world of Cyberspace has become our preferred means of social interaction and a powerful medium to transact cross border business. Internet has proven itself as one of the most dependable means of assimilating and disseminating information, a hi-tech platform for business opportunities and efficient means of communication. According to the E Bay Census Guide, 2009, India has experienced a broad shift in e commerce activity and online shopping has gained wide acceptance. In United States, online retail activity increased in the second quarter of 2009 constituting 3.6% of total retail sales. When the cyberspace experienced a flurry of social and commercial activity, disputes of varied nature arose between parties including disputes concerning defamatory speech, invasion of privacy, breach of e- contracts, domain name disputes, cyber-crimes including identity thefts, data, cyber terrorism amongst other disputes. The e-disputes not only involve new kinds of disputes that are peculiar to the internet but also include traditional disputes relating to sale and purchase of goods or unfair trade practice, defamation, intellectual property infringements amongst other conventional disputes where internet has a role to play . The disputes could arise between individuals and/or corporate entities or involve the government of a particular State. Whenever two parties belong to different jurisdictions, the parties are wary of submitting its disputes to the courts of different jurisdiction that will decide the disputes based on a different governing law. Contrary to the conventional litigation process, ODR provides a practicable solution to parties to e-dispute where they need not submit their disputes for adjudication before the courts within the jurisdiction of a particular state. In ODR, independent set of laws/rules of an ODR service

provider may apply to resolve disputes and an independent panel of judges could be appointed on request of the parties for settling their disputes.

ODR procedure: The ODR procedure entails filing of e-documents wherein the parties may use encryption or electronic signatures to safeguard the integrity of the documents and authentication of the transactions. Generally, the parties seek the assistance of an ODR service provider for appointing a neutral panel of judges or panelists to resolve disputes through online means. Parties prefer structured and clear procedure where resolution process is simple and definite. Institutions such as WIPO,SIAC and ICC have an established reputation in resolving online disputes through mediation or other alternative disputes resolution methods. By filing the complaint, the complainant seeks compensation or other remedies and the respondent if consents to take part in the process submits its detailed replies. The process may or may not involve oral hearing by use of teleconference or video conference facilities. Sometimes automated software could resolve a dispute without the necessity of appointing any third party. In case the claimant's offer falls within an acceptable range, the disputes between parties are resolved. Generally, an ODR service provider serves function of an administrator and infrastructure provider and not a judge that decides the disputes. ODR is known for its efficient and cost effective dispute resolution that also reduces acrimony between parties.

*Origins of ODR:*The origins of ODR can be traced back to 1996 when the Virtual Magistrate project was established to offer online arbitration system to resolve e defamation matters. The Online Ombudman's office at University of Massachusetts resolved a dispute of a website owner with a local newspaper owner involving a copy right infringement issue which was settled through mediation. Since 1999, many ODR service providers have actively resolved disputes both in the public and private domain involving government and commercial entities.

In India, ODR germinated from ADR when in the early days family related disputes were resolved by Kulas, Srenis (Businessmen who conduct the same business), Parishads (group of men who possess legal knowledge). In other jurisdictions as well, ODR was based on ADR practice wherein technology was added to the ADR process to make it more efficient and convenient to the parties. In India, use of ADR techniques is explicitly encouraged through Nyaya Panchayat System, Lok Adalat, Arbitration and Conciliation Act, 1996 based on UNCITRAL Model law of arbitration, provision of statutory arbitration amongst other initiatives. The Indian legal framework supports ODR including Section 89 of Code of Civil Procedure, 1908 that promotes use of alternative dispute resolution between parties. Similarly, Order X Rule 1A confers powers on the court to direct the parties to a suit to choose any ADR method to settle its disputes. In addition, the Information Technology Act, 2000 grants legal recognition to use of electronic signatures and electronic records. Recently, in ***State of Maharashtra vs Dr. Praful B. Desai*** , the Supreme Court of India established that the Video conferencing is an acceptable method of recording evidence for witness testimony. In ***Grid Corporation of Orissa Ltd. vs. AES Corporation,*** the Supreme Court held-

"when an effective consultation can be achieved by resort to electronic media and remote conferencing, it is not necessary that the two persons required to act in consultation with each other must necessarily sit together at one place unless it is the requirement of law or of the ruling contract between the parties".

Thus, the legal framework as well as the precedents laid down by the Supreme Court of India support use of technology for dispute resolution and encourage use of ODR practices.

*Scope of ODR:*ODR is used to resolve diverse nature of disputes including civil, commercial, industrial and banking disputes through banking Ombudsman scheme, construction or partnership disputes, protect liability and insurance related disputes. In Australia, family disputes are required to undergo mediation which is made mandatory. However, criminal law or constitutional law issues fall mainly within the domain of litigation process and largely stand excluded from the ODR domain. New subject areas such as telecommunications law or labour law are being added to the scope of application of ODR. For instance, in United States the Federal Mediation and Conciliation Service is using ODR to settle labour disputes. In e-governance many government departments are also using ODR to settle consumer grievances.

ODR vs litigation: In ODR, cost and time efficiency are typical characteristics as opposed to a judicial process with consumes substantial time and cost for adjudication of disputes. Tyler and Bretherton aptly stated-

"the difficulty of utilizing traditional dispute resolution methods in low value cross border disputes has led to interest in low cost cases, cross jurisdictional dispute resolution methods".

ODR denotes greater flexibility as it can be initiated at any point of a judicial proceeding or even before a judicial proceeding begins. ODR can also be terminated if the parties mutually decide that it is not leading to a workable solution. The parties have the autonomy to decide the mode and procedure for online dispute resolution in case disputes arise from a particular e- contract. Even in the absence of a written contract declaring ODR as method of dispute resolution, the parties may adopt ODR methods to resolve their disputes when such disputes arise. Contrary to litigation ,the parties are free to choose their governing law of contract, the procedure to resolve disputes ,decide on an ODR service provider and provide for other incidental matters. Use of ODR also allows selection of neutral third party from an experienced panel of mediator/arbitrators which means greater impartiality and parties may present their case on their own without apprehension that their private disputes will flow into the public domain through judicial precedents. The disputes and the negotiations that ensue between parties remains confidential at all times. In B2C transactions, ODR encourages customer loyalty, in C2C transactions it minimizes acrimony and risk of fraudulent transactions between concerned parties.

Different ODR techniques: ODR can involve varied methods of dispute resolution including Negotiation, Conciliation , Mediation, Arbitration and hybrid mechanisms including Last offer arbitration, Medola, Mini trial, Med Arb and Neutral Evaluation. ODR may adopt either adjudicatory or non-adjudicatory process. An example of an adjudicatory process is an arbitration where the award passed by the arbitrator is binding on both parties. To the contrary, in a nonadjudicatory process, the principal aim is to arrive at a settlement of the disputes between the parties without deciding on the merits of the matter. In mediation, the neutral third party suggests solutions to settle disputes between parties and actively takes part in the dispute resolution process. In Med Arb, initially mediation is used and if unsuccessful, arbitration is used. In Mini trial, the parties file summaries of their cases for assessing their

cases on merits and negotiate a settlement with a neutral advisor which involves a non-binding procedure. In fast track arbitration, a time frame is allocated to resolve the parties disputes through arbitration. In a Neutral listener agreement, the parties discuss their offers with a neutral third party in private and after the third party has heard both sides, he recommends the best offer for settlement. In Rent a Judge, the parties submit their dispute for adjudication before an appointed neutral Judge.

ODR service providers: In Canada, the Cyber Tribunal in Montreal has successfully resolved e disputes using ODR, in U.S the Online Ombudsman office uses e –mediation. Square Trade is a well-known ODR provider that resolves disputes between sellers and buyers that use the e-bay services by adopting negotiation and mediation methods.

In U.S, financial disputes are resolved through CyberSettle and ClicknSettle resolves insurance related disputes. Other ODR services providers include www.mediate.com, www.novaforum.com, www.icourthouse.com, www.etribunal. SmartSettle uses a negotiations software to settle disputes after the parties allocate priority to various interests which are affected by the disputes. In Europe, the European Small Claims Procedure was established with effect from 1st January, 2009 and in Netherlands, the NMI Mediation uses the mediation by experts to settle online disputes. In many ODR systems such as Adjusted Winner (Brams and Taylor, 1996) SmartSettle (Thiessen and Mac Mahon, 2000) adopt 'Bargain and Gain theory' for dispute resolution. In SmartSettle, an automated software renders assistance to parties to discuss multiple options to arrive at a settlement. In AdjustedWinner, the two parties assign values to each article in dispute on a 100 point range, whereas in Split up (STRANIERITAL, 1999) assist parties to distribute property after a divorce. BBB Online set up an online dispute resolution service to resolve consumer disputes in United States using conciliation and if unsuccessful mediation through engaging online resources.

One of the most successful ODR initiatives is the WIPO Domain name Dispute Resolution Policy adopted by ICANN 26th August, 1999.It provides for an administrative proceeding to resolve domain name related disputes through accredited service providers that follow the UDRP policy alongwith their own supplemental rules. WIPO, National Arbitration Forum, Asian Domain name Dispute Resolution Centre are amongst the accredited ODR service providers. The administrative proceeding stipulates that the disputes ought to be resolved within a particular time frame and the procedure may be invoked prior to a court proceeding. The decision of the administrative panel may be challenged within 10 days of the date of decision by any affected party. The disputes resolved through UDRP policy lead to transfer of the domain names which are registered by a respondent in bad faith and in which it has no legitimate interest, if the subject domain name is deceptively similar or identical to the trade mark of the Complainant . In ***Tata Sons Ltd. vs the Advanced Information Technology Association, WIPO*** directed that the domain name Tata.org should be transferred to the complainant Tata Sons Ltd. as all the three criterias of the UDRP policy were established in the case.

*Challenges in ODR:*In an online dispute resolution, many complex issues emerge and implications follow. There are different challenges including commercial and legal. Generally, for invoking ODR process the mutual consent of parties is essential, whether through an explicit clause in a contract or by mutual agreement between parties subsequent to

a dispute which may have arisen. In the absence of such mutual consent, no decision rendered by an ODR service provider shall be legally valid or enforceable. Most jurisdictions acknowledge and enforce standard ODR clause in a B2B website but in case of B2C contracts , particularly in European Union, consumers cannot be deprived of additional rights available to them by the law of the place of their residence through an agreement that limits the jurisdiction of a court to the country of ODR service provider if it provides lower protection standards which a consumer is entitled to in the country of its residence.

Preserving confidentiality and privacy of negotiations and any transactions that ensue between parties in dispute resolution is one of the paramount concerns of parties worldwide. Internet is still viewed as insecure media as cyber criminals may employ techniques to intercept data and communications between parties and any information flowing through internet network could be unauthorizedly stored or misused by cyber criminals. In this regard, sophisticated techniques for enhancing internet security such as use of digital signatures, electronic signatures are being used to conduct ODR process. Use technology to combat any loopholes in internet security will strengthen ODR process. Katsh and Rifkin also considered technology to be the fourth party in an ODR process and observed that ODR will not only effectively resolve online disputes but also strengthen the trust in the virtual space. Use of cookies often breaches the privacy of individuals and raise security concerns. The electronic court house uses multiple security layers including sophisticated server, complex pass word and software which backs up complete data of its servers and stores information submitted by the parties in a protected environment. Such technical infrastructures is required to alleviate any concerns a breach of privacy, confidentiality in the ODR process. Many paralegal rights such as money back guarantees and buyer protection clauses and authentication seals are becoming popular on most e commerce websites. This is only to generate more trust and promote e commerce and bring consumer confidence in ODR practice. Another issue that most parties consider important is that the panelists that decide their disputes ought to be independent and impartial in their decision making. To this end, they prefer institutionalized ODR which is more structured and transparent and reduces the chances of bias affecting decision making of panelists.

There are no existing homogenous laws for ODR in cyber space which poses a challenge on account of application of substantive and procedural law to resolve e- disputes. To decide on the jurisdiction applicable to an e dispute, ***the effects test*** and ***the zippo sliding scale approach*** may be used. In private international law, the place of performance of a contract is a significant parameter to decide substantive law or the jurisdiction which will apply to the facts of a case. The law of consumer protection grants stronger protection to the consumers in Europe and application of mandatory rules of law at ***Lex Situs*** are some challenges that emerge due to lack of homogenous cyber laws. Could there ever be an International Court of Justice that decides e disputes of all nature adopting homogenous cyber laws in ODR process and procedure? At this point an analogy can be drawn to ***Lex Mercatoria*** applicable to international trade. It will be beneficial if at least a homogenous ODR law or core legal principles for law and practice of ODR could be framed. Major International Legislative Texts, Treaties and Conventions and National initiatives could bring definiteness to the law and practice of ODR in cyber space.

In fact, the mission is half accomplished as some land mark initiatives have been made to bring more clarity in ODR .These initiatives include the Recognition and Enforcement of foreign arbitral awards,1958, Brussels Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial matters,1968, the Rome Convention on law applicable to Contractual Obligations,1980 .

In 1999, the OECD published its guidelines for Consumer Protection in the context of Electronic Commerce. The Guidelines provide that the consumer ought to be rendered fair, and cost effective means of dispute resolution and explain the significance of information technology while using ADR systems. In European Union, the E commerce Directive, provides in article 17 that in case of an e-dispute, the member states are required to ensure that the parties are not hindered from using ADR process for dispute resolution 'including appropriate electronic means'. The National Alternative Disputes Resolution Advisory Council drafted standards for ADR in 2001 and laid down the principles for ODR in 2002.

Thus, we have some legal initiatives already made to promote ADR and use of technology to bring speedy dispute resolution services. It is a matter of infusing new ideas and solutions to promote and streamline body of laws for ODR while also incorporating the legal principles enunciated by international initiatives by fair adaptation that will lead to unification in ODR law and practice.

Certain critics such as Drake and Moberg and Wilson, Aleman and Leatham have expressed an apprehension that lack of personal interaction between the parties to a dispute. reduces the chances of resolving disputes . Physical presence and body, language and tone of conversation is important to resolve a dispute. Similarly Goffman declared the 'face theory' that explains that a dispute resolution process and its success is directly dependent on the communications held between the parties and any negative or positive statements made during communications. However, in my view, in ODR cases mostly parties are not known to each other and bringing parties face to face may in fact reduce the chances of dispute resolution. In ODR, sometimes few technical rules such as automated software settle a party's disputes and the parties may not be required to participate in face to face or even video conference hearings where any negative remarks could be exchanged between parties. If the face theory is true in ODR the acrimony between parties is reduced as in many cases, automated online processes aid in dispute resolution. In any difference in language and cross cultural variations exists, general practice is to avail the services of translators and interpreters during ODR.

On the aspect of enforcement, critics may hold a view that when ODR is nonbinding, it is futile . However, in my view if a non-binding ODR is successful and leads to a binding contract of settlement, it is legally enforceable in a court of law. ODR also offers fair decisions as it considers and adopts principles of equity and natural justice in addition to the statutory rules to decide a dispute.

A debate which has evolved with time is 'self-regulation vs. government intervention' in ODR. Self-regulation was questioned by consumer groups for lack of authority and trust which brought in the government's role in ODR process. Initially American Board Association , ICC, Better Business Bureau laid down principles to regulate ODR and use of trust seals was emphasized. Entities such as Verisign and Trust e were established and

Square Trade and BBB online executed the trust marks concept as a self-regulation initiative in ODR practice. At a government level, ECODIR and other ODR projects were initiated as part of e governance as ODR proved as efficient means to resolve disputes. Schultz was of the opinion that government's role is more important as compared to the self-regulation approach.

According to Schultz, the 'symbolic capital' i.e. the social reputation of an ODR provider renders credibility and authenticity to an ODR process which is what a government is capable of providing. The government also grants financial aid to ODR projects and assists in creating the technical and administrative infrastructure required to set up an ODR process. In addition, Schultz suggests that accreditation is an essential function played by an ODR service provider who acts as a certifier, a clearing house that assists parties in choosing a service provider and facilitating e filing of forms and supervising an ODR process. He also advocated an online appeal system for reviewing decisions made by an ODR service provider which will impart greater transparency and accountability in ODR system. Similarly, Colin Rule states –

"To a large extent, government is the ideal host for dispute resolution, because government has a strong incentive to resolve disputes to keep society functioning smoothly. Government is also a good host for dispute resolution because it usually has no vested interest in the outcome of most of the matters it is in charge of deciding."

On analyzing the two approaches, it can be said that the growth ODR can be achieve its full potential using public private partnership. The role of government will be to impart trust and authority and the private sector will contribute advanced technology. In public-private partnership, best practices in ODR can be successfully established and implemented , greater awareness and participation in ODR process can materialize .

In USA, Australia, New Zealand, Singapore, Canada, U.K. special funding is being granted by the government to initiate ODR projects.

In Netherlands, the electronic commerce platform is a joint initiative of the business community and the Dutch ministry of Economic affairs that drafted the Code of Conduct for electronic commerce.

In Singapore, e ADR was launched which is jointly operated and supervised by Singapore Subordinate Courts, Ministry of Law, Singapore Mediation Centre and Singapore International Arbitration Centre, the Trade Development Board and Economic Development Board to resolve e commerce disputes.

E courts in India also aim to promote ODR and deal with litigation and court based ODR using online resources and CBI (Central Bureau of Investigation) is in the process of establishing e courts.

ADR and Cyberspace: The Role of Alternative Dispute Resolution in Online Commerce, Intellectual Property and Defamation: The growth of digital networked communication has presented some troubling questions for the legal field. In some instances, the nature of the medium does not pose much of a problem; the application by analogy to existing legal principles is fairly clear.1 Some issues arising from computer mediated

communication, however, are fundamentally new, with the novel and dynamic nature of the medium itself creating relationships unanticipated by a traditional, spatially-oriented body of law. The use and encouragement of alternative dispute resolution (ADR) methods could play a large and effective role in the adaptation process.

The dominant feature in the online landscape right now is the Internet, and most issues discussed in this Note will relate primarily to it. The term "cyberspace," however, carries a more comprehensive meaning incorporating many types of digital networked communication, whether or not they rely on the Internet for execution, and apparently includes everything from satellites to cellular phones to computer bulletin board systems (BBSs). Naturally, the role of ADR in cyberspace will probably be greatest where there is a high degree of interactivity between a wide variety of users; at this point the Internet is the framework for such an environment.

ADR's role in the decentralized regulation of cyberspace will be discussed in three suibstantive contexts: (1) the commercialization of cyberspace, (2) intellectual property and (3) defamation. Within each context, some problematic legal application issues will be presented, followed by an evaluation of the ameliorative role ADR might play. This chapter will conclude with a discussion of how ADR might be-and has been-implemented in the cyberspace context. Some recurring themes will become apparent. Often central to the question of traditional law's applicability in a given cyberspace-oriented instance, they also point to the relevance of ADR. The primary themes are:

- the importance of custom, and the recognition of its strong developing presence in cyberspace;
- jurisdictional concerns and other ramifications of an easily accessible international medium;
- the dominance of contract doctrine in cyber-space jurisprudence;
- the significance of "dynamic routing" and the basic elusiveness of the medium to top-down regulatory control;
- the strength of ADR generally in related non-cyberspace areas (in international intellectual property disputes, for instance); and
- The rapid growth of technology, as both the cause of legal application problems and as a source for self-regulatory solutions.

Troublesome applications:

Online Commerce: "Commerce on the Internet" encompasses a spectrum of definitions. Viewed simplistically, online commercial relationships could be categorized as one of a few types. The first is a detached' retail relationship, with a consumer (user) interactively evaluating the product and perhaps making a purchase online. "Electronic malls," prominent on the World Wide Web, are an example of this. Second are the contractual relationships of individual users and specialized online institutions, such as banks facilitating the use of "digital cash." (This definition could perhaps be expanded to include a user-service provider relationship.) A third type involves actors with greater ability to bargain and more power over contractual terms. It could better be described as "conducting business" over the network and would entail using the medium more directly for any or all stages of negotiation, the exchange of contracts, the transfer of money and perhaps the transfer of the "goods"

themselves if the commodity is information. Although commercial relationships on the Internet could be loosely described in terms of these three models, issues relating to the difficult application of law and the suitability of ADR are generally common to all three.

Of preeminent importance in this area is the recognition of custom, a concept with widespread implications in commercial law, particularly in international commercial law. Cyberspace is replete with customary ways of doing things; at an individual, e-mail and "chat" level, "netiquette" dictates the acceptable manners of online communication. As commerce increases on networks, custom will proliferate and develop on a larger, commercial scale and may, in fact, conflict with "real world" customs. ADR can be a means to an accurate reflection of custom in the dispute resolution process and is especially suitable where expertise in a specific area is needed. Custom and its impact on a dispute resolution process are exemplified in the Law Merchant, a historical concept with strong correlations to cyberspace.

The Law Merchant was a body of customary rules-the precursor to contemporary commercial law-that grew up in Medieval Europe as a response to the needs of international commerce….

…..It was simply an enforceable set of customary practices that inured to the benefit of merchants, and that was reasonably uniform across all the jurisdictions involved in the trade fairs. Two key elements of the Law Merchant for our purposes were first, that no statute or other authoritative pronouncement of law gave rise to its existence, and second, that the Law Merchant existed in some sense apart from and in addition to the ordinary rules of law that applied to non-merchant transactions.

In other words, the Law Merchant made no attempt to displace existing rules promulgated by the jurisdiction in which a given trade fair might be held; it merely supplemented those rules with specific rules applicable to merchants' transactions.... The emphasis of these merchant courts and the law they applied was a speedy resolution of disputes, an important element when time is money. But another significant attribute of these courts was practicality and flexibility. Merchant practices were not static, and a reliance on local judges, taken from the merchants' own ranks and following the known customs of merchants, gave the Law Merchant adaptability to changing times that statutory enactments would not have provided.

The parallels with cyberspace are strong. In modem, online commerce, technological innovations will inevitably result in the development of customary practices. The same innovations may also challenge some of the basic presumptions on which existing commercial law is based.

A primary concern surrounding modem online commerce is security. Stories of hacker activity and the number of perceived security threats are common. "Buyers and sellers must feel that transactions are secure, that the funds are moving to the proper place and that both parties to the transaction are who they say they are." As an effort to meet the security needs of electronic commerce, digital cash and the Digital Signature Standard have seen much development. These and other technological innovations will have a powerful influence on the way business is done in cyberspace.

The context of Internet security is an excellent example demonstrating how such technological innovations can raise a number of legal application problems:

…A large number of network security products have recently appeared on the market which claim to have solutions to the problem of the "Bad Internet." One new security product was described as "close to the level of 'bullet proof'". [sic] Some firms have even represented their products to be "hacker-proof." Because of the lag between the legal infrastructure and the new network security technologies, it is completely uncertain whether representations such as these would be deemed enforceable by a court of law.

….Common law negligence does not define a level of care for Internet security providers, and ambiguities result when the historical means of establishing such a standard are employed. Moreover, no statute has been enacted to define Internet security standards. The application of negligence doctrine to the business of providing on-line services highlights these open questions and exemplifies why current negligence theory is ill-equipped to deal with Internet security liability.

Currently, most users of the commercial Electronic Data Interchange (EDI) do not allocate risk and establish ground rules in separate paper trading partner agreements. "The EDI data as encoded is not designed for the exchange of textual material such as terms and conditions clauses." A recent Model Trading Partner Agreement is designed to be a one-time written agreement between partners, which establishes "the meaning, timing, interaction and responsibilities arising from electronic messages and sets forth the legal import of a particular transaction between the trading partners." Such an all-inclusive agreement is liable to be the subject of many disputes and contains a suggested arbitration clause.

In less formal, individual-level business relationships of cyberspace, "strangers need to be able to deal with each other electronically without negotiating paper trading partner agreements. " Like the above contexts of Internet security and large-scale commercial trading partner agreements, the development of the "pluralistic electronic market" will be accompanied by the further establishment and formalization of custom for a primary reason: dynamic technological development creates difficulties in the predictable application of traditional commercial law. U.C.C. provisions which support the reflection of custom will be important: "As sales of goods become more common via the NII [National Information Infrastructure], the U.C.C. will likely become more useful based on the flexible 'course of dealing' and 'usage of trade' definitions.” But the new technology designed to facilitate electronic commerce also raises questions regarding the U.C.C., in particular, issues of contract formation, receipt and verification and the statute of frauds. Some scholars feel the problem is a fundamental one:

The problem with the U.C.C. is the basic assumption that commercial transactions are conducted on paper. In a world where contract terms and even signatures may be made of electronic impulses rather than pen and ink, the union of the U.C.C.'s more arcane provisions and computer technology has been a rocky marriage at best. ... [B]ecause computer generated commercial transactions are not consistently protected by the courts, new means of conducting business are not effectively protected through the U.C.C. or the common law as currently applied by many jurists who do not, or choose not, to understand the technology and how the technology interacts with the purpose of the applicable law.

Even though the proposed U.C.C. Article 2B will undoubtedly clarify the situation by eliminating some strained legal fictions, commentators continue to note the desirability of a "uniform commercial law of the Internet."

Rather than rely on an uncertain and unpredictable body of law which in several ways has not yet adapted to technological developments, effective dispute resolution may be found in arbitration or mediation, with a neutral party versed in the subject and familiar with the customs of the cyberspace commercial community. Such -a tribunal would be particularly useful in situations where traditional law calls for a determination of "reasonableness." As the development of digital communication-and custom-continues to challenge the adaptability of law, the need for a more flexible method of dispute resolution will increase.

In addition to being a system of dispute resolution flexible enough to accommodate an extremely dynamic area, a primary strength of ADR here is its recent acceptance into commercial disputes generally. A strong incentive for the use of ADR in commercial disputes, with obvious relevance to cyberspace, is the opportunity to avoid potential jurisdiction problems. Parties can develop arbitration agreements which stipulate their choice of law, eliminating potential delays which may result from a dispute over jurisdiction.

The jurisdiction problem is considered by some to be the problem of the Internet. Is a virtual presence sufficient to establish personal jurisdiction? When people make information available over the Internet, have they subjected themselves to suit everywhere that information can be accessed? Recent court cases concerning Internet jurisdiction offer little guidance, and some appear to be dodging the issue.

The courts in general have strongly supported the expansion of ADR. "Courts may potentially scrutinize ADR at any one of three stages: agreements to arbitrate or mediate; the proceedings themselves; or the resulting awards or settlements. In all three areas, recent decisions have further limited the grounds for judicial review." This is especially true in contractual arbitration. The flexibility, speed and general commercial acceptance of ADR strongly suggest it will have a prominent role in the development of digital commerce. As a method of dispute resolution which can reflect developing custom and account for developing technology with little danger of stifling either one, ADR could be a valuable tool in an environment where the law is struggling to adapt.

*Intellectual Property:*The development of digital communication has produced, and will continue to produce, novel intellectual property issues. Many of these issues will no doubt be resolved via analogy to existing law, or perhaps after some minor tinkering. But in some cases, the nature of the medium digital, storable, instantaneous, global and elusive-seems to produce a very new question. The use of ADR can be a rational choice flexible enough to accommodate a rapidly changing technological medium. The status of the system administrator promises to be a difficult issue in online copyright cases. In *Playboy Enterprises, Inc. v. Frena*, a small, private BBS (Bulletin Board Service) was found liable for copyright infringement. The BBS provided a file-sharing service; users send files to the BBS which can then be downloaded, or copied, by other users. In the Playboy case, Playboy asserted copyright to photographs that existed in the BBS's file sharing service. The system administrator claimed he was unaware of the existence of the photographs, but the court held

that scienter was not an essential element and decided in favor of Playboy on a summary judgment motion.

It is quite true that scienter is not a normal requirement of copyright infringement. Yet this case will trouble many cyberspace users. It certainly will trouble system administrators, for it seems to impose a near impossible burden on them to screen all uploaded files. Many BBS systems experience hundreds of such uploads daily.

In the recording industry, performance rights are called into question. The Copyright Act of 1976 confers various rights on music publishers and recording artists, but those rights have not been delineated in cyberspace. Performance licenses, mechanical licenses and synchronization licenses are easily applied to the tangible and analog world for which they were created, but digital communication has caused confusion. For the payment of royalties, questions of duplication are central, and the nature of digital, computerized communication in which a storable, easily-transferred pattern of bits can constitute a copyrighted work has caused a gap between existing law and the policies which it seeks to promote. The Copyright Act of 1976 is central to the domestic digital communication-copyright debate and is subject to some changes. Notably, a U.S. working group recommending alterations to the Act came to a conclusion that implicates the very nature of computerized, networked communication as "copying" for the purposes of copyright law.

A simultaneous fixation (or any other fixation) meets the requirements if its embodiment in a copy ... is "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."... Electronic network transmissions from one computer to another, such as e-mail, may only reside on each computer in RAM (random access memory), but that has been found to be a sufficient fixation.

This definition includes uploading and downloading. In a medium which functions by "copying," this determination promises to have widespread effect.

The fair use doctrine might raise some questions. Courts have noted that fair use should be adapted to technological innovations and that it is based on the author's implied consent to "reasonable and customary" use. Also, second and third copies made by Web-site visitors (the first being the perusal of the information) for purposes of easier reading and to reduce online connection fees may constitute fair use.

The Copyright Act of 1976 ultimately may be a source of strong domestic protection for owners of copyrighted material because of its broad, powerful prohibitions against unauthorized "reproduction," "distribution" and "performance" contained in Section 106. "The legal system is far less clear, however, once one passes beyond the U.S. borders." Internationally, concepts of property and copyright vary considerably:

On an international scale, the difference affects the fundamental question of whether any property right exists and whether it can be transferred. This is largely uncharted territory for legal analysis. Consider, for example, a packet of data obtained by a Boston company from a German database through a remote access which passes through a Mexican computer. If the data is purely factual materials, and the EU Directive [adopting a "reciprocity" policy for the

protection of international intellectual property (IP) rights] had been implemented, the German company "owned" a right to prevent or control extraction of the material from its database. On the other hand, in the United States, a principle of national treatment would indicate that no rights exist in a purely factual database. The circumstances in Mexico might fit either model or a third one. Has an infringement occurred? Under which set of laws will it be litigated?

On an international level, the problem of copyright and digital communication is being debated under the aegis of the World Intellectual Property Organization (WIPO). The WIPO (which operates an intellectual property Arbitration Centre in Geneva) has convened a Committee of Experts on a Possible Protocol to the Berne Convention concerning developments since 1971, as well as a Committee of Experts on a Possible New Instrument for the Protection of Performers and Producers of Phonograms. The European Community and Canada have also produced reports. A consensus among the reports seems to be that fundamental copyright concepts, based on tangible or analog forms of property, are sound; there is simply an application problem that eventually can be worked out with international cooperation. But even with faith in the continued applicability of historical concepts of copyright, the reports appear to be strongly in favor of employing technological means to protect intellectual property and, in fact, discussed the possibility of banning certain anti-encryption software devices.

For now at least, the protection of intellectual property in cyberspace cannot rely solely on the threat of civil or criminal sanctions. 55 Several reactions could become even more apparent: (1) an increased use of technology as a means of protection; (2) the development of custom and (3) application of ADR principles. Technology itself plays an increasingly important role in the protection of intellectual property. 56 With the unprecedented ease of duplication in cyberspace, intellectual property in a digital form faces a constant threat of widespread infringement. The ideal system of intellectual property protection would be effective against both unintentional, non-commercial infringers, as well as digital pirates with an intent to make money through reproduction. The development of encryption technology will be one means of protection, but other possibilities exist. A form of digital watermarking could provide a means of determining ownership. Automatic metering systems and automatic debit systems currently in development will be other powerful tools for protection. Rather than completely eliminate the possibility of piracy, self-help technological techniques aim "to force the economics of commercial piracy to the point at which it can be profitable only on such a large scale that it will become visible to law enforcement and thereby vulnerable to criminal prosecution." A comprehensive system of technological intellectual property protection "would depend on the development of standards, protocols and systems that transcend various platforms, technologies and national boundaries.... Existing international legal systems and current day technological systems are each, in themselves, inadequate. Both law and technology will be needed to address the problem of unauthorized exploitation of intellectual property."

As in the commercial context, cyberspace custom may play a large role in the development of intellectual property "cyber-law." Based on the U.S. working paper mentioned earlier which included uploading and downloading as copying for the purposes of traditional copyright law, the Internet is essentially a huge morass of copyright violations. Every

duplication, through uploading and downloading, of any material from any computer on the Internet has a strong chance of technically being a copyright violation; this is custom developing in direct contradiction to the existing law.

We can look at the well-recognized cyberspace custom of copying e-mail messages and forwarding them to others. In real space, this might be a clear copyright violation, but if everyone in cyberspace "does it all the time," and knows that others do it all the time, might not some sort of estoppel or implied waiver of copyright rights arise?

Another specific example of developing custom can be found in the aforementioned recording industry. Performance-right societies (such as BMI and ASCAP) and online-system operators have begun developing a course of conduct that may become the industry standard. The performance-right societies "have begun enforcing their rights in cyberspace by demanding and receiving licenses from online-system operators using their repertoire over the Internet. This practical way of handling performance rights in the online community so far has helped to avoid precedent-setting lawsuits.

“In conjunction with the recognition that cyberspace custom is often incongruent with "real space," the utilization of ADR is a natural extension from its already-prominent use in intellectual property disputes. While the general use of ADR has increased dramatically, its development in intellectual property has been especially pronounced. As in the above commercial context, the strength of ADR in the intellectual property (IP) practice area itself in many ways parallels its suitability for networked communication. In addition, the choice to arbitrate has been firmly supported by the courts.

Recent trade agreements addressing intellectual property issues will cause an increase in the use of ADR for international IP disputes. The WIPO has opened the WIPO Arbitration Centre in Geneva to offer dispute settlement services for private, international IP disputes. In addition to eliminating a jurisdiction and choice-of-law question, ADR also offers a very flexible tribunal, necessary to accommodate the various international concepts of property.

Rather than spend large amounts of money unpredictably educating a judge or jury about a complex technological issue and hoping they empathize, many parties choose ADR as an opportunity to have the case decided by neutrals already versed in the subject and customs of the matter at hand. When technological development may have simply outpaced the law's ability to resolve disputes efficiently and effectively, ADR may be preferred as an alternative to the litigation.

Arbitration has already been used to resolve a few Internet-related IP disputes. In trademark, a three-person, mutually-agreed-upon arbitral panel recently disallowed the use of another's registered name as an Internet domain address. While the case has no legal precedential value, it has produced much comment and will likely serve as guidance in related disputes. Technology-related trademark cases as a whole are still inconsistent: "Solutions, unfortunately, aren't found in law, they're found in arbitration.”

Patent disputes focusing on the tools for the creation of the global information infrastructure will also increasingly use ADR: "The prevalence of such newly-developed, highly-technical inventions will increase the likelihood of patent disputes, and the value of resolution through

arbitration." Other reasons cited for the inclusion of ADR here include the opportunity for mutually-agreed-upon expert neutrals and the ability to stipulate choice-of-law questions. In the always-changing high-tech patent industry, timing is often extremely valuable, making quicker resolution of disputes through arbitration valuable. Faced with the unpredictability and inflexibility of litigation, IP parties may find that ADR can determine the applicable law between parties, enabling a flexible, trade-based approach that may even protect and facilitate development until the law becomes more settled and more predictable.

A recent high-profile computer software dispute exemplifies this problem of technological development and pressures of a dynamic market drastically outpacing law and was settled successfully through a flexible arbitration (which also, to a large degree, dictated the parties' relationship for the future). While not directly implicating digital networked communication, the dispute involved many similar considerations, and its use of "preventative law" may offer some guidance as an effective resolution of high-tech disputes in general and cyberspace-related disputes specifically. In the 1982 IBM-Fujitsu dispute, IBM claimed that Fujitsu, which makes IBM-compatible hardware and software, had violated IBM's software copyrights. Senior officials from each company spent eight months negotiating a settlement. In 1985, the companies used ADR to dictate a significant portion of their future relationship. The agreement established:

"Security Facility Regime," under which each company can examine, under elaborate safeguards, certain parts of the other company's software. In return for what is determined to be adequate compensation, the examining party could use the obtained information in developing its own software, and be assured of immunity from claims of copyright violations.

The settlement reached in the IBM-Fujitsu dispute incorporated an aspect of ADR known as "preventative law":

Preventative law provides a unique advantage as a means of settling complicated issues in evolving technological and legal fields. In the past, ...IBM had to wait until after the public release of a Fujitsu program and then conduct an elaborate technical examination of the program. Then, if it chose to pursue a claim, it was extremely expensive and time consuming. Meanwhile, of course, the Fujitsu program at issue was already in the marketplace. [This preventative law] exposes and resolves disagreements before public release of the software.

Intellectual property law must adapt to a global medium in which widespread duplication can be nearly instantaneous. The employment of ADR methods for cyberspace IP concerns is a natural extension from its already-prominent use in traditional IP disputes. Given the rapid development of technology (with new and better ways to infringe-and protect-intellectual property rights), a flexible method of dispute resolution such as ADR can be more appropriate than reliance on a relatively static body of traditional law.

Defamation:

Disputes relating to defamation traditionally do not implicate conventional ADR methods (such as arbitration) to the same degree as in the commercial and IP contexts. But ADR could have a large role in cyberspace libel disputes, perhaps more so than in traditional libel cases.

Again, this section will discuss some troublesome applications of traditional defamation law to cyberspace and will note some potential decentralized solutions.

The broad concepts of defamation law generally transfer easily to cyberspace. But there are some substantial unanswered questions. The determination of what constitutes a "public figure" in cyberspace is far from clear, and, once again, the role and liability of the system operator is a major question. The global nature of the medium raises serious jurisdictional and substantive issues; the Constitution is, after all, a local document. With the ease of publication in cyberspace, a vindication-based remedy could become more prominent, perhaps supported by ADR processes which more accurately reflect the realities and customs of global computer-mediated communication.

American defamation law itself is cumbersome and complex. When applied to cyberspace, it becomes especially murky. *New York Times Co. v. Sullivan* and its progeny established a framework based on whether the defamed is a "public figure": if he is found to be so, the plaintiff must show that the utterance was made with "actual malice," that is, with knowledge of falsity or with reckless disregard for the truth. The public figure determination, central too much defamation law, has called for the evaluation of up to nine different factors, according to one commentator. Of particular significance in cyberspace controversies are the traditional factors of (1) access to the media; (2) existence of a public controversy and (3) the plaintiff's imposition into the controversy.

The public figure determination for many potential cyberspace defamation cases is, at best, unpredictable. Given the increasing ease of access to the Internet; the proliferation, diversity and content of Usenet-type newsgroups and the potential audience for a single (perhaps careless) utterance, other ingredients of defamation law, may, at some point, face revaluation as well.

The liability of a BBS operator is another major problem. If a user posts a defamatory message on a BBS, is the BBS liable as an intermediary? In *Cubby, Inc. v. CompuServe,* Inc the court analogized CompuServe to a bookstore, finding no duty to screen or remove the defamatory utterance.

The conclusion and the analogy were based largely on practicality. *"Large commercial BBSs like Prodigy and America OnLine [sic] serve as the mail box for thousands of messages a day; it is not feasible for those companies to examine every message."*

But there are several reasons why the bookstore analogy may not serve as a blanket precedent relieving all BBSs from intermediary liability:

The policies behind relieving "real space" intermediaries of defamation liability are not clearly applicable in cyberspace, or at least not uniformly applicable because (1) the practicalities of screening messages for defamatory content differ from BBS to BBS; (2) the value of intermediaries [bookstores, for instance] in real space situations is far more well established than the value of on-line intermediaries; (3) those intermediaries in real space that are common carriers have made tradeoffs in the form of universal carriage and often monopoly positions that cyberspace system administrators do not typically make; and finally, (4) solvent publishers as potential defendants are more likely to exist in real space

intermediary situations than in cyberspace. The applicable legal rules of defamation... surrounding the system administrator as intermediary are therefore sufficiently uncertain to make them "new" enough to merit attention.

