Chapter 3

Cyberspace and Need for its Policing

3.1 Introduction

Virtually every aspect of our society is becoming linked to cyberspace from civilian, government and the military, to public utilities, communications, transportation, and financial systems. The cyberspace provides easy and relatively inexpensive access to a rich and growing body of digital content. Computer links the stretch around the world that transcends national and regional boundaries. Beijing and Baltimore are within a keystroke of each other. These links are creating vast efficiencies in the delivery of goods and services\(^1\).

Today, computers are used in all walks of life: they are in homes, and in various critical domains such as defense, education, finance, government, healthcare, and so on. Cyberspace provides a powerful but complex environment. This reliance of the world’s infrastructure on computer systems, and the consequent pervasiveness of the latter, makes their “security” an issue of great importance. Although cyberspace has greatly enhanced the efficiency, it has also brought about new vulnerabilities and challenges, thus necessitating the need for policing\(^2\).

3.2 Characteristic of Cyberspace: Need for policing

Currently, there is an enormous amount of attention being given to developing and enhancing a globally linked set of computer networks that has been

---


popularly labeled as cyberspace. This emerging space may not have divine qualities or origins but it is becoming a principal economic resource, one whose capacity, speed, and flexibility seem to be almost without limits. With rapid technology advances, trouble spots have emerged as well. There is no need to be physically present at a location, or even in the same country, to commit a wrong in cyberspace\(^3\).

Cyberspace has certain inherent peculiar technological and social features which have made the cyberspace undeniably open to exploitation thus necessitating regulation. These characteristics include\(^4\):

I. Technological Factors
   i. Increased access to technology
   ii. Increased familiarity with technology
   iii. Ability to disguise activities
   iv. Ability to destroy evidence of deviant activities
   v. Ability to remain anonymous

II. Social Factors
   i. Disinhibition
   ii. De-individualisation
   iii. Perceptions of power
   iv. Formation of strategic identities
   v. Lack of policing
   vi. Formation/emergence of deviant groups
   vii. Dehumanizing others

\(^4\)Available at: https://mujlt.law.muni.cz/storage/1205245545_sbl-drahokoupilova.pdf.
Chapter 3

Cyberspace and Need for its Policing

Due to these inherent features, in cyberspace, the threat can come from anywhere rapidly. By the time happening is noticed, it may be too late to prevent damage. While the cyberspace’s extraordinary capabilities have captured the interest of the public, much less attention has been given to assessing and confronting the obstacles that may be a by-product of a networked environment.

3.3 Information in Cyberspace: Need for policing

In cyberspace national boundaries have little meaning. Information flows continuously and seamlessly across political, ethnic, and religious divides. Even the infrastructure that makes up cyberspace—software and hardware—is global in its design, content and development. Because of the global nature of cyberspace, the vulnerabilities that exist are open to the world and available to anyone, anywhere, with sufficient capability to exploit them. So there is need for vulnerability testing.

Cyberspace provides a means for organized attack on our infrastructure from a distance. A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation’s critical infrastructures, economy, or national security. The attack tools and methodologies are becoming widely available and chances of causing havoc or disruption is increasing alarmingly.

---

Chapter 3	Cyberspace and Need for its Policing

There are over 2 million computers that comprise the unclassified, but nevertheless sensitive information database that is absolutely critical to national security. Over 90 percent of all Department of Defense voice and data traffic transits these networks, and the data includes sensitive research data and valuable intelligence information. Furthermore, these systems support critical defense missions related to troop movements, operational plans, procurement and weapons system maintenance, and also all the financial information. Cyberspace lacks uniform policies for protecting computer networks, responding to incidents, and assessing risk of damage from computer attacks like hacking, etc.⁸

3.4 Data in Cyberspace: Need for policing

Cyber attacks on databases and information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. These attacks require only information technology, and enable attackers to hide their identities, locations, and paths of entry. Not only does cyberspace provide the ability to exploit weaknesses in critical infrastructures, but it also provides a fulcrum for leveraging physical attacks by allowing the possibility of disrupting communications, hindering defensive or offensive response, or delaying emergency responders who would be essential following a physical attack. Although most visible data management problems have been traced to individuals, but organizations including governments are also capable of manipulating aspects of cyberspace for their own purposes⁹.

Data management problems in cyberspace can be generally divided into four areas: secrecy, authentication, non repudiation and integrity control. Secrecy has to do with keeping information from the unauthorized users. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a commercial deal. Non repudiation deals with signatures and being sure that a message received was really the one sent and not something that a malicious adversary modified in transit, concocted or adulterated. The data stored on computer could be deleted or there may be information theft and loss of privacy. Thief might be able to steal identity with unknowable, but probably serious consequences\textsuperscript{10}.

The information in the form of data stored on computer could be modified without knowledge. Hidden software could be installed on computer that would capture keystrokes and send them to another computer. This could compromise access to external sources, such as a protected web server, an e-mail server, financial transactions, or confidential information, etc. Authentication tokens such as credit card numbers and passwords could be obtained by the thief and used in later transactions for his or her personal gain. There could be denial-of-access to one’s own information, even though it has not been erased. It might appear in encrypted form, where only the intruder has the decryption key. Security violations can be categorised as either intentional (malicious) or accidental. It is easier to protect against accidental misuse than to protect against malicious misuse\textsuperscript{11}.

Chapter 3  Cyberspace and Need for its Policing

Among the forms of malicious access and attack on data management are the following:

i. Unauthorized reading of data (theft of information),

ii. Unauthorized modification of data and

iii. Unauthorized destruction of data, etc.

A number of software tools such as viruses, worms, bacteria, Trojan horses are being utilized to achieve these malicious objectives.12

a) Viruses

Viruses are pieces of software that can attach themselves to executable files, disk boot sectors, documents (whose loading is likely to cause embedded code execution at some point), and may even additionally hide elsewhere in the operating system, including the kernel. These “infected” entities become carriers of a virus’s malicious code, and thereby allow it to self-replicate.13

b) Worms

Worm also self-replicates like a virus, but usually over a network. Worms infiltrate computers usually by exploiting holes in the security of networked systems. By their nature, worms usually attack programs that are already running. The attack might result in creation of new processes, after which a worm can run independently, and self-propagate. Unlike a virus, a worm may not change existing programs, but like a virus, a worm may have some “payload” code, which in turn may modify existing programs or system configuration, etc.14

---

13 Available at www.kernelthread.com/publications/security/types.html.
14 Ibid.

56
c) **Bacteria**

A not-so-distinct category of digital creatures that is mentioned in literature, albeit rarely, is bacteria. These are programs that replicate themselves and feed off the host system by preempting system resources such as processor, time and memory.\(^{15}\)

d) **Trojan Horses**

Like the Greek Trojan horse, these programs have a hidden, negative, subversive, and thus potentially harmful aspect. Trojan horses are programs that masquerade as useful programs, but contain malicious code to attack the system or leak information. An unsuspecting user would typically run a Trojan horse willingly, to use its supposed (advertised) features.\(^{16}\)

e) **Logic Bombs**

A logic bomb is a program that does something, usually malicious, when some logical condition is satisfied. If the condition is time-related, such programs could also be termed time bombs. Consider some examples of logic bombs: \(^{17}\)

a) Introduction of a deliberate error in a program, say, by a disgruntled employee that will result in disaster in the future— usually may be after the employee is gone.

b) A program deletes files on every full-moon night.

c) A disgruntled administrator changes (administrator) passwords for certain systems, and leaves the company.

---

\(^{15}\) Ibid.

\(^{16}\) Ibid.

\(^{17}\) Ibid.
Chapter 3  Cyberspace and Need for its Policing

j) Backdoors

A backdoor opens a system for access by an external entity: by overthrowing, or bypassing, the local security policies. The goal of a backdoor usually is to allow remote access and control (over a network), although it may also work “locally”. Backdoors are sometimes referred to as trapdoors18.

g) Spyware

Spyware is apparently useful software that transmits private user data to an external entity, without the user’s consent or even knowledge. The external entity stands to gain from the information thus harvested. A common example is that it helps the external entity send targeted advertising to the user19.

h) Covert Channel

Sometimes, an information channel might be used to transfer certain information, possibly malicious, in a way that was not intended by the system’s designers. Such a covert channel can be an effective mechanism to help in subversive activities20.

i) Race Conditions

Race-conditions are flaws, either in design or implementation that involve an attacker exploiting a window of time in a sequence of (privileged) non-atomic operations21.

Over the past few years, information security attacks have increased dramatically in number and in strength. South Korea topped the list with 34% of attacks, followed by China with 29%, Japan 10%, Taiwan 7%, Hong Kong 4%,

---

18 Ibid.
19 Ibid.
20 Ibid.
21 Ibid.
Australia 3%, and both India and Singapore at 2%. By contrast, non-Pacific Rim countries posed a considerably lower threat profile, with Great Britain producing 7% of worldwide attacks and Germany just 2%.22

Nations with a strong communications infrastructure and free markets, which describes much of the Pacific Rim are, and very likely continue to be, the source of frequent information security attacks. Nations are in the early stages of building infrastructure and do not have the time, talent or funding to support security efforts, it is possible that internal attackers could take advantage of the lax security. This situation is compounded by external attackers who might use such situations as a jump-off point for further attacks. Countering such attacks requires the development of robust capabilities, where they do not exist today to reduce vulnerabilities and deter those with the capabilities and intent to harm critical infrastructures23.

3.5 Communication in Cyberspace: Need for policing

The ability to bypass geographical limits is a primary force behind the growth of the cyberspace. Use of the cyberspace allows people to shop, obtain professional literature, and browse through foreign art galleries without leaving home. When applied to tele-health, patients can receive multiple services without the stress and expense of traveling to a remote medical center. Whereas the potential advantages of such a communication are apparent, the laws and regulations that govern such communications in cyberspace are not yet well established. A third party can intercept voice and multimedia traffic in cyberspace and can manipulate situation adversely using same access points24.

23 Ibid.
An intruder can slither through a network cable and poke around in hard drive without leaving a trace. Anyone who can get into e-mail account can rifle mailbox and even send the messages. Computer networks play a role in essentially every attack today, and numerous attacks focus on the networks of the sensitive information passively (i.e. without modifying any data such as somebody monitors, or “sniffs” a network and gleans roaches and techniques, existing network connections could be hijacked; a third party could capture and replay transactions between two parties), or actively (somebody reroutes certain messages, introduces additional messages, or modifies existing messages).25

i) Features of communication in cyberspace

Interactions in cyberspace differ from interactions in the physical world in major ways. In contrast to interactions in the physical world, geography is not relevant when interacting in cyberspace. Communication occurs at the same speed whether the participants are in adjoining offices or on different continents. In addition, cyberspace interactions lack some of the context present in the physical world. The magnitude of this difference depends on the mode of communication. For example, e-mail communications allow for exchange of words only. Compared with a letter delivered by post, e-mail is missing even the writing style or choice of paper that complements the context of the communication.26