Another factor sure to cloud the application of defamation law to cyberspace is the vastly increased ability to communicate internationally. A reflection of the Internet's global nature, most network fora, such as Usenet, is not at all limited to the United States. Online communication transcends national boundaries and can be had with citizens of Australia or Europe just as easily and cheaply as with citizens of one's own country. "The extremely low cost of cyberspace communication makes practical the distribution of defamatory or other wrongful communications on a scale not before possible. For these reasons, the issue of international torts is likely to be much more significant in cyberspace than it has been to date in real space. "The U.S. Constitution is a local document and cannot be viewed as a blanket standard for online speech given the ease of international communication.

The immense reach of the Internet certainly has the potential to eviscerate or circumvent any traditional jurisdictional and choice of law limitations. It will undoubtedly prompt an increase in forum-shopping, especially where the dispute arises out of areas of law that are substantively different from state to state. The courts may need to re-evaluate their current rules and formulate new solutions to deal with the issues created by the Internet.

This is evidenced by a recent example: A British physicist filed suit against another physicist for a libel allegedly committed on Usenet. The plaintiff alleged that negative messages had been posted about him from laboratories in Germany and Switzerland, and charged that the messages were read by colleagues and students in Great Britain. He filed the suit in Great Britain, which has particularly harsh libel laws, but, theoretically, could have chosen any forum where the Internet is accessible, giving him the option of picking practically any forum in the world.

Rather than attempt to graft an already-complex body of domestic law onto a dynamic, international medium, other methods of combatting defamatory speech on computer networks are deserving of consideration. First, the ease of access and publication in cyberspace argues strongly for greater value to be placed on the effectiveness of counter speech. Second, ADR methods of arbitration and mediation could play a more prominent role than they have traditionally played in libel. A vindication-based remedy, grounded in the publication of a finding of falsity by the ADR tribunal, is conducive to the medium of cyberspace. ADR also has the potential to alleviate the jurisdictional problem and would more accurately reflect the developing customs of speech on computer networks.

The ease of access to the Internet and the global publication of many online fora (Usenet, for instance) promise to create a fertile ground for defamation problems in cyberspace. But the same factors also argue for greater emphasis to be placed on the value of counter speech. If the defamed has at least equal capacity to communicate, by posting to the same Usenet newsgroup or BBS where the defamatory utterance appeared, for instance, perhaps this should be encouraged rather than allow reliance on libel litigation:

Litigation isn't the only way to resolve conflicts over free speech on computer networks. America Online general counsel Ellen Kirsch recently lit a small candle of good sense in the

gathering cybergloom. A lawyer from a major mid-western firm complained to America Online about postings that, he wrote, "defamed" the product of one of his clients. Kirsch responded by sending the lawyer an AOL starter kit with three hours of free time and urged him to put up his own postings defending the product. Her move was in the tradition of Supreme Court Justice Louis Brandeis, who believed that the solution to "bad speech" was not censorship but more speech.

Counter speech will not always satisfy the defamed, of course, and an effective dispute resolution process for online defamation is necessary. ADR potentially could play a much greater role in cyberspace defamation cases than it does in 'real space' defamation cases. Its flexibility and reflection of custom are important considerations in such a novel, easily-accessible international medium.

With such a high potential for jurisdictional and forum-shopping difficulties, a uniform alternative to defamation litigation would be extremely valuable. One form of libel dispute resolution, pioneered by The University of Iowa Libel Research Project, could be a good fit for cyberspace. This ADR remedy is based not in money damages, but in vindication. A factual hearing is held to determine whether the statement was false and damaging, and the remedy is the publication of the finding of falsity. The publication of a finding of falsity could be particularly effective in cyberspace, where the vindicatory publication could be easily tailored to reach those whom the defamatory utterance most likely reached.

Like the use of ADR in other cyberspace dispute contexts, the involvement of specialized third-party neutrals in cyberspace defamation cases would promote an accurate reflection of custom in the dispute resolution process. In an environment with an increasingly well-defined 04 body of custom and where the type of publication, whether it be a permanent web page or a more transitory Usenet posting, is a significant factor in determining the damage done, the necessity of having a neutral well versed in the subject matter is great. A traditional jury simply may not be able to accurately grasp the ramifications of various types of online publication; an effort to effectively educate a jury would be expensive, time-consuming and precarious and would probably add to the already cumbersome nature of libel litigation. A vindication-based ADR remedy with an expert neutral could be more streamlined, cheaper, quicker and, potentially, a more accurate determination of the parties' interests.

Current and Future Implementation of ADR Processes for Cyberspace Disputes: Systemically, a bottom-up, flexible method of dispute resolution is much more suitable to the dynamic realm of cyberspace than sole reliance on top-down statutory or judicial authority and would not stifle the development of either custom or technology. There has been speculation that cyberspace eventually could evolve into a separate jurisdiction, with its own rules and adjudicatory authority existing in conjunction with territorial law. The effective resolution of disputes through ADR could be a first step-buying time against a potentially increasing need for more comprehensive blanket legislation and judicial rulemaking.

The rapid and unpredictable growth of technology compels the use, whenever possible, of flexible, bottom-up methods of control:

How do we determine when a "top down" rule such as a statute is best, and when a "bottom up" rule such as private contract... is best? The key to answering this question is the

recognition that the technology of computer communications is rapidly changing. The number of people using cyberspace, and the number and variety of services being offered on-line, are both growing with astonishing rapidity. In the face of this very dynamic situation, we ought to be reluctant to impose behavior control that is inflexible and uniform beyond the needs of the situation.

There is also a sociological reason for a flexible, bottom-up method of control: "Given the proprietary propensities of those who use computer mediated communication regularly, they would be the most unlikely candidates to relinquish control over their cyberspaces to an outside geopolitical jurisdiction." Persons who frequently communicate online seem to generally covet some degree of anarchy. They also generally have confidence in their ability to self-regulate, and a top-down implementation of law that conflicts with these customs-in-the-making could face severe opposition from those to whom it is meant to apply. One commentator, paraphrasing the conclusions of an online cyber-law conference, noted:

Clearly, there was no consensus about what the rules should be in cyberspaces. There was agreement, however, that these budding cyber communities should be given a chance to develop and test their own rules before the external authorities exert too heavy a hand to bring them into conformity with real-world rules.

As alluded to throughout this Note, the systemic use of ADR would allow custom to develop, rather than stifle it as a top-down regulatory framework or judicial pronouncement might. A reflection of custom is particularly important in disputes that might focus on what constitutes "reasonable" behavior "Most would rather be subjected to the judgments of their virtual community than the local laws of a physical place far from where they live....

"An intriguing possibility is the use of online "electronic dispute resolution." The use of e-mail technology, as well as real-time chat has the potential to fit very well with the objectives of ADR:

The process will allow for greater flexibility, more creative solutions and quicker decisions. More important, the impersonality will preserve the relationship between the parties once the dispute is resolved. This will bring to the forefront alternative dispute resolution options such as ... mediation, arbitration and mini-trials. All these dispute resolution alternatives are more conducive to the electronic medium than is the courtroom, especially when there is a lack of trust between the parties, and emotions stand in the way of effective communication. Even when there is a serious economic imbalance between the parties, access to the highway to resolve the dispute makes sense: The economic size of the parties is "invisible" to the particular dispute resolution process.

Online ADR is already being explored. At the forefront is the Virtual Magistrate project, directed by Robert Gelman and a joint venture of the Cyberspace Law Institute, the American Arbitration Association (AAA), the Villanova Center for Information Law and Policy and several online service providers and public interest groups.' The project is funded by the National Center for Automated Information Research (NCAIR), a New York-based law and technology research foundation.

Virtual Magistrates are available to resolve disputes catching service providers between conflicting claims over copyright, misuse of network communications channels or libel or slander. Such disputes can be submitted through a World Wide Web page maintained at Villanova, assigned to a magistrate by the AAA administrator, and resolved within 72 hours. Complaints, answers, hearings and awards all are electronic, exchanged through specialized Web pages and dockets maintained on the World Wide Web. In the first case resolved by a virtual magistrate, America Online was ordered to remove an advertisement offering to provide mailing lists of thousands of email addresses.

The resolution of online-oriented disputes online would eliminate fairness issues related to the expense of travel. Such issues are particularly important considering that disputes will increasingly raise international choice-of-law and jurisdictional questions. The ability to present the case and obtain a decision within three days, as the Virtual Magistrate project is designed to facilitate, is also a major selling point. The Virtual Magistrate is the prototypical online dispute resolution facility; while it has not been widely used thus far, awareness of the need for a specialized cyberspace dispute resolution mechanism has been growing.

Online ADR might appeal strongly to less sophisticated, individual parties with cyberspace grievances. While relatively simple disputes would probably be served very well by e-mail and chat-based communication, online ADR's ability to effectively resolve more complex disputes will likely increase as technology increases. Development will not stop with email and real-time chat; more "experiential" media such as two-way video and audio are developing rapidly.

Traditional applications of ADR, in the commercial or intellectual property contexts, for instance, typically rely to various degrees on the underlying body of law. A cyberspace-oriented ADR institution could lie somewhere between a pure adjudicatory model, with little reliance on preexisting rules, and a simple forum for the rule enforcement of a chosen legal system, incorporating expert neutrals to make determinations dependent on the unique nature of cyberspace ("reasonableness" determinations, for example).

Although rulemaking and adjudication are conceptually distinct modes of decision making they can be combined in practice. An adjudicator may make new rules just as a traditional common law court makes new rules to fit cases of first impression. It is possible to have a system in which there is only adjudication. A claimant need not make a claim of right in the sense that the claimant identifies some pre-existing rule under which his case falls. In such a system the adjudicator would have very broad discretion to decide whether a particular transaction is "fair." For example, a dispute arises over acceptable use of internetworking facilities, and a committee of members of the Internet meets to decide how the dispute should be resolved fairly, without reference to any pre-existing rules, because there are none. [sic]

Enforceability of the ADR arbitral decrees and of contracts to arbitrate should not be a problematic issue. First, judicial recognition of and enforcement of ADR decisions has increased. Assuming the procedure is facially fair, there should be few major problems with judicial aid in enforcing ADR decisions. And, as contract law will play a very large role in the development of cyberspace jurisprudence, a dispute resolution system which has its underpinnings in contract doctrine is particularly suitable:

Modem contract law retains the flexibility and malleability of traditional contract theory. Since contract law enables the parties to forge unique solutions to emergent legal problems, it is particularly well suited for the new information technologies. Contract law's capacity to evolve as a voluntary social institution is in contrast with the coercive features of tort law. General contract law principles fit well with the emergent culture of the Internet, which eschews involuntary obligations, whether imposed .from the state or from tort law.

The second major tool of enforceability could be a threat in the form of "cooperative exile" and would rely heavily on a "private association" model. This, too, is grounded in contract. An association of networks, or networks and system administrators, or system administrators and users, or simply system administrators, could contractually establish the validity of the ADR institution and its decisions. If a party fails to adhere to an ADR decree, he or she potentially could be "exiled" through the cooperative action of those in the association. Such a notion would require an extraordinary degree of cooperation, but it might be eased by some sort of technological improvement if the need for an ultimate source of enforcement is perceived to be great enough. If there is not enough cooperation to establish a sort of private association, this may be an appropriate area for a governmental authority to give its stamp of approval and support in enforcement.

ADR could play a very large role in the resolution of many disputes involving recent information technologies. There are many practical reasons in favor of choosing ADR over litigation. Its self-regulatory nature would promote, rather than stifle, the natural evolution of a coherent body of cyberspace customary law. And as a continuation of its recent growth, ADR would alleviate some legal-application problems relating to the rapid development of both technology and a global economy.

International Scenario: 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. Hence, this puzzle requires an answer to the question I would like to address

in this paper: does international law apply to states' conduct on cyberspace in the age of digital sovereignty? This article is divided into two main discussions: 1) Existing challenges on international law and governance on cyberspace, and 2) International law on cyberspace and digital sovereignty.

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 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 a room for deep state' intervention to citizen's data can be created. (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 cyber-security 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.

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-Apple Facebook-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.

International Dispute Resolution Mechanism: Drawing upon existing models of international dispute resolution and imagining new roles for international institutions,

proposals for both civil and criminal liability may be applicable. Crucially, these proposals are not mutually exclusive: a robust accountability regime could combine an international arbitration scheme to make victims whole with criminal prosecution to deter cyber criminals. The same attentiveness to the particularities of a given attack that counsels against reflexive reliance on either domestic criminal law or international humanitarian law also motivates the elaboration of a multi-pronged set of solutions. Transnational cyber offenses can vary in intensity and geographic reach, can be conducted by individuals or non-State actors, and can hit individuals, corporations, state entities, and international organizations, among other victims. The appropriate legal tool may be different from one case to the next; the aim of this Part is not to prescribe but to propose new tools for the toolbox.

A. International Arbitration and Civil Liability:

International arbitration offers one little-considered mechanism for holding perpetrators of cyber-attacks accountable. Even before the modern international arbitration regime emerged, countries used civil arbitration to regulate transnational activity and resolve disputes. International arbitration is not only for disputes between nations, however. International civil arbitration can also be used to hold private actors accountable, without impermissibly undermining State sovereignty.

Today, international commercial arbitration operates under the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 1958, more commonly known as the New York Convention. As of November 2017, 157 nations had ratified the Convention. Aimed at promoting international uniformity in the recognition and enforcement of arbitral awards, the New York Convention imposes two sets of rules on the national courts of member States. First, under Article II(3), national courts in member States must recognize arbitration agreements made between the parties. When confronted with a dispute governed by an arbitration agreement, courts must refer the parties to arbitration if either party so requests. Second, under Article III, the Convention requires States parties to recognize and enforce arbitral awards issued in the territory of another State. The Convention thus enables prevailing parties to collect on the assets of the losing party, even when the latter resides in another jurisdiction.

The New York Convention's widely adopted system of civil accountability for transnational wrongs could be harnessed to promote accountability for transnational cyber offenses. In the commercial context, businesses often agree to arbitration under the New York Convention, not only because arbitral awards are enforceable worldwide, but also because arbitration offers an efficient and confidential process with judges experienced in the subject area and no possibility for appeal. In turn, making this dispute resolution channel available to businesses is an important reason why so many States have chosen to ratify the Convention, despite having to sacrifice a degree of sovereignty in the enforcement of foreign arbitral awards. In the cyber context, software companies and Internet Service Providers could require, as part of their terms of service, that disputes relating to cyber-attacks be subject to arbitration. And because virtually every country in the world— including countries like Russia that are seen as cybercrime havens—has been hit by malware and DDoS attacks, countries may be incentivized by their own citizens and corporations to recognize the jurisdiction of an international arbitral body.

Significantly, there is precedent for tying a specialized arbitral scheme to the New York Convention. The Court of Arbitration for Sport (CAS), founded in 1984, harnesses the machinery of the New York Convention to resolve international sports-related disputes and to punish violators of international norms quickly, impartially, and cost-effectively. The CAS is widely regarded as the final decision-maker for international sports-related disputes, "to the exclusion of national courts." Once the CAS renders a judgment, sports organizations can enforce the judgment directly—for example, through bans on registering or playing—or parties can apply to national courts, typically the Swiss Federal Supreme Court, for enforcement under the New York Convention.

We might imagine a specialized arbitral tribunal for cyber-related disputes, analogous to the CAS disputes, analogous to the CAS. A cyber arbitration body could issue civil penalties for cyber infractions, with enforcement tied to the New York Convention such that a cyber - attacker's assets could be seized wherever they may be located. Just as CAS arbitrators generally have recognized expertise in sports and sports law, so too an arbitral tribunal for cyber issues could benefit from arbitrators with technology expertise.

A cyber arbitration scheme could also be tailored to the unique features of transnational cyber offenses. Individuals, corporations, or States could all sue perpetrators. Class actions could also be permitted, allowing parties affected by a malware or ransomware attack to aggregate their claims to meet harm thresholds and, conceivably, to financially wipe out cyber villains. We could even envision liability for parties that negligently fail to secure critical infrastructure or fail to comply with cyber hygiene requirements, thereby permitting their devices to become part of botnets.

There is already one international body within which a cyber-arbitration forum could reside. Under the aegis of the United Nations, the International Telecommunication Union (ITU) is a specialized agency that promotes international cooperation relating to telecommunications infrastructure and global technical standards. With a membership of 193 countries and nearly eight hundred private entities, the ITU has used its technical expertise to support less technically sophisticated countries and to engage in Internet related research and development. For example, the ITU in 2014 announced the creation of a Global Cyber-security Index to evaluate and compare cybersecurity strategies worldwide. Additional ITU activities include building capacity and helping countries establish national Computer Incident Response Teams. As a result of initiatives like these, there has been talk in recent years of the ITU taking on a bigger role in Internet regulation.

Proposals for the ITU to regulate the Internet have prompted outcries from those concerned that such regulation would destroy the open, decentralized governance system envisioned by Paul Baran and other pioneers of the early Internet. At worldwide telecommunications conferences in 2012 and 2014, a number of countries, including Russia and Saudi Arabia, rejected proposals to expand the ITU's role in Internet governance, supposedly "to correct historical imbalances resulting from the perceived dominance of the [United States] over the internet." If international resistance could be overcome, however, the ITU would seem to be a natural entity to call upon to develop cyber regulations and to arbitrate disputes. A 2016 meeting of the ITU Telecommunication Standardization Sector saw some significant compromises on Internet governance, including agreements that governments should take on a "broader policy role"; that global, interoperable processes for sharing information about

cybersecurity incidents should be promoted; and that the ITU should assist member States in establishing a framework for "rapid response to major incidents."

Two non-profit entities responsible for ensuring the reliable operation of the Internet could also take on a bigger role in cyber security and cyber dispute resolution. The Internet Engineering Task Force, an international open standards organization, develops voluntary standards for the Internet to promote interoperability and usability. The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the global Domain Name System (DNS), performs technical maintenance on DNS root zone registries, and manages IP address space. ICANN currently administers the Uniform DomainName Dispute-Resolution Policy (UDRP), a system for resolving disputes related to trademarks and Internet domain name registration. The UDRP administrative adjudication process could serve as a model for arbitrating disputes involving transnational cyber offenses. As of October 1, 2016, ICANN is no longer subject to U.S. government oversight, potentially making it more likely that other countries would accept a greater regulatory role for ICANN.

Whether tied to an existing entity likes the ITU or ICANN or entirely independent, an international civil arbitration system that allows victims of transnational cyber offenses to seek redress for losses could obviate the temptation to hack back. Further, the potential for individual victims to aggregate claims and obtain significant damages awards could meaningfully deter would-be cyber attackers. Of course, erecting an international arbitration system for cyber actions would present its own set of challenges that would have to be overcome—including developing an arbitration agreement analogous to the CAS and requiring or incentivizing Internet users to agree to submit to arbitration. Still, international civil arbitration tied to the New York Convention offers one possible new weapon in the legal arsenal for combating transnational cyber offenses.

B. Transnational Criminal Law:

In addition to civil remedies for victims, a robust liability scheme for transnational cyber offenses ought also to include criminal penalties. As Section II.B demonstrates, relying on individual States to apply their penal law is inadequate. Countries without strong legal sanctions for cyber criminals can—either advertently or inadvertently, by design or by neglect—become havens for cybercrime. One solution is therefore to harmonize laws across countries and to promote international cooperation on law enforcement, developing a transnational criminal law regime. While purely domestic crimes are criminalized only at the election of the State, and international law crimes create individual penal responsibility under international law, transnational criminal law indirectly creates criminal liability by imposing obligations on States to enact certain domestic penal laws.

Legal harmonization is an important part of developing a transnational criminal law for transnational cyber offenses. At a minimum, every country ought to enact laws prohibiting core cybercrimes, such as the deliberate release of malware. But international cooperation at the level of enforcement is also important. Countries should commit to assist one another with real-time collection of traffic data, and technologically sophisticated countries should provide training to less technologically advanced countries. Additionally, provided there is reasonable cause for suspicion, countries in which evidence is found should be required to turn over evidence, such as computer hard drives, for investigation in other countries that

may wish to attempt to decrypt files. A global agency, similar to Interpol, could also be charged with developing digital forensics techniques and conducting investigations to support national prosecutions. These proposals for developing international law norms of information-sharing and for assimilating those norms into domestic law suggest how transnational criminal law could promote accountability: countries would have to sacrifice a degree of State sovereignty as a precondition for more effective prosecutions of transnational cyber offenses.

Proposals for increasing criminal enforcement of cyber offenses are often met with concerns about attribution. In fact, the problem of attribution may be overstated. To be sure, the architecture of the Internet is built to ensure anonymity, complicating technical attribution. But legal attribution, even in the kinetic world, often relies upon the accumulation of multiple incomplete pieces of evidence, forensic tools with less-than-perfect accuracy, inferences, analysis of motive, and judgment. Those same strategies can be applied in the cyber context to find individuals criminally liable "beyond a reasonable doubt." To the extent a prosecution in one country depends upon evidence obtained in another country that reveals sensitive information about the latter country's information-gathering capacities, States could commit to requiring that courts review sensitive evidence in camera and to sealing the court records. While evidentiary issues in the cyber context are no doubt complex, attribution is a nuanced process that could benefit from the skills and resources—both technical and non-technical—of States acting together.

Some efforts to foster international cooperation along these lines are already underway. In 1997, the G-8 countries established the "24/7 Network of Contact Points" ("24/7 Network") for data preservation. Presently consisting of approximately seventy member countries, the G-8 24/7 Network allows countries to solicit the urgent assistance of other countries in cybercrime matters in order to preserve data for subsequent transfer through mutual legal assistance agreements. The 24/7 Network is just a first step; the United Nations General Assembly has repeatedly called for a global framework to protect cyber infrastructure and combat cybercrime. Several countries have also formed inter-jurisdictional task forces to address transnational cybercrime, and the ITU has drafted model cybercrime legislation and compiled resources to assist countries in drafting their own cybercrime laws and procedural rules.

The most important step toward a transnational criminal law for cyber offenses to date is the Budapest Convention on Cybercrime. Drafted by the Council of Europe and adopted in 2001, the Budapest Convention has so far been ratified or acceded to by fifty-six States, largely European nations but also the United States, Canada, Australia, Israel, and Japan. It represents, in former Secretary of State John Kerry's words, "[t]he best . . . legal framework for working across borders to define what cyber-crime is and how breaches of the law should be prevented and prosecuted."

The Budapest Convention assumes that criminal prosecutions will continue to take place at the level of the State but aims to harmonize national laws and promote international cooperation on evidence-gathering. Member States have jurisdiction over any offense that occurs in their territory, regardless of where the attacker is located. Additionally, States have jurisdiction over offenses committed by their nationals, provided that the offense was punishable under the criminal law of the State where it was committed or was committed

outside the territorial jurisdiction of any State. Further, the Convention facilitates mutual assistance and extradition by allowing for the Convention itself to be used as an extradition or legal assistance treaty in the absence of any preexisting MLAT between the relevant States.

While the Budapest Convention is an important step, so far it remains largely symbolic. Many important States, including Brazil, Russia, India, and China, have refused to join the Budapest Convention. Russia—the only Council of Europe nation not to have signed—insists that granting foreign countries access to stored data could undermine national security and sovereignty and has put forward its own alternative proposal. Until the Budapest Convention is universally adopted, countries like Russia and China can continue to shelter cyber criminals from prosecution. Additionally, many States that have formally ratified the Budapest Convention have yet to pass new domestic legislation to implement its provisions, while other countries have opted out of various provisions by making reservations. Finally, the Convention provides only vague definitions of several key terms and does not elaborate the elements required for various offenses, leaving such details to State discretion.146 As a result, notwithstanding the promise of legal harmonization, inconsistencies in cybercrime legislation and enforcement remain.

Several features of the Convention have also proven controversial. First, there is no dual criminality provision, meaning that activity does not have to be illegal in both the State requesting foreign cooperation and the State whose assistance is requested. A State could therefore be required to investigate acts it considers legal. Second, the Convention requires signatory States to have broad surveillance powers. Article 21 provides that States should collect or record—or compel an Internet Service Provider to collect or record—real-time traffic data associated with online communications, while Article 32 allows law enforcement in one member State to conduct an extraterritorial investigation in another State without notifying that State's authorities. A few commentators have argued that the Convention does not go far enough in authorizing data collection and sharing among States. For example, the Convention does not authorize unilateral cross-border searches, even in emergency situations, instead requiring that nations consult with local officials before seizing data. Many other commentators and civil liberties groups, however, have raised privacy concerns, objecting to the fact that the Convention incorporates the United States' lesser privacy protections rather than Europe's higher standards of data protection.

Concerns about individual privacy may represent the biggest obstacle to the development of a true transnational criminal law of cyber and to the deep international law enforcement cooperation on which national prosecutions often depend. When it comes to the Budapest Convention, though, concerns about privacy may be overblown. Article 15 of the Budapest Convention explicitly provides that each Party shall ensure that the implementation of the Convention is subject to the safeguards provided under its domestic law and respects human rights and liberties. The Convention also does not prevent member States from submitting to stricter privacy standards, like those found in the Council of Europe's Data Protection Convention.

Moreover, from a U.S. perspective at least, international cooperation could potentially promote rather than undermine respect for individual privacy. Perpetrators of transnational cyber offenses do not have a reasonable expectation of privacy in malware; code and other

information knowingly exposed to the public or shared widely with third parties are not protected under the Fourth Amendment, nor are communications that have been received by the intended recipient. Physical hard drives and server data, though, may be protected by the Fourth Amendment. Currently, under the exigent circumstances exception to the warrant requirement, law enforcement can lawfully search electronic evidence that is in imminent danger of destruction. Given concerns about data being perishable—for example, if it is overwritten or if a device is set to delete information after a certain amount of time—law enforcement may be more likely to rely on the exigent circumstances exception to avoid the warrant requirement. But if police can rely on other countries to effectuate cross-border preservation requests in accordance with the Budapest Convention, they may be less likely to resort to the exigent circumstances exception.

Conversely, if the U.S. government cannot rely on obtaining information relevant to an ongoing investigation from other countries, it may be more likely to try to obtain more data across the board and to retain that data for indefinite periods. Thus, rather than enabling law enforcement to evade Fourth Amendment privacy protections for U.S. residents by relying on other countries, international cooperation on cyber investigations could in fact empower law enforcement to seek appropriate permissions before searching private electronic devices or data. Furthermore, when assessing the privacy risks associated with international cooperation, countries should also factor in the privacy risks associated with the threat of more frequent cyber-attacks. If cyber attackers can hack into computers and access files with impunity, allowing law enforcement to collect, review, and share data subject to strict procedural rules may be preferable.

In sum, the Budapest Convention and other efforts to promote international cooperation on cybercrime legislation, investigation, and prosecution are promising, insofar as they recognize that cyber threats often cannot be solved by individual countries acting alone. Ultimately, the Convention's proposals, such as requiring countries to assist with national investigations and prosecutions, are largely traditional. By preserving the "localized, decentralized system of law enforcement we have had for centuries," the Budapest Convention may not be able to meet the challenge of punishing and reining in transnational cyber offenses. However, if more countries continue to ratify the Budapest Convention, if concerns about privacy can be overcome, and if transnational norm entrepreneurs support States in implementing and complying with the Convention's provisions, the first major international cybercrime treaty may yet prove to be an important instrument for fighting cybercrime. Further, as technology evolves, new protocols can be added to the Convention to strengthen its effectiveness: for example, the Cloud Evidence Group is currently preparing an additional protocol on access for criminal justice purposes to evidence stored on file servers in the cloud. Given the traction that the Budapest Convention has already gained, engaging in diplomatic efforts to bring in new stakeholders and entertaining compromises on certain human rights provisions may be the best way to harmonize the international regulatory environment and to promote accountability through transnational criminal law.

C. International Criminal Law:

While legal harmonization and international cooperation could facilitate criminal enforcement at the national level, international criminal law offers another possible accountability mechanism. Prosecution of cybercrimes as international offenses could take

place before the International Criminal Court (ICC), or before a sui generis international criminal tribunal for cyber offenses.

Presently, the ICC probably does not have subject-matter jurisdiction over cyber-crimes. The Rome Statute establishes the jurisdiction of the ICC over four crimes—the crime of genocide, crimes against humanity, war crimes, and crimes of aggression. Cyber offenses are not specifically recognized anywhere in the Rome Statute and likely do not fit any of the categories of crimes the ICC can hear.

Some commentators have suggested that cyber-attacks could constitute crimes of aggression. As originally drafted, the Rome Statute listed the crime of aggression in Article 5 as one of the four crimes over which the ICC had jurisdiction but did not provide a definition of the crime that would enable prosecutions. After the Rome Statute entered into force in 2002, the States parties established a Special Working Group on the Crime of Aggression, charged with drafting a definition of the crime and setting out the conditions under which the ICC would exercise jurisdiction. At a conference in Kampala in 2010, the States parties adopted a definition and jurisdictional regime for the crime of aggression. Since then, thirty-four States have ratified or accepted the Kampala amendments. States parties must additionally activate the Court's jurisdiction over crimes of aggression by a two-thirds majority.

Even assuming the ICC's jurisdiction is activated for crimes of aggression, the definition of the crime of aggression in the Rome Statute amendment is limited to persons "in a position effectively to exercise control over or to direct the political or military action of a State." By limiting potential culpability to those with direct political or military control, the so-called "leadership clause" excludes most perpetrators of transnational cyber offenses. Cyber offenses rarely occur in the context of a strict chain of command; most are carried out "by individuals with only tenuous affiliations to a collective," and those collectives may or may not be affiliated with, or sponsored by, a State. At least one commentator has suggested that, in exceptional cases, a DDoS attack may meet the leadership clause requirements insofar as the attacker effectively controls the *victim* State, such as when Russian DDoS attackers crippled the Georgian government's ability to act or to communicate with its own people. Still, in most cases, limiting ICC jurisdiction to high-level State actors prevents regulation even of cyber offenses with major international repercussions.

An additional challenge for prosecuting cybercrimes as crimes of aggression is the list of acts of aggression provided in Article 8 bis of the Rome Statute, adopted at Kampala. Those actions include an armed invasion, bombardment, and blockade by the traditional armed forces of another State.

While the phrasing of the definition suggests that the list is exemplary, rather than exhaustive, it is not clear whether cybercrime could qualify as an act of aggression. The enumerated examples all involve the use of armed force, which transnational cyber offenses typically do not, as noted in Section II.A. Cyber attacks resulting in physical damage could conceivably count as crimes of aggression if the list were understood to be merely illustrative, but standard DDoS attacks that disrupt service and cause even significant economic harm would not qualify.

Another possibility for ICC jurisdiction might be to treat transnational cybercrimes as war crimes. Article 8 of the Rome Statute provides jurisdiction over war crimes and enumerates several categories of war crimes, including grave beaches of the Geneva Conventions and violations of other laws applicable in international armed conflict. Most relevant to the cyber context, war crimes include the "extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly" in violation of the 1949 Geneva Conventions, and attacks on civilian objects that are not military objectives.

To the extent a cyber-attack destroys, rather than simply interferes with, civilian data and communications, cyber-attacks carried out in the context of armed conflict could conceivably rise to the level of war crimes. However, it bears emphasizing that war crimes necessarily entail a breach of international humanitarian law; as the previous Part showed, international humanitarian law does not apply neatly to cyber operations and, insofar as it does, very few cyber operations to date qualify as attacks subject to international humanitarian law. Moreover, Article 22 emphasizes the principle of ***nullum crimen sine lege,*** according to which a person shall not be criminally liable unless the conduct was clearly criminal. The definition of a crime is to be strictly construed and interpreted in favor of the defendant and is not to be extended by analogy. As a result of this inflexibility, cybercrimes that were not explicitly contemplated in Article 8 would be unlikely to qualify as war crimes. At least as currently drafted, then, the ICC's Rome Statute offers a useful model for prosecuting crimes with international effects but would not likely cover transnational cyber offenses.

The Rome Statute could be amended, however, to expand the jurisdiction of the ICC to cover grave cyber offenses. Another solution would be to create a new international criminal tribunal with specialized competency in computer technology. Along these lines, Stein Schjolberg, a former Norwegian judge and an international expert on cybercrime, has long called for an International Criminal Tribunal for Cyberspace and has published a Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace.

The availability of an international criminal tribunal, whether the ICC or a specialized tribunal, would mitigate many of the problems of State jurisdiction, including jurisdiction shopping, conflict of laws difficulties, and the challenge of cross-border collaboration on evidence-gathering and enforcement. Recent evidence suggests that international criminal tribunals can deter some criminal activity, particularly by governments and rebel groups seeking legitimacy. Moreover, ICC investigations can expose government corruption and unwillingness to comply with international standards, eventually increasing domestic prosecutions in the intermediate term. Thus, international criminal prosecutions of cyber criminals could help to deter cyber offenses on multiple levels.

International law offers two possible ways an international criminal tribunal could obtain jurisdiction over an alleged perpetrator of a transnational cyber offense: universal jurisdiction and complementarity.

i. Universal Jurisdiction:

Universal jurisdiction, recognized for centuries as applicable to piracy offenses, offers one solution to the problems of territorial jurisdiction when it comes to criminal liability. Rooted in "the accused's attack upon the international order as a whole," universal jurisdiction

enables an international criminal tribunal (or the courts of any nation) to claim criminal jurisdiction over an accused, regardless of where the crime occurred. Criminal law typically requires some sort of nexus between the prosecuting State and the offense, such as the offense being committed in that State's territory or by a national of that State. But pirates, considered ***hostis humani generis***—an enemy of mankind—could historically be prosecuted wherever they were found. In the modern era, piracy continues to be subject to prosecution by any nation under the United Nations Convention on the Law of the Sea (UNCLOS), as well as under customary international law. Cyber criminals, too, might be considered ***hostis humani generis***: cyber space can be thought of as the modern-day "high seas" and transnational cyber offenses the equivalent of pirates' indiscriminate acts of depredation.

Scholars often assume that universal jurisdiction for piracy is justified only because no State has jurisdiction over the high seas. However, the Court of Appeals for the D.C. Circuit has held that, as Article § 101(c) of UNCLOS, which criminalizes the facilitation of privacy, does not explicitly mention the high seas, aiding and abetting piracy does not need to take place on the high seas to be illegal under the Convention. Thus, it is not a prerequisite for a finding of universal jurisdiction that the crime take place outside the territorial jurisdiction of any country. As applied to the cyber context, the fact that some countries could have jurisdiction to prosecute a crime should not preclude the application of universal jurisdiction to transnational cyber offenses.

Perhaps a better justification for universal jurisdiction over piracy is that it endangers international trade. Transnational cyber offenses can similarly threaten international trade, such as when DDoS attacks disable access to major commercial websites, or when ransomware attacks threaten the destruction of international corporations' records and files. By the same logic, then, severely disruptive transnational cyber offenses could, like piracy, be subject to universal jurisdiction.

The challenge in applying universal jurisdiction to the cyber context is defining the scope of threats for which universal jurisdiction is authorized. The scope must be defined narrowly enough to prevent countries like Russia and China from taking advantage of universal jurisdiction to shut down online dissent. If the crimes subject to universal jurisdiction could be carefully drawn, an international criminal tribunal empowered to hear cases against and ultimately sentence cyber criminals anywhere in the world could prove a powerful deterrence mechanism.

ii. Complementarity:

A second basis for jurisdiction over international crimes is complementarity, upon which the ICC relies. Under the complementarity principle, domestic courts retain priority in the exercise of jurisdiction; the ICC may only assert jurisdiction if a domestic court has not already investigated or prosecuted the case.189 In this way, complementarity is respectful of State sovereignty and may make States more likely to join an agreement like the Rome Statute because they can retain control over matters of importance to them.

Applying the complementarity principle to the prosecution of cybercrimes before the ICC solves some, but not all, of the problems of territorial jurisdiction. If a country proved unable, perhaps for lack of technical capacity, or unwilling to prosecute a case domestically, the case

could potentially be tried before the ICC. A time limit would have to be established within which the State would be required to commence a prosecution, if it so chose; if a State failed to take action during that time, a victim State could request that the Prosecutor of the ICC press charges. Thus, the availability of an international criminal tribunal with jurisdiction to hear cases involving grave harm to any member State would solve the problem of States being unwilling to prosecute or extradite their nationals. Complementarity may also incentivize countries to adopt and enforce legislation criminalizing transnational cyber offenses in order to keep cases in their own courts. At the same time, complementarity fails to address some of the problems of territorial jurisdiction, including the risk of an Internet actor being subject to the potentially differing laws of many different countries, without having meaningfully consented to the jurisdiction of those countries.

Even if victim States wanted the ICC to exercise jurisdiction, the ICC's jurisdiction is largely limited to ratifying States, which can refer cases to the ICC if the alleged crime is committed by a national of, or on the territory of, that State. Precisely what it would mean for a cybercrime to be committed on a State's territory is not clear. Taking a very broad view of ICC jurisdiction, according to which the physical routing of attacks would determine whether a State party to the Rome Statute was the site of a crime, both the primary State victim and the State whose infrastructure was exploited could provide the jurisdictional hook. Since transnational cyber offenses are often routed through a large number of territories, the jurisdictional bar could often be overcome. But taking a narrower view of jurisdiction, crimes with a merely incidental relationship to a country would not qualify as a crime committed on that country's territory. Finally, even if the ICC could properly exercise jurisdiction over a defendant who was not a national of a member State, it could face the same extradition problems described above.

Clearly, there are significant challenges to prosecuting cyber criminals under international criminal law. However, international criminal tribunals are a still-recent development, and a new tribunal could potentially be created to hear cases of cyber-terrorism and other serious cybercrimes that threaten governmental institutions, cause large economic losses, or substantially interfere with civilian Internet usage. Were such a tribunal to exist, it would send a powerful message to the online community and could go a long way towards ending impunity.

INDIA: Arbitration is considered as an essential part of dispute resolution among commercial and business entities these days. Even in non-commercial cases, arbitration and other alternative dispute resolution (ADR) mechanisms are used by the parties to the dispute. Gradually even ADR mechanisms have become time consuming and expensive. Therefore, commercial and business world is now looking towards information and communication technology (ICT) for a better option than ADR for early and effective resolution of their disputes.

Online dispute resolution (ODR) has emerged as an alternative to ADR that is primarily technology driven. It has many advantages over traditional litigation methods and even over ADR methods. However, online dispute resolution (ODR) in India is still evolving. This is happening when e-commerce disputes and litigations are set for big rise in India. Even the so called smart cities of India would require a techno legal smart dispute resolution mechanism.

International Commercial Arbitration And Dispute Resolution In India Using ODR Platforms: Recently 800 Indian companies approached the Ministry of Labour for an online labour law compliance system. The Parliament of India has also passed the Insolvency and Bankruptcy Code, 2016 to ensure ease of doing business in India. Indian government is also working in the direction of amending the Arbitration and Conciliation Act, 1996 and formulating a citizen friendly national litigation policy of India.