Even with the most advanced technology in cyberspace, some aspects of interaction found in the physical environment are missing. In cyberspace, individuals mostly interact with each other in the absence of embodied cues. The disembodied mode of communication, such as online text chat, conceals the identities of the interlocutors, allowing individuals to get to know each other

25 Ibid.
26 N.Cavus and H.Bicen, “A study to find out the preferred free e-mail services used by university students,” Vol. 1, Procedia Social and Behavioral Sciences, 419 (2009).
without seeing each other. In other words, individuals can simultaneously be intimately familiar with and completely anonymous to each other at the same time. Anonymous communications in cyberspace lead to the rise of a new realm of social relations in the life world characterized by anonymous intimacy or intimate anonymity. People in this realm interact with one another under aliases or pseudonyms. A person interacts with others behind a character he or she creates and seeks to maintain. A married man can thus pretend to be a teenage girl, an obese lady a slender boy, and a school nerd a football fan. Under the protection of anonymity, people come to explore the innermost part of themselves as well as those of others through constructing and maintaining multiple identities of their selves and through getting intimate with complete strangers.27

In cyberspace neitizens communicate in a number of ways such as e-mails, blogging, social networking sites, etc.28 Each and every mode of communication has certain pitfalls which necessitate steps for their policing such as:

ii) Concerns about blogging

Unfortunately, a small segment of the population uses blogs in hurtful and illegal ways. Predators and bullies use the information that was intended to allow expression and inspire contact to spam, con, stalk, harass, and groom victims of every age. Because the blog format is often so geared toward enabling people to reveal their attitudes, feelings, and personal information in a public way, they are attracting predators and criminals who hunt for the emotionally vulnerable or unwary. All types of cybercriminals leverage information posted online to help them identify opportunities. Identity thieves look for identifying information,

robbers look for items to steal, scam artists target people who seem susceptible to scams, and sexual predators search for victims. Middlemen aid these criminals by building catalogs of people and items that might be of interest: information about children, identities, addresses of homes whose owners are away, and locations of vulnerable cars, etc.

iii) Communications in furtherance of Criminal Conspiracies

Just as legitimate organisations in the private and public sectors rely upon information systems for communications and record keeping, so too are the activities of criminal organisations enhanced by communication in cyberspace. There is evidence of communications in cyberspace being used to facilitate organized drug trafficking, gambling, prostitution, money laundering, trade in weapons and child pornography (in those jurisdictions where such activities are illegal). The use of encryption technology may place criminal communications beyond the reach of law enforcement agencies. Encryption and other advanced technologies may be used, with direct impact on law enforcement and therefore some restrictions are necessary in the interests of national security.

iv) Dissemination of Offensive Materials

Content considered by some to be objectionable exists in abundance in cyberspace. This includes, among much else, sexually explicit materials, racist propaganda, and instructions for the fabrication of incendiary and explosive devices. Communication in Cyberspace can also be used for harassing, threatening or intrusive communications, from the standard obscene telephone call to its

---

29L.Criddle, Look both ways, 75 (2006).
contemporary manifestation in "cyber-stalking", in which persistent messages are sent to an unwilling and passive recipient\textsuperscript{32}.

\textit{v) Illegal Interception of communications}

Developments in communications in cyberspace provide new opportunities for electronic eavesdropping. From activities as time-honoured as surveillance of an unfaithful spouse, to the newest forms of political and industrial espionage, communications interception in cyberspace has increasing applications. Here again, technological developments create new vulnerabilities. The electromagnetic signals emitted by a computer may themselves be intercepted. Cables may act as broadcast antennas. Existing law does not prevent the remote monitoring of computer radiation\textsuperscript{33}. Thus there is urgent need to regulate, control and monitor cyberspace communication so as to prevent abuse of cyberspace for illegal activities.

\textbf{3.6 Commerce in Cyberspace: Need for policing}

Electronic commerce is a modern business methodology that addresses the needs of organization, merchants and consumers to cut costs while improving the quality of goods and services using cyberspace. Electronic commerce is rapidly growing in the world and is expanding into what is known as e-services\textsuperscript{34}.

\textit{i) Application of cyberspace in commerce}

E-commerce is defined as “the sharing of business information, maintaining business relationships and conducting business transactions using computers inter-
Chapter 3  Cyberspace and Need for its Policing

connected by a telecommunication system”. There are a variety of e-commerce applications. Some of these are as listed below:

a) Retail stores such as those selling books, music, toys etc.

b) Auction sites by using which an individual buyer/seller can buy/sell goods.

c) Cooperating businesses connected using their own private telecommunication network carrying out transactions in a semi-automated way.

d) Banks connected to their customers providing services such as deposits, payments, and providing information on status of an account.

f) Filing tax returns with government agencies on-line and obtaining immediate acknowledgements.

g) Electronic publishing to promote marketing, advertising, sales and customer support.

h) Web-based educational material, which allow students to learn anytime and anywhere.

Thus cyberspace has converged to facilitate the proliferation of e-commerce. However, the exponential growth in connectivity of computing and communications creates parallel opportunities for prospective offenders, and parallel risks for prospective victims. For companies and consumers alike, conducting business in cyberspace entails not only traditional risks of sales and

contracting, but also a new set of risks related to the electronic environment. Further as electronic commerce is becoming more prevalent, the application of cyberspace to fraudulent endeavors has also become much greater. Its use for fraudulent sales pitches, deceptive charitable solicitations, or bogus investment overtures is increasingly becoming common. Fraudsters can now enjoy direct access to millions of prospective victims around the world, instantaneously and at minimal cost. The risks, uncertainties and legal issues related to conducting business in cyberspace include concerns about Jurisdiction, Generation of Monopolies, phishing attacks, potential liability for unauthorized payments, employee theft, consumer fraud, tax issues, etc. This means that organizations must examine their own ‘risk appetites’ to arrive at their own ideal balance of E-risks against E-benefits.37

ii) Concerns about Jurisdiction

Contracting in cyberspace presents a challenge because the cyberspace is a form of communication that rises above spatial boundaries. Its domain flows indiscriminately across international boundaries as easily as it flows across the street. This creates jurisdiction problems in disputes between e-commerce buyers and sellers, such as where a contract was formed or which state’s law applies.38 One area of uncertainty is whether a business website owner is making an offer or merely an invitation to make an offer. There are also issues of contract validity; changes and errors in transmission; authentication and attribution; Message integrity; Non repudiation, rigours of the terms which are either harsh or which

other party could not be supposed to have reasonable notice, etc. To deal with all these legal issues there is need to regulate commercial transactions in cyberspace.

**iii) Concerns about Generation of Monopolies**

Cyberspace has no fixed borders. Cyber market is a global market place. It is certainly not a defined territorial unit, and the use and movement of resources is not restricted to any territory. National boundaries hardly apply to Cyberspace, and protective policies such as customs and other trade barriers become less feasible and least restrictive. Such barriers can be easily bypassed in Cyberspace by shifting the “location” of the transacting players. What is complicated and costly in the non-virtual world, can be achieved by pressing a button on the computer and thus mitigate all geographical barriers. Thus, Cyberspace has several features that, on the one hand, are likely to decrease monopoly problems and, hence, to reduce legitimate central intervention, but, on the other hand, may create new types of monopoly problems, which might call for innovative controls, maneuver and solutions.

**iv) Concerns about Phishing Attacks**

The term phishing ("password harvesting fishing") describes the fraudulent acquisition, through deception, of sensitive personal information such as passwords and credit card details by masquerading as someone trustworthy with a real need for such information. Phishing is the practice of sending out fake emails, or spam, written to appear as if they have been sent by banks or other reputable

---

organisations, with the intent of luring the recipient into revealing sensitive information such as usernames, passwords, credit card details or any other form of confidential information. Phishing is perpetrated in many different ways such as Deceptive Phishing, Malware-Based phishing, Keyloggers and Screen loggers, Session Hijackers, Hosts File Poisoning, System Reconfiguration Attacks, Data Theft, DNS-Based Phishing (“Pharming”), Content-Injection Phishing, Man-in-the-Middle Phishing, Search Engine Phishing, etc\(^42\).

Typically, phishing attacks will direct the recipient to a web page designed to mimic a target organisation’s own visual identity and to harvest the user’s personal information, most often leaving the victim unaware of the attack. Obtaining this type of personal data is attractive to blackhats because it allows an attacker to impersonate their victims and make fraudulent financial transactions and go scot free\(^43\).

\(v\) Concerns about Identity theft

Malware may gather information about your computer and its files and send this information back to its author. Since it can read any files on your computer (often including encrypted files), whatever you have is fair game. If you store information about your bank accounts or credit cards on your computer, this data may be of interest to an attacker. A lot of personal information from commercial and government sources has made its way to the web. Commercial Websites might contain e-mails or credit card purchases; federal, state, and local government sites might have personal information like marriage license records and property tax data, etc. which raises risk of identity theft\(^44\).

\(^{42}\) Available at www.pcworld.com/article/135293/article.html.
vi) Commercial frauds

Countless goods and services are already being sold over the Internet and the numbers continue to escalate. Aside from the standard warranty and misrepresentation claims cyberspace sales also raise the increasingly important issue of transmission security. The lack of a secure means of paying for a product over the Internet has been a major impediment to direct sales online. At the same time, new ways of separating us from our possessions, usually money, are being thought up every day and new form of fraudulent transactions such as Online E-Commerce Store Frauds, Electronic Funds Transfer Fraud, Sales and Investment Fraud etc., have emerged. Old fraud schemes have successfully made the transition to cyberspace\(^45\) thus necessitating policing.

vii) Electronic Vandalism and Terrorism

As never before, western industrial society is dependent upon complex data processing and telecommunications systems in cyberspace. Damage to, or interference with, any of these systems can lead to catastrophic consequences. Whether motivated by curiosity or vindictiveness electronic intruders cause inconvenience at best, and have the potential for inflicting massive harm and go scot free\(^46\).

Therefore it can be inferred that technology does not always come in the form of benefits and advantages and the concept of E-commerce is not an exception to it. Advances in technology have always brought with them increasing criminal applications and the cyberspace is not an exception. The big issue facing e-trade is the absence of a clear regulatory framework worldwide. The traditional


commerce and its components have been challenged by e-commerce. Consumers should be protected in e-commerce not less than the protection they enjoyed within traditional commerce\textsuperscript{47}.

Consumers or neitizens are not sure of a complete regulatory mechanism which would govern them and at the same time ensure them of a complete regulatory mechanism which would govern them, and the same time ensures them of complete security and privacy. The growth of e-commerce has fuelled the need for vibrant and effective regulatory mechanisms which would surpass all risks and would further strengthen the success of e-commerce\textsuperscript{48}. India with its complex regulatory framework needs to define transparent rules for e-commerce to keep pace with global growth.