Perry4Law Organisation (P4LO) suggests that India must speed up the process of adoption of ODR for resolving e-commerce and international commercial disputes. E-commerce disputes resolution in India may be resolved using ODR in the near future. In fact, the techno legal centre of excellence for online dispute resolution in India (TLCEODRI) has launched a beta version of ODR platform that can be used for dispute resolution by national and international stakeholders alike. This is possible as the test platform is guided by the digital India principles and mere access of Internet would be sufficient to resolve the disputes by using our ODR platforms. In fact, the emerging trends in international commercial arbitration in India are already pointing towards this direction.

The parties intended to be covered by the present and future techno legal initiatives of Perry4Law Organisation (P4LO) and TLCEODRI include national and international stakeholders like Central/State Governments, Foreign Governments, Indian companies, multi -national companies (MNCs), Public Sector Undertakings (PSUs), individuals, e-commerce websites, etc. We hope that all stakeholders would find this beta version initiative worth trying and making the same part of their business ventures and public dealings. To test the same, please create a ticket as per the category in which you fall.

Further, a special service of conducting Online Arbitration or Cyber Arbitration is also there where parties to the dispute can submit their disputes to the platforms of P4LO or TLCEODRI. The parties to the dispute must have incorporated the sample clause for getting their disputes resolved through P4LO or TLCEODRI while entering into an agreement/contract. Interested stakeholders may also contact us for drafting of such agreements/contracts where such ODR clause would be part of the same. This way parties need not to go to the courts and they can settle their disputes amicably, expeditiously and in an economical manner. Once the Arbitrator/Arbitration Tribunal is appointed, the appointed Arbitrator/Arbitration Tribunal of P4LO or TLCEODRI would then proceed to deal with the dispute and pass a binding Arbitration award by which the parties to the dispute would be legally bound.

Dispute resolution framework under the Information Technology Act, 2000: More than 131 million Indian consumers have been victims of cybercrime and India has lost INR 1.24 trillion in cyber-attacks in the previous year. Most victims of cyber-attacks or frauds in India do not know how to proceed against a cyber-attack. Although multiple online cybercrime complaint portals exist, the procedure after filing such complaint is blurry.

The Information Technology Act, 2000 ("**IT Act**") sets out a framework for resolution of disputes arising out of cyber-attacks like hacking, data theft, and phishing. The framework allows victims of such attacks to claim damages and compensation from the attackers. The IT Act lays down a two-tier dispute resolution process: (i) Adjudication of disputes; and (ii) appeal against the outcome of such adjudication. However, this process seems to exist mostly

on paper, and hasn't really been implemented. Cybercrimes are mostly dealt with by 'cybercrime cells' of the respective police departments. In addition to briefly discussing the current framework for dispute resolution under the IT Act, this blogpost also seeks to discuss the existing challenges in this framework, and how they can be addressed.

Key Details of the Framework: The scope of the framework is limited; it only applies to disputes that relate to the violations listed in the IT Act. There are two categories of violations under the IT Act: (i) contraventions relating to damage to computer, computer systems; protection of data; failure to furnish information, violation of any provision, rule, regulation or direction under the Act; and (ii) offences including cyber terrorism, violation of privacy and cheating. Only disputes relating to contraventions can be resolved through the dispute resolution framework. Offences are criminal in nature, they are dealt with under the criminal laws of India. The IT Act is applicable to persons and entities both within and outside India. Once a cyber-dispute is adjudicated as per the dispute resolution framework of the IT Act, the same dispute cannot be taken up by a civil court.

The process of adjudication under the IT Act: The power to adjudicate is given to an 'Adjudicating Officer' ("**AO**") appointed by the central government. As per the Ministry of Electronics and Information Technology ("**MeitY**"), the secretary of the department of information technology of each state is appointed as the AO for that state by default. The AO is a quasi-judicial body, as it has dual-powers to: (i) order investigation i.e. hold inquiry into the violation of the IT Act on the basis of evidence produced before it; and (ii) adjudicate i.e. it decides the quantum of compensation or penalty to be awarded in case of a violation. The AO can exercise its jurisdiction over matters in which the claim for compensation or damage does not exceed INR 5 crore. The process of adjudication is as follows–

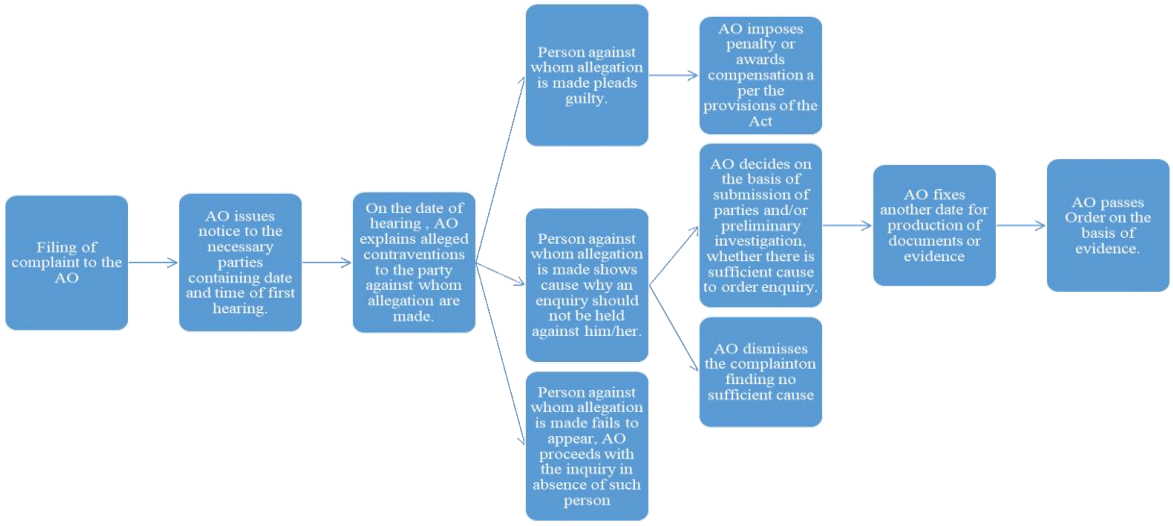


Figure 1: Adjudication Process under the IT Act: The AO is entitled to order investigation into a complaint at any time from the receipt of a complaint by it. This investigation is

conducted by an officer in the Office of Controller of Certifying Authorities or CERT-In, or by a Deputy Superintendent of Police.

Appeal: Orders issued by an AO are appealable before the Telecom Disputes Settlement and Appellate Tribunal ("**TDSAT**") . A party can appeal against AO's order before the TDSAT within 45 days of receiving the order. The right to appeal is not available to the parties if the adjudication order was passed with the consent of the parties.

The TDSAT may confirm, modify or set the adjudication order appealed against, after giving the parties a reasonable opportunity to be heard. The TDSAT has the same powers as are vested in a civil court to summon the parties, order production of documents and to review its decisions. A party can file an appeal against TDSAT's order to the High Court, within 60 days of receiving the order.

Issues with the Dispute Resolution Framework under the IT Act

The framework may look promising in theory, but it has not been as effective in practice. There is hardly any reportage on a cyber-dispute and there is no data available on the number of cases adjudicated upon by officers or the tribunal. We have identified certain issues that highlight the lacunae in the system:

Possibility of conflicting orders passed by AOs:

They AOs enjoy wide powers. They can adjudicate on violation of any provision, rule, regulation or direction passed under the IT Act. AOs have sometimes passed orders with significant ramifications. For example, in one case, an AO held a bank liable for not exercising due diligence to prevent phishing. The AO referred to the prevailing RBI guidelines on internet banking to arrive at this conclusion. Thus, AOs can play a significant role in interpreting the IT Act.

There are multiple AOs, who address similar kind of issues, at the same time. This results in the problem of conflicting opinions on the same issue. For instance, in a case, the AO had held that Section 43 of the IT Act was not applicable to the bank as it was a body corporate. However, AOs in other states had held otherwise. In multiple cases, Section 43 has been invoked against body corporates. This can make it difficult for an entity to comply with the IT Act, as it may have to consider the opinion of multiple AOs to function across India.

Poor availability of orders passed by AOs:

To access adjudication orders passed under the IT Act, one has to search through websites of state governments which are not easy to navigate. There is no reportage of these disputes by popular legal databases as well. There should be a central database for adjudication orders. This will enable officers and other stakeholders to refer to these adjudication orders while dealing with violations under the IT Act. It will also enable businesses to keep a track of cyber disputes.

Excessive burden on department secretaries appointed as AOs:

Secretaries of the department of information technology of the states are AOs by virtue of an old MeitY Order from 2003. They are responsible for the administration of their department, and are actively involved in the governance of the state, in addition to performing their duties as AOs. The dual-aspect of their job is extremely burdensome. Considering the high amount of cyber-offences in the country, there is a need to revamp this system for appointment of AOs. There are other Indian laws where AOs are given independent roles for adjudicating violations. For instance, the Prevention of Money Laundering Act, 2002 ("**PMLA**") lays down a similar adjudication procedure for offences. However, instead of appointing AOs, the PMLA has established an 'Adjudicating Authority'. This authority comprises of a chairperson and two other members. This authority is only involved in adjudication of offences, it is also allowed to have its own staff for assistance. The IT Act could adopt a mechanism similar to the other laws to ensure efficacy and speedy disposal of adjudications.

Need for capacity building in adjudication of cyber offences: There is a need to build the capacity of AOs. The Crown Prosecution Service of the United Kingdom has issued 'Cybercrime-prosecution guidance'. This guidance has defined major kinds of cybercrimes like hacking, social media related offences, etc. They provide basic principles for adjudication of cybercrimes. A guidance of a similar nature should be introduced in India to ensure better handling of complaints.

Investigation and appreciation of evidence during the adjudication process: Investigation into violations is conducted by an officer in the Office of Controller of Certifying Authorities or CERT-IN; or by the Deputy Superintendent of Police. However, the capacity of these bodies to conduct cyber investigations is questionable.

Most cyber-offences are reported to the police departments, as the National Cyber Crime Portal functions under the domain of the Ministry of Home Affairs. Complaints on this portal are referred to the police department of the state in which the alleged cyber-offence was committed. The police personnel are not equipped to deal with cybercrimes; they may not have the requisite expertise in areas like cyber forensics and investigation. They often appoint private firms to investigate into such matters. There is no guiding document under the Indian regulatory framework on cyber investigation or cyber forensics. The Information Technology (Amendment) Act, 2008 has established a body called the "Examiner of Electronic Evidence". This body provides expert opinion on electronic evidence. The MeitY has appointed various forensic science laboratories as the examiner. These laboratories hold expertise in conducting cyber investigation. However, the Holding of Enquiry Rules, 2003 have not been updated post the coming of the 2008 amendment act. The rules must be amended to give AOs the power to order such examiners to investigate into the matters before them.

There should be guidelines or principles on investigation of cyber offences to better equip the police and other investigating agencies to handle such cases. For instance, the United States Department of Justice had issued a guide on 'Electronic Crime Scene Investigation' in 2001. This is a comprehensive guide which sets out investigation techniques for different kinds of cyber violations like frauds, identity theft etc. A similar national guideline on cyber investigations must be issued in India. A cybercrime investigation manual was launched by

the Data Security Council of India. Steps must be taken by the central government to notify such guidelines.

Issues with the TDSAT: Initially, a "Cyber Appellate Tribunal" was established under the IT Act to deal with appeals from orders of AOs. In 2015, a Parliamentary Standing Committee was constituted to study the conditions of tribunals and pendency of cases. This committee in its report highlighted that the position of the Chairperson of the Cyber Appellate Tribunal was vacant since 2011 and was thus dysfunctional. As of 31 December 2014, only 34 cases were pending in this tribunal. Considering the state of affairs, this tribunal was merged with the TDSAT in 2017.

As per the TRAI Act, the TDSAT consists of a chairperson and two other members only. Considering that telecom and information technology are separate subjects, a different set of expertise is required to decide upon them. It is necessary that the TDSAT increase its strength and involve experts having a background in information technology to decide upon cases relating to the subject. There should be a separate bench to decide upon cyber appeals.

Adjudication and handling of cyber violations by sectoral authorities: Most instances of cyber violations relate to online banking frauds, including KYC frauds and phishing related cases. For this, the RBI has an "Ombudsman Scheme for Digital Transaction, 2019". This allows victims of cyber violations to file online complaints. Such complaints should relate to default of the bank, payment system or prepaid payment instruments provider. The ombudsman is empowered to award compensation up to INR 20 lakh rupees to the victim. Similarly, the Ministry of Home Affairs had introduced a National Cyber Crime Reporting Portal. Complaints pertaining to online financial frauds, social media related frauds and hacking can be reported on this portal.

However, the procedure post filing a complaint on this portal is not set out. It is good to have sectoral regulations for handling cybercrimes. Sectoral regulators may be better equipped to deal with the cybercrimes pertaining to their particular area. At the same time, different sets of regulations may lead to potential conflict between authorities under the IT Act and the sectoral authorities. There should be a channel for sectoral regulators to seek consultation from the authorities under the IT Act, where required. For instance, Section 21 of the Competition Act, 2002 lays down a framework for references by statutory authorities. This section allows other statutory authorities to take the Competition Commission of India's opinion on whether any decision taken by such authority would be contrary to the Competition Act. A similar framework should be incorporated into the IT Act.

Conclusion: ODR will gain maximum acceptance with public- private partnership, when the technical, commercial and legal challenges have been adequately addressed and satisfactory solutions have been provided for an ideal ODR regime. ODR process needs to be affordable, accessible, convenient, flexible, transparent, infrastructure equipped , secure, efficient and enforceable. ODR process requires mass awareness, manpower training in technology, funding for projects and codification of ODR law and practice (akin to lex mercatoria or Internationally accepted principles in arbitration) to effectively resolve e disputes. ODR has all the attributes of becoming efficient method to resolve e disputes that will bring long term benefits including secure e commerce and build greater trust and confidence in cyber space.

In the absence of viable tools to hold cyber attackers responsible, individuals, States, and businesses may be tempted to resort to retaliation and cyber-vigilantism. While scholars have long recognized the need for accountability for cyber wrongs, there has been little agreement as to what legal framework for accountability is most appropriate. The very fact that experts have struggled to settle on an appropriate legal framework suggests that there is no single legal framework that can properly regulate all cyber hostilities. In the cyber realm, we may encounter conventional crimes properly subject to domestic criminal law as well as violations that fall under the international law of armed conflict.

Critically, however, the cyber context also gives rise to a third category of wrongs that do not fit comfortably within either domestic criminal law or the law of armed conflict: transnational cyber offenses. The jurisdictional rules developed for the nineteenth-century world of West phalian nation-states are in many ways at odds with the network architecture of modern computing and the inherently cross-border character of transnational cyber offenses. Regulation and deterrence of transnational cyber offenses require novel legal solutions. While the elaboration and implementation of those solutions may seem like a formidable challenge, there is reason to be cautiously optimistic.

Transnational cyber offenses, unlike many acts that the international community has sought to condemn, harm all countries; no country is immune from the threat of cyber hostilities. The WannaCry ransomware attack, to give just one recent example, made clear that even supposed cybercrime havens like Russia may find themselves victims of transnational cyber offenses. As Internet-connected devices proliferate and the security risks multiply, countries may face both internal and external pressures to develop and enforce a comprehensive international accountability regime— to form, as Barlow himself alluded to, a "Social Contract" of the digital world.

In India, Considering the large number of incidents of cyber-attacks in the country, it is the need of the hour to bolster the current dispute resolution framework under the IT Act. The dispute resolution framework can create a strong deterrent for cyber offenders by forcing them to pay damages and compensation. It can also serve as an effective complaint redress platform for victims. In its current state it has failed to achieve the desired result. The authorities under the IT Act function in a vast domain, which encompasses issues relating to cyber-security, intermediary liability, data privacy, and cyber offences. Therefore, these authorities must be adequately equipped to exercise their wide ranging powers.

The government has stressed heavily upon its Digital India initiative which will support India's goal of becoming a $5 trillion economy by 2025. Also, India has a large user base of 697 million internet users. Considering India's quest to digital transformation, it is pertinent to give teeth to the Act, especially to its dispute resolution framework. This will ensure that disputes in the cyberspace are effectively managed and resolved. This will increase the confidence of the masses as well as the stakeholders towards the regulatory framework.

MODULE - VI

INFORMATION TECHNOLOGY LAW IN INDIA

MODULE- VI: INFORMATION TECHNOLOGY LAW IN INDIA

IT Law in India: Human life in today's world is surrounded by technology. Technology has left hardly any space for non-technical things. A small change in an individual's life brings about a change in the entire society. When society is influenced, the legal system or the way that society is governed changes for sure. It's a social phenomenon. With the enormous speed of development in information technology, the challenges of reforming the regulatory mechanism governing the information technology are also increasing. Though law cannot possibly be expected to keep pace with changes in technology, still there are few areas in the current information technology law which needs some attention.

Indian Parliament provided a progressive legislation in the form of The Information Technology Act, 2000. As is the case with any information technology legislation in any country, the expectations of incorporating new technological challenges were many in India. To cater the need to incorporate new technological challenges and protect more and more rights of the users of the information and communication technology, contraventions and offences were added in The Information Technology Act, 2000. There were series of amendments passed in The Information Technology Act, 2000.

There were two major amendments in The Information Technology Act, 2000 in the year 2004 and 2008 encompassing the development of technology and the challenges raised by the commission of contraventions and offences with the use of technology. The most comprehensive one was The Information Technology (Amendment) Act, 2008. The Information Technology (Amendment) Act, 2008 had a major impact on Section 43, which prescribed for contraventions and provided remedy to the victims of contraventions in the form of compensation. The Amendment in 2008 made a comprehensive change in the way the contraventions were dealt within the Indian legal framework.

Technology poses different challenges in different countries. There were positive as well as negative aspects of the said amendment. As this amendment was made comprehensively and in quick time, the limitations and shortcomings were evident in certain important provisions under the legislation, as was the case with Section 43 of The Information Technology Act, 2000.

Given the magnitude of the amendments, it is indeed strange and amazing that this Act was passed in an unprecedented hurry, without any discussion in both the houses of the Parliament in the last week of December, 2008. Even though, the amendment in 2008 was a much celebrated and much hyped phenomena, there are few unanswered questions before every user of information technology which are awaiting one more significant amendment by legislature.

With the advancement of technology, new methods of crime are coming to the fore. Criminals and anti-social elements with their ingenuity manage to exploit the technological developments for illegal pecuniary gain or plain pleasure causing monetary loss as well as mental disturbance to the innocent citizens. In order to protect the fundamental rights of the law abiding citizens, it becomes inevitable for the state to intervene and regulate human activity as well as legislate on various subjects and ensure enforcement of the legislations in

letter and spirit through the police, thus making the police an essential part of governance by the state.

As society relies increasingly on computers, the amount of crime perpetrated with the machines has risen in kind. To law enforcement's delight, electronic records have proved to be a fertile ground for detectives.

The Internet: Internet is one of the most wonderful inventions of the last century. Now, it has become integral part of our life and it is continuously making human life easier and simpler in various ways. From information accessing to money transfer, all kinds of tasks are performed using the internet. Today, more and more people are relying on online banking and online shopping. There are many networks that exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. This requires connecting together different, and frequently incompatible networks, to make the connection and provide the necessary translation, both in terms of hardware and software. A collection of interconnected networks is called an internetwork or just internet. An internetwork is formed when distinct networks are connected together.

"Internet" refers to the global formation system that – (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suits or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein. New communication systems and digital technology have made dramatic changes in the way we live and the means to transact our daily business. Businessmen are increasingly using computers to create, transmit and store information in electronic form instead of traditional paper documents. It is cheaper, easier to store and retrieve speedier to communicate. Although people are aware of the advantages which the electronic form of business provides, people are reluctant to conduct business or conclude transaction in the electronic form due to lack of appropriate legal framework. Electronic commerce eliminates the need for paper based transactions. The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance are the requirements of writing and signature for legal recognition. At present, many legal provisions assume the existence of paper based records and documents which should bear signatures. The Law of Evidence is traditionally based upon paper-based records and oral testimony. Hence, to facilitate e-commerce, the need for legal changes has become an urgent necessity.

The latest threat to privacy, property and peace of individuals all over the world is from abuse of technology relating to computers, their network or hardware devices, where the computer or device may be agent of crime, the facilitator of the crime or the target of crime. However, the rapid evolution of Internet has also raised numerous legal issues and questions. As the scenario continues to be still not clear, countries throughout the world are resorting to different approaches towards controlling, regulating and facilitating electronic communication and commerce.

The Way Internet Works: There are many types of internet traffic. The most familiar is related to the World Wide Web, which was first developed at the European Organization for Nuclear Research (CERN) at the end of 1980s. The web was first conceived as a system of documents containing links to other documents – a concept known as 'hypertext' that had been proposed as early as the 1930s.

By clicking on a link in a web browser, a series of operations is initiated which results in the display of a new webpage on a computer. The first step is to translate the human-readable name of a service, such as www.target.com, to the numerical Internet Protocol (IP) address that computers can use to locate other computers on the internet. This is done using a Doman Name System (DNS) server, usually operated by the user's Internet Service Provider (ISP), whose location is usually provided to the user's computer when they first connect. Several alternative DNS servers are available – well known examples are operated by Open DNS, as well as Google.

Benefits of Internet: The Internet can be used for a variety of purposes from anywhere in the world. Some of the users are:

- To exchange e-mail instantly with friends or institutions in India or abroad.
- To participate in teleconferences with people on topics of interest or research problems.
- To find out educational information from universities worldwide, libraries and book stores.
- To surf on different topics for pleasure.
- To read about interesting sports and games.
- To find out information on agriculture, irrigation, crops, seeds, pesticides, labour, health, diseases, medicines, livestock and many other rural problems.
- To use it for e-commerce, e-governance, e-banking, e-medicines etc.
- To interact with government departments on registration, taxation, water & drainage, gas, income tax etc.,
- To improve literacy, adult education, gender equality and promote cultural heritage.
- To search on-line library catalogues for bibliographic data and other databases for textual data.
- To have access to electronic journals, newsletters and in-house information of many organizations and institutions.
- To communicate with others through the sites of social network.

Cyber Space: The New Shorter Oxford Dictionary explains the expressions 'Cyber Space' as 'notional environment within which electronic communication occurs especially when represented as the inside of a computer system, space perceived as such by an observer, but generated by a computer system and having no real existence, the space of virtual reality'.

Definitions of Cyber Crime: The Information Technology Act, 2000 (I.T. Act) defines Cyber Crime as *"the act of a person which is intentionally conceals or destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or network is cyber-crime".*

An act or omission, which is punishable under the law in force, is known as crime. The same explanation is also applicable to cyber-crime. But, there is no legal definition for cyber-crime.

The purpose of adding the word cyber with crime is only to indicate that the computer has been used to commit an illegal act and to caution the users for safeguarding the digital evidence, which is of fragile in nature. In short, cyber-crime can be known as digital crime. In literal sense, cyber was a word coined by William Gibson in his 1984 fictional novel ***'Neuromancer'***. Cyber is the prefix relating to the worldwide field of electronic communication. Crimes involving stealing, fabricating, leaking or circulating forbidden digital information are collectively branched under the umbrella term cyber-crime.Cyber-crimes can be broken down into two types through the Information Technology Act does not make such a distinction. The first type of cyber-crimes is actually pranks in which the intention of the perpetrator is merely to create a nuisance. Thus, he may hack into a website and deface it, or break into one's email account and read private mail, or post obscene material. This type of offender is generally a computer buff who is essentially trying to show off his prowess such people get a kick by doing things which are arcane to most people. They may not really intend to derive any criminal, financial or sexual benefit out of their activities.

The second type of cyber-crime is real crime in the sense that the offender intends to derive pecuniary or sexual benefit by it. Thus, he may indulge in credit card or bank fraud, selling of secret commercial or security information obtained by hacking or helps in transmission of criminal information. Whether he is a prankster or a real criminal, the offender is necessarily a person who has a great deal of knowledge of computer, networks, security system and the Internet. It can be safely presumed that he knows a great deal more than perhaps the best investigators and can easily take them for a ride. Cyber-crime may be said to be those species of the conventional crime and there, either the computer is an object or subject of the conduct constituting crime.

Cyber-crimes share three elements:

1. Tools and techniques to perpetrate a crime.
2. Approach or methodology for executing the criminal plan – known as vector.
3. Crime itself that is the end of those plans and activities (a cyber-crime is the ultimate objective of the criminal's activities).

Cyber-crimes are committed mostly by persons who are said to be learned and hence, it is called as white collar crime. Cyber-crimes are very serious threat in the modern era and for the times to come and pose one of the most difficult challenges before the law enforcement machinery, especially to investigate, collect evidence, and to penalize. In the information age, the rapid development of computers, telecommunications and other technologies has led to the evolution of new forms of transnational crimes known as "cyber-crimes". Cyber-crimes have virtually no boundaries and may affect any country in the world. A generalized definition of cyber-crime may be "Unlawful acts where in the computer is either a tool or target or both". Most cyber-crimes do not involve violence, but rather greed, pride or play on some character weakness of the victims. Although it is difficult to identify the culprit, as the Net can be a vicious web of deceit and can be accessed from any part of the globe. The damage caused are almost an unrealizable, expect for certain financial damage which runs in

billions every year and shall create irreplaceable loss to the individuals and corporate. A cyber-crime is generally a domestic issue, which may have international consequences in most of the instances.

Types of Cyber Crimes

There are several Cyber Crimes which some of them detailed as follows:

Hacking: Hacking is the unauthorised access to computer system or networks. Hackers are people with sufficient technical ability to gain access to another person's computer or to a network through the use of stolen passwords, or interference technology which provides access to networks and individual computers.

Cyber Terrorism: In the context of Information Technology security, terrorists can come in many forms such as politically motivated, anti-government, anti-world trade and pro-environmental extremists. The term cyber terrorism was coined in 1996 by combining the terms cyber space and terrorism. Cyber-attacks may be carried out through a host of technologies, but have an attack pattern that may be modeled.

Identity Theft: Identity theft involves acquiring key pieces of someone's identifying information in order to impersonate them and commit various crimes in that person's name. Besides basic information like name, address, telephone number, identity thieves look for social insurance numbers, driver's license numbers, bank account numbers, birth certificates or passports etc. These informations enable them to commit numerous forms of fraud.

E- Bombing: A programme planted surreptitiously with intent to damage or to destroy a system in some way – for example to erase a hard disk or cause it to be unreadable to the operating system through Trojan horse, virus, worms.

E-mail spoofing: Spoofing is the process of pretending to be another person or process with the goal of obtaining unauthorized access. E-spoofing usually done by using a bogus IP address, but it could be done by using someone else's authentication credentials.

Cyber Stalking: Stalking generally involves harassing or threatening behavior repeatedly such as following a person, appearing at a person's home or business, making harassing through phone calls or vandalizing a person's property. Cyber stalking is one of the most common crime which are commenced on internet and using the internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse.

Software Piracy: According to Microsoft Company, software piracy is defined as *"the copying of a computer software programme without the permission of the copyright owner".* Certain reports indicated that more than $7.5 billion worth of American software illegally copied and distributed around the world each year. In China, 96% of all business software is pirated, but in Vietnam, it is peaked to 98%.

Digital Forgery: Digital technology facilitates to forge a document through printers and scanners by developing counterfeit currencies, postal cards, revenue stamp, mark sheet, birth certificate etc.

Cyber Squatting: It has similarities with old strategy or registering trademarks only to prevent others from using it. Here, the site names in the internet are blocked and then traded by unscrupulous persons for monetary benefits. Well-known celebrities, governmental establishments etc., are the victims of these activities.

Child Pornography: Pedophiles and child pornography is nothing unknown to the world. But, the internet has made it so easy for the pedophiles to organize and distribute the offensive materials throughout the world. Also, the pedophiles make them vulnerable of exploitation.

Data Diddling: This kind of an attack involves altering new data just before a computer processes it and then changing it back after the processing is completed. The Electricity Board faced similar problem of data diddling while the department was being computerised.

Web Jacking: This term is derived from the term hijacking. In this kind of offence, the hacker gains access and control over the website of another. He may even mutilate or change the information on the site.

Distributed Denial of Service: This is an attack in which thousands of separate computers, which are usually part of a botnet, bombard a target with bogus data to knock it off the net. These attacks have been used by extortionists who threaten to knock a site offline unless a hefty ransom is paid. Apart from the above, other types of cyber-crimes are Online Gambling, Intellectual Property crimes, Cyber Defamation, Internet Time Thefts, Theft of Computer System, Physically Damaging a computer system, etc.

History of the formation of The Information Technology Act: Prof. H.L.A Hart in one of his classic works entitled "The Concept of Law" has stated that human beings are vulnerable to unlawful acts which are crimes, and therefore, rules of law are required to protect them against such acts. The eminent English jurist Salmond has rightly observed that law seeks to regulate the conduct of individuals in the society. Computer systems are vulnerable. This technological progress can easily dupe, exploit a person by illegal or unauthorized access. The result is damage to the computer system. With the help of networks the cyber criminals indulge in criminal activity without any fear of being apprehended and tried for the offences committed by them.

The Genesis of IT legislation in India: Mid 90's saw an impetus in globalization and computerisation, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Until then, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records ie the data what is stored in a computer or an external storage attached thereto. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favourable considerations to the said Model Law, which provides for

recognition to electronic records and according it the same treatment like a paper communication and record.

The reasons for committing cybercrimes by criminal may briefly be stated as;

1. Wider accesses to information.
2. Complexity of computer system.
3. Negligence of network users.
4. Non- availability or loss of evidence.
5. Lack of Jurisdiction leading to fearless crimes.

Legislation and Frameworks: Legal measures play a key role in the prevention and combating the cyber- crime. These are required in all areas, including criminalization, procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability. At the national level, both existing and new (or planned), cyber-crime laws most often concern criminalization and indicating a predominant focus on establishing specialized offences for core cyber-crime acts.

Globally, 82 countries have signed and/or ratified a binding cyber-crime instrument. In addition to formal membership and implementation, multilateral cyber-crime instruments have influenced national laws indirectly, through use as a model by non-States parties, or via the influence of legislation of States parties on other countries. The last two decades have seen significant developments in the promulgation of international and regional instruments aimed at countering cyber-crimes. These include binding and non-binding instruments.

Functions of cyber-crime legislation:

1. Setting clear standards of behaviour for the use of computer devices.
2. Deterring perpetrators and protecting citizens.
3. Enabling law enforcement investigations while protecting individual privacy.
4. Providing fair and effective criminal justice procedures.

Cybercrime Evolution or Neo-criminology: Computer Technology and Internet with its advancements has bought about new variety of crimes thereby providing ever increasing opportunities for the criminals to indulge in illegal activities unabated. The last quarter of twentieth century witnessed several sophisticated ways through which the perpetrators of cybercrime found it easy to penetrate into the system of software and internet to commit cybercrime which may be characterized as the new species of white collar crime. These crimes have global ramifications sabotaging the national economy and business ventures. They are not restricted to any geographical area or territory and may be committed within a fraction of a second affecting victim who may be thousands of miles away. These new variety of crime have thrown a big challenge before the law enforcement agencies and they are required to evolve a neo-criminological approach to handle these internet crimes. Here the risk in such crimes is that the victims are totally unaware of the crime committed on their property or on person.

The challenge faced here is that the police were not able to tackle these crimes by the traditional

approach .The need was felt to tackle these crimes by using new strategies and methods and by
the use of new tools and techniques. The technique which the judiciary applied was that the application of the doctrine of ***mensrea*** while solving crimes, but such remained absent especially in crimes where there exists hacking, e-mail bombing, spoofing etc. Since such crimes are committed by teenagers and minors. These criminals remain out of the purview of law and yet the consequences are disastrous. Today the cyber criminals are Hi-tech knowledgeable and skilled in computer technology and invade the rights. The Rights that are generally encroached upon by the cyber criminals are a person's right to freedom of expression,
right to privacy, unlawful interference in e-commerce, intellectual property rights etc.

Groups of Cyber Criminals

A. **Children and Adolescent age between 8-18 years**
B. **Professional Hackers / Crackers**
C. **Disgruntled Employees or vengeful persons**
D. **Cyber abuser.**

By the use of internet the incidences of cybercrime have increased, therefore the need for such
crimes to be channelized and regulated by effective cyber laws. Cyber laws are that branch of law which deals with the newly emerging issues out of the development of the internet and other
communication mediums functioning over the cyberspace. These laws need to regulate all aspects of transactions of the internet and the cyberspace.

There are many issues faced by the development of the internet and the corresponding crimes arising there from-

i. **Domain name**
ii. **Intellectual Property Rights**
iii. **E-commerce**
iv. **Encryption**
v. **Electronic contracts**
vi. **On-line banking**

Cyber law may be defined as the law governing cyberspace which is a non-physical terrain created with two or more computers networked together .Online system create a cyber space. Cyberspace is not restricted to internet alone, but has computers, its networks and software. Therefore cyber law refers to the law relating to computer, computer networks and includes all activities that take place in relation to information stored, exchanged or retrieved using the computer system.

Reasons to Pass Cyber Laws

- To prevent computer abusers to carry on their illegal activities for personal gains.
- To prevent political rivalry so that innocent people do not become a victim of their criminal act. E.g.) A person staying in one country can easily dupe a person having a

bank account in any other nation, by transferring millions in the bank of a third nation, within no time with the help of laptop and cell phone.

Like many other countries India to has developed independent laws, to tackle cybercrime. But still in some countries there exists traditional laws to deal with such offences.

Importance of Cyber Laws

1. To regulate all the features of contacts and actions with respect to the internet.
2. To tackle issues on e-commerce, encryption, electronic contracts, on-line banking.
3. To tackle multidimensional crimes.
4. To have laws as cybercrime recognizes no territorial boundaries
5. Requiring minimum protection standards in areas such as data handling and retention.
6. Enabling co-operation between countries in criminal matters involving cyber-crime and electronic evidence.

Information Technology: Due to immense increase in the use of internet and dependency of individuals in every field, a number of new crimes related to Computer and other gadgets based on internet have evolved in the society. Such crimes where use of computers coupled with the use of internet is involved are broadly termed as Cyber Crimes.

National Association of Software and Services Companies (NASSCOM) is one of the main organisation for paving the way for enacting Information Technology Act, 2000. To improve the commercial ability of our nation, the modern methods have to be followed in e-commerce. Existing laws were not enough for these kinds of improvements. For recognizing this, an act needs to be implemented. Hence, the Government of India accepted the version of NASSCOM. The Government also accepted the suggestion of NASSCOM in creating this law.

The internet was considered as main for passing the information worldwide. The famous advocate Alan Chudin who was the legal advisor for major computer concerns worldwide had said that India is having lot of intellectual talents and law has to be created by India in the field of information technology and e-commerce. He also stated that by creating this law, India will gain lot of benefits. Hence, it was realised that creation of new law for internet was necessary. Following the UN Resolution, the Government of India has passed its first Cyber law, the **Information Technology Act, 2000** which provides the legal infrastructure for E-Commerce in India. The said Act has received the assent of the President of India and has become the law of the land in India on October 17, 2000. India is 12th nation in the world to adopt cyber laws. The effort was taken in the year 1998 itself. Alan Chudin was also one amongst the main person for enacting this law.

Provisions: The Information Technology Act, 2000 comprises 94 sections which are divided into 13 chapters. The chapters cover digital signature, electronic governance, attribution, acknowledgement and dispatch of electronic records, security of electronic record and digital signatures, regulation of certifying authorities, duties of subscribers to digital signature certificates, penalties, cyber regulations appellate tribunal, offences and liabilities of network

service providers. The Act has four schedules that lay down the relative amendments to be in the Indian Penal Code, Indian Evidence Act, Banker's Book Evidence Act, and the Reserve Bank of India Act. This is an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.

The object of the Information Technology Act, 2000 as defined therein is as under: *"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."*

Key Progress Features of the Act: The Information Technology Act, 2000 provides a much-needed legal framework for electronic transactions in India. Some of its key progress features can be summarized as follows:

- First of all, these provisions have approved e-mail as a valid and legal form of communication in India that can be duly produced and approved in a Court of law.
- Companies are able to carry out electronic commerce using the legal infrastructure provided by the Act.
- The Act bestows legal validity and sanction on digital signatures.
- The Act allows companies to become certifying authorities that may issue digital signature certificates.
- The Act allows the government to issue legal notifications on the internet, a first step towards e-governance.
- The Act enables companies to file any form, application or other document with any office, authority, body or agency owned or controlled by the government in such electronic formats as may be prescribed by the government.
- The Act also addresses important issues of security that are critical for the success of electronic transactions. It includes a legal definition of the concept of secure digital signatures that must undergo a security procedure as stipulated thereunder.
- The Act offers companies a statutory remedy in case anyone should break into their computer systems or network and cause damage or copy data. The remedy provided by the Act, is in the form of monetary compensation for damages for exceeding Rs.1 Crore.
- The Act has extra-territorial jurisdiction to cover any offence committed outside the country by any person.

The I.T Act, 2000 does not apply to the following

a. A Negotiable Instrument Act 1881.(Amended in IT Act 2008)
b. A Power of attorney as defined in section 1-A of Powers of Attorney Act 1882.
c. A Trust as defined in section 3 of The Indian Trusts Act 1882.
d. A will as defined in clause (h) of the Indian Succession Act 1925.

e. For agreements in the form of contracts with respect to sale of fixed assets or property.
f. Any kind of document or transactions as stated in the official gazette.

Definitions: The ITA-2000 defines many important words used in common computer parlance like 'access', 'computer resource', 'computer system', 'communication device', 'data', 'information', 'security procedure' etc. The definition of the word 'computer' itself assumes significance here.

'Computer' means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

So is the word 'computer system' which means a device or a collection of devices with input, output and storage capabilities. Interestingly, the word 'computer' and 'computer system' have been so widely defined to mean any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities. A careful reading of the words will make one understand that a high-end programmable gadgets like even a washing machine or switches and routers used in a network can all be brought under the definition.

Similarly the word 'communication devices' inserted in the ITAA-2008 has been given an inclusive definition, taking into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video etc like what was later being marketed as iPad or other similar devices on Wi-fi and cellular models. Definitions for some words like 'cyber café' were also later incorporated in the ITAA 2008 when 'Indian Computer response Emergency Team' was included.

*Digital Signature**:*** 'Electronic signature' was defined in the ITAA -2008 whereas the earlier ITA -2000 covered in detail about digital signature, defining it and elaborating the procedure to obtain the digital signature certificate and giving it legal validity. Digital signature was defined in the ITA -2000 as "authentication of electronic record" as per procedure laid down in Section 3 and Section 3 discussed the use of asymmetric crypto system and the use of Public Key Infrastructure and hash function etc. This was later criticized to be technology dependent ie., relying on the specific technology of asymmetric crypto system and the hash function generating a pair of public and private key authentication etc.

Thus Section 3 which was originally "Digital Signature" was later renamed as "Digital Signature and Electronic Signature" in ITAA - 2008 thus introducing technological neutrality by adoption of electronic signatures as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone. While M/s. TCS, M/s. Safescript and M/s. MTNL are some of the digital signature certifying authorities in India, IDRBT (Institute for Development of Research in Banking Technology – the research wing of RBI) is the

Certifying Authorities (CA) for the Indian Banking and financial sector licensed by the Controller of Certifying Authorities, Government of India.

It is relevant to understand the meaning of digital signature (or electronic signature) here. It would be pertinent to note that electronic signature (or the earlier digital signature) as stipulated in the Act is NOT a digitized signature or a scanned signature. In fact, in electronic signature (or digital signature) there is no real signature by the person, in the conventional sense of the term. Electronic signature is not the process of storing ones signature or scanning ones signature and sending it in an electronic communication like email. It is a process of authentication of message using the procedure laid down in Section 3 of the Act.