3.7 Education in Cyberspace: Need for policing

The cyberspace has created the fastest and simplest form of learning platform. With the rapid progress in the area of information, communication and technology, students can access information in cyberspace at their convenience, at anytime and anywhere. They can open online journals, access online newspapers, and logon to various websites within split seconds. However, e-learning, its’ importance in comparison with other forms of learning is mixed, depending on a complex range of factors such as personal preferences, experiences of technologies, relevance and peer/tutor pressure\textsuperscript{49}. Addiction to the cyberspace can wreck as much or even more havoc in people’s lives as alcohol, drugs, and gambling. Cyberspace

addiction is an emerging cause of morbidity\textsuperscript{50}. Therefore, there is need to acknowledge various risk involved during e-learning in cyberspace.

\textit{a) Risk of online profiling}

Many students are unaware when they are being profiled. Online profiling is the collection of information from and about an individual while in cyberspace. This can be accomplished either through the collection of personal data a user provides or through the use of screen name or identifier “cookies” placed on a hard drive by the Web site or third-party delivering ads to a Web site. This lack of understanding is a special concern for students and young children, unsophisticated as they are in the importance of protecting information privacy. Children, and even teenagers, may not have yet developed the sophisticated skills to understand why they should not provide information to others online\textsuperscript{51}.

\textit{b) Risk of exposure to violence, pornography etc.}

A more direct threat is children’s exposure to violence, pornography, and predators on the web. A recent study entitled online victimization: A Report on the Nation’s Youth, conducted interviews with a nationally representative sample of 1,500 youths ages 10-17 who use the cyberspace. The study found that large numbers of youths are encountering offensive experiences on the Internet. Twenty percent were sexually solicited. Six percent were harassed. The offenses and offenders are diverse, not just men trolling for sex. Much of the offending behavior comes from other youth, and some from women. Teenagers are the primary targets, creating a different sort of challenge than would be the case if younger children, over whom parents have more control, were the primary targets. Although most


\textsuperscript{51}P.M.Yellowlees and S.Marks, “Problematic Internet use or Internet addiction?,” Vol. 23, Computers in Human Behavior, 1447 (2007).
solicitations fail, the sheer numbers are alarming. Several million young people, ages 10 to 17, are sexually propositioned in the cyberspace every year. Learning that there are dark streets on the web and in real life is a necessary lesson in the education of today’s modern student. Regrettable as is it may be, this lesson is an integral part of becoming a learner in today’s society.  

c) Concerns about Plagiarism in cyberspace

Plagiarism is….“the appropriation or imitation of another’s ideas and manner of expressing them, as in art, literature, etc., to be passed off as one’s own”. Plagiarism and the overuse of secondary sources are misuses of print copy. At the very least, unintentional plagiarism is a lowering of the standards of academic integrity and an impediment to student learning. Where plagiarism is intentional and/or systematic, it is cheating. Plagiarism is always unacceptable but can occur as a result of inadequate understanding of the procedures of appropriate referencing or because of lack of skills in academic writing. Plagiarism issues must be seen as a serious matter which cannot be separated from teaching-learning activities.

Cyberspace permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. Information in cyberspace is more fragile than when it is on paper because it can be more easily changed and it is more vulnerable to unauthorized access. It is more problematic because of the ease

---

of moving texts around, of separating pieces from the whole, and of performing unethical actions faster. Words are lifted, reused, redrafted and passed on.\footnote{J. Osen, “The Cream of Other Men’s Wit: Plagiarism and Misappropriation in Cyberspace,” Vol. 11, Computer Fraud & Security, 13 (1997).}

Means of authorization and authentication are lacking which expose technology to unethical practice. The questions of intellectual property rights, plagiarism, piracy, privacy and paparazzi become active issues in cyberspace. Efforts to protect information integrity, confidentiality, and availability often conflict with the desire for the benefits of information sharing. Further, the autonomous and depersonalized electronic world contributes to plagiarism and to the lack of accountability on the part of the student and on the part of the contributor of the text. The symptom of “cut-and-paste” culture seems to have spread rapidly among students, especially in cultures where copyright laws have always been ignored. A study in Melbourne of 700 students from the Monash University and the Swinburne University of technology were surveyed about their attitudes toward and actual practices of plagiarism. Almost 80% of the students surveyed admitted some form of cheating. This self-reporting study also found that 54% of post-graduates admitted to cheating.\footnote{S. O’Connor, “Cheating and Electronic Plagiarism- Scope, Consequences and Detection,” Vol. 3, Proceedings Educause in Australia Conference, 1 (2003).} A high standard of academic integrity is the prime need of the hour.

3.8 Healthcare problems in Cyberspace: Need for policing

Cyberspace also affects the health and well-being of users in different ways. eHealth is defined as “patients and the public using the internet or other electronic
media to disseminate or provide access to health and lifestyle information or services”. However, it is still not clear whether use of cyberspace in Health is a promise or peril?57

**Commercial influences on patients**

The cyberspace has always stood up for individuality, competition, and freedom. Cyberspace has implications for the education, training, and supervision of health professionals. Despite its promise for some patients or clinical settings, eHealth technology may not be safe or cost effective. Organizations need to explore the implications of substituting cyber care for face to face consultations. New ethical and legal issues are arising. Surely a wider market for health services, information, and products should be welcomed. However, if the cyberspace means that commercial suppliers can influence (or mislead) patients, or that “cyber physicians” can undercut physical primary healthcare services, whether and how to regulate e-Health must be considered58.

a) **Cyber divide in healthcare facilities**

People with lower educational achievement or income have worse health. They also make less use of the cyberspace. If more healthcare services are shifted to cyberspace, health inequalities will further worsen. The “cyber divide” worries many policy makers. Given some of these concerns, people may rise up en masse and reject the use of cyberspace in health care, leading to a “Great Revulsion”, by

58 Ibid, at 1393.
analogy with the anti-genetically modified foods campaign. Poor or elderly people feel ever more disconnected from the high tech e-Health service cyberspace59.

b) Problem of loss of Privacy

Health scare stories and urban myths spread across the cyberspace like viruses with uncontained fears about privacy, safety and fragmentation of care affecting even cautious patients. If health records become public due to unauthorized access in cyberspace this can play havoc with individual’s right to privacy. Society, led by the media, starts to see technology as inhuman. This can lead to rejection of use of eHealth services in cyberspace with substitution by a conservative “Holistic health service” emphasizing face to face contact60. As such the balance of benefits and risks of cyberspace for individual patients and clinicians is unclear.