The other forms of authentication that is simpler to use such as biometric based retina scanning etc. can be quite useful in effective implementation of the Act. However, the Central Government has to evolve detailed procedures and increase awareness on the use of such systems among the public by putting in place the necessary tools and stipulating necessary conditions. Besides, duties of electronic signature certificate issuing authorities for bio-metric based authentication mechanisms have to be evolved and the necessary parameters have to be formulated to make it user-friendly and at the same time without compromising security.

e-Governance: Chapter III discusses Electronic governance issues and procedures and the legal recognition to electronic records is dealt with in detail in Section 4 followed by description of procedures on electronic records, storage and maintenance and according recognition to the validity of contracts formed through electronic means.

Procedures relating to electronic signatures and regulatory guidelines for certifying authorities have been laid down in the sections that follow.

Chapter IX dealing with Penalties, Compensation and Adjudication is a major significant step in the direction of combating data theft, claiming compensation, introduction of security practices etc discussed in Section 43, and which deserve detailed description.

Section 43 deals with penalties and compensation for damage to computer, computer system etc. This section is the first major and significant legislative step in India to combat the issue of data theft. The IT industry has for long been clamoring for a legislation in India to address the crime of data theft, just like physical theft or larceny of goods and commodities. This Section addresses the civil offence of theft of data. If any person without permission of the owner or any other person who is in charge of a computer, accesses or downloads, copies or extracts any data or introduces any computer contaminant like virus or damages or disrupts any computer or denies access to a computer to an authorized user or tampers etc…he shall be liable to pay damages to the person so affected. Earlier in the ITA -2000 the maximum damages under this head was Rs.1 crore, which (the ceiling) was since removed in the ITAA 2008.

The essence of this Section is civil liability. Criminality in the offence of data theft is being separately dealt with later under Sections 65 and 66. Writing a virus program or spreading a virus mail, a bot, a Trojan or any other malware in a computer network or causing a Denial of Service Attack in a server will all come under this Section and attract civil liability by way of

compensation. Under this Section, words like Computer Virus, Compute Contaminant, Computer database and Source Code are all described and defined.

Questions like the employees' liability in an organisation which is sued against for data theft or such offences and the amount of responsibility of the employer or the owner and the concept of due diligence were all debated in the first few years of ITA -2000 in court litigations like the bazee.com case and other cases. Subsequently need was felt for defining the corporate liability for data protection and information security at the corporate level was given a serious look.

Thus the new Section 43-A dealing with compensation for failure to protect data was introduced in the ITAA -2008. This is another watershed in the area of data protection especially at the corporate level. As per this Section, where a body corporate is negligent in implementing reasonable security practices and thereby causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. The Section further explains the phrase 'body corporate' and quite significantly the phrases 'reasonable security practices and procedures' and 'sensitive personal data or information'.

Thus the corporate responsibility for data protection is greatly emphasized by inserting Section 43A whereby corporates are under an obligation to ensure adoption of reasonable security practices. Further what is sensitive personal data has since been clarified by the central government vide its Notification dated 11 April 2011 giving the list of all such data which includes password, details of bank accounts or card details, medical records etc. After this notification, the IT industry in the nation including techsavvy and widely technology-based banking and other sectors became suddenly aware of the responsibility of data protection and a general awareness increased on what is data privacy and what is the role of top management and the Information Security Department in organisations in ensuring data protection, especially while handling the customers' and other third party data.

Reasonable Security Practices

- Site certification
- Security initiatives
- Awareness Training
- Conformance to Standards, certification
- Policies and adherence to policies
- Policies like password policy, Access Control, email Policy etc
- Periodic monitoring and review.

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules have since been notified by the Government of India, Dept. of I.T. on 11 April 2011. Anybody corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies containing managerial, technical, operational and physical security control measures commensurate with the information assets being protected with the nature of business. In the event of an information

security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies. The international Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).

In view of the foregoing, it has now become a major compliance issue on the part of not only IT companies but also those in the Banking and Financial Sector especially those banks with huge computerised operations dealing with public data and depending heavily on technology. In times of a litigation or any security breach resulting in a claim of compensation of financial loss amount or damages, it would be the huge responsibility on the part of those body corporate to prove that that said “Reasonable Security Practices and Procedures” were actually in place and all the steps mentioned in the Rules passed in April 2011 stated above, have been taken.

In the near future, this is one of the sections that is going to create much noise and be the subject of much debates in the event of litigations, like in re-defining the role of an employee, the responsibility of an employer or the top management in data protection and issues like the actual and vicarious responsibility, the actual and contributory negligence of all stake holders involved etc.

The issue has wider ramifications especially in the case of a cloud computing scenario (the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server, with the services managed by the provider sold on demand, for the amount of time used) where more and more organisations handle the data of others and the information is stored elsewhere and not in the owners’ system. Possibly, more debates will emanate on the question of information owners vis a vis the information container and the information custodians and the Service Level Agreements of all parties involved will assume a greater significance.

Adjudication: Having dealt with civil offences, the Act then goes on to describe civil remedy to such offences in the form of adjudication without having to resort to the procedure of filing a complaint with the police or other investigating agencies. Adjudication powers and procedures have been elaborately laid down in Sections 46 and thereafter. The Central Government may appoint any officer not below the rank of a director to the Government of India or a state Government as the adjudicator. The I.T. Secretary in any state is normally the nominated Adjudicator for all civil offences arising out of data thefts and resultant losses in the particular state. If at all one section can be criticized to be absolutely lacking in popularity in the IT Act, it is this provision. In the first ten years of existence of the ITA, there have been only a very few applications made in the nation, that too in the major metros almost all of which are under different stages of judicial process and adjudications have been obtained in possibly less than five cases. The first adjudication obtained under this provision was in Chennai, Tamil Nadu, in a case involving ICICI Bank in which the bank was told to compensate the applicant with the amount wrongfully debited in Internet Banking, along with cost and damages. in April 2010.

This section should be given much popularity and awareness should be spread among the public especially the victims of cyber-crimes and data theft that such a procedure does exist without recourse to going to the police and filing a case. It is time the state spends some time and thought in enhancing awareness on the provision of adjudication for civil offences in cyber litigations like data theft etc so that the purpose for which such useful provisions have been made, are effectively utilized by the litigant public.

There is an appellate procedure under this process and the composition of Cyber Appellate Tribunal at the national level, has also been described in the Act. Every adjudicating officer has the powers of a civil court and the Cyber Appellate Tribunal has the powers vested in a civil court under the Code of Civil Procedure. After discussing the procedures relating to appeals and the duties and powers of Cyber Appellate Tribunal, the Act moves to the actual criminal acts that come under the broader definition of cybercrimes. It would be pertinent to note that the Act only lists some of the cybercrimes, (without defining a cybercrime) and stipulates the punishments for such offences. The criminal provisions of the IT Act and those dealing with cognizable offences and criminal acts follow from Chapter IX titled "Offences".

Section 65: Tampering with source documents is dealt with under this section. Concealing, destroying, altering any computer source code when the same is required to be kept or maintained by law is an offence punishable with three years imprisonment or two lakh rupees or with both. Fabrication of an electronic record or committing forgery by way of interpolations in CD produced as evidence in a court (***Bhim Sen Garg vs State of Rajasthan and others,*** 2006, Cri LJ, 3463, Raj 2411) attract punishment under this Section. Computer source code under this Section refers to the listing of programmes, computer commands, design and layout etc. in any form.

Section 66: Computer related offences are dealt with under this Section. Data theft stated in Section 43 is referred to in this Section. Whereas it was a plain and simple civil offence with the remedy of compensation and damages only, in that Section, here it is the same act but with a criminal intention thus making it a criminal offence. The act of data theft or the offence stated in Section 43 if done dishonestly or fraudulently becomes a punishable offence under this Section and attracts imprisonment upto three years or a fine of five lakh rupees or both. Earlier hacking was defined in Sec 66 and it was an offence.

Now after the amendment, data theft of Sec 43 is being referred to in Sec 66 by making this section more purposeful and the word 'hacking' is not used. The word 'hacking' was earlier called a crime in this Section and at the same time, courses on 'ethical hacking' were also taught academically. This led to an anomalous situation of people asking how an illegal activity be taught academically with a word 'ethical' prefixed to it. Then can there be training programmes, for instance, on "Ethical burglary", "Ethical Assault" etc. say for courses on physical defence? This tricky situation was put an end to, by the ITAA when it re-phrased the Section 66 by mapping it with the civil liability of Section 43 and removing the word 'Hacking'. However the act of hacking is still certainly an offence as per this Section, though some experts interpret 'hacking' as generally for good purposes (obviously to facilitate naming of the courses as ethical hacking) and 'cracking' for illegal purposes. It would be relevant to note that the technology involved in both is the same and the act is the same, whereas in 'hacking' the owner's consent is obtained or assumed and the latter act 'cracking' is perceived to be an offence.

Thanks to ITAA, Section 66 is now a widened one with a list of offences as follows:

66A Sending offensive messages through communication service, causing annoyance etc through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment upto three years or fine.**(which has now been held unconstitutional in the *Shreya Singhal vs. UOI [2015])*.**

66B: Dishonestly receiving stolen computer resource or communication device with punishment upto three years or one lakh rupees as fine or both.

66C: Electronic signature or other identity theft like using others' password or electronic signature etc. Punishment is three years imprisonment or fine of one lakh rupees or both.

66D Cheating by personation using computer resource or a communication device shall be punished with imprisonment of either description for a term which extend to three years and shall also be liable to fine which may extend to one lakh rupee.

66E Privacy violation – Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both.

66F Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization. Acts of causing a computer contaminant (like virus or Trojan Horse or other spyware or malware) likely to cause death or injuries to persons or damage to or destruction of property etc. come under this Section. Punishment is life imprisonment.

It may be observed that all acts under S.66 are cognizable and non-bailable offences. Intention or the knowledge to cause wrongful loss to others i.e., the existence of criminal intention and the evil mind i.e., concept of *mens rea,* destruction, deletion, alteration or diminishing in value or utility of data are all the major ingredients to bring any act under this Section.

To summarize, what was civil liability with entitlement for compensations and damages in Section 43, has been referred to here, if committed with criminal intent, making it a criminal liability attracting imprisonment and fine or both.

Section 67 deals with publishing or transmitting obscene material in electronic form. The earlier Section in ITA was later widened as per ITAA 2008 in which child pornography and retention of records by intermediaries were all included.

Publishing or transmitting obscene material in electronic form is dealt with here. Whoever publishes or transmits any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely to read the matter contained in it, shall be punished with first conviction for a term upto three years and fine of five lakh rupees and in second conviction for a term of five years and fine of ten lakh rupees or both.

This Section is of historical importance since the landmark judgment in what is considered to be the first ever conviction under I.T. Act 2000 in India, was obtained in this Section in the famous case *"State of Tamil Nadu vs Suhas Katti"* on 5 November 2004 (discussed in detail below).

The strength of the Section and the reliability of electronic evidences were proved by the prosecution and conviction was brought about in this case, involving sending obscene message in the name of a married women amounting to cyber stalking, email spoofing and the criminal activity stated in this Section.

Section 67-A deals with publishing or transmitting of material containing sexually explicit act in electronic form. Contents of Section 67 when combined with the material containing sexually explicit material attract penalty under this Section.

Child Pornography has been exclusively dealt with under Section 67B. Depicting children engaged in sexually explicit act, creating text or digital images or advertising or promoting such material depicting children in obscene or indecent manner etc., or facilitating abusing children online or inducing children to online relationship with one or more children etc., come under this Section. 'Children' means persons who have not completed 18 years of age, for the purpose of this Section. Punishment for the first conviction is imprisonment for a maximum of five years and fine of ten lakh rupees and in the event of subsequent conviction with imprisonment of seven years and fine of ten lakh rupees.

Bonafide heritage material being printed or distributed for the purpose of education or literature etc are specifically excluded from the coverage of this Section, to ensure that printing and distribution of ancient epics or heritage material or pure academic books on education and medicine are not unduly affected.

Screening videographs and photographs of illegal activities through Internet all come under this category, making pornographic video or MMS clippings or distributing such clippings through mobile or other forms of communication through the Internet fall under this category.

Section 67C fixes the responsibility to intermediaries that they shall preserve and retain such information as may be specified for such duration and in such manner as the Central Government may prescribe. Non-compliance is an offence with imprisonment upto three years or fine.

Transmission of electronic message and communication:

Section 69: This is an interesting section in the sense that it empowers the Government or agencies as stipulated in the Section, to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource, subject to compliance of procedure as laid down here. This power can be exercised if the Central Government or the State Government, as the case may be, is satisfied that it is necessary or expedient in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence. In any such case too, the necessary procedure as may be prescribed, is to be followed and the reasons for

taking such action are to be recorded in writing, by order, directing any agency of the appropriate Government. The subscriber or intermediary shall extend all facilities and technical assistance when called upon to do so.

Section 69A inserted in the ITAA, vests with the Central Government or any of its officers with the powers to issue directions for blocking for public access of any information through any computer resource, under the same circumstances as mentioned above. Section 69B discusses the power to authorise to monitor and collect traffic data or information through any computer resource.

Commentary on the powers to intercept, monitor and block websites:

In short, under the conditions laid down in the Section, power to intercept, monitor or decrypt does exist. It would be interesting to trace the history of telephone tapping in India and the legislative provisions (or the lack of it?) in our nation and compare it with the powers mentioned here. Until the passage of this Section in the ITAA, phone tapping was governed by Clause 5(2) of the Indian Telegraph Act of 1885, which said that "On the occurrence of any public emergency, or in the interest of the public safety, the Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order". Other sections of the act mention that the government should formulate "precautions to be taken for preventing the improper interception or disclosure of messages". There have been many attempts, rather many requests, to formulate rules to govern the operation of Clause 5(2). But ever since 1885, no government has formulated any such precautions, maybe for obvious reasons to retain the spying powers for almost a century.

A writ petition was filed in the Supreme Court in 1991 by the ***People's Union for Civil Liberties, challenging the constitutional validity of this Clause 5(2).*** The petition argued that it infringed the constitutional right to freedom of speech and expression and to life and personal liberty. In December 1996, the Supreme Court delivered its judgment, pointing out that "unless a public emergency has occurred or the interest of public safety demands, the authorities have no jurisdiction to exercise the powers" given them under 5(2). They went on to define them thus: a public emergency was the "prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action", and public safety "means the state or condition of freedom from danger or risk for the people at large". Without those two, however "necessary or expedient", it could not do so. Procedures for keeping such records and the layer of authorities etc were also stipulated.

Now, this Section 69 of ITAA is far more intrusive and more powerful than the above-cited provision of Indian Telegraph Act 1885. Under this ITAA Section, the nominated Government official will be able to listen in to all phone calls, read the SMSs and emails, and monitor the websites that one visited, subject to adherence to the prescribed procedures and

without a warrant from a magistrate's order. In view of the foregoing, this Section was critizised to be draconian vesting the government with much more powers than required.

Having said this, we should not be oblivious to the fact that this power (of intercepting, monitoring and blocking) is something which the Government represented by the Indian Computer Emergency Response Team, (the National Nodal Agency, as nominated in Section 70B of ITAA) has very rarely exercised. Perhaps believing in the freedom of expression and having confidence in the self-regulative nature of the industry, the CERT-In has stated that these powers are very sparingly (and almost never) used by it.

Critical Information Infrastructure and Protected System have been discussed in Section 70. The Indian Computer Emergency Response Team (CERT-In) coming under the Ministry of Information and Technology, Government of India, has been designated as the National Nodal Agency for incident response. By virtue of this, CERT-In will perform activities like collection, analysis and dissemination of information on cyber incidents, forecasts and alerts of cyber security incidents, emergency measures for handling cyber security incidents etc.

The role of CERT-In in e-publishing security vulnerabilities and security alerts is remarkable. The Minister of State for Communications and IT Mr.Sachin Pilot said in a written reply to the Rajya Sabha said that (as reported in the Press), CERT-In has handled over 13,000 such incidents in 2011 compared to 8,266 incidents in 2009. CERT-In has observed that there is significant increase in the number of cyber security incidents in the country. A total of 8,266, 10,315 and 13,301 security incidents were reported to and handled by CERT-In during 2009, 2010 and 2011, respectively," These security incidents include website intrusions, phishing, network probing, spread of malicious code like virus, worms and spam, he added. Hence the role of CERT-In is very crucial and there are much expectations from CERT In not just in giving out the alerts but in combating cybercrime, use the weapon of monitoring the web-traffic, intercepting and blocking the site, whenever so required and with due process of law.

Penalty for breach of confidentiality and privacy is discussed in Section 72 with the punishment being imprisonment for a term upto two years or a fine of one lakh rupees or both.

Considering the global nature of cybercrime and understanding the real time scenario of fraudster living in one part of the world and committing a data theft or DoS (Denial of Service) kind of an attack or other cybercrime in an entirely different part of the world, Section 75 clearly states that the Act applies to offences or contravention committed outside India, if the contravention or the offence involves a computer or a computer network located in India.

This Act has over-riding provisions especially with regard to the regulations stipulated in the Code of Criminal Procedure. As per Section 78, notwithstanding anything contained in the Code of Criminal Procedure, a police officer not below the rank of an Inspector shall investigate an offence under this Act. Such powers were conferred to officers not below the rank of a Deputy Superintendent of Police earlier in the ITA which was later amended as Inspector in the ITAA.

Due Diligence: Liability of intermediaries and the concept of Due Diligence has been discussed in Section 79. As per this, intermediary shall not be liable for any third party information hosted by him, if his function is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted or if he does not initiate the transmission, select the receiver of the transmission and select or modify the information contained in the transmission and if he observes due diligence and follows the guidelines prescribed by the Central Government.

This concept of due diligence is also much being debated. Due Diligence was first discussed as an immediate fallout of the famous bazee.com case in New Delhi, when the NRI CEO of the company was arrested for making the MMS clipping with objectionable obscene material depicting school children was made available in the public domain website owned by him, for sale (and later the CD was sold). The larger issue being discussed at that time was how far is the content provider responsible and how far the Internet Service Provider and what is due diligence which as the CEO of the company, he should have exercised.

After passage of the ITAA and the introduction of 'reasonable security practices and procedures' and the responsibility of body corporate as seen earlier in Section 43A, and to set at rest some confusion on the significance of due diligence and what constitutes due diligence, the DIT came out with a set of rules titled Information Technology (Intermediaries Guidelines) Rules on 11 April 2011. As per this, "the intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes….."

In essence, an intermediary shall be liable for any contravention of law committed by any user unless the Intermediary can prove that he has exercised due diligence and has not conspired or abetted in the act of criminality.

Power to enter, search etc., has been described in Section 80. Notwithstanding anything contained in the Code of Criminal Procedure, any police officer, not below the rank of an Inspector or any other officer ….authorized ….may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act. This is another effective weapon that has been rarely and almost never utilized by the police officers.

The Act is applicable to electronic cheques and truncated cheques (ie the image of cheque being presented and processed curtailing and truncating the physical movement of the cheque from the collecting banker to the paying banker).

Overriding powers of the Act and the powers of Central Government to make rules and that of State Governments to make rules wherever necessary have been discussed in the Sections that follow.

The Indian Penal Code, 1860: Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended many time since, it covers almost all substantive aspects of criminal law and is supplemented by other criminal provisions. In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well.

ITA 2000 has amended the sections dealing with records and documents in the IPC by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (eg 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc.,) have since been amended as electronic record and electronic document thereby bringing within the ambit of IPC, all crimes to an electronic record and electronic documents just like physical acts of forgery or falsification of physical records.

In practice, however, the investigating agencies file the cases quoting the relevant sections from IPC in addition to those corresponding in ITA like offences under IPC 463,464, 468 and 469 read with the ITA/ITAA Sections 43 and 66, to ensure the evidence or punishment stated at least in either of the legislations can be brought about easily.

Indian Evidence Act, 1872: The Indian Evidence Act 1872: This is another legislation amended by the ITA. Prior to the passing of ITA, all evidences in a court were in the physical form only. With the ITA giving recognition to all electronic records and documents, it was but natural that the evidentiary legislation in the nation be amended in tune with it. In the definitions part of the Act itself, the "all documents including electronic records" were substituted. Words like 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations.

Admissibility of electronic records as evidence as enshrined in *Section 65B* of the Act assumes significance. This is an elaborate section and a landmark piece of legislation in the area of evidences produced from a computer or electronic device. Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied: (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly.... by lawful persons.. (b) the information ...derived was regularly fed into the computer in the ordinary course of the said activities; (c) throughout the material part of the said period, the computer was operating properly ..... and .....a certificate signed by a person .....responsible..... etc.

To put it in simple terms, evidences (information) taken from computers or electronic storage devices and produced as print-outs or in electronic media are valid if they are taken from system handled properly with no scope for manipulation of data and ensuring integrity of data produced directly with or without human intervention etc., and accompanied by a certificate signed by a responsible person declaring as to the correctness of the records taken from a system a computer with all the precautions as laid down in the Section.

However, this Section is often being misunderstood by one part of the industry to mean that computer print-outs can be taken as evidences and are valid as proper records, even if they are not signed. We find many computer generated letters emanating from big corporates with proper space below for signature under the words "Your faithfully" or "truly" and the signature space left blank, with a Post Script remark at the bottom "This is a computer generated letter and hence does not require signature". The Act does not anywhere say that 'computer print-outs need not be signed and can be taken as record'.

The Bankers' Books Evidence (BBE) Act, 1891: Before passing of ITA, a bank was supposed to produce the original ledger or other physical register or document during evidence before a Court. After enactment of ITA, the definitions part of the BBE Act stood amended as "bankers' books' include ledgers, day-books, cash books, account books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device". The above amendment in the provisions in BBE Act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided, such print-out or electronic document is accompanied by a certificate in terms as mentioned above.

Digital signatures have been accorded legal acceptance by the I.T. Act. The Controller of Certifying Authorities, set up to implement the IT Act, has issued licences to four players who can issue digital signatures. These are Safescrypt Limited, National Informatics Centre (NIC), Institute for Development and Research in Banking Technology (IDRBT) and Tata Consultancy Services (TCS).

Later, in July 2001, a set of laws known as the Information Technology (Certifying Authority) Regulations, 2001 were issued by the Government of India. These regulations detail the functioning of the certifying authorities in issuing digital signatures. These rules specify the manner in which information has to be authenticated by means of digital signatures, the creation and verification of digital signatures, licensing of certification authorities and the terms of the proposed licenses to issue digital signatures.

Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence:

Parallel Provisions in the IPC and IT Act: Many of the cyber-crimes penalised by the IPC and the IT Act have the same ingredients and even nomenclature. Here are a few examples:

Hacking and Data Theft: Sections 43 and 66 of the IT Act penalise a number of activities ranging from hacking into a computer network, data theft, introducing and spreading viruses through computer networks, damaging computers or computer networks or computer programmes, disrupting any computer or computer system or computer network, denying an authorised person access to a computer or computer network, damaging or destroying information residing in a computer etc. The maximum punishment for the above offences is imprisonment of up to 3 (three) years or a fine or Rs. 5,00,000 (Rupees five lac) or both.

Section 378 of the IPC relating to "theft" of movable property will apply to the theft of any data, online or otherwise, since section 22 of the IPC states that the words "movable property" are intended to include corporeal property of every description, except land and

things attached to the earth or permanently fastened to anything which is attached to the earth. The maximum punishment for theft under section 378 of the IPC is imprisonment of up to 3 (three) years or a fine or both.

It may be argued that the word "corporeal" which means 'physical' or 'material' would exclude digital properties from the ambit of the aforesaid section 378 of the IPC. The counter argument would be that the drafters intended to cover properties of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

Section 424 of the IPC states that "*whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment of either description*[1] *for a term which may extend to 2 (two) years, or with fine, or with both.*" This aforementioned section will also apply to data theft. The maximum punishment under section 424 is imprisonment of up to 2 (two) years or a fine or both.

Section 425 of the IPC deals with mischief and states that "*whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits mischief*". Needless to say, damaging computer systems and even denying access to a computer system will fall within the aforesaid section 425 of the IPC. The maximum punishment for mischief as per section 426 of the IPC is imprisonment of up to 3 (three) months or a fine or both.

Receipt of stolen property: Section 66B of the IT Act prescribes punishment for dishonestly receiving any stolen computer resource or communication device. This section requires that the person receiving the stolen property ought to have done so dishonestly or should have reason to believe that it was stolen property. The punishment for this offence under Section 66B of the IT Act is imprisonment of up to 3 (three) years or a fine of up to Rs. 1,00,000 (Rupees one lac) or both.

Section 411 of the IPC too prescribes punishment for dishonestly receiving stolen property and is worded in a manner that is almost identical to section 66B of the IT Act. The punishment under section 411 of the IPC is imprisonment of either description for a term of up to 3 (three) years, or with fine, or with both. Please note that the only difference in the prescribed punishments is that under the IPC, there is no maximum cap on the fine.

Identity theft and cheating by personation: Section 66C of the IT Act prescribes punishment for identity theft and provides that anyone who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

Section 66D of the IT Act prescribes punishment for 'cheating by personation by using computer resource' and provides that any person who by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

Section 419 of the IPC also prescribes punishment for 'cheating by personation' and provides that any person who cheats by personation shall be punished with imprisonment of either description for a term which may extend to 3 (three) years or with a fine or with both. A person is said to be guilty of 'cheating by personation' if such person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.

The provisions of sections 463, 465 and 468 of the IPC dealing with forgery and "forgery for the purpose of cheating", may also be applicable in a case of identity theft. Section 468 of the IPC prescribes punishment for forgery for the purpose of cheating and provides a punishment of imprisonment of either description for a term which may extend to 7 (seven) years and also a fine. Forgery has been defined in section 463 of the IPC to mean the making of a false document or part thereof with the intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed.

In this context, reference may also be made to section 420 of the IPC that provides that any person who cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security shall be punished with imprisonment of either description for a term which may extend to 7 (seven) years, and shall also be liable to fine.

The only difference between the punishments prescribed under sections 66C and 66D of the IT Act and section 419 of the IPC is that there is no maximum cap on the fine prescribed under the IPC. However, the punishment under section 468 is much higher in that the imprisonment mat extend to 7 (seven) years. Further, whilst the IT Act contemplates both the imposition of a fine and imprisonment, the IPC uses the word 'or' indicating that the offence could be punished with imprisonment or by imposing a fine. Most importantly, the fundamental distinction between the IPC and the IT Act in relation to the offence of identity theft is that the latter requires the offence to be committed with the help of a computer resource.

Obscenity: Sections 67, 67A and 67B of the IT Act prescribe punishment for publishing or transmitting, in electronic form: (i) obscene material; (ii) material containing sexually explicit act, etc.; and (iii) material depicting children in sexually explicit act, etc. respectively. The punishment prescribed for an offence under section 67 of the IT Act is, on the first conviction, imprisonment of either description for a term which may extend to 3 (three) years, to be accompanied by a fine which may extend to Rs. 5,00,000 (Rupees five lac), and in the event of a second or subsequent conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which

may extend to Rs. 10,00,000 (Rupees ten lac). The punishment prescribed for offences under sections 67A and 67B of the IT Act is on first conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac) and in the event of second or subsequent conviction, imprisonment of either description for a term which may extend to 7 (seven) years and also with fine which may extend to Rs. 10,00,000 (Rupees ten lac).

The provisions of sections 292 and 294 of the IPC would also be applicable for offences of the nature described under sections 67, 67A and 67B of the IT Act. Section 292 of the IPC provides that any person who, inter alia, sells, distributes, publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 2 (two) years, and with fine which may extend to Rs. 2,000 (Rupees two thousand) and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 5,000 (Rupees five thousand).

Section 294 of the IPC provides that any person who, to the annoyance of others, does any obscene act in any public place, or sings, recites or utters any obscene song, ballad or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to 3 (three) months, or with fine, or with both.

Cyber-crimes not provided for in the IPC

The following cyber-crimes penalised by the IT Act do not have an equivalent in the IPC.

Section 43(h) of the IT Act: Section 43(h) read with section 66 of the IT Act penalises an individual who charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network. A person who tampers with the computer system of an electricity supplier and causes his neighbour to pay for his electricity consumption would fall under the aforesaid section 43(h) of the IT Act for which there is no equivalent provision in the IPC.

Section 65 of the IT Act: Section 65 of the IT Act prescribes punishment for tampering with computer source documents and provides that any person who knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code (i.e. a listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form) used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment for up to 3 (three) years or with a fine which may extend to Rs. 3,00,000 (Rupees lac) or with both.

To a certain extent, section 409 of the IPC overlaps with section 65 of the IT Act. Section 409 of the IPC provides that any person who is in any manner entrusted with property, or with any dominion over property in his capacity as a public servant or in the way of his business as a banker, merchant, factor, broker, attorney or agent, commits criminal breach of

trust in respect of that property, shall be punished with imprisonment for life or with imprisonment of either description for a term which may extend to 10 (ten) years, and shall also be liable to a fine. However, section 65 of the IT Act does not require that the person who tampers with or damages or destroys computer source documents should have been entrusted with such source code. Under section 409 of the IPC, criminal breach of trust should have been committed by someone to whom the property was entrusted.

Violation of privacy: Section 66E of the IT Act prescribes punishment for violation of privacy and provides that any person who intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to 3 (three) years or with fine not exceeding Rs. 2,00,000 (Rupees two lac) or with both.

There is no provision in the IPC that mirrors Section 66E of the IT Act, though sections 292 and 509 of the IPC do cover this offence partially.

Section 292 of the IPC has been discussed above. Section 509 of the IPC provides that if any person intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, such person shall be punished with simple imprisonment for a term which may extend to 1 (one) year, or with fine, or with both. Unlike section 66E of the IT Act which applies to victims of both genders, section 509 of the IPC applies only if the victim is a woman.

Section 67C of the IT Act: Section 67C of the IT Act requires an 'intermediary' to preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. The section further provides that any intermediary who intentionally or knowingly contravenes this requirement shall be punished with imprisonment for a term which may extend to 3 (three) years and also be liable to a fine. An 'intermediary' with respect to any particular electronic record, has been defined in the IT Act to mean any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes. There is no corresponding provision in the IPC.

Cyber terrorism: Section 66F of the IT Act prescribes punishment for cyber terrorism. Whoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people, denies or causes the denial of access to any person authorized to access a computer resource, or attempts to penetrate or access a computer resource without authorisation or exceeding authorised access, or introduces or causes the introduction of any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect critical information infrastructure, is guilty of 'cyber terrorism'. Whoever knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of

such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, is also guilty of 'cyber terrorism'.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

There is no provision in the IPC that mirrors section 66F of the IT Act, though section 121 of the IPC (waging, or attempting to wage war, or abetting waging of war, against the Government of India) does cover this offence partially.

Whether Compoundable, Cognizable and Bailable

Section 77A of the IT Act provides that, subject to certain exceptions, all offences under the IT Act for which the punishment is imprisonment for a term of 3 (three) years or less, are compoundable. The provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 ("CrPC") shall apply with respect to such compounding.

Section 77B of the IT Act provides that notwithstanding anything contained in the CrPC, all offences punishable with imprisonment of 3 (three) years and above under the IT Act shall be cognizable and all offences punishable with imprisonment of 3 (three) years or less shall be bailable.

Most of the cyber-crimes covered under the IT Act are punishable with imprisonment of 3 (three) years or less. The cyber-crimes which are punishable with imprisonment of more than 3 (three) years are:

i. publishing or transmitting obscene material in electronic form under section 67 of the IT Act;
ii. publishing or transmitting of material containing sexually explicit act, etc., in electronic form under section 67A of the IT Act;
iii. publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form under section 67B of the IT Act; and
iv. cyber terrorism under section 66F of the IT Act.

All of the cyber-crimes under the IPC are bailable other than offences under section 420 (cheating and dishonestly inducing delivery of property), section 468 (forgery for the purpose of cheating), section 411 (dishonestly receiving stolen property), section 378 (theft) and section 409 (criminal breach of trust by public servant, or by banker, merchant or agent), which are non-bailable.

Offences under sections 463 and 465 (forgery), sections 425 and 426 (mischief), section 468 (forgery for the purpose of cheating), section 469 (forgery for the purpose of harming reputation) and section 292 (sale, etc., of obscene books, etc.) of the IPC are non-

compoundable offences while offences under sections 378 and 379 (theft), 420 (cheating and dishonestly inducing delivery of property), sections 425 and 426 (mischief when the only loss or damage caused is loss or damage to a private person), section 509 (word, gesture or act intended to insult the modesty of a woman), section 411 (Dishonestly receiving stolen property) and section 419 (Punishment for cheating by personation) of the IPC are compoundable offences. Of these, offences under sections 420 and 509 can be compounded only with the permission of the court. Most of the cyber-crimes under the IPC are cognizable other than the offences under sections 425 and 426 (mischief) and sections 463 and 465 (forgery) which are non-cognizable.

The overlap between the provisions of the IPC and the IT Act may sometimes lead to an anomalous situation wherein certain offences are bailable under the IPC and not under the IT Act and vice versa and certain offences are compoundable under the IPC and not under the IT Act and vice versa. For instance, in case of hacking and data theft, offences under sections 43 and 66 of the IT Act that are bailable and compoundable while offences under section 378 of the IPC are non-bailable and offences under section 425 of the IPC are non-compoundable. Further, in case of the offence of receipt of stolen property, the offence under section 66B of the IT Act is bailable while the offence under section 411 of the IPC is non-bailable. Similarly, in case of the offence of identity theft and cheating by personation, the offences under sections 66C and 66D of the IT Act are compoundable and bailable while the offences under sections 463, 465 and 468 of the IPC are non-compoundable and the offences under sections 468 and 420 of the IPC are non-bailable. Finally, in case of obscenity, the offences under sections 67, 67A and 67B of the IT Act are non-bailable while the offences under section 292 and 294 of the IPC are bailable. This issue has been dealt with by the Bombay High Court in the case of Gagan Harsh Sharma v. The State of Maharashtra2 (discussed below) wherein offences under sections 408 and 420 of the IPC that are non-bailable and cannot be compounded other than with the permission of the court were in conflict with offences under sections 43, 65 and 66 of the IT Act that are bailable and compoundable.

Conflict between the IPC and the IT Act: Case Law: In the case of ***Sharat Babu Digumarti v. Government of NCT of Delhi***, the conflict between provisions of the IPC and the IT Act came to the fore. In this case, on November 27, 2004, an obscene video had been listed for sale on baazee.com ("Bazee"). The listing was intentionally made under the category 'Books and Magazines' and sub-category 'ebooks' in order to avoid its detection by the filters installed by Baazee. A few copies were sold before the listing was deactivated. Later Delhi police's crime branch gave charge-sheet Avinash Bajaj, Bazee's managing director and Sharat Digumarti, Bazee's manager. The company Bazee was not arraigned as an accused and this helped Avinash Bajaj get off the hook since it was held that, vicarious liability could not be fastened on Avinash Bajaj under either section 292 of the IPC or section 67 of the IT Act when Avinash's employer Bazee itself was not an accused. Later changes under section 67 of the IT Act and section 294 of IPC against Sharat Digumarti were also dropped, but the charges under section 292 of the IPC were retained. The Supreme Court then considered if, after the charges under section 67 of the IT Act was dropped, a charge under section 292 of the IPC could be sustained.

The Supreme Court quashed the proceedings against Sarat Digumarti and ruled that if an offence involves an electronic record, the IT Act alone would apply since such was the legislative intent. It is a settled principle of interpretation that special laws would prevail over general laws and latter laws would prevail over prior legislation. Further, section 81 of the IT Act states that the provisions of the IT Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

In the case of ***Gagan Harsh Sharma v. The State of Maharashtra***, certain individuals were accused of theft of data and software from their employer and charged under sections 408 and 420 of the IPC and also under sections 43, 65 and 66 of the IT Act. All of these sections, other than section 408 of the IPC, have been discussed above. Section 408 of the IPC deals with criminal breach of trust by clerk or servant and states that "whoever, being a clerk or servant or employed as a clerk or servant, and being in any manner entrusted in such capacity with property, or with any dominion over property, commits criminal breach of trust in respect of that property, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine".

Offences under sections 408 and 420 of the IPC are non-bailable and cannot be compounded other than with the permission of the court. Offences under sections 43, 65 and 66 of the IT Act are bailable and compoundable. Therefore, the petitioners pleaded that the charges against them under the IPC be dropped and the charges against them under the IT Act be investigated and pursued. It was further argued that if the Supreme Court's ruling in Sharat Babu Digumarti were to be followed, the petitioners could only be charged under the IT Act and not under the IPC, for offences arising out of the same actions.

The Bombay High Court upheld the contentions of the petitioners and ruled that the charges against them under the IPC be dropped

A Suitable Home for Cyber Offences: We currently have a situation where a number of offences are penalised by both the IPC and the IT Act, even though the ingredients of both offences are the same. There are subtle differences in punishments under these statutes, especially in aspects like whether the offence is bailable or compoundable or cognizable. An offence such as obscenity may take place through different types of media, both online or offline. However, it could result in unfairness if 2 (two) different statutes apply to the same offence on the basis of the media used.

The sum and substance of the Supreme Court's ruling in the Sharat Babu Digumarti case is that no individual may be charged under the IPC for an offence arising out of certain acts or omissions if the IT Act could also be applied to the same acts or omissions. Though we are in full agreement with the Supreme Court's ruling, it is our contention that all cyber offences ought to be housed in the IPC and not in the IT Act. The "cyber" component of an offence is not sufficient reason for differential treatment of sub-categories of the offence. Even though the supreme court's ruling in the Sharat Babu Digumarti case has ensured that no individual may be charged under the IPC for an offence arising out of certain acts or omissions if the IT Act could also be applied to the same acts or omissions, it is a fact that offences such as theft and obscenity will be punished differently if they involve a 'cyber' element. Currently, an individual who distributes a hard copy book containing obscene materials will be punished under the IPC whilst an individual who distributes obscene materials through the internet will

be punished under the IT Act, though the underlying offence is the same. A person who steals a car will be punished under the IPC whilst an individual who indulges in theft of online data will be punished under the IT Act.

Theft is theft, irrespective of whether the stolen property is digital or physical. Obscenity transmitted through the internet should be treated at par with obscenity which is transmitted offline.

IPC's treatment of stalking: The legislature's treatment of the offence of "stalking", accomplished through the insertion of new section 354D in the IPC through the Criminal Law (Amendment) Act, 20135, is a case in point. Section 354D penalises the offence of "stalking" whether it has a cyber component or not. If a man follows a woman and contacts, or attempts to contact, such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman, it amounts to stalking. If a man monitors the use by a woman of the internet, email or any other form of electronic communication, it will also result in the offence of stalking. There are a few exemptions to this offence of stalking, and all the defences apply irrespective of whether the stalking is cyber stalking or not. The punishment prescribed for stalking by Section 354D of the IPC does not discriminate on the basis of the presence or absence of the "cyber" component.

Bad and ill-thought out drafting: Article 14 of the Constitution of India, 1950 ("Constitution") states that the State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India. It is not our contention that the current state of affairs results in a per se violation of Article 14 of the Constitution even though it has created an unhappy state of affairs. The legislature does have the freedom to make specific laws for specific matters or situations. However, the docking of cyber-crimes in the IT Act does not appear to have been well thought through.

When the IT Act was enacted, its focus was on putting in place technology law fundamentals like digital signatures, providing legal recognition for electronic documents and the like. Its preamble stated that its objective was to "*provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.*"[11]

Even though the IT Act penalised cyber-crimes with a broad brush through sections 43, 66 and 67, it was only in 2008 that the IT Act was amended[12] and provisions were made for specific cyber-crimes such as sending offensive messages through communication servers, dishonestly receiving a stolen computer resource or communication device, identity theft, violation of privacy, cyber terrorism etc. through sections 66A to 66F and sections 67A to 67C. These amendments stick out like an unwieldy appendage.

Therefore, it is submitted that all cyber offences in the IT Act ought to be repealed and the IPC be suitably modified (to cover all of the cyber-crimes, including those currently covered under the IT Act) at the earliest possible convenience of the legislature.

UNCITRAL model and Impact of Technology Act: The I.T. Act, 2000 is based on the United Nations Commission on International Trade Law (UNCITRAL) to which India is a signatory member. The working of the Act in subsequent years brought to light certain lacunae and short comings inherent therein which obstructed its smooth operation and therefore it was amended in 2002 and again amended in 2006 and later on in 2008, where it received the president's assent on 5thFebruary, 2009 to be enforced as the I.T. (Amendment) Act of 2008. The amended Act seeks to plug the loopholes in the existing Information Technology law so as to make it more effective.

The UNCITRAL Model was created by the General Assembly of the United Nations in December 1996, by passing a resolution, in order to streamline, harmonize and unify the law of International Trade. Some inadequacies and impediments had crept in the law affecting trade and it was felt necessary to remove those short comings. A Draft model Law was prepared for feedback from International Organization. This was created by the United Nations Commission on International Trade Law (UNCITRAL). It was created to bear in mind the interest of all people. This was to develop international trade by adopting different Model Laws.

After examination of the comments of various governments the commission adopted the text of the Model Law at its 605th meeting on 12th June 1996. Earlier in India there existed no law to regulate information and business transacted through electronic form. There existed a steep increase in the use of computers for business and various commercial transactions through electronic records. A resolution was passed and adopted by The United Nations General Assembly by resolution on 30 January 1997, according to the Model Law on E-Commerce. This is based on United Nations Commission on International Trade Law. This is referred to as the UNCITRAL Model Law on E-Commerce. As per the UN Resolution, India made the Information Technology Act, 2000, in May 2000. In May that year the Indian Parliament passed The I.T. Bill. This received the assent of the president in August 2000. All the Cyber provisions are stated in the IT Act, 2000.

Need of Today: The goal of any country is to codify a commercial law so that it can be used across multiple political states. This can be achieved through harmonization and unification of laws. This process is difficult as it involves balancing issues and choices revolving around different social cultures and legal systems having different historical traditions. Alternatively, the various other states like USA already have homogenous attitudes with some issues. The economic systems of the USA are highly developed, as compared to many parts of the world. The disparities existing in legal traditions, cultures, and economic development make harmonization project a complex task, most particularly at the international level. However, only through such harmonization can the uniformity of law that is so crucial to support efficient and fair commercial transactions be advanced. This is achieved to a certain extent through the UNCITRAL Model.

Lacunas in the initials stages of the Act:

1. Problematic for courts to determine jurisdictional issues to bring criminals for trial.
2. Ambiguity in application of country's laws either at place of origin of crime or at place of commencement of crime/victim is located / both these laws.

In a landmark case, an internet news service was sued for trademark violation and misusing the plaintiff's domain name. The Court held that a passive website which only made information available to interested users was subject to Court's jurisdiction, unless it entered into specific contract knowingly and repeatedly transferred computer files to the plaintiff.

The Information Technology (Amendment) Act, 2008

The Information Technology (Amendment) Act, 2008 (ITAA) was passed by the two houses of the Indian Parliament on December 23 and 24, 2008 and came into effect from 27th October 2009. It has extended the scope for the law to cover a few more cyber-crimes under its ambit. The new and improved Act aims at tightening procedures and safeguards for monitoring and interception of data to prevent cyber-crimes. The Bill seeks to achieve the following objects. This Act was amended by Information Technology Amendment Bill 2006,by the Loksabha, on Dec 22nd and on 23rd December in Rajyasabha 2008.

The statement of Objects and Reasons for ITAA-2006 were laid down by Mr. Dayanidhi Maran which is given as follows:

The I.T Act 2000 incorporated legal recognition for ecommerce and e-transactions and its governance, to prevent computer crimes, to protect personal data in consonance with I.T. Act, 2000, to protect critical information.

Due to the increase in internet activity by users, new form of crimes evolved like publishing, sexually explicit materials, video voyeurism, breach of confidentiality , leakage of data by intermediary, e-commerce frauds and offensive messages through communication services. Therefore the need was felt to make appropriate amendments and incorporate penal provisions in the I.T. Act, the I.P.C, the Indian Evidence Act and the CrPC so as to prevent such crimes. The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signature for harmonization with domestic laws. The Act lays down that the state or central government can authorize service providers to provide computer facilities and to collect services charges.

*Salient Features of ITAA:*The salient features of the amended IT Act are introduction of a system of electronic signatures on par with international law; delivery of services by service provider; corporation responsibility for data protection with the concept of reasonable security practices, recognition of Computer Emergency Response Team-India (CERT-In) as the nodal agency at the national level empowered to monitor, intercept and even block websites under specific circumstances in order to deal with computer security and situations arising from cyber-attacks.

This section also means that there is no need for a complaint and *suo moto* action is possible.

Power of investment: It is generally felt that with enactment of IT Act, 2000, the realm of investigation of computer related crimes is restricted to Deputy Superintendent of Police or officers of higher rank under section 80 of I.T. Act. This was amended in IT (Amendment) Act, 2008 that the Inspector of Police can investigate the cyber -crime cases.

Section 69 empowers the Central Government/State Government/its authorized agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in

any computer resource if it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence. They can also secure assistance from computer personnel in decrypting data.

CERT-IN

Computer Emergency Response Team-India (CERT-IN) shall be the single authority for issue of instructions in the context of blocking websites. CERT-IN, after verifying the authenticity of the complaint and after satisfying that action of blocking of the website is absolutely essential, shall instruct Department of Telecommunication (DoT)-Latest Release (LR Cell) to block the website. DoT, under whose control the Internet Service Providers (ISPs) are functioning will ensure the blocking of websites and inform CERT-IN accordingly. The Director General of Police of all the State and such other enforcement agencies could approach CERT-IN. The blocking of website may be the need of several agencies engaged in different walks of public and administrative lives due to a variety of reasons. Explicit provision for blocking the website under the Information Technology Act, 2000 is available only in Section 67, relating to pornographic content on the website.

Such blocking can be challenged if it amounts to restriction of freedom of speech and expression. But websites promoting hate content, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography, and violent sex can reasonably be blocked since all such websites may not claim constitutional right of free speech. Blocking of such websites may be equated to "balanced flow of information" and not censorship.

Shortcomings of I.T. Act 2008:

1. Infringement of copyright excluded from this law.
2. Domain names lack protection
3. Power of attorney trusts and wills not covered under the Act.
4. Act is silent on taxation.
5. Electronic documents have no stamp duty.
6. No proper laws governing credit card frauds.
7. The Act did not cover all the offences.

Advantages of I.T. Act 2008

1. Promotes e-commerce

- Valid Email contacts
- Valid Digital signature
- Valid credit card payment
- Valid online communications

1. Improve business

Through issue of digital signature by the authorities authorized by the Act.

2. Filling online forms:-

Filling online forms for different purposes like promoting e-governance has made task easy for all the citizens of India.

3. High penalty

High penalty is imposed for persons doing any cybercrime due to which the rate of cybercrime has reduced.

Chapter-wise overview of the ITAA 2008:

Chapter I– It includes a series of definition as to computer network. It includes one or more computers are connected either by satellite, microwave or wire or may be wireless and by attachment of terminals.

Section 1(n) Definition of Appellate Tribunal

Section 1(na) Definition of Cyber Café facilities provided to access the internet.

Section 1(nb) Definition as to "Cyber Security" for protecting information and equipment which may be any devices.

Section 1(ta) defines electronic signature.

Section 1(tb) defines "Electronic Signature Certificate" and includes Digital Signature Certificate"

Section 1 (w) as to "Intermediary" is any person who obtains, supplies or provides any service
for service providers and makes material available on the internet.

Chapter II - Digital Signature and Electronic Signature: Section 3A - Electronic Signature is used for authentication of electronic records.

Chapter III- E – Governance **Sec 6-A –** The appropriate government authorize service providers to perform services. They may be any individual or agency. They require permission
by the government.

Sec 7-A – provides Provisions for audit of e-documents.

Section 10- Rules made as to Electronic Signature.

Sec 10-A – The validity of contracts formed through e-form which may be as to acceptance, revocation or acceptance of proposal expressed through electronic form or electronic record shall be deemed to be enforceable.

Chapter VIII Amendment as to Sec 40-A where the subscriber may perform such duties as prescribed in respect of Electronic Signatures Certificate.

Chapter IX where Section 43-A has been amended making provisions for the body corporate
accountable to pay damages by way of compensation.

Chapter X Under this chapter, Section 52-A, 52- B, 52-C, 52-D, have been inserted. It states the composition of Cyber Appellate Tribunal.

Chapter XI- Govt. can appoint cyber Committee who will be vigilant on cybercrime with respects to uploads. He is further liable if he overlooks his duty. He will be liable for 2, 00,000 rupees and 3 years jail.

Chapter XIIA - Amended chapter in the ITA -2000, it included the provision for 'Examiner of Electronic Evidence', [Section 79A]- Transferred with help of any electronic gadgets.

Chapter XIII Miscellaneous:

1. Some miscellaneous sections inserted in the ITA 2000 are as under: Section 80 Power of Police Officer and Other Officers i.e. to Enter, Search, as against mentioned in Cr.P.C, 1973),
2. Section 81 - provisions as to The Copyright Act 1957 or The Patents Act 1970.

Observations on ITA and ITAA

Having discussed in detail all the provisions of ITA and ITAA, let us now look at some of the broader areas of omissions and commissions in the Act and the general criticism the Acts have faced over the years.

Awareness: There is no serious provision for creating awareness and putting such initiatives in place in the Act. The government or the investigating agencies like the Police department (whose job has been made comparatively easier and focused, thanks to the passing of the IT Act), have taken any serious step to create public awareness about the provisions in these legislations, which is absolutely essential considering the fact that this is a new area and technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large. Especially, provisions like scope for adjudication process are never known to many including those in the investigating agencies.

Jurisdiction: This is a major issue which is not satisfactorily addressed in the ITA or ITAA. Jurisdiction has been mentioned in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected with and again in Section 80 and as part of the police officers' powers to enter, search a public place for a cybercrime etc. In the context of electronic record, Section 13 (3) and (4) discuss the place of dispatch and receipt of electronic record which may be taken as jurisprudence issues.

However some fundamental issues like if the mail of someone is hacked and the accused is a resident of a city in some state coming to know of it in a different city, which police station does he go to? If he is an employee of a Multi- National Company with branches throughout the world and in many metros in India and is often on tour in India and he suspects another individual say an employee of the same firm in his branch or headquarters office and informs

the police that evidence could lie in the suspect's computer system itself, where does he go to file he complaint. Often, the investigators do not accept such complaints on the grounds of jurisdiction and there are occasions that the judicial officers too have hesitated to deal with such cases. The knowledge that cyber-crime is geography-agnostic, borderless, territory-free and sans all jurisdiction and frontiers and happens in 'cloud' or the 'space', has to be spread and proper training is to be given to all concerned players in the field.

Evidences: Evidences are a major concern in cyber-crimes. Pat of evidences is the 'crime scene' issues. In cyber-crime, there is no cyber-crime. We cannot mark a place nor a computer nor a network, nor seize the hard-disk immediately and keep it under lock and key keep it as an exhibit taken from the crime scene.

Very often, nothing could be seen as a scene in cybercrime! The evidences, the data, the network and the related gadgets along with of course the log files and trail of events emanating or recorded in the system are actually the crime scene. While filing cases under IT Act, be it as a civil case in the adjudication process or a criminal complaint filed with the police, many often, evidences may lie in some system like the intermediaries' computers or some times in the opponent's computer system too. In all such cases, unless the police swing into action swiftly and seize the systems and capture the evidences, such vital evidences could be easily destroyed. In fact, if one knows that his computer is going to be seized, he would immediately go for destruction of evidences (formatting, removing the history, removing the cookies, changing the registry and user login set ups, reconfiguring the system files etc) since most of the computer history and log files are volatile in nature.

There is no major initiative in India on common repositories of electronic evidences by which in the event of any dispute (including civil) the affected computer may be handed over to a common trusted third party with proper software tools, who may keep a copy of the entire disk and return the original to the owner, so that he can keep using it at will and the copy will be produced as evidence whenever required. For this there are software tools like 'EnCase' with a global recognition and our own C-DAC tools which are available with much retrieval facilities, search features without giving any room for further writing and preserving the original version with date stamp for production as evidence.

Non coverage of many crimes: While there are many legislations in not only many Western countries but also some smaller nations in the East, India has only one legislation -- the ITA and ITAA. Hence it is quite natural that many issues on cybercrimes and many crimes per se are left uncovered. Many cybercrimes like cybersquatting with an evil attention to extort money. Spam mails, ISP's liability in copyright infringement, data privacy issues have not been given adequate coverage.

Besides, most of the Indian corporate including some Public Sector undertakings use Operating Systems that are from the West especially the US and many software utilities and hardware items and sometimes firmware are from abroad. In such cases, the actual reach and import of IT Act Sections dealing with a utility software or a system software or an Operating System upgrade or update used for downloading the software utility, is to be specifically addressed, as otherwise a peculiar situation may come, when the user may not know whether the upgrade or the patch is getting downloaded or any spyware getting installed. The Act does not address the government's policy on keeping the backup of

corporates including the PSUs and PSBs in our county or abroad and if kept abroad, the subjective legal jurisprudence on such software backups.

We find, as has been said earlier in the chapter, that most of the cybercrimes in the nation are still brought under the relevant sections of IPC read with the comparative sections of ITA or the ITAA which gives a comfort factor to the investigating agencies that even if the ITA part of the case is lost, the accused cannot escape from the IPC part.

To quote the noted cyber law expert in the nation and Supreme Court advocate Shri Pavan Duggal, *"While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian Cyber law and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyber law a cybercrime friendly legislation; - a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; ..... a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cybercrime capital of the world……"*

Let us not be pessimistic that the existing legislation is cybercriminal friendly or paves the way to increase crimes. Certainly, it does not. It is a commendable piece of legislation, a landmark first step and a remarkable mile-stone in the technological growth of the nation. But let us not be complacent that the existing law would suffice. Let us remember that the criminals always go faster than the investigators and always try to be one step ahead in technology. After all, steganography was used in the Parliament Attack case to convey a one-line hidden message from one criminal to another which was a lesson for the investigators to know more about the technology of steganography. Similarly Satellite phones were used in the Mumbai attack case in November 2008 after which the investigators became aware of the technological perils of such gadgets, since until then, they were relying on cell phones and the directional tracking by the cell phone towers and Call Details Register entries only.

Hopefully, more and more awareness campaign will take place and the government will be conscious of the path ahead to bring more and more legislations in place. Actually, bringing more legislations may just not be sufficient, because the conviction rate in Cybercrime offences is among the lowest in the nation, much lower than the rate in IPC and other offences. The government should be aware that it is not the severity of punishment that is a deterrent for the criminals, but it is the certainty of punishment. It is not the number of legislations in a society that should prevent crimes but it is the certainty of punishment that the legislation will bring.

Comparative Analysis of IT Act 2000 and IT Act 2008:

When we compare the IT Act 2000 and 2008 we can come to a conclusion that a new amendment introduced in the Act overall have incorporated provisions to cater to the new developed crime .Chapter XIIA where expert opinion is required then the government can appoint a person or body corporate from any section, agency of the Government as an examiner.

They conduct examination in Electronic Evidence. The ITAA 2000 has taken into account Electronic Signature for Digital Signature which helps in e-filing of documents with the government and its agencies. The Act promotes skilled transfer of electronic record for making them a source of evidence and making them possible for electronic storage of data. The authentication of information in an electronic form is validated by the use of digital signature and electronic signature. Its use is easy and does not require any specific technical knowledge. This type of signature provides that a person is not liable for consequences arising out of any forgeries of his signature or other unauthorized signatures. The Act secures and legalizes electronic fund transfer by banks and financial institutions and electronic books of accounts and it secures the Serious Information Infrastructure for Countrywide Security, community health and care. For the effectiveness and betterment of the I.T. Act 2000 the corresponding amendments were made to the following:-

a. The Indian Penal Code
b. The Indian Evidence Act 1872
c. The Banker's Books Evidence Act 1891
d. The Reserve Bank of India Act, 1934

Supreme Court Ruling on Freedom of Expression:

The Apex Court's Verdict on 24th MARCH 2015 the highest court of the land The Apex Court of India squashed section 66A of I.T. Act 2000 as unconstitutional as beyond the ambit of Article 19 of the constitution of India. This verdict was based on the following case laws namely:-

- *Dilipkumar Tulsidas* case,
- *Rajeev Chandrasekhar's* case
- *Shreya Singhal* case

Article 19 (1) (a) of the Constitution of India, 1949, has been quoted that all citizens shall have the right to freedom of speech and expression. It has been used by the citizens of our country through social networking sites viz. Facebook, Whatsapp etc. In a landmark judgment pronounced by the Hon'ble Supreme Court of India on 24th March 2015, The SC quashed Section 66A of the Information Technology Act, 2000 which clamped down on freedom of speech and allowed the State to arrest people posting "offensive content". The new judgment means no one will be arrested for a Facebook post, tweet or cartoon. The court also quashed Section 118 (D) of the Kerala Police Act, a similar Act that enabled the state to arrest people. The petition against Section 66A was first filed by 23-year-old Shreya Singhal, after two girls from Palghar were arrested in 2012 when one of them made a Facebook post on a bandh called after the death of Shiv Sena leader Bal Thackeray, and the other like it. Seven other petitions, including those by People's Union for Civil Liberties, Mouthshut.com and the Internet and Mobile Association of India followed and the SC clubbed these together. The Supreme Court has said that the petitions against the Section "raise very important and far-reaching questions relatable primarily to the fundamental right of free speech and expression is guaranteed by Article 19 (1) (a) of the Constitution of India." No social media posts can be taken out without a court order. The Supreme Court ruling categorized freedom of speech in three sections: for discussions, advocacy and incitement. Any expression that discusses or advocates cannot be punishable under law.

Registration of First Few cases in Cybercrime

The first possible case registered under Sec66 of IT Act 2000 against Amit Pasari and Kapil Juneja. It was registered under Sec 66 and Sec 406 under IPC. This case involved a web hosting business run by Amit Pasari and Kapil Juneja under the name of soft web.

Magnitude of Computer And Information Technology Crimes in India:

Despite penal provisions and preventive measures provided in the Indian Penal Code and the Information Technology Act, the statistics of the preceding years clearly show that there has not been any decline in the crime rate and in fact there is a steady rise in the crimes. Many crimes exist which need improvised investigation and legal techniques and skills to handle them efficiently. Crimes like Credit Card Fraud are much on the rise. Crime statistics have an important role in formulating preventive crime strategy as they contain relevant data on specific crimes and criminals, which helps the criminal law enforcement agencies to make best possible use of them for working out effective strategy to tackle such crimes efficiently.

Incidences of Cybercrimes in Urban areas:

A lot of cases have been registered in India from different urban areas in India. The following statistics show that cybercrime have increased. Cybercrime have shot up in Bengal. This is a biggest jump nationwide according to National Crime Record Data for 2012. Such cases have increased by a whopping 355.8 % in the state.

Kolkata shows a 1033.3 % jump in 2012 compared to 2011. This is due to the fact that the trends followed by the police to register cyber-crime cases under the traditional IPC sections thereby giving the IT Act, 2000, a pass. Kolkata had registered six cases in 2011, and then the Police have registered 68 cases in 2012 showing an increase in the number of crimes. In the state of Maharashtra a whooping rises of 42.7% in cybercrimes in 2012 over the year before.

In another report by National Crime Records Bureau (NCRB) the year 2013, saw a jump of 122.5% in cyber offences over 2012. Hacking formed close to 60% of all cyber offences (under IT Act) in India followed closely by Obscene or Derogatory posts (28%). 45% of all Hacking cases were reported from the 88 cities covered. Making 55% coming from small towns or rural areas. Today Indian rural areas report of 60% cases on obscene/derogatory posts rural. Of the 2516 cases of hacking, 1382 were reported from small towns and rural areas. Similarly, of 1203 obscene/derogatory posts on social media and other websites, only 483 were reported from cities.

Maharashtra has recorded the maximum number of cases that violated the Information Technology Act and other cybercrime laws in the last three years. The state witnessed a total of 919 cases filed and 693 persons arrested for cybercrime, in the last three years i.e. 2011, 2013, 2014. After Maharashtra, Andhra Pradesh followed in second place with 883 cases and in third place was Karnataka with 716 cyber cases. Out of this, Andhra Pradesh made 493 arrests and Karnataka 195.

As per the data maintained by National Crime Record Bureau (NCRB), a total of 5,693, 9,622 and 11,592 cybercrime cases were registered during the years 2013, 2014 and 2015,

respectively, showing a rise of 69 per cent during 2013 to 2014 and 20 per cent during 2014 to 2015. Also, RBI has registered a total of 9,500, 13,083, 16,468 and 8,689 cases of frauds involving credit cards, ATM/debit cards and internet banking during the year 2013-14, 2014-15, 2015-16 and 2016-17 (upto December 2016), respectively. Further, CBI has registered a total of 87 cases during 2014 to 2016. Out of these 87 cases, charge sheets have been filed in 36 cases, status report filed in copmpetent court in 4 cases, 6 cases were closed and 41 cases are under investigation by CBI.

In fact, according to a 2017 report, Indian consumers had lost over 18 billion U.S. dollars due to cyber-crimes. In 2018, there were over 27 thousand cases of cyber-crimes recorded in the country, marking an increase of over 121 percent compared to the number of cases just two years back. While the nature of crimes ranges from petty online frauds to lottery scams and sexual harassment, the most targeted crimes seem to be in the banking and finance sector.

Even then, it is important to remember that cyber vulnerabilities aren't just limited to private sectors. Some of the most dangerous data breaches have been with respect to government data. One such security breach was that involving India's unique citizen identification system- the Aadhaar, which got hacked in early 2018, compromising extensive personal information including bank details, address and biometrics of over a billion Indians.

Along with economic losses, cyber-crimes also impact public safety- especially for minors and vulnerable sections of the society through incidents of cyber bullying and exploitation. In 2018 alone, India recorded over two thousand cases of cyber-crimes related to sexual harassment and over 700 cases of cyber bullying against women and minors. Perhaps these high number of cases had led to an increased awareness about the issue of cyber-bullying, and a large share of Indians felt that the responsibility for abusive behavior on social media lay with both the users as well as social media platforms.

However, one of the biggest impediments in curbing cyber-crimes has been the lack of awareness on cyber hygiene leading to critical digital vulnerabilities. Most cyber-crime incidents in India went unreported. And even when crimes were reported to authorities, the infrastructure and process to tackle such cases were largely inefficient. On the bright side, in 2018 the Indian government launched its National Cyber Crime Reporting Portal for citizens to register their complaints online. Under this initiative, cyber cells in various cities across the country have also been training police and government employees how to handle digital security incidents and increase public awareness at the same time.

According to the 2019 NortonLifeLock Cyber Safety Insights Report, which was conducted online by The Harris Poll for NortonLifeLock among 10,063 adults in 10 countries finds that Rs. 131.2 million is the number of cyber-crime victims in India in 2019, compared with 350 million worldwide. Rs. 1.24 trillion is the amount lost in India in the past 12 months due to cyber- crime. 81% Indians are alarmed about their privacy, the highest in 10 countries, with the global average being 67%. 4 in 10 consumers in India have experienced identity theft, with 10% impacted in the past year.

The Internet Crime Report for 2019, released by USA's Internet Crime Complaint Centre (IC3) of the Federal Bureau of Investigation, has revealed that India stands third in the world among top 20 countries that are victims of internet crimes. As per the report, excluding the

USA, the UK tops the list with 93,796 victims of internet crimes followed by Canada (3,721) and India (2,901).

Concept of cyber security in India: India does not have a dedicated cybersecurity law. The Information Technology Act 2000 (the IT Act) read with the rules and regulations framed thereunder deal with cybersecurity and the cybercrimes associated therewith. The IT Act not only provides legal recognition and protection for transactions carried out through electronic data interchange and other means of electronic communication, but it also contains provisions that are aimed at safeguarding electronic data, information or records, and preventing unauthorised or unlawful use of a computer system. Some of the cybersecurity crimes that are specifically envisaged and punishable under the IT Act are hacking, denial-of-service attacks, phishing, malware attacks, identity fraud and electronic theft.

In accordance with the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 (the CERT Rules), the Computer Emergency Response Team (CERT-In) has been established as the nodal agency responsible for the collection, analysis and dissemination of information on cyber incidents and taking emergency measures to contain such incidents.

Other relevant rules framed under the IT Act in context of cyber security include:

- the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the SPDI Rules), which prescribe reasonable security practices and procedures to be implemented for collection and the processing of personal or sensitive personal data;
- the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018 (the Protected System Rules), which require specific information security measures to be implemented by organisations that have protected systems, as defined under the IT Act. More information on protected systems is provided in ‘Scope and jurisdiction’; and
- the Information Technology (Intermediaries Guidelines) Rules, 2011 (the Intermediaries Guidelines), which require intermediaries to implement reasonable security practices and procedures for securing their computer resources and information contained therein. The intermediaries are also required to report cybersecurity incidents (including information relating to such incidents) to CERT-In.

Other laws that contain cyber-security-related provisions include the Indian Penal Code 1860 (IPC), which punishes offences, including those committed in cyberspace (such as defamation, cheating, criminal intimation and obscenity), and the Companies (Management and Administration) Rules 2014 (the CAM Rules) framed under the Companies Act 2013, which requires companies to ensure that electronic records and security systems are secure from unauthorised access and tampering.

In addition to the above, there are sector-specific regulations issued by regulators such as the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India Act 1999 (IRDA), the Department of Telecommunication (DOT) and the Securities

Exchange Board of India (SEBI**)**, which mandate cybersecurity standards to be maintained by their regulated entities, such as banks, insurance companies, telecoms service providers and listed entities.

Sectors of the economy are most affected by cyber-security laws and regulations:

Regulated entities operating in sensitive sectors, such as financial services, banking, insurance and telecommunications, have exhibited higher standards of cyber-security preparedness and awareness, partly because of regulatory intervention as well as voluntary compliance with advanced international standards. Sectors such as e-commerce, IT and IT-enabled services that have seen infusion of foreign direct investment have also proactively deployed robust cyber-security frameworks and policies to counter the evolving nature of cyber fraud as they have borrowed advanced cyber-security practices and procedures from their parent entities in the United States, the European Union and other matured jurisdictions.

With the rise of digital payments, cybercrimes involving payment transactions in the online space have significantly increased and become complex. While the RBI has been active in requiring companies operating payment systems to build secure authentication and transaction security mechanisms (such as 2FA authentication, EMV chips, PCI DSS compliance and tokenisation), given that these payment companies often offer real-time frictionless payments experiences to their consumers, it leaves less time for banks and other entities operating in the payment ecosystem to identify and respond to cyber-threats. In light of the above, there is an increased need to identify and develop cyber-security standards commensurate with the nature of information assets handled by them, and the possible harm in the event of any cyber-security attack, to ensure that these emerging risks are mitigated.

Cyber Security and Cyber-crime under IT Law:

Under the IT Act, 'cybersecurity' means protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction. 'Cybercrime' on the other hand has been defined by the National Cyber Crime Reporting Portal (a body set up by the government to facilitate reporting of cybercrime complaints) to 'mean any unlawful act where a computer or communication device or computer network is used to commit or facilitate the commission of crime'.

The courts in India have also recognised cybercrime (eg, the Gujarat High Court in the case of ***Jaydeep Vrujlal Depani v State of Gujarat*** R/SCR.A/5708/2018 Order), to mean 'the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)'.

While the IT Act does not make any distinction between cyber-security and data privacy, in our view, these issues are distinct but also deeply interconnected as ensuring privacy of an individual's data requires adequate cyber-security processes to be implemented by

organisations. Further, cyber-security and information security frameworks are developed by organisations at a broader level to build resilience against various forms of cyber-threat, including cybercrimes that entail more extensive engagement with regulatory authorities depending on the extent of harm caused, the nature of information handled by the body corporate, sector sensitivities, etc.

International standard related to cyber security adopted by India:

SDPI Rules framed under the IT Act require body corporates that handle sensitive personal data or information to implement 'reasonable security practices and procedures' by maintaining a comprehensive documented information security programme. This programme should include managerial, technical, operational and physical security control measures that are commensurate with the nature of the information being protected. In this context, the SPDI Rules recognise the International Standard ISO/IEC 27001 on Information technology – Security techniques – Information security management systems – Requirements as one such approved security standard that can be implemented by a body corporate for protection of personal information. All body corporates that comply with this standard are subject to audit checks by an independent government-approved auditor at least once a year or as and when they undertake a significant upgrade of their processes and computer resources.

Sector-specific regulators have also prescribed security standards specifically applicable to regulated entities. For instance, the RBI guidelines mandate banks to follow the ISO/IEC 27001 and ISO/IEC 27002 standards for ensuring adequate protection of critical functions and processes. Similarly, SEBI requires stock exchanges, depositories and clearing corporations to follow standards, such as ISO/IEC 27001, ISO/IEC 27002 and COBIT5.

Minimum protective measures for organisations to take to implement to protect data and information technology systems from cyber-threats:

As mentioned above, as per the SPDI Rules, anybody corporate that possesses, deals with or handles any sensitive personal data or information in a computer resource is required to implement prescribed security standards (ISO/IEC 27001 on Information technology – Security techniques – Information security management systems – Requirements).

Sector-specific cybersecurity measures have been made mandatory by regulators for some regulated businesses. For instance, in the banking sector, the RBI requires banks to undertake certain security measures including, inter alia, logical access controls to data, systems, application software, utilities, telecommunication lines, libraries and system software; using the proxy server type of firewall; using secured socket layer (SSL) for server authentication; and encrypting sensitive data, such as passwords, in transit within the enterprise itself. The RBI specifically mandates that connectivity between the gateway of the bank and the computer system of the member bank should be achieved using a leased line network (and not through the internet) with an appropriate data encryption standard and that 128-bit SSL encryption must be used as a minimum level of security.

Additionally, in the telecommunications sector, the licence conditions imposed by the DOT require every licensee to implement the following measures:

a. ensure protection of privacy of communication so that unauthorised interception of messages does not take place;
b. have an organisational policy on security and security management of its network, including network forensics, network hardening, network penetration tests and risk assessment; and
c. induct only those network elements into its telecom network that have been tested as per relevant contemporary Indian or international security standards (eg, the IT and ITES elements) against the ISO/IEC 15408 standards (eg, the ISO 27000 series standards for information security management systems and the 3GPP and 3GPP2 security standards for telecoms and telecoms-related elements).

Laws or regulations that specifically restrict sharing of cyberthreat information:

In a recent judgment of ***Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors*** (Writ Petition (Civil) No. 494 of 2012), the Supreme Court of India held the right to privacy to be a fundamental right that is an intrinsic component of the right to life and personal liberty under article 21 of the Constitution of India and therefore a basic right of all individuals. Although there are precedents where the courts have held private communications between individuals to be covered within the purview of 'right to privacy', there are also precedents where Indian courts have admitted recordings obtained without consent as valid evidence. Given that this issue is unsettled, permissibility of recordings will need to be determined on a case-by-case basis.

In any case, the SPDI Rules require body corporates to disclose personal data or sensitive personal information subject to prior consent of the data subject. However, this condition can be waived if the disclosure is to government agencies mandated under the IT Act for the purpose of verification of identity, or for the prevention or investigation of any offences, including cybercrimes.

Certain laws, such as the Indian Telegraph Act 1885 (the Telegraph Act) and the IT Act, permit governmental and regulatory authorities to access private communications and personally identifiable data in specific circumstances. The Telegraph Act empowers the government to intercept messages in the interest of public safety, national security or the prevention of crime, subject to certain prescribed safeguards. In that scenario, the telecoms licensee that has been granted a licence by the DOT is mandated to provide necessary facilities to the designated authorities of the central government or the relevant state government for interception of the messages passing through its network.

The IT Act also grants similar authority to the government and its authorised agencies. Any person or officer authorised by the government (central or state) can, inter alia, direct any of its agencies to intercept, monitor or decrypt, or cause to be intercepted, monitored or decrypted, any information that is generated, transmitted, received or stored in any computer resource, in the event it is satisfied that it is necessary or expedient to do so in the interest of sovereignty and the integrity of India, the defence of India, the security of the state, friendly relations with foreign states, public order or preventing incitement to the commission of any cognisable offence relating to the above, or for the investigation of any offence. In our view, the instances described in the IT Act can be relied on by the government agencies to intercept data for cybersecurity incidents if they relate to contravention or investigation of any crime.

However, There are no separate set of laws or regulations that regulate the provision of cloud computing services in India. However, given that cloud computing services are rendered and received over the internet or through the digital medium, certain provisions of the IT Act, the SPDI Rules and the Intermediaries Guidelines may be relevant to these services.

For instance, the SPDI Rules allow a body corporate to transfer data to any other body corporate or a person in India or in any other country that ensures the same level of data protection that is adhered to by the body corporate. However, the transfer may be allowed only if it is necessary for the performance of a lawful contract between the body corporate and the data subject or where the person has consented to the data transfer. Accordingly, in our view, any entity engaged in the cloud computing business will need to ensure that it maintains the same level of information security standards as that of the data controller (ie, the person collecting the information from the data subject).

Also, depending on the business model, a cloud services provider may fall within the definition of an intermediary under the IT Act (defined as any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecoms service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cybercafes). As an intermediary, the cloud service provider will need to comply with due diligence measures to claim safe harbour protection from liability arising from the content stored by it. These due diligence measures include taking all reasonable steps to secure its computer resource and the information contained therein by adopting the security practices prescribed under the SPDI Rules, as mentioned in 'Legislation'.

In addition to the minimum cybersecurity standards mentioned in 'Legislation', various regulatory bodies have advised businesses to adopt more robust measures in areas of cybersecurity. For example, the Ministry of Communication and Information Technology released the National Cyber Security Policy in 2013, which recommended creating a secure cyber ecosystem and strengthening laws, and creating mechanisms for the early warning of security threats, vulnerability management and the response to security threats. The policy intended to encourage all organisations to develop information security policies integrated with their business plans and implement the policies in accordance with international best practices. This policy is expected to be updated in 2020.

Under the Digital India initiative, the Ministry of Electronics and Information Technology (MeitY) has set up the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre), operated by CERT-In, to work with internet service providers and product or antivirus companies to provide information and tools to users on botnet and malware threats. Similar proactive measures are deployed by sector-specific regulators from time to time.

Penalties provided under IT Act:

The IT Act provides for penalties for varied instances of cybersecurity breach, some of which are described here. Section 43 of the IT Act provides that any person accessing a computer or a computer system or network without permission of the owner, downloading copies and extracting any data or causing disruption of any system will be liable to pay damages to the

person affected. Section 66 of the IT Act also provides for punishment of imprisonment for a term up to three years or with a fine of up to 500,000 rupees if the person dishonestly or fraudulently commits the offence.

Section 66C of the IT Act provides that a person who, fraudulently or dishonestly, makes use of the electronic signature, password or any other unique identification feature of any other person will be punished with imprisonment of up to three years and will also be liable for payment of a fine of up to 100,000 rupees.

Additionally, the IT Act provides for imprisonment of up to one year or a fine of up to 100,000 rupees, or both, for any failure by an entity (service provider, intermediary, data centre, body corporate, etc) to provide requisite information requested by CERT-In. Furthermore, sector-specific authorities (such as the RBI) may also levy penalties for non-compliance with their respective cybersecurity standards.

Rules requiring organization to report cyber-security breaches to regulatory authorities.

Reporting under the IT Act

The CERT Rules permit cybersecurity incidents to be reported by any person to CERT-In. However, specified types of cybersecurity incidents (target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, etc) need to be mandatorily reported to CERT-In by service providers, intermediaries, data centres and body corporates within a reasonable time of the incident occurring or being noticed to aid timely action.

The Intermediaries Guidelines require the intermediaries, as part of their due diligence obligations, to notify CERT-In of security breaches. CERT-In publishes the formats for reporting cybersecurity incidents on its website from time to time, which requires mentioning the time of occurrence of the incident, the type of incident, information regarding the affected systems or network, the symptoms observed, the relevant technical systems deployed, the actions taken, among others.

Reporting in other sectors

In addition to the reporting requirements under the IT Act, separate reporting requirements exist in respect of cybersecurity incidents in other regulated sectors. For instance, the Cyber Security Framework in Banks issued by the RBI requires banks to inform the RBI of any cybersecurity incident within two to six hours of the breach. Similarly, as per the Guidelines on Information and Cyber Security for Insurers issued by the IRDA, insurers are required to report cybersecurity incidents that critically affect business operations and a large number of customers within 48 hours of having knowledge of the cybersecurity incident.

Any failure by intermediaries to report cybersecurity incidents to CERT-In is punishable under the IT Act by a monetary penalty not exceeding 25,000 rupees. Any failure of a body corporate to report specific cyber breaches mandated under the IT Act is punishable by the same amount. Further, if CERT-In specifically requests for any information from an entity (including the service provider, intermediary or body corporate), then a failure to submit the

information is punishable by imprisonment of up to one year or a fine which may extend to 100,000 rupees, or both.

In addition, sector-specific regulators have their own reporting requirements. For instance, failure to report within the timelines prescribed for banks under the Cyber Security Framework in Banks may result in the imposition of penalties by the RBI.

Role of Cyber Law policy 2013 in securing cyber security in India:

With an aim to monitor and protect information and strengthen defences from cyber attacks, the National Cyber Security Policy 2013 was released on July 2, 2013 by the Government of India. The purpose of this framework document is to ensure a secure and resilient cyberspace for citizens, businesses and the government. With rapid information flow and transactions occurring via cyberspace, a national policy was much needed.

The document highlights the significance of Information Technology (IT) in driving the economic growth of the country. It endorses the fact that IT has played a significant role in transforming India's image to that of a global player in providing IT solutions of the highest standards.

The Cyber Security Policy aims at protection of information infrastructure in cyberspace, reduce vulnerabilities, build capabilities to prevent and respond to cyber threats and minimize damage from cyber incidents through a combination of institutional structures, people, process, technology and cooperation. The objective of this policy in broad terms is to create a secure cyberspace ecosystem and strengthen the regulatory framework. A National and sectoral 24X7 mechanism has been envisaged to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC). Computer Emergency Response Team (CERT-In) has been designated to act as a nodal agency for coordination of crisis management efforts. CERT-In will also act as umbrella organization for coordination actions and operationalization of sectoral CERTs. A mechanism is proposed to be evolved for obtaining strategic information regarding threats to information and communication technology (ICT) infrastructure, creating scenarios of response, resolution and crisis management through effective predictive, prevention, response and recovery action.

The policy calls for effective public and private partnership and collaborative engagements through technical and operational cooperation. The stress on public-private partnership is critical to tackling cyber threats through proactive measures and adoption of best practices besides creating a think tank for cyber security evolution in future.