3.9 Social problems in Cyberspace: Need For Policing

Cyberspace is having a long lasting effect on individual as well as society. Even though cyberspace makes communication at great distances easier, cheaper, and faster, people are suffering emotionally, maybe even physically. It is having serious behavioral, affective, cognitive and physiological effects on individuals. Addiction in cyberspace is an emerging cause of morbidity leading to emergence of number of social, political and psychological issues61.

Chapter 3  Cyberspace and Need for its Policing

a) Concern on emerging digital divide

While some post-industrial societies have experienced a remarkably fast switch over to the cyberspace, at present about one in 20 of the world’s population is connected. But vast masses of the population from the Sub-Saharan Africa, Latin America, and Asia are excluded from this privilege. A heavy 79 per cent of the Internet users live in high-income countries which are home to only 14 percent of the world population. In India, only 0.4 percent of the people use the Net. A global divide in access to cyberspace is substantial and it is growing. The main challenges in providing universal access to the cyberspace are high access cost, lack of infrastructure, security risks, illiteracy and the existing social inequalities. Barely 2 percent of the world population of more than six billion has access to cyberspace. Majority of world population have not even made a telephone call, what to speak of access to cyberspace. Groaning under basic problems such as illiteracy, malnutrition and sheer poverty, India’s rural populace may as well be living on a planet different from, say, Bangalore, which, according to the United Nations Development Program (UNDP) Human Development Report for 2001, is better off than many cities in the United States, Europe and Japan when it comes to technological innovation. The report clearly brought out India’s digital divide between a few urban centers and the vast rural hinterland. Among India’s 1.4 million Internet connections, more than 1.3 million are cornered by the states of Delhi, southern Karnataka (of which Bangalore is the capital), Tamil Nadu and western Maharashtra.

The issue of widening technological disparities around the world has

---

generated considerable concern amongst international agencies and national
governments. Be it the UN, the UNESCO, World Bank, European Union, or the G-
8, all have highlighted the problems of exclusion from the knowledge economy. To
cross the digital divide and put ICT to effective use to improve people’s lives,
countries and communities must be “e-ready” in terms of infrastructure, access,
training, and a legal and regulatory framework that will foster ICT use. If the
digital divide is to be narrowed, these issues must be addressed in a coherent,
achievable strategy that is tailored to meet local needs. There is need to take keen
interest in addressing the issue of digital divide.

Inequalities seen at the global level is also reflected at national levels. To
make new technologies succeed, cyberspace have to be made more people oriented
and address some of the local concerns first before catching the fancy of common
man. The American government was probably the first country to pass Digital
Empowerment Act, which envisages universal access to the cyberspace and
provides a framework for how they want to go about the same. Similar kinds of
efforts are also required in India to regulate digital divide in cyberspace. Initiative
and encouragement by government will go long way in digital empowerment of the
general masses.

The changes brought about by ICT are rapid and ubiquitous. The uneven
diffusion of this fast-changing technology has also caused the digital divide within
the countries and between the countries. It is almost certain that the countries
which do not adopt and adapt to these changes will be marginalized, widening the
digital divide. Third World countries are precariously poised at this juncture and a

---

65 J. Lull, Culture in the Communication Age, 3 (2001).
careful planning on their part would decide if the ICT would bring economic
growth for them or push them deeper into technological isolation\(^6\).

b) Exploitation of teens by on-line contacts

The cyberspace has become integral part to adolescent life. Teens develop
and maintain contacts, and many anonymously discuss intimate topics in the
privacy of their rooms, without their parents’ knowledge. “Hanging out” in chat
rooms has become commonplace. While some adults are still adjusting to the
explosion of on-line information and communication, it is common for adolescents
to communicate and to seek health information or information for homework
assignments on-line. Concern has been expressed in the medical literature about
risky on-line behaviour, particularly teen-to-stranger cyberspace contact. There is
increasing evidence that the absence of basic social cues, such as age, and the
common use of constructed identities in on-line interactions could facilitate
exploitative relationships. While personal sharing in cyberspace provides
emotional support for some teens, there is evidence that on-line peer support could
reinforce off-line antisocial behavior\(^7\).

c) Risk for sexually transmitted diseases

Recent studies report that increasing numbers are acquiring new sexual
partners through cyberspace chat rooms and that those who seek partners on the
Internet have higher rates of sexually transmitted diseases\(^8\). Accelerated intimacy
and increased dis-inhibition are commonly experienced in on-line relationships and

\(^{66}\)N.Balakrishnan, “Information and communication technologies and the digital divide in the

\(^{67}\)S.J.Genuis, “Internet interactions Adolescent health and cyberspace,” Vol. 51, Canadian

\(^{68}\)M.McFarlane, S.S.Bull, C.A.Rietmeijer;“The Internet as a newly emerging risk environment
on-line sexual activity has a high likelihood of resulting in off-line sexual contact. Young adults who seek sex partners on-line are at significantly greater risk for sexually transmitted diseases than their peers. This trend represents a serious public health challenge which needs policing.\textsuperscript{69}