Another strategy which has been emphasized is the promotion of research and development in cyber security. Research and development of trustworthy systems and their testing, collaboration with industry and academia, setting up of 'Centre of Excellence' in areas of strategic importance from the point of view of cyber and R&D on cutting edge security technologies, are the hallmarks of this strategy laid down in the policy.

The policy also calls for developing human resource through education and training programmes, establishing cyber security training infrastructure through public private partnership and to establish institutional mechanisms for capacity building for law enforcement agencies. Creating a workforce of 500,000 professionals trained in cyber

security in the next 5 years is also envisaged in the policy through skill development and training. The policy plans to promote and launch a comprehensive national awareness programme on security of cyberspace through cyber security workshops, seminars and certifications with a view to develop awareness of the challenges of cyber security amongst citizens.

The policy document aims at encouraging all organizations whether public or private to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cyber security initiatives. Organizations are required to develop their information security policies properly dovetailed into their business plans and implement such polices as per international best practices. Provisions of fiscal schemes and incentives have been incorporated in the policy to encourage entities to install trustworthy ICT products and continuously upgrade information infrastructure with respect to cyber security.

The release of the National Cyber Security Policy 2013 is an important step towards securing the cyber space of our country. However, there are certain areas which need further deliberations for its actual implementation. The provisions to take care security risks emanating due to use of new technologies e.g. Cloud Computing, has not been addressed. Another area which is left untouched by this policy is tackling the risks arising due to increased use of social networking sites by criminals and anti-national elements. There is also a need to incorporate cyber-crime tracking, cyber forensic capacity building and creation of a platform for sharing and analysis of information between public and private sectors on continuous basis.

Reasons for India's increasing number of cyber-crime:

Lack of Criminal Statutes:

Many countries are either without cybercrime laws or don't have updated and effective cybercrime statutes. India has an alarming cybercrime rate. "According to the Indian Computer Emergency Response Team (CERT-In), 27,482 cases of cybercrime were reported from January to June 2017". Cybercrime rate from January- June of 2017 in India is one cybercrime after every 10 minutes. The ratio between conviction and detection of cybercrime in India is abysmally low. Maharashtra which is having highest cybercrime rate, from 2012 to July 2017, 10,419 cybercrimes were filed, out of which only 34 were convicted. The rate of conviction is just 0.3%.The major reason of low conviction rate is lack of criminal statutes and also improper implementation of Information Technology Act, 2008 by concerned officials.

Lack of Procedural Powers:

To investigate Cybercrime high tech resources and procedural tools are required. India lacks both of the pre- requisites. The low conviction rate of India is also due to the lack of standard procedures for seizure and analysis of digital evidence. "There are no standard documented procedures for searching, seizing of digital evidence and standard operating procedures for forensic examination of digital evidence". India also need to allocate more resources towards fighting cybercrime in terms of updating cyber security cells using state of the art technology

and regular training of officials to impart highly specialized skills in them for making them competent to fight cybercrime.

Lack of enforceable mutual assistance provisions:

India has not substantially updated its cybercrime statutes, but even though, India has adequate criminal statutes and standard procedures are followed by investigating agencies, still it is not possible to convict a cyber-criminal as cybercrimes often extend beyond the boundaries of the country, host and victim are usually in multiple jurisdictions. In this scenario securing electronic evidence is challenging as data is usually on cloud, distributed over multiple jurisdictions anddifferent service providers where mutual legal assistance is often not feasible. Due to lack of cooperation between countries these cases reach to dead end and are closed without any conviction. India has signed legal assistance treaties with other countries like Israel to fight Cybercrime but it is inadequate and India need to be part of a global village with common criminal policy across borders and that is where Budapest convention has its role to play.

Indian Reluctance and Persuasion:

India amended its Information Technology Act in 2008 to make it closer to the provisions of Budapest convention, but still has not so far signed the convention and continues to be a non-signatory to the Budapest convention on cybercrime. India is reluctant to join giving following reasons:

India didn't participate in drafting Budapest Convention:

India is reluctant to sign the convention as it did not participate in the negotiation of the Convention and India feels that convention is not in accordance to Indian needs. There are many such states which didn't participate in negotiation but later joined perceiving the benefits of joining and also as a member they can now tailor the treaty as per there requirements.

Violation of Sovereignty:

Article 32b of the Budapest convention is a major reason why India is reluctant to become a member. The article 32 is about accessing stored computer data across borders, it states that: A Party may, without the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 3b is a major concern, as India believes that it violates its sovereignty. Indian apprehension is that this article can be used by enemy states to access computers in India with an intention of spying. "The Cybercrime Convention Committee (T - CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective

use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments". According to Guidance Notes "*Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32. Normally, service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent". Guidance Notes emphasizes the trustworthiness of member states as it is presumed that "the Convention form a community of trust".* Indian concerns are the hostile states which are not trustworthy, but according to article 37 of the Convention, India as a member can veto and stop any hostile or non-friendly state from joining the convention as according to article 37 any new member can be invited to join only if all member parties have no issues with that state.

Faulty Mutual legal assistance:

Provision Indian reluctance to sign Budapest convention is also due to the assessment report on mutual legal assessment and its efficiency by the Convention itself. MLA is increasingly decentralized and requests are sent or received directly between relevant judicial authorities and not only via central authorities. Central authorities are usually not executing requests themselves. Multiple offices may be involved in the sending or receiving of requests and in particular the execution of requests…

MLA is considered too complex, lengthy and resource-intensive to obtain electronic evidence, and thus often not pursued. Law enforcement authorities tend to attempt to obtain information through police to-police cooperation to avoid MLA, even though the information thus obtained in most cases cannot be used in criminal proceedings. Frequently, authorities contact foreign (in particular USA- based) service providers directly to obtain subscriber or traffic data. Often investigations are abandoned.

MLA provisions of Budapest Convention as per the 2014 recommendations of the convention are not efficient but this area is improving through the follow up to these recommendations. After 2014 recommendations MLA procedures are made efficient, streamlined and for instant cooperation between states 24/7 points of contact are in place now. India can be an active partner to address and remove these shortcomings by joining the convention, by sidelining itself India is denying its chance to tailor it as per its requirements.

India has signed Mutual Legal Assistance Treaty(MLAT) with many countries:

India for assistance in criminal matters has signed Mutual Legal Assistance Treaty(MLAT) with few countries like India is currently a signatory to UN Convention against Transnational Organized Crime. These MLATs can deal with general criminal matters, but are inadequate and ineffective particularly to cybercrime. To deal with cybercrime more robust laws are required which bring "harmonization in both substantive and procedural laws governing cooperation from other countries on legal assistance in cybercrime matters". Budapest Convention is such an ideal convention to bring harmonization and uniformity in legal cooperation. India can join Budapest convention and still can continue MLAT provisions to deal with other crimes.

Cyber Crime during Pandemic: Working from home' (WFH) has become the order of the day during this precarious lockdown. The way of accomplishing the tasks has drastically changed, with working from home as the only viable option. One's dependence on the internet has increased manifold since the COVID-19 pandemic has caused restrictions on physical gesticulations. Online traffic has escalated due to jaked up video conferencing, meetings, online classes, and chatting. The use of apps like Paytm, Google Pay, BHIM, Phonepe, etc. as a mode of making payments has also witnessed a surge.

During this lockdown, along with the working habits, the modus operandi of the crimes has also changed. No doubt the crime rate has subsided as people are staying back but online frauds have seen an upsurge. Apart from being interaction/communication interfaces, sometimes these also serve as platforms for criminal elements and eventually end up being the epicenters of immeasurable security concerns. This working from home has now become an opportunity for cybercriminals to exploit the people through e-mail scams, hacking passwords, phishing, ransom attacks, online sexual harassment, etc.

Though cyber-crimes have been increasing continuously, there has been an upsurge during the lockdown due to people doing all the official as well as un-official work from their laptops or phones. Besides hackers directly attacking the systems, fake websites are being created to trap the users.

1. *Phishing:* Phishing is the cybercrime where the criminal accesses the information and details of the user through a link or e-mail that seems legitimate but is in fact, fraudulent. Phishing attacks have mushroomed to a large number during this lockdown. Spy-attacks and Ransom attacks are posing a threat to people submitting personal information online. Spyware steals the personal information and account details of the users, whereas a ransom attacker dominates and takes over the login credentials of the user. An app called 'Covidlock' is used as ransomware to target the anxious population, misrepresenting the same as an app to keep track of the spread of coronavirus.

2. *Hacking at Companies and Offices:* According to a recent report by Price water house Coopers, the number of cyber-attacks on various firms has increased manifold times since the corona outbreak. Companies have set up a VPN structure, to let the employees have access to all the information, which has become the target of the hackers. Hackers are trying to hack the software of the companies in order to gain access to all their important details and data. The use of an already-made malware 'AZORult' has increased for phishing into the companies. There have been cases of unwanted software trying to infiltrate to the companies' systems for theft and malicious payloads. Hackers have even attempted to hack the computers of the Indian State Tax Department to steal sensitive information of PAN Cards, GST numbers, phone numbers, and e-mails. There have been several attempts made by the hackers at banks and Stock Markets leading to the brokerage. PM's COVID fund has also been one of the targets of the Hackers.

3. *Patients at Risk:* There have been cyber-attacks not only at local hospitals or test centers but also at the World Health Organization (WHO) to steal the passwords of WHO workers. Ransomware attacks have been detected in hospitals and other test centers where the important files of the patients are taken and not returned till a particular amount of ransom is paid. Hospitals have been alerted about ransom sites that claim themselves to be

government advised sites to keep a check on the corona patients but then hacks the system.

4. *Other Online Crimes Related to Social Media:* Social networking apps like Facebook, WhatsApp have become an important tool to spread fake information. The Digital infrastructure across the globe is immensely comprised of these international tech-giants like YouTube, Google, Facebook, Twitter etc. The social world has witnessed a complete transformation by these corporations, without any regulation or accountability of their Modus Operandi. These fake news' triggers the people, as they blindly believe these reports, and start reacting accordingly. Besides this, these online chatting apps are misused to sexually harass people. It has become inevitable for the employees to stay in touch with each other, so they opt for these communication platforms and sometimes end up being exploited in some way or the other.

   Global police body Interpol has already warned of an "alarming" rate of cybercrime during the coronavirus pandemic, with criminals taking advantage of people working from home to target major institutions. It is certain that the security standards have deteriorated as many organizations were not ready to work remotely and a rise has been witnesses in cyber-crime due to coronavirus. With a little vigilance and due diligence we can protect our data and privacy. It is always better to stay on the side of precaution but if, even after taking all the precautions, we fall into a trap then a quick action can salvage the loss. It is advisable to lodge a complaint with the appropriate authority.

Conclusion: It is cleared from the previous studies and records that with the increment in technology cybercrimes increases. Qualified people commit crime more so, there is need to know about principles and computer ethics for their use in proper manner. Cybercrime and hacking is not going away, if anything it is getting stronger. By studying past incidents, we can learn from them and use that information to prevent future crime. Cyber law will need to change and evolve as quickly as hackers do if it has any hopes of controlling cybercrime. Law must also find a balance between protecting citizens from crime, and infringing on their rights. The great thing about the internet is how vast and free it is. Will it be able to remain the same way while becoming tougher on criminals? Only time will tell. There will always be new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists but we can win only through partnership and collaboration of both individuals and government. There is much we can do to ensure a safe, secure and trustworthy computing environment. It is crucial not only to our national sense of well-being, but also to our national security and economy. Yet India has taken a lot of steps to stop cybercrime but the cyber law cannot afford to be static, it has to change with the changing time.

Cyber threats can potentially target and damage anything like planes, trains, power grids, nuclear warfare's, communication system and anything which is digital. The report on cybercrime by Cybersecurity Ventures sponsored by Herjavec Group "predicts global annual cybercrime costs will grow from $3 trillion in 2015 to $6 trillion by 2021, which includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm". Cyberattacks can be so powerful that it can wash away economy of a city, state or country. To counter cyber threats there is a huge spending

worldwide, it “reached $75 billion in 2015, according to Gartner, Inc., the leading IT analyst firm. Cybersecurity Ventures forecasts global spending on cybersecurity products and services will exceed $1 trillion over the next five years, from 2017 to 2021”

Cyber Crime is a global problem, it is not only the magnitude of loss it is causing but the ease with which it can be committed across borders without any geographical constraints. Jurisdiction is the major hurdle to successfully prosecute such criminals, as evidence may be in some other country with its own laws. Cybercriminals are international criminals, and thus need special laws and legislation which can deal with jurisdiction issues. Cybercrime laws need to be harmonized and international cooperation on cybercrime is requisite to successfully prosecute cybercriminals. “The jurisdictional problem of cybercrime manifests itself in three ways: lack of criminal statutes; lack of procedural powers; and lack of enforceable mutual assistance provisions with foreign states”.

The tremendous growth of internet use in world and particularly in India is laterally accompanied by substantial surge in cybercrime and has made India vulnerable to such crimes. Cybercrimes are of global nature and criminals are not bound to a particular geographical area. Cyberspace is a free flowing, borderless and not guarded by local geographical constraints. These crimes can’t be deterred by local laws, India in such scenario is like sitting ducks. India to counter Cybercrime has engaged itself in various bilateral agreements like cyber agreement with Russia and a framework agreement with the US, resent visit of prime minister of India Mr. Modi to Israel to sign *Indo-Israe*l cyber framework is yet another effort of India to streamline its cyberspace. These bilateral agreements have limited scope and are inadequate and ineffective to deal with cybercrime.

India needs a multilateral treaty which will harmonize its laws by a common criminal policy, and deal with international co-operation for combating cybercrimes at global level. The treaty should help in formulating effective legislation and robust investigative techniques, which can foster international co- operation to combat cybercrime. The Council of Europe’s Budapest Convention on Cybercrime, is such international multilateral treaty dealing with international co-operation for combating cybercrimes at global level. India should sign the convention to combat cybercrime, even the US and Israel with whom India is having bilateral agreements to combat cybercrime have joined Budapest cybercrime convention.

MODULE - VII

INDIAN JUDICIARY AND IT LAW

MODULE- VII: INDIAN JUDICIARY AND IT LAW

Response of Indian Judiciary to Cyber Crimes: In every legal system, which accepts the democratic form of government, the Judiciary plays an important role. It is most important wing of the government, which resolves the conflicts among the parties. For the development of the society, the smooth and powerful adjudicative authority is required. The changing nature of the society increases the role of the adjudicatory authority in the present days. In the era of Information and technology, the criminals are using new technology to commit the crime. Therefore, appropriate judicial approach towards the technological offences is required for prevention of the crime. For the proper working of the judiciary the rules of jurisdiction plays an important role. The main problem that is going to face in case of cyber-crime is concern with the jurisdiction. India is a developing country. The Indian judiciary is an Independent judiciary. Effective legal machinery can be identified on how properly rules and regulations are drafted by legislation and more importantly how precisely principles of jurisdiction are laid down. A court must have jurisdiction, venue and appropriate service of process in order to hear a case and render an effective judgment.

In India, there is only one set of court, which administers national as well as state laws. The constitution has by Article 247, clothed parliament with power to provide for the establishments of additional court for the better administration of law made by the parliament and of any existing law with respect to the matter enumerated in the union list. The courts in India are generally controlled by the state. The courts and the other tribunals are under the superintendents of High court in the territorial jurisdiction of the function. The officers of the courts are appointed by state. The President of India appoints the Judges of the High Court and Supreme Court. The Indian judiciary is quite independent, because all the laws and conflicts regarding that laws, whether made by center or State going to entertain by the regular court. This is the independent of the court system in India. Whenever any conflicts arise about any law, either central or state law or even the offence is technical it is going to adjudicated by the regular Court. Recently the Indian legal system has established certain tribunals, which deals with certain special matters as like the recovery of debt, or certain tribunals for Income tax etc., but lastly the all tribunals are subjects of the judicial review of High Court and Supreme Court. Therefore, the judiciary plays an important role in all laws.

However the basic problem arise when the offences are of that nature which require the technical knowledge to understand the nature of the act whether it is an offence or not. Due to this nature of cyber-crime, the legal system is facing various problems. The laws are insufficient but the policy and the operative system facing the difficulty of lack of knowledge. In case of judicial perspective, the basic question arising regarding the jurisdiction. The conventional law as like Indian Penal Code and the procedural law that Code of Criminal Procedure has provide provisions regarding the territorial and extra territorial jurisdiction, but the basic nature of the cyber-crime somewhere require something more than the provided rules therefore some reformations are required. If we see the decided cases on the cyber-crime, we can find that whenever the provision of Information Technology Act, is attracted then along with that certain provisions of conventional criminal law, that is the Indian Penal Code is also attracted so it shows that the cyber-crime is nothing but the expansion of the conventional law.

Court's Jurisdiction in Internet Disputes: Jurisdiction is one of the debatable issues in the case of cyber-crime due to the universal nature of the cyber-crime. The problem of jurisdiction is not only concern in investigation process but may arise in the trial proceeding also. With the ever-growing arm of the cyber space, the territorial concept seems to vanish. New Methods of dispute resolution should give way to the conventional methods. Thus, the Information Technology Act, 2000 is silent on these issues. Cyber-crime cannot be territorial but global because internet is network of networks as we have seen earlier. It has wide range of functioning; limiting it to physical boundaries is not possible. Thus even in case of cyber-crime their might be a possibility where extra territorial jurisdiction arises.

Jurisdiction plays a vital role for undertaking a successful criminal procedure. Dealing with the issue of cyber-crime it has been noted that even when investigating officer succeeds in establishing geographical identity of an accused of cyber-crime, officer has to face many other difficulties in pursuing his investigation, such as an accused may fall beyond the jurisdictional powers of criminal justice system. In the cyber world where speed is an essence, any attempt to acquire such consent of courts or cooperation will thwart any chance of identifying the culprits and collecting evidence of the crime.

The Doctrine of ubiquity aims determining the place of commission. According to this doctrine, the offence will considered to have been committed in its entirety within a country's jurisdiction, if one of the constituent elements of the offence or the ultimate result occurred within the country's territorial limit. Common Law countries also use effects doctrine in addition to focusing on the physical act. The doctrine locates crime in the territory where it intended to commit or actually took place. Territoriality might grant jurisdiction to many countries in single cyber-crime.

Though S. 75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation's for exchange of material and evidence of computer crimes between law enforcement agencies. As we are known that internet is network of networks, and thus in the field of cyber space no activity is subject to any one particular jurisdiction. In such cases, territorial borders have no relevancy. For Example: A person who is resident of China, with the use of system of some another country, might commit a crime in India. In such a case what will be the territorial nexus of India? And under what circumstances it can bind such an accused for conviction? To settle this question the Court must have the universal jurisdiction and that must be recognized all over the world.

Universal Jurisdiction Approach: Universal jurisdiction is the new concept, which is emerged, in the international society due to the recent development. The principal of universality is controversial due to various reasons. The main reason for the controversy of this concept is the political and jurisdictional sovereignty of the nations of the world. Though the sovereignty of the state is well emerged, however the globalization and due to special situation for humanity, the municipal laws cannot insure the effective administration of justice. The problem of jurisdictional aspect cannot be excuse for the criminal justice; State has to provide justice on any account in the present welfare state. This problem of jurisdiction does not ensure the justice in certain nature of crimes and criminals particularly in cyber cases. This universal jurisdiction never ensure alternate jurisdiction, it merely

provide additional jurisdiction. When the municipal law is unable to provide justice due to the present structure then the universal jurisdiction can apply to provide justice.

The states under this principles, claim criminal jurisdiction over a person, who is alleged to have committed crime either in prosecuting state result of which is having effected in another sovereign state or outside the territory of the prosecuting state, irrespective of the nationality, country of residing or with any other relation with the prosecuting state. The universal jurisdiction can be exercise by the prosecuting state, even the crime has not been committed in the territory of prosecuting state or the same territory has not been use for any purpose concerned with the commission of crime. The state can claim it on the ground that the crime committed is a crime against all, which any state authorized to punish, as it is too serious to tolerate jurisdictional arbitrage. The concept of universal jurisdictional is therefore closely linked to the idea that certain international norms are owed to the entire world community as well as the concept of certain international law obligation are binding on all the state and cannot be modified by treaty.

This concept of universal jurisdiction is necessary to address problem of cyber-crime, but it require to extend the scope of the cyber-crimes and criminals particularly of the serious nature offences where administration of justices become impossible for technical requirements of laws of municipal jurisdiction. Considering the need and requirements of the present developing situation, the concept of universal jurisdiction is the need of the hour. Not only the cyber-crimes and cyber world, but whenever the municipal law and its application is impossible due to the technicalities to prosecute the criminal in the serious matter, this universal jurisdiction can apply to meet the needs. The concept of universal jurisdiction was applied by various countries in various matters. Belgium was the first country, which applied the concept of universal jurisdiction in the year 1993. The concept of universal jurisdiction emerged from the Geneva Convention, 1949 and U. N. Convention against Torture, 1984 due to these conventions this concept was incorporated in municipal Law of various countries as like Belgium, Canada, Germany, Spain, United Kingdome, etc.

Universal jurisdiction is based on the nature of the crime. National court can exercise the Universal jurisdiction to prosecute and punish which is necessary to deter the dangerous acts, which are recognized serious crime under the International Law. Now a day the cyber-crime is really a worldwide problem moreover the cyber-crime like cyber terrorism is dangerous for the peace and security of the entire world at a large.

Indian Courts are independent and having jurisdiction on all the laws made by state and central, but due to the nature of the cyber-crime, in certain situation the problem of jurisdiction may arise. The cyber-crime is transnational crime and therefore the universal jurisdiction requires in case of the cyber-crime. The Information Technology Act, 2000 has contended certain provision, which is based on the universal jurisdiction. Apart from the entire technicality, it is necessary that all court must have the conform jurisdiction to prosecute the cyber criminals, because cyber-crime is based on the techniques and the cyber criminals are technically expert and there is no barriers of the boundaries and territory. The cyber world is different from the physical world, therefore the traditional rules of jurisdiction cannot useful in prosecution of cyber criminals. Therefore, the universal cooperation is needed for the cyber-crime trial in any country as well as in India.

Computer Generated Evidence and their Admissibility: Once the jurisdiction is conforming then another important issue is the admissibility of evidence. Therefore, the Indian Evidence Act deals with the Evidence and its admissibility. This act is applicable to all kinds of proceeding, civil and criminal. Generally, in criminal proceeding, the guilt of the accused must prove beyond the reasonable doubt. If any doubt arises, the benefit of doubt always goes to the accused. Therefore, the evidence in criminal proceeding must clear and beyond the reasonable doubt. In traditional crime, the evidence can be collected which may be in the direct form. As like the weapons and the object or the subject matter in the damage form, however this is not possible in the cyber-crime. The evidences in cyber-crimes are usually unable to collect in the physical form therefore; they cannot produce in the court as like the evidences in traditional crime and trials in traditional crimes.

The concept of evidence has to be discussed in two aspect at the time of investigation and during the trial. Therefore, the applicability and admissibility of computer evidence is base on the different footing. Therefore, the Indian Evidence Act has amended to make computer-generated evidences admissible in the court of law. To meet with these challenges, the Amendment made in the existing law, without which the cyber law of India that is Information technology Act cannot work. Section 3 of the Indian evidence act has amended which include the electronic record in the evidence. The insertions of section 65A and Section 65 B in the second schedule are the most important among the amendments, which contended special provision as to evidence related to electronic records.

The sections enacted by considering the nature of the computer crimes and the electronic evidences. The constitution of this section shows the specialty of the evidences in the technical offences as like the cyber-crimes. The criminal court follows the general rules of evidence in trial and the conventional evidence is generally appreciated in the court of Law. The cyber-crime is quite different due to its mode of commission; therefore, it is not having the evidence as like the conventional crime. The effect of conventional crime can be seen by the common man, as like theft or the grievous hurt can be prove by the statements of the common person, because it can perceived by our senses. However, the effect of cyber-crime is though danger than the conventional crime but cannot see by a common person. Therefore, it must be prove on the different bases and it can appreciate on the different principles. If we see the wording of Section 65 A and 65 B, it shows some, different from the general evidence which are going to produced in the general court in the conventional trial.

Section 65-A Special Provisions as to Evidence relating to Electronic Record: The content of electronic record may be proved in accordance with the provisions of section 65 B.

Section 65-B Admissibility of Electronic Records:

1. Notwithstanding anything contained in this Act, any information contended in an electronic record which is printed on a paper, stored, recorded on copied in optical or magnetic media produced by a computer (herein after refer as a computer output)shall be deemed to be also document, if the condition mention in this section is satisfied in relation to the Information and computer in question shall be admissible in any proceeding, without further proof or production of the original or any fact stated there in or which direct evidences would be admissible.

2. The condition referred to in sub-section (1) in respect of a computer output shall be the following, namely:-
   a) The computer output containing the information was produced by the computer during the period over which the computer was need regularly to store or process information for the purpose of any activities regularly carried on over that period by the person having lawful control over the use of computer;
   b) During the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly feed into the computer in the ordinary course of the said activities;
   c) Throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during the part period, was not such as to effect the electronic record or the accuracy of its contents; and
   d) The information contended in the electronic record reproduced or is derived from such information feed into the computer in the ordinary course of the said activities.
3. Where over any period, the function of storing or processing information for the purpose of any activities or any regularly carried on over that period as mention in clause (a) of sub-section (2) was regularly perform by computer whether-
   a) By a combination of computers operating over that period; or
   b) by different computer operating in succession over that period; or
   c) by different combination of computer operating in succession over that period, or
   d) In any other manner involving the successive operation over that period, in whatever order, of any or more computer and one or more combinations of computer. All the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.
4. In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—
   a) identifying the electronic record containing the statement and describing the manner in which it was produced;
   b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
   c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.
5. For the purposes of this section,—
   a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or
   b) (with or without human intervention) by means of any appropriate equipment; whether in the course of activities carried on by any official information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly

supplied to that computer, shall be taken to be supplied to it in the course of those activities;

c) A computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation: For the purposes of this section, any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process;

Thus, the amendment in the Evidence Act leads to recognize the electronic evidence and its admissibility. The wording of the amended section brings the electronic data and the material under the preview of the Evidence Act. Otherwise, the working of court is impossible because the evidence act originally never recognized the electronic data. Therefore, it is necessary to bring the computer and its generated things under the regular criminal trial. The interpretation of various provisions of IT Act has made according to the natural meaning flowing from it. The recent pronouncement of Supreme Court stating that the recording of evidence through video conferencing is valid in law under section 273 of Criminal Procedure Code has an appreciable development in the field of appreciation of evidences.

Due to this Amendment in Evidence Act, the Indian court get power to admit the evidences in any form as like electronic form, the Indian court started the trial of cyber-crime. However, most of the cyber-crimes are yet subject to the conventional crime, the investigation machinery yet working in the same manner. The cyber law cannot work without the traditional law. The appreciation of evidences is yet subject to the conventional ways. The amendment in the Evidence Act attempted to supplement the traditional provisions requiring a document to be in writing by allowing matter in electronic form to be treated as written if the arises. This action of Indian Legal system will solve various problems in future. However the work of adjudication yet facing various problem because loopholes in the technical aspects, that can be seen in various judgments of Indian courts.

Judicial Perspective of India in cyber-crime: The current litigation system of India is not only antique in nature but has become cumbersome and time consuming as well. The backlog of cases is increasing day by day affecting the outcome of various cases. There is an emergent need of judicial and legal reforms in India so that courts in India can meet the expectations of the 21st Century. This can done only by maintaining a stance that preserves the courts reputation and supports the courts critical role in maintaining public confidence in the protection afforded to them by the law. The Indian conventional laws are yet not suitable to deal with the correct issues, the laws regarding to cyber law and Information Technology sector are far away from the real need. The Indian system already facing the problem of low conviction rate in the all criminal matters, and the cyber-crime and new technology has created the much hurdles in the said aspect.

Indian Penal Code is universal criminal law of Indian legal system. However, it amended time to time, however its implementation is also not satisfactory in the view of people. The public confidence in the Criminal Justice System of India is declining and the same has forced the Government of India to bring this issue write back to the top of the political agenda. Its aim is to cut crimes by increasing the number of criminals brought to trial and

reducing the time taken to complete the legal process. Apart from that, the trial brings before the court, the appropriate appreciations of evidences and the conviction on that matter. Mere proper investigation is not sufficient but the proper appreciation of the evidences by the court is also necessary for the effective criminal justices system.

The Indian Legal system passed the Information Technology Act in 2000, the Act as contended previously is enacted for the regulation of e-commerce. However having certain penal provision but they are not sufficient to curtail the offences takes place by using computer as a tool or target. The various judgments of the Honorable High Courts and the Hon'ble Supreme Court are prima facie based on the provisions of the traditional criminal law, i.e. Indian Penal Code.

Landmark cases under Cyber Law in India: These are various landmark cases, in which the issues are regarding the crime, which are subject to the use of computer or internet, though the offences are registered in different sections of the Information technology, and then it is subjected to the conventional criminal laws also, i.e. Indian Penal Code. The Judgments shows the effectiveness of the conventional criminal laws in the informational technology. Only the amendments in the procedural laws are necessary for the effective prevention of the cyber laws. Some of the cases may have been repeated again in the later part of this chapter for the purpose of detailed discussion and understanding and also some of them are important to the context of cyber security in India as well.

1. ***Anvar P.V. vs. P.K. Basheer and others:***

In this significant judgment, the Supreme Court has settled the controversies arising from the various conflicting judgments as well as the practices being followed in the various High Courts and the Trial Courts as to the admissibility of the Electronic Evidences. The Court has interpreted the Section 22A, 45A, 59, 65A & 65B of the Evidence Act and held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate U/s 65 B(4) of Evidence Act. It has been elucidated that electronic evidence without certificate U/s 65B cannot be proved by oral evidence and the opinion of the expert U/s 45A Evidence Act cannot be resorted to make such electronic evidence admissible.

The judgment would have serious implications in all the cases where the prosecution relies on the electronic data and particularly in the cases of anticorruption where the reliance being placed on the audio-video recordings, which are being forwarded in the form of CD/DVD to the Court. In all such cases, where the CD/DVD are being forwarded without a certificate U/s 65B Evidence Act, such CD/DVD are not admissible in evidence and further expert opinion as to their genuineness cannot be looked into by the Court as evident from the Supreme Court Judgment. It was further observed that all these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic records sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice.

In the anticorruption cases launched by the CBI and anticorruption/Vigilance agencies of the State, even the original recording which are recorded either in Digital Voice Recorders/mobile phones are not been preserved and thus, once the original recording is

destroyed, there cannot be any question of issuing the certificate under Section 65B(4) of the Evidence Act. Therefore in such cases, neither CD/DVD containing such recordings are admissible and cannot be exhibited into evidence nor the oral testimony or expert opinion is admissible and as such, the recording/data in the CD/DVD's cannot become a sole basis for the conviction. In the aforesaid Judgment, the Court has held that Section 65B of the Evidence Act being a 'not obstante clause' would override the general law on secondary evidence under Section 63 and 65 of the Evidence Act. The Section 63 and Section 65 of the Evidence Act have no application to the secondary evidence of the electronic evidence and same shall be wholly governed by the Section 65A and 65B of the Evidence Act. The Constitution Bench of the Supreme Court overruled the judgment laid down in the ***State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru[(2005) 11 SCC 600*** by the two judge Bench of the Supreme Court. The court specifically observed that the Judgment of Navjot Sandhu supra, to the extent, the statement of the law on admissibility of electronic evidence pertaining to electronic record of this Court, does not lay down correct position and required to be overruled.

The only options to prove the electronic record/evidence is by producing the original electronic media as Primary Evidence in court or it's copy by way of secondary evidence U/s 65A/65B of Evidence Act. Thus, in the case of CD, DVD, Memory Card etc. containing secondary evidence, the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible. This case is important, which discuss in detail the admissibility of the digital evidence. The provisions regarding the digital evidence are discussed however, this judgment deals with the digital evidence and the admissibility of the digital evidence.

2. State of Tamil Nadu vs. Suhas Kutti:

It was the first conviction case under the Information technology Act, 2000. Indian court firstly convicted for the offence of cyber-crime. The judgment was pronounced in the year 2004, within the seven month after filling the FIR, which brings the conviction for the cyber-crime. The Honorable Judge of the Additional Chief Metropolitan Magistrate has passed the order of conviction. In this case, the victim was a divorcee who constantly harassed by annoying phone calls presuming that she would solicit them because of a massage posted on yahoo message group followed by forwarding emails. The massage was extremely obscene, defamatory and annoying. The accuse turn out to be her family friend and interesting in marrying her. The accused held guilty of offences under Section 469, 509 IPC and 67 of IT Act 2000. The accused had convicted and sentenced for the offence to undergo RI for 2 years. Under section 469 IPC to pay fine of Rs.500/-and, for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/-, and for the offence u/s 67 of IT Act 2000 to undergo rigorous imprisonment for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.

In the said case the offences registered under Indian Penal Code, though the entire illegal activity were perform by the accuse by using the computer and the internet, The Information technology Act 2000, mere provide punishment for publishing of information which is obscene in electronic form. This provision has not contended about the specific act whether the obscene material is about a particular person or victim. Therefore, the Indian Penal code

is requiring for the specific act. Accuse in this case publishing the obscene material regarding a victim, who is the widow of his friend, accuse is having family relation with the victim. Accuse intentionally posting post on yahoo messages grouped followed by the forwarding of emails. The massage was obscene, defamatory and annoying. The Section of the Information technology cover the obscenity but Indian Penal Code has provided the special provisions regarding forgery for purpose harming reputation under section 469; the I T Act has not provided any provision regarding this specific act or offence. Therefore, the Asst. Commissioner of Police, Cyber-crime Cell, C.C.B. Egmore, Chennai, has filed the Final Report against the accused.

In the investigation of this offence, it is found that the main reason behind the act of accuse is to defame the reputation of the victim, therefore he use the way of internet and yahoo message. Due to this only the Information Technology Act is attracted, but this Act cannot cover the act intending of insulting the modesty of woman, and defamation therefore the Indian Penal Code is attracted. The investigation machineries use the information technology, where it found that accuse created user id in the name of her and composed an obscene message intending that such document shall be used for posting in different obscene Yahoo Group, with the intention to make others to believe that the document was made by her, so that the persons seeing the obscene message would send offending calls to her, in harming her reputation and by insulting her modesty by the words exhibited in the email and in the course of same transaction. The agency used to find out the I P address in the said offences, which helps to trace the real accuse.

The Defense argued that the offending mails would have been given either by ex-husband of the complainant or the complainant herself to implicate the accused as accused alleged to have turned down the request of the complainant to marry her. Further the Defense counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime proved beyond reasonable doubt. Additional Chief Metropolitan Magistrate, delivered the judgment on 5-11-04.

This is the first conviction under the IT Act 2000 in India, the investigation is completed in minimum period means within seven month, the judgment is pronounce by the Additional Chief Metropolitan of Egmore, in the year 2004. The investigation and the trial completed in minimum period and the conviction given in the said matter. The Case of Suhas Katti is notable for the fact that the conviction achieved successfully within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case, which happened to be the first case of the Chennai Cyber-crime Cell going to trial deserves a special mention.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the woman in the belief that she was soliciting.

3. Avnish Bajaj vs. State (N.C.T.) of Delhi

This is landmark case on cyber-crime, which is known as Baazee.com case. This was a bail petition filed in the High Court of Delhi by the CEO of the Baazee.Com. Where in Mr. Avinish Bajaj, CEO, was arrested for the offence registered under section 67 of the Information technology Act, 2000 along with the Section 292 of Indian Penal Code. The allegation made against the MD of the Baazee.com and arrested for disturbing cyber pornography. The petitioner was arrested because someone had sold copies of a pornographic CD through the Baazee.com web site, being MD of the company offence was register against him.

The Court granted bail to him while considering the major factor as like no prima facie evidence is available against the accuse regarding the publication of the pornography. The obscene recording could not be view on the said web site. The Court finds out that there is no evidence that the accused had not actively perform any role for publication of the said material. The investigation of the crime is concern, the said accuse is fully cooperating with the crop machineries. The basic problem in this matter is, the offence is registered against the accused in the vicarious liability, being M D of the Baazee.com. There is no direct evidence against the accused for this offence. Indian Penal Code also not deals with the liability of manager in applied sections. So far as the petitioner is concern, the IPC does not recognized the concept of an automatic criminal liability attaching to the director where the company is an accused, not even a prima facie case for offence under Section 292 IPC is made out even when the charge sheet is read as a whole. It only seeks to implication him in his designation as MD of BIPL and not in his individual capacity. Therefore, the petitioner will discharge as far as the offences under section 292 and 294 IPC are concern.

While dealing with the Information technology Act, 2000, Section 67 in this matter, a prima facie case for the offence under section 67 with section 85 of IT Act is made out against the petitioner. Since the law as explain by the decision of the Supreme Court recognizes the deemed criminal liability of the director even where the company is not arranged as an accused and particularly since it is possible that BIPL may be hereafter summoned to face trial . It was held that the accused has actively participated in the investigations, and nothing was even argued before it in contrary by Counsel for the State. The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof. Even though the accused is no longer an Indian National, he is of Indian origin with family roots in our country. It cannot possibly be argued that a foreign national is disentitled to the grant of bail The accused is enlarged on bail subject to furnishing two sureties in the sum of Rs.1,00,000/- each to the satisfaction of the concerned Court. The Accused shall also not leave the territories of India without the leave of the Court and for this purpose; he shall surrender his passport to the Magistrate. It is implicit in the grant of bail that he shall participate and assist in the investigation. The Bail Application stands disposed of.

4. ***Devidas Ramachandra Tuljapurkar v. State of Maharashtra***,

The Supreme Court of India considered whether framing of charges be made for offence punishable under section 292 of IPC ode in relation to publication of a poem of historically respected personalities. The issue for consideration was whether the poem titled “Gandhi Mala Bhetala” (‘I met Gandhi’) in the magazine named the ‘Bulletin’ published, in July-

August, 1994 issue, which was privately circulated amongst the members of All India Bank Association Union, could give rise to framing of charge under section 292 IPC against the author, the publisher and the printer.

The court held that considering the fact that appellant (publisher) had published the subject poem which had already been recited and earlier published by others and that on coming to know about reactions of certain employees, he tendered unconditional apology before inception of proceedings (since when more than two decades had passed), for these reasons, the court held that charge framed was liable to be quashed.

5. Andhra Pradesh Tax Case

Dubious tactics of a prominent businessman, from Andhra Pradesh, were exposed after officials of the department got hold of computers, used by the accused in one of the many cyber fraud cases in India. The owner of a plastics firm was arrested and Rs 22 crore cash, was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days.

The accused submitted 6,000 vouchers, to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers, it was revealed that all of them were made after the raids were conducted. It was later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

6. Sanjay Kumar vs. State Of Haryana (10th Jan, 2013 CRR No.66 of 2013 (O&M) 1)

This is another landmark case on the cyber-crime. This is a criminal revision petition decided by Punjab-Haryana High Court. The Information Technology Acts 2000 Section 65 and Section 66 are involved in it. The offence registered against the petitioner, who was a software system supplier to the Bank along with the other Bank Manager, Vijay Bank, NIT, Faridabad moved a complaint dated 11.02.2003 before the Police stating that the petitioner was deputed by M/s Virmati Software and Telecommunication Ltd. to maintain the Software System supplied by them to the bank. He was also looking Software System of certain other banks. In connection with rendering such services, the petitioner was having access to their accounting system, which computerized and in a position to enter into ledgers and various other accounts. While reconciling the accounts, certain discrepancies were pointed out by the officials of the bank and in that process, it was revealed that the accused-petitioner, who was having SB Account No. 21499 in his CRR No.66 of 2013 (O&M) 3 personal name in their bank, manipulated the entries by forging and fabricating certain entries from one account to another.