\textbf{d) Cyberbuddies: an unseen peer group}

Peer influence has a profound effect on the attitudes, choices, and behaviour of teens and “one of the strongest predictors of adolescent behavior is the perceived or actual behavior of friends.” The pediatric literature strongly recommends that physicians encourage parents to monitor their children’s friends and to discourage close friendships with peers who exhibit problem behaviour. The cyberspace, however, makes this difficult, rather impossible for parents to monitor their children’s friends and weed out the deviant ones. As such the Internet is an open system, where heterogeneous agents can appear and disappear unpredictably. As the number of agents in the cyberspace increases, there is a need to regulate services and content.\textsuperscript{70}

\textbf{e) Deviant Behavior in Cyberspace.}

Feeling relatively safe with their real-world identity hidden, people say and do things they otherwise would not normally say or do in the face-to-face world. The absence of relational cues (visual, tactile, auditory) as well as physical proximity to another person may result in behavior that is nonconforming according to usual social norms and social controls. A wide variety of deviant behavior may arise as the population of an online multimedia community increases.


That behavior can span the range from simple mischievous antics to more serious expressions of psychopathology, including depression, sociopathy, narcissism, dissociation, and borderline dynamics. In some cases the deviant behavior may be a process of pathological acting out—in others, a healthy attempt to work through. Deviant behavior seen in cyberspace can vary in degree from being immoral to illegal or both. The various deviant behaviors commonly seen are a) Mischief, b) Graffiti, c) Wannabes, d) Deviant enclaves, e) Sleepers, f) Commercials, g) Flashing, h) Prop-dropping, i) Hate and violence avatars, j) Abusive blocking, k) Eavesdropping, l) Breathers, m) Verbal exhibitionists, n) Stalkers, o) Guest bashers, p) Wizard bashers, q) Self destroyers, r) Event crashing, s) Revolutionaries, t) Freedom fighters, u) Bible thumpers, v) Identity theft, w) Impostoring, x) Identity switching, y) Depressives, z) Pedophiles, etc., etc. Thus there is urgent need to detect and control any deviant behavior to prohibit any abuse or misuse of cyberspace.

f) **Problem of Disinhibition**

It’s well known that people say and do things in cyberspace that they wouldn’t ordinarily say or do in the face-to-face world. They loosen up, feel more uninhibited, and express themselves more openly. Researchers call this the “isinhibition effect.” It’s a double-edged sword. Sometimes people share very personal things about themselves. They reveal secret emotions, fears, wishes. Or they show unusual acts of gullible, kindness and generosity. On the other hand, the disinhibition effect may not be so benign and involve out spills, rude language, harsh criticisms, anger, hatred, even threats which needs policing in public interest.

---

Chapter 3: Cyberspace and Need for its Policing

g) The politically motivated websites

Cyberspace is a powerful tool by which non-state actors can alter the global powers. Terrorists and other extremists are known to make extensive use of the Internet. The number of extremist websites has increased at an enormous rate, and by one account the cyberspace is becoming ‘the most important meeting place for jihadis all over the world, to communicate, discuss, and share their views. With instruction manuals so readily available, the cyberspace has become a place of teaching and instruction. Interactive tutorials can be offered, in a wide range of subjects from weapon handling through to the skills needed to write malicious code and sabotage computer networks. Tactical and operational training can be conducted through simulators and even online computer games. With all this activity, the Internet is often described as a ‘virtual training camp’ or ‘open university’ for extremists, where recruits can be prepared to the level necessary to mount a terrorist or insurgent attack, or selected to attend a live training camp such as those in Iraq and Pakistan. Illustrative examples of websites representing the demand for an independent territory of Khalistan are the websites of The Council of Khalistan, CoK, (www.khalistan.com), the Khalistan Affairs Center, KAC, (www.khalistan-affairs.org), etc. The cyberspace is an anarchic common ground – some might call it an ungoverned space – which extremists can exploit in unremarkable ways, just as society does, for such purposes as communication and information sharing. These politically motivated uses of cyberspace if not properly regulated and controlled can lead to public unrest and can pose a great threat to political stability.

---

73 Available at www.chathamhouse.org.uk.


Chapter 3  Cyberspace and Need for its Policing

Problem of electronic waste

Globally, electronic waste (e-waste) is identified as a popular, informal name for electronic products after the end of their “useful life”. Electronic product discards are one of the fastest-growing segments of the current waste stream. The volume of e-waste has been growing exponentially over the last few decades as has been the ever increasing use of e-products (electronics in products). The existing system of e-waste processing in India is mostly handled by a very well-networked informal sector where the disposal and recycling of computer waste are very elementary and pose grave environmental and health hazards. The process followed by these recyclers is product reuse, conventional disposal in landfills, open burning and backyard recycling. The major sources of e-waste in India are the government, public and private sectors, retailers, individual households, PC manufacturing units, the secondary markets and illegally imported scrap. The current Indian legislation on classification of e-waste as hazardous remains ambiguous with none of the laws directly referring to e-waste or it’s handling. Consequential to the lack of appropriate legal instruments, there is an alarming concern over illegal trans-boundary shipment of e-waste.\textsuperscript{76}

3.10 Crime in Cyberspace: Need for policing

Cyber space creates new and favorable contexts for crime. In the world of cyber crime, evil bytes are fast replacing whizzing bullets. It is rightly said, The modern thief can steal more with a computer than with a gun. Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb.\textsuperscript{77}


Chapter 3 Cyberspace and Need for its Policing

It is rightly said, “Computers have ushered in a new age filled with the potential for good. Unfortunately, the computer age also has ushered in new types of crime for the police to address. Law enforcement must seek ways to keep drawbacks from overshadowing the great promise of the computer age.”