After this from the computer system by handling the software and got the entries pertaining to the amount of the bank and withdraw the amounts from the bank on various dates by issuing cheque in his own favors and withdraw the amount from the cash counter of the bank as well as through transfer/clearing transactions. As per enquiry, it has been revealed that the accused by carrying out forgery, fabricating the entries in the computer system of the bank, illegally and wrongfully, withdrew Rs.17,67,409/- from the bank and thus, caused wrongful gain to himself and wrongful loss to the bank. The said Bank came to know regarding the

fraud committed by the accused on 07.02.2003. Thereafter, the accused called to the bank. He was confronted with the details of the fraud but he gave evasive replies as only admitted having embezzled a sum of Rs. 17 lacs without giving further information or revealing the exact amount of fraud or the modus operandi of the same and also assured to pay back the amount to the bank.

On receipt of the complaint, a case bearing FIR No. 165 dated 11.02.2003, under Sections 406, 420, 467, 468, 469, 471 of the Indian Penal Code and Sections 65, 66 and 72 of the Information and Technology Act, 2000 was registered against the petitioner. The learned trial Court, after appreciation of the evidence, found guilty under section Sections 420, 467, 468 and 471 IPC and Sections 65 and 66 of the Information & Technology Act, 2000 and convicted and sentenced the petitioner as aforesaid vide judgment and order dated 01.09.2011 and 03.09.2011 respectively. Thereafter, the petitioner preferred an appeal, which was dismissed by the learned Sessions Judge, Faridabad vide judgment dated 21.08.2012. Hence, this criminal revision.

The important issue for the discussion in this matter is that, the offences which are committed by the petitioner are whole cyber-crime, but the various provisions of the conventional criminal laws were attracted and the learned trial court convicted the accuse considering the ingredients of conventional law, which has proved by the prosecution beyond the reasonable doubt. But so far as the Section 72 of the Information Technology Act is concern, the petitioner is acquitted from the said charges. Because the petitioner is the authorised person to access the data, so his access cannot call unauthorized.

The High Court dismissed the revision petition filed by the petition against the order of appeal of Session Court. The High Court held that The learned Trial Court was wholly justified in convicting the accused-petitioner and the learned Appellate court, as can be clearly seen CRR No.66 of 2013 (O&M) 9 had not committed any error in upholding the conviction of the accused petitioner. Learned counsel for the petitioner failed to point out any misreading or non-reading of any evidence and could not point out any infirmity in the judgments of the Courts below. The findings of guilt, reached against the accused-petitioner does not, thus, suffer from any infirmity, legal or factual and does not therefore, warrant interference by this Court in exercise of this Court's revisional jurisdiction. In view of the above, there is no merit in the contentions raised by the learned counsel for the petitioner.

The Judgment in the said case shows that, though the crime is pure cyber-crime, for the registration and the conviction of the accuse in any cyber-crime, the conventional criminal law is require and plays the main role. Though the offence is committed in cyber space and the tool and the target of the offence is computer and the data of the computer, but the Indian penal code is attracted and therefore we can say that cyber-crime is part of the conventional crime. The investigation made in this matter is based on the conventional process, only the technical assistant is taken and the electronic evidence is used to prove the guilt of the accuse .Otherwise, the offences is same and one, the object is nothing the wrongful gain. The offences, which are registered against the accused, in this case, are nothing the criminal breach of trust and the offence of cheating. These are the conventional crime.

The IT Act is attracted only because the offender uses the computer source to commit the crime; otherwise, the guilty intention and act are the same. There is nothing different in this

but the use of the tool to commit the crime makes it cyber-crime. Thought the technical investigation is use to bring the evidences before the court, but the role of prosecution is similar to prove the ingredients, which are going to prove in the traditional crime. The difference between the cyber-crime and the conventional crime is mere the technical process of the investigation, that is nothing but the electronic evidence and its appreciation before the court. Apart from this, there is no difference between the cyber-crime and the conventional crime.

Thus, all the judgments show that the cyber-crime is part of the conventional crime, not different from the traditional crime. The main ingredients are similar. Therefore, the cyber-crime is not the different species of the crime, but it is the crime, which is committed by using the new techniques of the communication. All the traditional crime, which is subject to the need of communication between the accused and victim, can commit by the informational technology that can be called as a cyber-crime. The offences as like extortion even can commit by using the internet or the email that is called cyber-crime. Though this case is well known case of the cyber-crime, but the court while delivering the judgment, discuss more regarding the conventional criminal law rather than cyber-crime. The traditional crimes were committed by using the computer therefore the relevant section of Information Technology Act,2000 were refer, but firstly confirms the conviction according the Indian Penal Code.

7. Fatima Riswana v. State Rep. by A C P., Chennai & Ors:

The appellant is a prosecution witness in S.C. No. 9 of 2004. wherein respondents 2 to 6 are the accused facing trial for offences punishable under Section 67 of Information Technology Act, 2000 r/w Section 6 of Indecent Representation of Women (prohibition) Act, 1986, and under Section 5 & 6 of Immoral Traffic (Prevention) Act, 1956, Under Section 27 of Arms Act, 1959 And Sections 120(B), 506(ii), 366, 306 & 376 of I.P.C. The said trial relates to exploitation of certain men and women by one of the accused Dr. L. Prakash for the purpose of making pornographic photos and videos in various acts of sexual intercourse and thereafter selling them to foreign websites. The said session's trial came to be allotted to the foreign websites. The said Session's trial came to be allotted to the V Fast Track Court, Chennai that is presided over by a lady Judge. When the said trail before the V Fast Track Court was pending certain criminal revision petitions came to be filed by the accused against the orders made by the said court rejecting their applications for supply of copies of 74 Compact Discs (CDs) containing pornographic material on which the prosecution was relying.

This revision petition were rejected by the Madras High Court by its order dated 13th February, 2004, holding that giving all the copies of the concerned CDs might give room for copying such illegal material and illegal circulation of the same. However, the court permitted the accused persons to peruse the CDs of their choice in the Chamber of the Judge in the presence of the advocates, the expert, the public prosecutor and the investigating Office. It also observed that the case be transferred to another court with competent jurisdiction presided by a male officer at the option of the sessions judge and taking the same the accused filed a revision petition for transferred to Fast track 4 court presided by the male officer and the Appellant alleged that she would be embarrassed. If the trial is conducted by the male presiding officer and that the lady sessions judge didn't object or the trial of the case

in the fast track 5 and the high court has erred in transferring the case and the Appellant was not given any opportunity of being heard before the alleged transfer.

The learned counsel for the respondents contended that the Appellant learned though arrayed as witness is for all purpose an accused herself and law officer appearing in the case had expressed their embarrassment in conducting the trial before a lady Presiding Officer and even though the Presiding Officer did not expressly record her embarrassment, it was apparent that she too wanted the case to be transferred to another court, therefore, this Court should not interfere with the order of transfer. It was held that this appeal has to be allowed in the sessions case No. 9 of 2004 now transferred to the IV Fast Track Court Chennai be Transferred back to the V Fast Track Court, Chennai.

This is another landmark case in which section 67 of the Information Technology Act is involved. Wherein the accused is prosecuted for making and publishing the pornographic video, the said act also covered various other crimes. It also deals with the Indian Penal codes. The technical problem arises in this case, due to the technical problem the session court not allow the accused to give the copies of CD on the technical matter. The accused filed the revision petition against the order of the session Court. This problem arises due to the technical nature of the evidence, which is important to adjudicate the matter. The Judiciary is facing the problem of the technical matter.

8. Nirav Navinbhai Shah & 4 ors. Vs. State of Gujarat and Anr.

The applicants, original accused in crime I.C.R. No. 54 of 2004 dated 26.02.2004 registered with sector 7 police station Gandhinagar for offences punishable under sections 381, 408, 415, 418, 420 read with sections 34 and 120B of the Indian Penal Code and section 66 and 72 of the Information Technology Act, 2000 (herein after referred to as 'the IT Act for short) have preferred this application under section 482 of the Code of Criminal Procedure 1973. (herein after referred to as 'the code' for short) for quashing of FIR I.C.R. No. 54 of 2004 dated 26.02.2004 registered with Sector No. 7 Police Station, Gandhinagar and the resultant Criminal Case No. 54 of 2004 dated 26.02.2004 registered with sector No. 7 Police station Gandhinagar and the resultant Criminal case No.3528 of 2004 pending before the Judicial Magistrate First Class Gandhinagar, mainly on the grounds that the facts and allegation leading to lodging FIR show that the real dispute was a civil dispute and as the same has been amicably settled between the parties, no useful purpose would be served in continuing the criminal proceedings, rather continuation of same would be counterproductive to the interest of justice.

The complaint also does not contain any essential ingredient for maintaining criminal proceeding for the alleged offences. It was stated in the arguments of the learned counsels that the parties have filed civil suits also in respect of the same dispute. The entire dispute between the parties is resolve by amicable settlement. The alleged hacking is perpetrated on the complainants computer system only which said to have data pertaining to its client. The Counsels have submitted that on some of the web sites these data are already available. The dispute appears to be private in nature. The offence alleged is not strictly affecting or infringing any other individual or citizen. Thus looking to the nature of the disputes, it can well be said that continuation of the same is not in interest of justice. It was held that the FIR 54 of 2004 registered at sector 7 Police Station Gandhinagar and resultant Criminal Case No.

3528 of 2004 pending before the JMFC Gandhinagar deserve to be quashed in the interest of just and hereby they are quashed. Rule is made absolute.

9. Syed Asifuddin and Ors. vs. The State of Andhra Pradesh & Anr.:

This is another landmark case of cyber-crime, decided by the Hon'ble HighCourt of Andhra Pradesh. The Hon'ble court decide two writ petition in this matter, Wherein the partitions filed the application under section 482 of the Criminal Procedure code, to quash the FIR filed by the CID, against the petitioner for the offences register under Indian Penal Code and the Informational Technology Act. So far as the Information Technology Act,2000 is concern the offence is register under section 65, 66,2(1), deals with the punishment for tampering with the computer sources. The petitioners were arrested who are the employee of the Tata Indi come. Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocom.

While deciding the petition, the Hon'ble Court discussed section 65, 66 and 2(1) of the Information technology Act,2000 to decide that which is include into the electronic devise and computer network. While dealing with the petition the Court finds so far these sections are concern in the manner as "Allegation against the petitioners that the Mobile identification number (MIN) of Reliance phone is irreversibly integrated with Electronic serial Number(ESN) and the petitioner hacked ESN so as to wean way RIM customers to Tata indicom services. Clauses (i), (j) and (1) of Section 2(1) of Information Technology Act would shows that any electronic, magnetic of optical device used for storage for information received through satellite, microwave or other communication media and device which are programmable and capable of retrieving any information by manipulations of electronic magnetic or optical impulses is computer, which can be used as a computer system in the computer network.

All cell phone services provides like Tata Indicom and Reliance India mobile have special code dedicated to them and these are intended to identify the phone, the phone owner and the service provider: To understand how the cell phone works it is necessary to know certain terms in cell phone parlance. System Identification Code (SID) is a unique 5 digit number that s assigned to each carrier by the licenser. Electronic Serial Number is unique bits 32 bit number programmed into the phone when it is manufacture by the instrument manufacturer. Mobile identification number is 10-digit number derived from the cell phone numbers given to the subscriber. By the very definition of the computer source code, a) List of program; b) computer commands; c) design and layout and program analysis of computer resources in any form is a computer source code for the purpose of Section 65 of IT Act Going by the identification. Therefore, prima facie, when the ESN is altering, the offence under section 65 of IT Act is attracted because every service provider like respondent has to maintain its own SID code and also gives a customer's specific number to each instrument used to avail the services provides."

The Hon'ble High Court discusses the scope of the computer program and computer sources. While dealing with this matter the court widen the scope of the computers and includes the cell phones in the concept of the computer and rejected the said petition of the petitioner. The ESN and SID come within the definition of "computer source code" under section 65 of the

Information Technology Act. So once the ESN recognized as a computer source code, then if it alters unauthorized, it attracting the offence made punishable under section 65 of the Information Technology Act, 2000. The decision gives the proper meaning to the computer source code and the changing it amount to the tampering with the computer sources. Apart from that the offences which are registered against petitioner are under certain section of Indian Penal Code and also considered prima facie case made out.

10. State vs. Mohd. Afzal and others:

This is the one of the landmark case, which deals with the electronic evidences, and the court recognizes the electronic evidence as reliable to convict the accused. Several terrorists had attacked the Parliament House on 13th December, 2001. Digital evidence played an important role during their prosecution. The accused had argued that computers and digital evidence can easily be tamper, hence should not be relied upon. The computer and the digital world is sole based on the techniques, so it can change according to the accused so it was argue that the court should not rely on the digital evidences. However, the court rejected the arguments of the accused and admitted the digital evidences.

The validity of the Section 65B of the evidence Act was challenge by the petitioner, considering that, it can change by the techniques so Court should not relay on it. While court considering that the Section 65B of the Indian Evidence Act and Section 69 of the Act in England have same effect, therefore Court reject the contention of the petitioner. The Court discuss Section 69 of The Police & Criminal Evidence Act, 1984 of England 280 reads as under:

In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown (a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer. (b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents.

Thus Hon'ble Court recognized the principle given in this section and rejected the contention of the petitioner. The Court held that, the accuracy of the Computer cannot be challenge, still the alleged misused cannot be proved. Therefore, the Court Conclude that if someone challenges the accuracy of computer evidence on the ground of misuse of system or operating failure or interpolation, then the challenger has to establish the challenge. Mere theoretical and generic doubts cannot be cast on the evidence.

Thus, the Indian Judiciary has recognized the validity of the computer or digital evidence, and realized that the Amendment in Indian Evidence Act after passing the Information Technology Act, 2000 is need of the hours. The decision of this case shows that the digital world is expanding its scope and therefore, the amendments in procedural laws needed for the appropriate administration of justice in India. The Indian Laws are mostly depending on the legislative and judicial principles of Great Britain, and the judgment in this case retreat the same thing.

11. Sony.Sambandh.Com Case:

India saw its first cyber-crime conviction recently. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online. The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The company lodged a complaint for online cheating at the Central Bureau of Investigation, which registered a case under Section 418, 419 and 420 of the Indian Penal Code.

The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site. The CBI recovered the colour television and the cordless head phone .In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code this being the first time that a cybercriminal has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year. The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cyber-crimes, which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

12. Ritu Kohli's case:

The case is deals with offence of cyber stalking. Where in the young Indian girl being cyber stalked by a former colleague of her husband, by sending obscene massages ad emails. The Delhi Police arrested Manish Kathuria the culprit of the case. In the said case, Manish was stalking a person called Ritu Kohli on the Net by illegally chatting on the website www.mirc.com with the name of Ritu Kohli. Manish was regularly chatting under the identity of Ritu Kohli on the said Website, using obscene and obnoxious language, was distributing her residence telephone number and inviting chatter to chat with her on telephone. Consequently Ritu Kohli was getting obscene calls from different chatters from various parts of India and abroad. Ritu Kohli reported the matter to the police and the Delhi

Police swung into action. The police had registered the case under Section 509 of the Indian Penal Code for outraging the modesty of Ritu Kohli.

The Indian Penal Code, section 509 deals with the words or gesture intended to outrage the modesty of woman, but it does not deals with the massages through the internet or computer. Even the IT Act 2000 also not deals with such kind of crime. None of the Act and the section deals with such kind of act. In such situation after all the Indian penal code, conventional criminal law and the sections can use to deals with such kind of offences. Section 503 of Indian penal code deals with the sending the threading emails, but it not cover the modesty. This case compels the Indian legal system to enact the effective rules, which include the stalking. Due to this Section 66A of the Information Technology Act, 2008 (Amendment 2008) is inserted which states, "Punishment for sending offensive messages through communication service, etc. Indian Penal Code also dealing with the stalking under section 354 D, which is included by the Criminal Law Amendment Act, 2013.

13. Shreya Singhal v. U.O.I:

This is a landmark judgment, concerning section 66A of the Information Technology Act, 2000. This Section was not in the Act as originally enacted, but came into force by virtue of an Amendment Act of 2009 with effect from 27.10.2009.

The reason behind the insertion of section 66A according to the Amendment Bill was: "A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism, and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes".

Facts: The Petitioners have raised a large number of points as to the constitutionality of section 66A. According to them, first and foremost Section 66A infringes the fundamental right to freedom of speech and expression and is not saved by any of the eight subjects covered in Article 19(2).

Further, in creating an offence, section 66A suffers from the vice of vagueness because unlike the offence created by section 66 of the same Act, none of the aforesaid terms are even attempted to be defined and cannot be defined, the result being that innocent persons are also roped in. Such persons are not told clearly on which side of the line they fall; and it would be open to the authorities to be as arbitrary and whimsical as they like in booking such persons under the said section. In fact, a large number of innocent persons have been booked. The Court held that the provision of section 66A of the IT Act is derogative to the Article 19(1) (a) and as such it is an arbitrary provision which breaches the right of citizen to have freedom of speech and expression of their views on internet. As such the provision concerned is constitutionally invalid and as such struck down in its entirety.

14. Well-known orthopedist in Chennai got life imprisonment:

Dr. L Prakash stood convicted of manipulating his patients in various ways, forcing them to commit sex acts on camera and posting the pictures and videos on the Internet. The 50-year-old doctor landed in the police net in December 2001 when a young man who had acted in one of his porn films lodged a complaint with the police. Apparently the doctor had promised the young man that the movie would be circulated only in select circles abroad and had the shock of his life when he saw himself in a porn video posted on the web. Subsequent police investigations opened up a pandora box. Prakash and his younger brother, settled in the United States, had piled up close to one lakh shots and video footages, some real and many morphed. They reportedly minted huge money in the porn business, it was stated. Fast track court judge convicted all the four in Feb 2008, also imposed a fine of Rs 1.27 lakh on Prakash, the main accused in the case, and Rs 2,500 each on his three associates - Saravanan, Vijayan and Asir Gunasingh. The Judge while awarding life term to Prakash observed that considering the gravity of the offences committed by the main accused, maximum punishment under the Immoral Trafficking Act (life imprisonment) should be given to him and no leniency should be shown. The Judge sentenced Prakash under the Immoral Trafficking Act, IPC, Arms Act and Indecent Representation of Women (Prevention) Act among others.

15. Juvenile found guilty for sending threatening email

A sixteen year old student from Ahmedabad who threatened to blow up Andheri Railway station in an email message was found guilty by the Juvenile Court in Mumbai. A private news channel received an email on 18 March 2008 claiming sender as Dawood Ibrahim gang saying a bomb would be planted on an unspecified train to blow it up. The case was registered in Andheri Police station under section 506 of IPC and transferred to cyber-crime investigation cell. During Investigation CCIC traced the cyber cafe from which the email account was created and threatening email was sent. Cafe owner told police about friends which had come that day to surf the net. Police summoned them and found that the system which was used to send email was accessed by only one customer. On 22nd March 08, police arrested the boy a Class XII science student who during interrogation said that he sent the email for fun of having his prank flashed as “breaking news’’ on television.

16. Two Nigerians sentenced seven years RI for online fraud

A local court in Malappuram district in Kerala sentenced two Nigerians to five years rigorous imprisonment on July 20, 2011 in a cyber-crime case. The two had cheated a doctor in the district of Rs 30 lakh about two years ago. Johnson Nwanonyi (32) and Michel Obiorahmuozboa (34), both hailing from Anambra state in Nigeria, were sentenced each under sections 420 (cheating)-5 years, and 468(forgery)-5 years of IPC and section 66(D) (phishing) of Information Technology (Amendment) Act 2008 -2 years and a fine of Rs 1.25 lakh by a Chief Judicial Magistrate V Dileep in Manjeri in Malappuram district. The sentence would run concurrently.

According to the charges filed by the Karipur police, the duo had cheated the doctor Dr. C Thomas, hailing from Valluvambram in Malappuram district after they sent an e-mail asking to pay Rs 30 lakh as processing fee. But a planned move by the police and the doctor

succeeded when the Nigerians were lured into Kerala in March 2010. They were then arrested by the Karipur police. The strong evidence based on which the prosecution presented the case became crucial in the first verdict against financial fraud under the Information Technology Act.

17. AP High Court dismisses Google's Petition contending being intermediary it cannot be held liable for defamation

The petitioner/A-2 is accused of offences punishable under Sections 120-B, 500, 501/34 I.P.C in C.C. No.679 of 2009 on the file of XI Additional Chief Metropolitan Magistrate, Secunderabad along with another. The petitioner/A-2 is Google India Private Limited represented by its Managing Director (Sales and Operations). The 1st respondent/complainant is Visaka Industries Limited, Secunderabad represented by its authorised signatory who is its Deputy Manager- Legal. The complainant is engaged in business of manufacturing and selling of Asbestos cement sheets and allied products. It is alleged that A-1 viz., Gopala Krishna is a Co-ordinator "Ban Asbestos India" a group which is hosted by A-2 and publishes regular articles in the said group and that on 21.11.2008 an article was published in the said group and it was captioned as "poisoning the system; Hindustan Times" aiming at a single manufacturer of Asbestos cement products viz., the complainant and names of renowned politicians of the country G.Venkata Swamy and Sonia Gandhi who have nothing to do with the ownership or management of the complainant-company were named in that article.

1. It is further alleged that on 31.07.2008 another article captioned as "Visaka Asbestos Industries making gains" and that both the above articles contained defamatory statements against the complainant and they are available in Cyber space in the form of articles for worldwide audience. In the complaint, details of defamatory remarks made in several other articles published by A-1 in A-2 group are given in detail, which details may not be necessary for the purpose of disposal of this criminal petition.
2. It is contended by the senior counsel appearing for the petitioner/A-2 that actions of intermediaries such as Google Inc., which is a service provider providing platform for end users to upload content, does not amount to publication in law and consequently the question of holding such intermediaries liable for defamation does not arise. Senior Counsel appearing for the petitioner placed reliance on Section 79 of the Information Technology Act, 2000 (in short, the Act) in support of this contention.
3. Section 79 which occurs in Chapter XII of the Act originally as it stood enacted in the year 2000 reads as follows:

   "Chapter XII Network Service Providers Not To Be Liable In Certain Cases”

   79. Network service providers not to be liable in certain cases: For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Explanation. For the purposes of this section,

a. "network service provider" means an intermediary;
b. "third party information" means any information dealt with by a network service provider in his capacity as an intermediary."

The said provision exempts network service providers from liability under the Act, rules or regulations made thereunder for any third party information or data made available by him. It did not exempt a network service provider from liability much less criminal liability for the offences under other laws or more particularly under the Indian Penal Code. Further, the above provision exempts network service provider from liability, only on proof that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Proof in that regard can be let in by way of leading evidence by the accused. Therefore, the said question is a question of fact which this Court may not go into in this petition filed under Section 482 Cr.P.C.

4) Chapter XII of the Act including Section 79 was amended by the Information Technology (Amendment) Act, 2008 (10 of 2009) dated 05.02.2009 with effect from 27.10.2009 by way of substituting the following in the place of original chapter:

"Chapter XII Intermediaries Not To Be Liable In Certain Cases

Exemption from liability of intermediary in certain cases:

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
(2) The provisions of sub-section (1) shall apply if-

i. the functions of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
ii. the intermediary does not-
   a) initiate the transmission,
   b) select the receiver of the transmission, and
   c) select or modify the information contained in the transmission;
iii. the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of Sub-section(1) shall not apply if-

a) The intermediary has conspired or abetted or aided or induces whether by threats or promise or otherwise in the commission of the unlawful act;
b) upon receiving actual knowledge, or on being notified by information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.- For the purposes of this section, the expression "third party information" means any information dealt with an intermediary in his capacity as an intermediary."

It is only under the said amendment, non-obstenti clause was incorporated in Section 79 keeping application of other laws outside the purview in a fact situation covered by the said provision. Now, after the amendment, an intermediary like a network service provider can claim exemption from application of any other law in respect of any third party information, data or communication link made available or hosted by him; provided he satisfied the requirements under Sub-section (2) of Section 79.

Further, as per amended Sub- section (3) of Section 79, the exemption under Sub-section (1) cannot be applied by any Court and cannot be claimed by any intermediary in case the intermediary entered into any conspiracy in respect thereof. Also, the intermediary cannot claim exemption under Sub-section (1) in case he fails to expeditiously remove or disable access to the objectionable material or unlawful activity even after receiving actual knowledge thereof. In the case on hand, in spite of the 1st respondent issuing notice bringing the petitioner about dissemination of defamatory material and unlawful activity on the part of A-1 through the medium of A-2, the petitioner/A-2 did not move its little finger to block the said material or to stop dissemination of the unlawful and objectionable material. Therefore, the petitioner/A-2 cannot claim any exemption either under Section 79 of the Act as it stood originally or Section 79 of the Act after the amendment which took effect from 27.10.2009. The present case in the lower Court was instituted in January, 2009 relating to the offences which are being perpetrated from 31.07.2009 onwards i.e., since long prior to the amendment to the said provision.

a) There is no exemption of any criminal liability in respect of a company which is a juristic person and which has no body that can be damned or contemned. In case found guilty, the petitioner company can be awarded with appropriate punishment though not corporal punishment. In that view of the matter, I find no merit in this criminal petition.
b) Accordingly, the Criminal Petition is dismissed.

4. Father & son convicted under IT act in Kerala

The Additional District and Sessions Court here has upheld a lower court's verdict in the first cyber case filed in the State sentencing a Pentecostal Church priest and his son to rigorous imprisonment in 2006. The appeal filed by the priest T.S. Balan and his son, Aneesh Balan, against the order of the Chief Judicial Magistrate was disposed of. Additional District Judge T.U. Mathewkutty said it was time the government took effective measures to check the growing trend of cyber-crimes in the State.

The court upheld the magistrate's order sentencing the two to three-year rigorous imprisonment and imposing a fine of Rs. 25,000 under Section 67 of the information technology (IT) Act; awarding six months rigorous imprisonment under Section 120(B) of the Indian Penal Code; and ordering one year rigorous imprisonment and imposing a fine of Rs. 10,000 under Section 469 of the code. The court revoked the sentence under Section 66 of the IT Act. The cyber case dates back to January-February 2002 and the priest and his son became the first to be convicted of committing a cyber-crime. The two were found guilty of morphing, web-hosting and e-mailing nude pictures of Pastor Abraham and his family. Balan

had worked with the pastor until he fell out with him and was shown the door by the latter. Balan joined the Sharon Pentecostal Church later.

The prosecution said the duo had morphed photographs of Abraham, his son, Valsan Abraham, and daughter, Starla Luke, and e-mailed them from fake mail IDs with captions. The morphed pictures were put on the web and the accused, who edited a local magazine called The Defender, wrote about these photos in his publication. Valsan received the pictures on the Internet and asked his father to file a complaint to the police. A police party raided the house of Balan and his son at Perumbavoor and collected evidences.

The magistrate's verdict came after a four-year trial, for which the court had to procure a computer with Internet connection and accessories. The police had to secure the services of a computer analyst too to piece together the evidences. Twenty-nine witnesses, including the internet service provider and Bharat Sanchar Nigam Ltd., had to depose before the court.

Cyber-crime related issues in India:

Jurisdictional issues: In India, there are also certain provisions that have a bearing on the issue of jurisdiction for cybercrimes and cyber-investigations. Section 3 of the IPC, 1860 provides for the punishment of offences committed beyond India, but which, by law, may be tried within India. Punishment of offences committed beyond but which by law may be tried within India- any person liable by any Indian law to be tried for an offence committed beyond India shall be dealt with according to the provisions of this Code for any act committed beyond India in the same manner as if such act has been committed with in India.

Section 4 of the IPC provides for an extension of the provisions of the Code to extraterritorial offences: 'The provisions of this Code apply also to any offence committed by

1. Any citizen of India in any place without and beyond India;
2. Any person on any ship or aircraft registered in India where it may be.

Explanation- In this section the word 'offence' includes every act committed outside India, if committed in India, would be punishable under this code.

Clearly, cybercrime brings along with it numerous issues concerning jurisdiction. The Indian legislators were possibly aware of the potential challenges that the tricky subject. That is the reason why they have adopted two distinct provisions relating to jurisdiction, in sections 1(2) and 75 IT Act. Normally, the applicability of laws within India can be broadly divided into the following major categories: laws applicable to all states of India barring Jammu and Kashmir, laws applicable to Jammu and Kashmir; and laws applicable to the entire country. Jammu and Kashmir has been granted a special status under the Constitution of India, and special laws are applicable to that state. Keeping in mind the universal nature of the impact of computers and the internet, the legislature has decided that the IT Act shall be applicable to the whole of India including Jammu and Kashmir. However, the law has gone much further.

Section 1 IT Act deals with the issue of applicability of this new law.

1. This Act may be called the Information Technology Act,2000

2. It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person.

This means that law applies to any violation or contravention of the provision confers jurisdiction over those who violate the IT Act while outside the territorial boundaries of India. This worldwide scope is attributable, no doubt, to the fact that, as many have pointed out, cyberspace knows no territorial boundaries; the internet is a network of computers, joined together by telephone lines throughout the world. It is difficult to say which portion of cyberspace is within India or which outside India as boundaries cease to have any meaning. Today, people, in order to fulfill their criminal motives, are using cyberspace and computers with impunity.

This provision enables Indian law-enforcement agencies to pursue cyber criminals outside the territorial boundaries of India and who violate the provisions of IT Act. This point made by some, i.e., that a law assuming extraterritorial jurisdiction is not enforceable in the real world, has some merit. It is contrary to the principle of international law to assume jurisdiction over citizens of another country, and so, it is likely to lead to a conflict of jurisdiction concerning different courts situated in different national jurisdictions. Also, it is important to note that there are differences between national legislations, laws, legal processes and procedure. Further compounding the problem is the issue that a particular act in one national jurisdiction can be legal and not barred by law but, at the same time, it is illegal and barred by law prevailing in another national jurisdiction.

Another ground of criticism has been that section 1 does not lay down the parameter of how such provision would be enforceable in practical terms across transnational boundaries and jurisdictions. Government can use extradition process to bring cybercriminals to their territory for prosecution, if there is a valid extradition treaty in place between the relevant countries. But the route stipulated in section 1 IT Act is likely to throw up complex arena of difficulties in actual day to day implementation. The existing international law pertaining to the sovereignty of a nation also details that a sovereign nation can make laws affecting people who reside within territorial boundaries. However, the birth of the internet has seen geography become history, and transaction taking place over networks are transnational in nature, thereby complicating the entire issue of jurisdiction.

Section 75 IT Act deals with the issue of applicability of Indian Cyber law for an offence or contravention committed outside of India. Section 75 thus makes the provisions of the IT Act applicable to any offence committed outside India by any person, irrespective of his nationality. This enables the law to assume jurisdiction over cybercriminal outside the territorial boundaries of India. The caveat to section 75(1) is explained in section 75 (2); in other words, section 75(1) is subject to the provisions of section 75(2). The caveat provided by section 75(2) is that the IT Act shall apply to any offence or contravention committed outside India by any person if and only if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. Section 75(2) of the Indian IT Act uses the phrase ‘involving a computer, computer system or computer network located in India.’ The word ‘involving’ is an all-embracing term which leaves no exceptions.

Thus, regardless of whether the involvement of computer, computer system, or computer network is intentional or unintentional, deliberate, accidental or otherwise, all such scenarios would cover within ambit of the word 'involving'. Therefore, the physical location of the computer, computer system, or computer network within territorial boundaries of India is a condition precedent to the applicability of this Act to any offence or contravention committed outside India by any person irrespective of his nationality. Section 75 thus takes a somewhat saner view of the issue of extraterritorial jurisdiction than section 1(2) IT Act. It has been argued in India that the necessity of having the present provision is because of the emergence and growth of cyberspace, which does not have any boundaries.

As the internet is making geography history, it is imperative that nations enact laws that have an all pervasive applicability and impact. Further, such an approach facilitates nations to catch cybercriminals who are located physically outside territorial boundaries. On the other hand, the provision is liable to be criticized in as much as no country can assume jurisdiction over the citizen of another country, merely on the ground that that citizen has violated the national laws of that nation. The move has been criticized as being contrary to the established principle of international law.

The Indian approach given in section 1(2) as modified by section 75 IT Act has created confusion in the actual implementation of the law. This becomes all the more evident from the emerging principles from various judgments relating to jurisdiction over the internet. From the beginning of the internet, the issue of jurisdiction has continued to challenge legal minds, societies, and nations in the context of the peculiarly inherent character of the internet.

Different principles were being evolved in different national jurisdiction in this regard. In the traditional notions of jurisdiction, the courts assumed jurisdiction on the basis of the place where the cause of action arisen. Due to the peculiarity of cyberspace, the well -established principles of jurisdiction no longer provide clarity. The courts, while acknowledging some of the challenges which the internet poses for the law of jurisdiction, have tried resolving issues with the application of well-established judicial principles.

In the beginning, the courts of different countries, including India, began making access to the internet a sufficient ground for assuming jurisdiction over inter-related transaction. However, there has been a kaleidoscopic shift in the principles of assumption of jurisdiction in the areas relating to cyberspace. Considering the entire issue of cybercrime jurisdiction from Indian perspective, there is by far no established principles. However, case law relating to civil law jurisdiction has been developed. Such jurisprudence is indeed relevant and can be helpful in the evolution of cybercrime case law over a period of time. As such it will be relevant to examine the said civil-law jurisdiction jurisprudence in India at this stage. Section 19 of the Code of Civil Procedure, 1908 is a provision that clarifies the position under Indian law in the case of multiple jurisdictions. Section 19 provides that:

Where a suit for compensation for wrong done to the person or to moveable property, if the wrong was done within the local limits of the jurisdiction of one court and defendant resides, or carries on business, or personally works for gain, within the local limits of jurisdiction of another court, the suit may be instituted at the option of the plaintiff in either of the said courts.

The same principle has safely been applied to the internet within India. However, in case of disputes arising in two different countries, the problems are complex, to say the least. Section 1(2) and section 75 IT Act provide for extraterritorial jurisdiction of the Indian courts which, however, seems unlikely to be implemented. The courts in India at present have been sporadic in following the trend of asserting jurisdiction on the basis of active accessibility of website. So far in various cases related to internet domain names, the Delhi High Court has assumed jurisdiction on the basis of accessibility of websites in India. In Indian context, in the beginning, the inter-related disputes that emerged were domain name disputes. Many of these disputes arose prior to the coming into effect of the domain-name Uniform Dispute Resolution Policy of Internet Corporation for Assigned Names and Numbers (ICANN). Consequently, various civil suits for injunctions and declarations were filed under existing trademark law. In a majority of these initial cases, the courts of India, including Delhi High Court, assumed jurisdiction over internet domain names disputes merely on the ground of access to the internet. In a majority of these cases court assume territorial jurisdiction over the disputes on the ground that internet could be accessed from territories within their territorial boundaries of the concerned court. In the judgment rendered in the famous Yahoo! France case, the judicial thinking on jurisdiction was further refined.

The Supreme Court of India, in the case of ***SIL Import vs. Exim Aides Silk Importers*** has recognised the need of the judiciary to interpret a statute by making allowances for any relevant technology change that has occurred. Until there is specific legislation in regard to the jurisdiction of the Indian Courts with respect to internet disputes, or unless India is a signatory to an international treaty under which the jurisdiction of the national courts and the circumstances under which they can be exercised are spelt out, the Indian Courts will have to give a wide interpretation to the existing statutes, for exercising internet disputes.

The US judgment has had far-reaching significance and consequences on the entire subject jurisdiction. Until it is issued, the courts anywhere in the world could assume, and were assuming, jurisdiction over internet transactions and web sites that were located outside the country. This decision underlines the principle that even if a foreign court delivers a judgment or direction against legal entity of a particular country, say country A, then that judgment or direction would not be applicable automatically to country A's legal entities or citizen. This is completely contrary to the earlier French Court's decision on the same matter, where the French court assumed jurisdiction over Yahoo! (a US company, based in the United States and amenable to US laws) and held them liable for anti-Semitic material. Some scholars are of the view that The US decision is more pragmatic approach and is liable to be the forerunner of the evolution of jurisprudence on this subject. This is all the more evident from the current internet governance debate that is going on, at the time of writing, where countries across the world are moving towards the exercise of their sovereign rights in the context of the internet.

The decision or direction of a foreign court will need to be scrutinized by country A's courts, keeping in mind the touchstone and basic principles enshrined in its constitution and in its local laws, before it can be forcible in country A. It is evident that the courts are looking at totality are looking of the circumstances when determining whether to exercise jurisdiction over individuals involved in internet related activities. It is still to be seen how the Indian

approach on jurisdiction will emerge with the coming of the IT Act and with its provisions on extraterritorial jurisdiction.

It is likely that the Indian courts are likely to adopt the principle of law enunciated in Yahoo! case in US, as that is in sync with the assertion of the sovereignty of the state, which has been upheld by the courts of India on numerous occasions. The likelihood of this outcome is further supported by various events that have taken place in India. In mid-2001, the government of India's Ministry of External Affair website was hacked. The year 2001 also saw hacking of the websites of AIIMS, the Atomic Energy Research Board and many other governmental and semi-governmental web sites. All these hacking attacks emerged from computers and entities located outside India. However, in none of the cases was jurisdiction under sections 1(2) and 75(1) IT Act invoked, either for purposes of the registration of criminal cases under section 66 IT Act or for claiming damages under section 43 IT Act. Even the case that was registered by law-enforcement agencies in the matter relating to the hacking of the web site of the CBDT has not seen much progress.

2. *Evidentiary issues:*

As regards electronic evidence and its admissibility in India, the law has provided for special provisions. The evidentiary status of electronic data in India is governed by provisions of Section 65B of the amended Indian Evidence Act, 1872, (hereinafter IEA) as amended by the IT Act. The relevant provisions are section 65A and 65B of the IEA. These provisions provide for admissibility and mode of proving electronic evidence as well as printouts of the same. Section 65 of the amended IEA prescribes the manner in which electronic evidence may be produced and proved in a court of law in India. However, the law does not stipulate what kind of electronic evidence can be permitted as admissible. Thus, in the event of electronic data obtained in the course of extraterritorial investigation in another country of cybercrime matter that has occur in India, especially if that country and India have different opinions about the lawfulness of such extraterritorial investigation, the important question to determine in such case would be as to the legality of the said collected evidence in India. The relevant and competent forum to determine this would be a court of law within India.

Digital evidence is any probative information stored or transmitted in digital form. A Party in court case may use the same a trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is secondary evidence and whether a copy is acceptable or the original is required.

The Indian courts have adopted innovative, pragmatic, and proactive strategies in terms of permitting the use of gathering evidence across by means of video conferencing. In various cases, Indian court have permitted and have indeed recorded evidence by way of videoconferencing, tendered by witnesses physically located in different territorial areas outside the boundaries of India. Such evidence has been made legal and valid in Indian law and Indian court procedure by various laws, including the IT Act and IEA. However if it can be shown that data so obtained could not have been obtained in a legal manner or that it was obtained outside the parameters of or in violation of existing laws, then the court of law in India is likely to be inclined not to take the said data into consideration.

In the case of ***State of Maharastra vs. Dr Praful B Desai ,*** the Supreme Court observed that video conferencing is an advancement of science and technology which permits seeing, hearing and talking with physically present. The Court allowed the examination of a witness through video conferencing. In this case, it was observed that "there is no reason why the examination of a witness by video conferencing should not be an essential part of electronic evidence."

In the case of ***Amitabh Bagchi v. Ena Bagchi*** , it was held that the physical presence of person in Court is not required for purpose of adducing evidence and the same can be done through medium like video conferencing.

In the case of ***Dharmbir v. Central Bureau of Investigation,*** the Hon'ble Court distinguished as there being two levels of an electronic record. One is the hard disc which once sent, itself becomes an electronic record in relation to the information regarding the changes the hard disc has been subject to and which information is retrievable from the hard disc by using a software program. The other level of electronic record is the active accessible information recorded in the hard disc in the form of a text file, or sound file or a video file etc. Such information that is accessible can be converted or copied as such to another magnetic or electronic device like a CD, pen drive etc. Even a blank hard disc which contains no information but was once used or recording information can also be copied by producing a cloned had or a mirror image.

An electronic record by way of Secondary evidence shall not be admitted in evidence: On 18 September 2014, the landmark ruling of the hon'ble Supreme Court in the ***Anvar P.V. v. P.K. Basheer and others,*** the Court noted that "there is a revolution in the way that evidence is produced before the court", that computer output is not admissible without compliance of Section 65B & 65A overrules the judgment laid down in the ***State (nct of delhi) v. Navjot Sandhu alias Afzal***, by the two judge Bench of the Supreme Court. The Courts specifically observed that the judgment of navjot sandhu supra, to the extent, the statement of the law on admissibility of electronic pertaining to electronic record of this court, does not lay down correct position and is required to be overruled. The legal interpretation by the Court of the following sections 22A, 45A, 59, 65A & 65B of the Evidence Act has confirmed that the stored data in CD/DVD/Pen Drive is not admissible without a certificate u/s 65B(4) of Evidence Act and further clarified that in absence of such a certificate, the oral evidence to prove existence of such electronic evidence and the expert view under section 45A Evidence Act cannot be availed to prove authenticity thereof.

Admissibility of e-mail: In the case of ***Abdule Rahman Khunji v. The State of West Bengal***, the Hon'ble High Court of Calcutta while deciding the admissibility of email held that an email downloaded and printed from the email account of the person can proved by virtue of Section 65B r/w Section 88A of Evidence Act. The testimony of the witness to carry out such procedure to download and print the same is sufficient to prove the electronic communication. Admissibility of Telephone call in a CD and CDR: In the case of ***Amar singh v. Union of India*** saw all the parties, including the state and the telephone company, dispute the authenticity of the printed transcripts of the CDRs, as well as the authorization itself.

In the case of ***Ratan Tata v. Union of India,*** a compact disc (CD) containing intercepted telephone calls was introduced in the Supreme Court without following any of the procedure contained in the Evidence Act

In the case of ***Jagdeo Singh v. The State and Ors***, the Hon'blle High Court of Delhi, dealing whith the admissibility of intercepted telephone call in a CD and CDR which were without a certificate u/s 65B Evidence Act, the court observed that the secondary electronic without certificate u/s 65B Evidence Act is inadmissible and cannot be looked into by the court for any purpose whatsoever.

Interview telecasted on Doordarshan: In the case of ***Sharad Yadav and Ors. Vs. Union of India & Anr,*** the Court observed that tested on the touchstone of the principles of law enunciated by their Lordships of the Privy Council and the Supreme Court, the aforesaid video recorded interviews of Shri Sharad Yadav do not amount to confessions and cannot, therefore, be used to complete the offence, with which Shri Sharad Yadav was charged. In this case, considering the dicta in ***R. V. Pearce, Palvinder Kaur v. State of Punjab, Om Prakash Vs. State of U.P.*** and ***C.B. I. V. V.C. Shukala and Ors,*** it was observed that "it would be unfair to admit only the statements against interest while excluding part of the same interview or series of interviews.

In the case of ***Pradeep kumar vs The State of Bihar Through Central***, There is no iota of evidence adduced on behalf of prosecution to substantiate the demand made survive. It has also been submitted that electronic evidence so brought up at the end of the prosecution under P.C. Act, more particularly, relating to Section 7 as well as 13 thereof. The prosecution has to substantiate whether there happens to be evidence relating to demand, acceptance followed with recovery of tainted amount out of dominance of the accused/delinquent. Mere recovery of tainted amount without having evidence of demand, acceptance will fail the prosecution case in its entirety. Presumption though rebuttable against an accused is to be taken only after success of prosecution in properly discharging the burden.

In the case of ***Harpal Singh Bundela vs The State of Madhya Pradesh*** , The Trial Court has relied on the transcription and recorded evidence. The Court further observed that the CD was played before the medium of laptop. In CD, same conversion was found which was mentioned in the transcription. From aforesaid evidence, it is clear that the voice recorder was not produced before the Court by which complaint. The voice was transferred to laptop and thereafter, the CD was played before the Court through laptop. Investing Officer specifically admitted in para 30 of his cross-examination that he had prepared the CD from the laptop. He further admitted the fact no certificate as required under Section 65(b) of Evidence Act was produced before the Court. Neither another person produced the certificate required under Section 65(b) of Evidence Act.

In the case of ***L.V.sejappa vs State by Police Inspector Lukayukta, Chitradurga*** ,The Hon'ble Court has held as under; "In order to constitute an offence Under Section 7 of the Prevention of Curruption Act, proof of demand is a sine quo non."

Freedom of Speech: In the case of ***Shreya Singhal vs. Union of India***, is a judgment by a two bench of the Supreme Court of India in 2015, on the issue of online speech and intermediary liability in India. The Supreme Court struck down Section 66A of the IT Act,

2000, related to restrictions on online speech, unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1)(a) of Constitutional of India .The Court further held that the Section was not covered for being virtue of being 'reasonable restrictions' on the freedom of speech under Article 19(2). The case was a watershed moment for online free speech in India.

Ministry of Home website Hacked: The Ministry of Home Affairs website, was hacked on Sunday, promoting authorities to temporarily block it, an official said. The MHA website was immediately blocked by the national Information Centre after hacking was noticed. Computer emergency response teams are looking into incident, the official said Last month, suspected Pakistan affiliated operatives had hacked the official website of the elite National Security (NSG) and defaced it with a profanity laden message against the Prime Minister and anti- India content.

Offensive WhatsApp Posts Can Land Group Admin in Jail: Think twice before becoming administrator of a group on WhatsApp or Facebook as one is liable for prosecution if any rumor or fake news is circulated on it. Social media platforms allow a person to create a group on which members can hare views, photographs or videos with fabricated local narratives can easily be circulated that can trigger tension and even communal rift in an area. In a joint order issued by District Magistrate, it has been made clear that any factually incorrect, rumor or misleading information on a social media group administrator.

Hyderabad Engineer Held For 'Live Steaming" Sex with wife: A 33-year-old former software engineer386 was arrested by Hyderabad Police here last week for allegedly live streaming sexual acts with his wife, without her knowledge, on a porn site for money, police registered a case under section 509 (word, gesture or act intended to insult the modesty of a woman) of IPC and under sections of the IT Act.

Kaspersky Lab Joins Interpol in a Cybercrime Operation across Asian Nation: Cyber Security film Kaspersky Lab has identified nearly 9,000 botnet command and control servers and hundreds of compromised website, including government portals.

Chennai Journalist Files Case against Abuse Trolls: The case comes a day after other cases of stalking led to massive outrage in north India. In Chennai, the case relates to trolls who took umbrage with Dhanya Rajendra's tweet that expressed her opinion about a movies.

Three billion yahoo accounts hacked: With the announcement Tuesday Oct 2017 that all three billion accounts were affected by a 2013 hack, version-owned yahoo became the victim of the biggest overall data breach. In recently high profile hacks have been bigger and more frequent. Part of that trend is due to greater use of online storage and social media, as well as massive amounts of personal data now stored in the cloud. Some linked to more sophisticated tools being deployed to illicitly access personal information. last year, yahoo announced that more than a billion accounts had likely been affected by the hack, which occurred in 2013. The compromised accounts came to light after an unidentified third partly gave law enforcement officials data files they claimed contained yahoo user information, the company said in December In the breach, attackers accessed email addresses, passwords, birth dates and other bits of personal information.

Analysis of Indian Approach to Cyber Jurisdiction: The Indian approach to deal with cyber-investigation jurisdiction is not very well developed. Currently, in the Indian law enforcement agencies are in the process of evolving and crystallizing their practices and procedure relating to cyber-investigation. When one examines the provision of the IT Act, 2000, one realizes that, although on paper technically the law has granted extraterritorial jurisdiction in relation to cybercrime cases, yet in reality it has not really been applicable beyond the territorial boundaries of India. There is now growing realization that the Indian Cyber law, despite its paper-tiger extraterritorial jurisdiction provisions, pragmatically and practically speaking, cannot be made applicable to jurisdiction outside the territorial boundaries of India. This is because such provisions directly conflict with exercise of sovereignty by foreign governments within their national boundaries. This is also exemplified by the famous case relating to the hacking of the website of the CBDT in 2002.

The CBDT is a statutory body in India whose website was hacked by allegedly Pakistani hackers. This was not new instance. The previous Kargil war in 1999 had seen numerous Indian government websites being reportedly hacked and brought down by Pakistani hackers. While in previous cases, the government did not register cases hacking, in the case of the website hacking of the CBDT, the police did register.

However, despite more than three years after registration of this case, no effective breakthrough has been achieved nor any progress made in this case. The reason behind this non action has been that the allegedly Pakistani hacker located outside the territorial boundaries of India. India has no legitimate right to arrest such person outside its territorial boundaries. To complicate matter further, the neighboring country does not recognize such people as hackers and instead refers to them as patriots. Therefore in this scenario, it becomes an increasingly futile exercise to register any cybercrime case, wherein the perpetrator of the cybercrime is physically located outside the territorial boundaries of India. In this dilemma, India as a nation is not alone and shares the same boat with other nation facing similar challenge.

There is complete lack of case law on this issue of cybercrime jurisdiction in India. Apart from that, India, being a large country, is also likely to see interstate jurisdiction issues relating to the registration, investigation, and prosecution of different cybercrime cases in different states of India. Until such time Indian law in this regard is amended as universally accepted international best practices and principles evolve, it would be prudent for Indian law enforcement agencies to detect, investigate, and prosecute cybercrimes within the ambit of existing principles of law as are enshrined in section 1 and 75 IT Act. Section 81 of IT Act declares law to be special law and states that the provisions of this law shall prevail over anything inconsistent contained therewith in any other law currently in force in India.

As much the manner of crime investigation and prosecution as embodied in normal criminal law in India would indeed continue to the extent that they do not conflict with the provision of the IT Act. However, the provision of sections 1 and 75 IT Act as discussed above shall continue to guiding principles concerning cybercrime jurisdiction in India until the government of India comes up with some new legal provision in this regard. There were hopes that IT (amendment) Act would proceed to deal with the complicated issue of jurisdiction but the amendment Act has not addressed the issue. At the time when the internet has made geography history, it was expected that 2008 amendments to IT Act 2000, would

throw far more clarity on complicated issues pertaining jurisdiction. This is because numerous activities on the internet take place in different jurisdictions and that there is a need for enabling the Indian authorities to assume enabling jurisdiction over data and information impacting India in more comprehensive way than in the manner as sketchily provided under current laws.

Seen from the holistic perspective, India promises to be an action spot that is likely to develop rapidly various principles relating to cybercrime jurisdiction. This is not just because of the tremendous use of information technology and internet within India. It is also courtesy of the huge spurt in the business-process outsourcing or knowledge-process outsourcing industries in India. In the context of Asia Pacific, India is more likely to be the probable candidate to emerge with practical and pragmatic guidelines and solutions for tackling various tricky issues concerning cybercrime jurisdiction within India.

Role of Judiciary on Cyber security: "The Courts apply the law, and settle disputes and punish law-breakers according to the law. Our judiciary system is a key aspect of our democratic way of life. It upholds peace, order and good government. Citizens look to the judiciary to uphold their rights and governments look to the courts to interpret laws." The judiciary acts as the guardian of the Constitution. The Constitution is the supreme law of the land and it is the responsibility of judiciary to interpret and protect it. This power of the court is called the power of judicial review. Judiciary gave new legal theories and interpret the law according to new social-economical circumstances; here we review case law which is decided by the Hon'ble Court and gave judge made law. The first Indian case convicted under section 67 of IT Act, 2000 was ***State of Tamil Nadu vs. Suhas katti.*** In this case it was held that "The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 year under 469 IPC and to pay fine of rs.500/- and for the offence u/s 509 IPC sentenced undergo 1 year simple imprisonment ad to pay fine of RS.500/- and for the offence u/s 67 of IT 2000 Act to undergo RI for 2 year and to pay fine of Rs.4000/- All sentence to run concurrently."

Hicklin Test has been adopted by the Supreme Court in a leading case ***Ranjit D. Udeshi v. State Maharashtra*** The apex court didn't consider obscenity a vague concepts a word that is well understood even if person differ in their attitude to what is obscene what is not. The court has to see whether a class has not isolated case into whose hands the book, article or story false suffer in their moral outlook or become depraved by reading it or might have impure and lecherous thought aroused in their mind. In further court adopted new morality standard.

The Supreme Court in ***K.A. Abbas vs. Union of India*** recognized that standard of morality is not uniform or flexible standard but varies according to different communities or ages as well as a number of historical, ethic and social conditions.

In the case of ***The Gold Case***, The Court of Appeal observed, 'that condition amounted in essence to dishonesty gaining access to the relevant Prestel data bank by a trick. This is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislation rather than the courts.'

In ***the case of Yahoo Case***, The Court held that it could properly exercise jurisdiction over two French civil liberty groups and denied their motion to dismiss the case. There was an actual controversy causing a real and immediate threat to yahoo. Enforcement of the French orders I the US would violate the First Amendment of the US constitution and they were unenforceable in the US.

In the case of ***Yournetdating, LIc, v. Scott Mitchell*** and ***Webscapades, Inc,*** The court observed that persons who signed up to get an online date did not necessarily want to visit porn site; and therefore it would be in the public interest to grant preliminary injunction. Thus the people who did not want hardcore porn will be subjected to pornography because of Mitchell's misconduct, added the Court. The Court did not heed to Mitchell's claim that, Sexetera, the porn site in question, was no more functional since it had itself been hacked, and would probably not be reconstituted.

In the case of ***Ashcroft, Attorney General et al v. Free Speech Coalition,*** et al,339 The US Supreme Court affirmed the judgment of Court of Appeal for the Ninth Circuit Where it had declare that the law banning 'virtual child pornography' was unconstitutional, distinguish it from 'child pornography' that the law aimed to criminalize. The Federal Supreme Court observed that in the light of the First Amendment to the American Constitution, the government had no right to dictate 'what to see or read or speak or hear'; nor could any speech be banned only on the premise that it might acquire illegal proportions. The Court observed:

"Congress may pass valid laws to protect children from abuse, and it has. The prospect of crime, however, by itself does not justify laws suppressing protected speech".

The Court declined to accept the version of the government that "virtual child pornography whets the appetites of pedophiles and encourages them to engage in illegal conduct", because, in the opinion of the court "the mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it".

In the case of ***Syed Asifuddin and other v. the state of Andhra Pradesh and another***, this petition dealt with sec.65, 66, 2(1) of IT Act an petitions dismissed with direction to the CID police to complete investigation and file a final report before metropolitan magistrate competent to take cognizance o case within a period of three months.

In the case of ***Orissa Consumer Association, Cuttack and another v. Orissa Electricity regulatory Commission and other*** , the Delhi high court, while issuing an interim injunction, has brought to light the significant requirement and nee for adequate legislation in India, to provide protection to Internet users from privacy intrusion caused by unsolicited e-mail, by making it a violation for spammers to send message without a return address, r with a forged return address, or with misleading subject line.

In the case of ***Bhim sen Garg v. State of Rajasthan and other*** , it was held by High Court of Rajasthan that in view of test laid down by Hon'ble Supreme Court in case ***Bhajanlal Lal*** impugned FIR no.21/2006 cannot be said to be false and the petition officials consequently with petition disposed.

In the case of State of Punjab v. Amritsar , it was decided by the Supreme Court that fulfillment of conditions laid down in the proviso contained in clause (b) of sub-section (3) of sec.14 of I.T. Act are imperative in character, therefore the authority must follow procedure in respect of seizure of Hard Disc.

In the case of ***Bodale Murli Krishana v. Smt. Bodale Prathima***, Andhra Pradesh High Court allowed examination of witnesses in criminal cases through video conferencing is permissible in law provided necessary precaution must be taken as to identify of the witnesses and accuracy of the equipment used for the purpose.

In the case of ***B.N. Firos v. State of Kerala and other*** , it was held that while interpreting sec.70 of IT Act, a harmonious construction with copy right Act is needed.

In the case of ***M/s. P.R.Transport Agency v. Union of India*** , involve the question of jurisdiction of court where the contract between the parties residing in different places has been made on e-mail. In this case, Bharat Cooking Coal Ltd. (BCCL) held an e-auctionfor coal in different lots in which plaintiff's bid for 40000 metric tons of coal from Dobari colliery was accepted. The BCCL communicated the acceptance of bid by e-mail on July 19, 2005. In response, the plaintiff deposited the amount of 81.12 lakhs through a cheque in favour of BCCL which accepted the cheque and encashed it but did not deliver the coal to the plaintiff. Instead, it informed the plaintiff through e-mail communication that the said e-auction stands cancelled "due to some technical and unavoidable reasons". The plaintiff found that e-auction of sale of coal was cancelled by BCCL as there was some other person whose bid for the same was higher, which had not been considered earliar due to some flaw in the computer or its program or feeding of data. The plaintiff challenged the validity of cancellation of its contract by the defendant in the High Court of Allahabad.it was held that Action of respondent improper and violative of rules of natural justice and held that Allahabad High Court would have territorial jurisdiction to entertain writ petition.

In the case of ***M/s, Info seek Solutions and another v. M/s Kerala Law times and others***, it was held that, if one quotes a particular portion of a document for the purpose of specifying a particular view, it cannot be said that the said quotation is merely a copy of the main text made without any intention to serve a purpose.

In the case of ***Baazee.com case,*** CEO of Baazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber-crime cases and a lot of education is required.

In the case of ***NASSCOM v. Ajay Sood*** who elaborated the concept of 'phishing'. The Delhi High court held that the act of phishing as passing of and tarnishing the plaintiff's image, thereby bringing within the realm of trademark law.

In the case of ***Official website of Maharashtra Government Hacked***, IT experts said that the hackers had identified themselves as "Hackers Cool Al-Jazeera" and claimed they were based in Saudi Arabia. They added that this might be a red herring to throw investigators off their trail.

In the case of ***Major credit card hacking fraud case***, Federal prosecutors said on Thursday they have charged five men responsible for a hacking and credit card fraud spree that cost companies more $300 million and two of the suspects are in custody, in the biggest cyber-crime case filed in U.S. history.

In the case of ***Google India Pvt Ltd. v. M/s.Visaka Industries Limited and another***, The question of holding such intermediaries liable for defamation does not arise. Senior Counsel appearing for the petitioner placed reliance on Section 79 of the Information Technology Act, 2000 (in short, the Act) in support of this contention.

In the case of ***Ram Jethmalani and Ors. v. Union of india and Ors*** , the Supreme Court of India prescribed guidelines seeking to prevent the unwarranted manipulation of bank account details of individuals caused by inquisitive individuals or unauthorized agencies. The petitioners in this case alleged that a former employee of a bank or banks in Liechtenstein had acquired the names and bank account details of some eminent personalities and made the same information available to various entities. The same information was then secured by the Federal Republic of Germany (Germany) which further disseminated the information.

In the case of ***Sanjay Kumar vs State of Haryana***, The petitioner has been convicted for offences punishable under Sections 420, 467, 468, 471 of the Indian Penal Code and Sections 65 and 66 of the Information & Technology Act, 2000 and sentenced to undergo rigorous imprisonment as follows: Under Section Period Fine 420 IPC Two years Rs.1,000/- 467 IPC Three years Rs.2,000/- 468 IPC Two years Rs.1,000/- 471 IPC Two years Rs.1,000/- 65 I.T. Act Two years Rs.1,000/- 66 I.T. Act Two years Rs.1000/- In default of payment of fine, the petitioner shall further undergo simple imprisonment for a period of two months. All the sentences were ordered to run concurrently.

In August, 2014 cyber pornography was in highlight when PIL petition ***Kamlesh Vaswani*** urged the Supreme Court to direct the central government to "block 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 PIL demanding a ban on child pornography and blocking of adult porn sites in India referred to the Delhi gang rape of December 2012 when the accused had allegedly watched porn on their phones before assaulting a medical student. The petition claimed that pornography triggered crimes against women in India. Concerned over the increasing number of pornographic websites, the Supreme Court said these sites were "hydra-headed," and that "If you block one, 10 others will pop up in other countries.

In the case of ***Manish kathuria*** who was recently arrested by New Delhi Police. He was staking an Indian lady, Ms Ritu Kohli by illegally chatting on the Website MIRC using her name. In a state of shock, she called the Delhi police and reported the matter.

In the case of ***SMC Pneumatics (India) Private Limited vs Joges Kwatra a company's*** employee started sending derogatory, defamatory and obscene emails about company's Managing Director. Delhi High Court granted an injunction and restrained the employee from sending, publishing and transmitting emails which are defamatory or derogatory to the plaintiffs.

The issue of violation of privacy rights through newspaper publications was addressed in a subsequent case in a 2010 judgment of Madras High Court in ***A. Raja. Srinivasan Publisher and Ors and M.A. Parameshwari vs. P. Srinivasan Publishers& Ors*** in the case filed an appeal before Madras High Court seeking permanent injunction and damage for loss of reputation caused by respondent by publishing certain news regarding the appellants, that is, publishing photographs of the minor child and family photos of Ms. A. Raja, former minister of information Technology. The respondents simultaneously field an application to vacant the adinterim injunction already granted in the appellants favour whereby respondents were restrained publishing any further news regarding the appellants. The Court held, that the documents placed by appellants clearly indicated that the respondents were constantly publishing photographs of the minor child of A. Raja, former Minister of Information Technology as well as family photographs, with write-up on different dates on the front cover page of their magazine. The respondents had published a family photograph of the appellants where there was no necessity for publishing the photograph of a minor child and same is an act of infringement of the privacy rights of child by exposing identity and family relationship of the appellant

In the case of ***Durga Dutt Sharma v. Navratna Pharmacy Laboratories***, the Supreme Court of India has laid down the following guidelines regarding trademark infringement cases:

(i) the onus of establishing infringement of trademark is on the plaintiff
(ii) In a case where the infringing trademark is identical to the registered trademark, no further inquiry is required by the Court.
(iii) In a case where the infringing trademark is not identical to the registered trademark, the plaintiff would have to establish that the use of the defendant's trademark is likely to deceive or cause confusion among the relevant section of public.

While comparing two trademarks, the Court has to look into their degree of resemblance. The degree of resemblance is determined by noting the essential features of the two trademarks.

In the case of ***Teletech Customers Care Management v. Tele Tech Co,*** the court restrained the Tele Tech Co. to use 'teletech.com' because the plaintiff was a provider of telephone and internet customer services and owned a federal service mark registration for Tele Tech.

In the case of ***Toy 'R' US Inc v. Akaoui,*** Akaoui's domain name 'adultsrus.com' and the term "Adults 'R' US" tarnished the plaintiffs famous trademarks "Toys 'R' US" and "KID 'R' US". The court restrained the defendant to use the domain name 'adultsrus.com' and ordered for the cancellation of domain name.

How to improve response to the cyber-crimes by the judiciary:

i. *Awareness Building*

Whenever we discuss solutions related to Cyber Crimes and Cyber Security, "Creating Awareness" continues to top the discussion table and often ends with it. There is no doubt that "Creating Awareness" is necessary but we need to also address to whom should we create awareness and regarding what.

First level of awareness building is to the public that there is a law called ITA 2000/8 and if they have any issues, they can seek protection from law. But immediately they will ask, which Police Station should I reach out and which Court should I approach. Given the general reluctance of public to step into any Police Station, unless people feel that there would be a definite benefit they will not approach the Police. While there are many knowledgeable Police officers, there are more number of station level policemen who are not familiar with Cyber Crimes and are reluctant to accept any complaints.

There is therefore a need to create awareness amongst all the Police Stations. Despite some efforts there is still a lack of effort in ensuring that our police stations are equipped to accept a Cyber Crime complaint. Today we see a board in most Police stations about the number of complaints received under various types of crimes. Workshops on Cybercrimes should be conducted in every police station. Advanced courses can be conducted for SIs and investigating officers but base level awareness is required to everybody. Similarly, awareness needs to be created with advocates, Public prosecutors, Magistrates and judges at all levels. CJIs need to monitor how may judicial officers are in the state and how many of them are proficient in Cyber Crimes. Judicial Academies need to work on a specific target in this regard so that 100% of magistrates and civil judges go through at least the base level workshop within the next one year.

An action plan for this can be developed and implemented by every State under the guidance of the Chief Justice of the State High Court.

Awareness also needs to be built for every IT Secretaries in India since they are "Adjudicators" and function like a Civil Judge in respect of all offences under ITA 2000 upto a loss of Rs 5 crores. Lack of awareness at any level whether it is the victim, or the Police or the Lawyers or the Judiciary should not be a reason why Cyber Crimes donot get registered.

ii. *Crime Reporting*

Assuming that awareness is built up at all levels, the next problem to be tackled is the means of reporting of a Cyber Crime incident. If we want to get the correct picture of the Cyber Crime scenario in the country, we need to break the reluctance to register Cyber Crime complaints at the police level. It is appreciated that if Complaints are registered but not resolved, some may interpret it as an inefficiency of the Police and hence Police are reluctant to register a complaint which they are not confident of resolving.

We therefore need an "Impersonal System of Crime Reporting" where the incident is reported online. Every incident reported should be numbered whether they are converted into a complaint or not. Police should establish a network of "Friends of Cyber Police" in

different parts of the City who may be approached by the victims for guidance. These FOCPs can vet the complaint and load it onto the system on behalf of the victim.

The system should escalate the complaint to a suitable Police officer for conversion into a formal complaint and issue of an acknowledgement. The higher authorities in Police may take follow up action as may be required though the first task of recognition of Cyber Crime is achieved through this process.

Every incident may be technically considered as an "Attempt" to commit a crime and therefore can be recognized as a registerable Cyber Crime. Hence there should be no technical issue is mandatory registration of FIRs for all verified complaints. This will help in the assessment of the resources that need to be committed to Cyber Crime mitigation in the long run.

iii. *Adjudication*

Adjudication was a wonderful system which ITA 2000 suggested for resolution of civil claims for damages arising out of contravention of any provision of ITA 2000. It provided for quick resolution, and *suo-moto* powers to the adjudicators to take remedial action. In 2003 in view of the fact that the Judicial system was not prepared to take up the challenge of adjudicating on technology related issues, Government made all IT Secretaries of states as "Adjudicators" for the respective state. These officers were tech savvy and senior enough in the bureaucracy to conduct proceedings of adjudication as an "Enquiry" process. Appeals were available to the CyAT.

However over a period the Adjudicators have shown no enthusiasm to take up this responsibility both because they are otherwise engaged in the developmental activities as also because there is a conflict of interest since some of the cases involve business interests of IT companies. Additionally just as Judicial officers were lacking in technical knowledge, the IT Secretaries were also found to fumble with the legal knowledge when required. As a combination of all these factors, today the system of Adjudication is almost non-existent.

There is therefore a need to review and revive this system. One way out is for the State Judiciary to train some of their Judicial officers in Cyber Crime related issues and set up a parallel team of Adjudication Empowered Judicial Officers. Once the IT ministry issues necessary notification, these officers can start taking up complaints.

Alternatively, every Adjudication set up which today consists of the IT Secretary can be made a two member bench with the Law Secretary of the State being the second person. This will provide the relief in terms of knowledge deficiency but may not solve the problem of lack of time for these state level senior officers. The team of trained judicial officers may therefore be a better solution to meet the requirements of Adjudication.

These Adjudicating officers should be mandated to use Video Conferencing wherever feasible so that the cost of adjudication is reduced. Again a suitable framework for training and sustaining this system can be developed if the State High Court Chief Justice takes interest.

iv. *CyAT*

The issue of CyAT has been discussed earlier. Presently there is a set up in Delhi with a good infrastructure and also a technical member. If only a Chair person can be appointed, the system can restart its activities.

However there is a need for CyAT to sit in different States and use Video Conferencing so that victims need not travel to Delhi for their cases. It should be mandated that the CyAT regularly sits in different State Capitals and conducts its proceedings and also set up at least one bench in South India to enable economical access to the public.

v. *Special Magistrate Courts*

While the Adjudication and CyAT takes care of the civil disputes, there is also a need to set up special magisterial courts in the States to handle Cyber Crime cases exclusively. This will speed up delivery of justice and also build expertise in specific Judges who can support the system at higher levels as days go by. This is an action which again needs to be handled by the State High Court.

vi. *Special Mediation Centers*

ITA 2000/8 provides for compounding of most offences including those which come under the category of criminal offences. Hence there is a scope for mediation and Conciliation both in the case of Civil and Criminal proceedings. If therefore a good system of mediation can be developed, this will reduce the burden in the system of Adjudicators and Magistrates and help in the quicker delivery of Justice to victims.

There could be many other measures that may help in improving the Cyber Judicial systems but what is discussed above is a list of suggestions that can be considered. It is to be remembered that an efficient Cyber Justice System is not only required for the success of the Digital India program but also is essential for India maintaining a good "Ease of Doing Business " index on a global scale.

Conclusion and recommendations:

Regarding the role of judiciary in combating cybercrime, the number of Cyber-crimes are going to be adjudicated by the Indian Courts, while dealing with the cyber-crime the Court depends heavily on the conventional Criminal Law, that is Indian Penal Code. Cyber-crime is not very different from the conventional crime. All the cases, which are known as important cases of cyber-crime in India are subjected to the Indian Penal Code. Though the special law that is Information Technology Act 2000 is recognized as cyber law of India, but cyber-crimes are more concern with the Indian penal Code, without applying the traditional criminal law, the law enforcing agencies cannot work. All the cases discuss here are subject to the Indian Penal Code, and this conventional criminal law provides the relating section to all the offences, which are recognized as a cyber-crime. Therefore, the cyber-crime and the conventional crime are not different from each other, however the techniques, which are going to use for performing the crime, are different and subjected to the cyber world or cyber space is use to commit the cyber-crime.

Regarding the cyber security in India, there is a dire need for cyber law in India which includes parts of the Information Technology Act and solves new and potential disputes involving the internet. The outdated parts of the Information Technology Act need to be repealed as, in the time since it was made the great progress technology has made needs legal recognition.

The new law should contain:

1. Apt and unambiguous definition of terms used in it
2. Provisions striking a balance between media and privacy Law to check whether media following someone's online presence could violate privacy law
3. Online Applications and Privacy Law - whether public availability of applications to authorities made using online processes would infringe privacy law
4. Right to Freedom of Expression and Internet Censorship - the processes developed for censorship and delineation of contingencies which require their application
5. Provisions making censorship to go down well with privacy law - when censorship measures may infringe upon the online privacy of a person without their consent
6. Strong authority on technological and Internet related issues with good amount of expertise and technological knowledge
7. Specifically mention the situations which are exceptions to application of cyber law. This law needs to comply with Article 19(2), and be mindful of Article 21, of the Constitution of India.

RECOMMENDATION 1:

*Designing for Information Security:*Professional and developers of ICT-software, -middleware and -hardware and others responsible for ICT innovations have a crucial role in providing the knowledge and means by which information protection can be enhanced. As home users and small- and medium-sized enterprises (SMEs) usually do not have the resources or professional skill sets to design ICT systems and their means of protection in face of the growing number of cyber incidents, there are double responsibilities for public 16 and private institutions, and for countries to establish security procurement policies and standards.

It is therefore recommended to

- Establish means and processes of evaluating new ICT developments and products that might include establishing accreditation agencies, certification policies and procedures of information security enhancing measures.
- Continue development of national CERTS (Computer Emergency Response Teams) around the world, and their liaison with the international FIRST (Forum of Incident, Response and Security Teams) community. Their activities should include not only information sharing, analysis case studies and warning roles, but also a response capability operated by ICT security professionals. This will improve end-user awareness and responsibilities with respect to safeguarding information, security and privacy. Unwittingly, these end users in cooperation, SME’s, and at home can become a,, launch point (pad) “for attacks on the basic communication and other infrastructure.

- Heighten awareness of end users in developing – as well as in developed - Countries, as they acquire or upgrade ICT capabilities, of major risks, and of the importance of security policies and capabilities. This recommendation pinpoints the need especially for home users and SMEs to learn more about information protection and privacy, by, inter alia, participation in education and training programmes; the development of model education curricula and "drivers licenses" for computer users; • Develop warning and reporting points'(WARPs, at www.niscc.gov.uk) which serve as a means information sharing about incidents at a local community and business level. These can be developed in association with local government, the local branches of the International Chamber of Commerce, and likeminded SMEs and other civil society groups. Unlike CERTs/FIRST they do not have an operational response role.

RECOMMENDATION 2:

Cost-effective cyber security and privacy in nascent information societies: The integrated privacy and security of information for enterprise users of the internet in nascent information societies will depend upon their implementing effective procedural and technological tools to bring to life privacy and security plans and to monitor the effectiveness of and compliance with privacy and security procedures that meet at least minimal standards established and tested by expert developers of information system for small and medium sized enterprises.

The World Federation of Scientists recommends that the WSIS

- Initiate the development of quantitative risk management tools specifically tailored for enterprise managers in nascent information societies that include model information security plans scaled to the size and nature of the enterprise, templates for assessing their vulnerabilities and returns on investment for employing cyber security tools, training modules to promote awareness in employees in secure computing practices and procedures. Self-help modules for conducting periodic cyber security audits.
- Endorse the use of network security tools including strong forensic capabilities at the early installation phases of networking hardware in nascent information societies.
- Urge the articulation of a uniform, transnational legal guideline for enterprise managers that can be embodied in the laws of nascent information societies.

RECOMMENDATION 3:

An effective, transnational anti-spyware strategy: Executable applications and monitoring chips deployed without adequate notice, consent, and control of a computer owner and outside judicial control represent an increasingly malicious threat to the operability of personal computer systems and to the privacy of information on these systems. Moreover, the data gathered by spyware can easily be used to convert the host computer to be used as an unwitting accomplice computer in large-scale denial of service attacks. Indeed, the growing evidence that organized criminals are controlling networks of spybots (botnets) makes the development of uniform transnational criminal statues and attendant evidentiary standards imperative. As botnets can be used to attack commercial and governmental websites, DNS servers, email systems, and voice-over internet (VoIP) services, their potential for disruption is especially severe for countries with nascent information infrastructures. Unfortunately with

respect to criminal anti-spyware statutes, the legal Framework is in the early stages of development.

The World Federation of Scientists recommends that the WSIS

- Strongly encourage adopting transnational industry wide definitions of spyware in both hardware and software forms to guide anti-spyware development.
- Initiate developing consistent, transnational guidelines and evidentiary standards guidelines that provide a uniform legal framework to stiffen penalties for the use of spyware and give relevant national entities specific enforcement authority over spyware interlopers.

RECOMMENDATION 4:

A Global Framework of Cyber law:

The loopholes in, and the piece-meal nature of, current national legislation on cyberspace, especially on the side of criminal law and law enforcement, open vulnerabilities that enable exploitation by criminals and miscreants, and create increasing dangers to global populations, not least in countries with an as yet nascent information infrastructure. There is a clear and urgent need for uniform or harmonized legislation world-wide.

With this perspective, the World Federation of Scientists

- Welcomes the work which is being done under the aegis of the ICT Task Force of the United Nations to prepare draft proposals for a Law of Cyberspace. Discussions on this subject must obviously incorporate the view of all stake holders, namely, governments, the private sector, and civil society. It is the long-held view of the World Federation of Scientists that these discussions can take place only in a central multilateral forum for which the United Nations or one of its agencies offers the best and most convenient location.
- Recommends that the WSIS endorse the conclusions and recommendations of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice (Bangkok, 18-25 April 2005), in particular those of its Workshop on Measures to Combat Computer-related Crime and its underlying background paper, tending to promote the creation of a seamless world-wide system of criminal law on cybercrime and corresponding international cooperative law enforcement. The work results of the Eleventh United Nations Congress are fully in accordance with the World Federation's own previous Recommendations and, inter alia, highlight suitably the importance of the Council of Europe Convention on Cybercrime.
- Recommends, pending progress towards a uniform or harmonized legal order for cyberspace, especially as regards criminal law and law enforcement, that the WSIS examine the feasibility of, and possibly the initiation of steps towards, the negotiation of a Code of Behavior of Governments and the Private Sector in cyberspace designed to impede hostile action against other countries and to create optimum legal and factual conditions for preventing cyber-attacks.

RECOMMENDATION 5:

Denial of information access through Internet filtering: Internet censorship through the use of advanced routers with an unlimited filtering capacity is increasingly employed by governments in a number of countries to block access to the Internet, or control such access, in a comprehensive manner, thus impairing internationally accepted norms of freedom of information and opinion. This censorship often goes beyond legitimate concerns of national security and other public interests and deprives the citizens in these countries of the full benefits of the information society. It is therefore recommended that the WSIS:

- Affirm unequivocally the principle of freedom of all to receive and impart information regardless of frontiers, as a principle to govern the Internet and as an indispensable element of an international information society;
- Discuss, within an appropriate conference framework, the extent and relevance of filtering practices, with a view to raising international public understanding and awareness of the danger to the freedom of information and the functioning of the information society emanating from them;
- Initiate an international monitoring procedure or mechanism to follow and clarify internet filtering practices, thus promoting the principles of transparency and accountability that should govern them, and permitting their evaluation against international standards;
- Examine the feasibility of setting up a complaint procedure available to all Internets Stakeholders to enable the monitoring and evaluation of Internet censorship practices;
- Provide a forum for discussion of the responsibilities of the corporate providers of Internet filtering technologies in settings where negative use of their technologies in grave detriment of the freedom of information is to be anticipated.
- Confirm the importance of the wide-spread opening of Internet Cafés as a means for promoting the information society, and declare the in admissibility of the closure or restriction of use of such means of access to the Internet.

RECOMMENDATION 6:

Protecting the information society from cyber war: No country is immune from the growing threats of cyber terrorism and cyber war that May strike vulnerable societies – those in possession of inadequately protected ICT Structures - with particularly devastating and destabilizing consequences.

- It is therefore Recommended that the WSIS, in striving towards the fulfillment of its goals, Incorporate in its work programme an in-depth discussion of the potential adverse impact of cyber war activities, in order to heighten the understanding and consciousness of ICT users in government and corporate entities with respect to the dangers associated with such misuse of the ICT systems on which their societies depend;
- Encourage specifically governments and the operators of critical national infrastructures to build adequate levels of protection against cyber-attacks into those ICT systems that fulfill important societal, including economic, functions and enable the tranquil operation of the information society, including industrial infrastructures, public services and national defense;

- Given the potential of cyber-attacks to constitute a breach of international peace and security, support the urgent initiation of work at the United Nations to study and clarify the scenarios, criteria and international legal implications and sanctions that may apply, and, in particular, to examine how traditional principles of international law relating to armed conflict are applicable to conflicts in the information age.