Carter & Katz.\(^\text{78}\)

Characteristics of cyber crime

The variety of criminal activity, which can be committed with or against information systems is surprisingly diverse. Some of these are not really new in substance; only the medium is new. Others represent new forms of illegality altogether. The four characteristics of cyber crime are\(^\text{79}\):-

- They are easy to learn how to commit;
- Require few resources relative to the potential damage caused;
- They can be committed in a jurisdiction without being physically present in it;
- They are most often clearly illegal.

The following generic forms of illegality involve information systems as instruments and/or as targets of crime.\(^\text{80}\). These are not mutually exclusive, nor are the following list necessarily exhaustive.\(^\text{81}\):


\(^{79}\)J. Patel, K. Soni, M. Prashar, et.al., Information technology act rather than information and technology giving rise to more cyber crime, 12-19 (2008).

\(^{80}\)Ibid.

\(^{81}\)Available at www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf.
### Chapter 3: Cyberspace and Need for its Policing

<table>
<thead>
<tr>
<th>S.no.</th>
<th>Name</th>
<th>Crime defined</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Cyber Defamation</td>
<td>It implies defamation by anything which can be read, seen or heard in cyberspace.</td>
</tr>
<tr>
<td>2.</td>
<td>Digital Forgery</td>
<td>Digital forgery implies making use of digital technology to forge a document.</td>
</tr>
<tr>
<td>3.</td>
<td>Cyber Pornography</td>
<td>Cyber pornography involves writings, pictures or films designed to be sexually exciting over the Internet. Such materials can be transmitted all over the world in a matter of seconds.</td>
</tr>
<tr>
<td>4.</td>
<td>Cyber Stalking / Harassment</td>
<td>The term is used to refer to the use of the Internet, e-mail, or other electronic communication devices to pursue, harass or contact another in an unsolicited fashion.</td>
</tr>
<tr>
<td>5.</td>
<td>Online Gambling</td>
<td>This means that people offer gambling services on the Internet.</td>
</tr>
<tr>
<td>6.</td>
<td>Online Sale of Illegal Articles</td>
<td>The sale of illegal articles is being committed through the Internet where one gets a better and bigger market along with the benefit of anonymity.</td>
</tr>
<tr>
<td>7.</td>
<td>Hacking / Unauthorized Access</td>
<td>Hacking is the gaining of unauthorized access to the data stored in computer systems. It is an intention act of breaking into computer system with the objective of stealing data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Denial of Service</td>
<td>It is an attempt to prevent users from assessing a specific computer resource such as a website. It involves overwhelming the targeted computer with requests so that it is no longer able to communicate with its intended users.</td>
</tr>
<tr>
<td>9.</td>
<td>E-mail Bombing</td>
<td>It refers to sending a large amount of emails to the victim resulting in the victim's account/mail server crashing.</td>
</tr>
<tr>
<td>10.</td>
<td>E-mail Spoofing</td>
<td>It is the act of electronically disguising one computer as another for gaining access to a restricted system.</td>
</tr>
<tr>
<td>11.</td>
<td>Cyber Frauds</td>
<td>It involves use of internet for carrying out fraudulent schemes.</td>
</tr>
<tr>
<td>12.</td>
<td>Virus, Worms, Trojan Horses and Logic Bombs</td>
<td>These are unauthorized software programs.</td>
</tr>
<tr>
<td>13.</td>
<td>Theft of Internet Hours</td>
<td>It involves usage by an unauthorized person of the internet hours paid for by another person.</td>
</tr>
<tr>
<td>14.</td>
<td>Data leakage</td>
<td>It pertains to illegally copying the master file information of the computer for ransom, blackmailing, or any other fraudulent purpose.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>15</td>
<td>Data Diddling</td>
<td>It involves altering the raw data just before computer processes it and then changing it back after the processing is completed.</td>
</tr>
<tr>
<td>16</td>
<td>Spam</td>
<td>It is the practice of sending unsolicited emails to others</td>
</tr>
<tr>
<td>17</td>
<td>Phishing</td>
<td>It involves the use of “spoofed” emails and websites — designed to resemble those of legitimate companies, financial institutions, and even government agencies — in order to obtain valuable personal and financial data for criminal purposes such as fraud.</td>
</tr>
<tr>
<td>18</td>
<td>Identity Theft</td>
<td>It involves pretending to be someone else in order to steal money or get other benefits. The identity of another individual is impersonated in order to commit credit card fraud, create false profiles at networking sites and operate false e-mail identities</td>
</tr>
<tr>
<td>19</td>
<td>Key loggers</td>
<td>It is a device or a software program designed to secretly monitor and log all keystrokes</td>
</tr>
<tr>
<td>20</td>
<td>Bots and botnets</td>
<td>These are programs installed covertly on a users system which allows the attacker to remotely control the targeted computer through a communication channel</td>
</tr>
</tbody>
</table>

---

Chapter 3  Cyberspace and Need for its Policing

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>21.</td>
<td>Electronic Vandalism and Terrorism</td>
<td>It means use of cyber tools to shut down critical national infrastructure such as energy transportation, communication, etc.</td>
</tr>
<tr>
<td>22.</td>
<td>Cyber bullying&lt;sup&gt;83&lt;/sup&gt;</td>
<td>Harassment of targets over the Internet.</td>
</tr>
<tr>
<td>23.</td>
<td>Cyber stalking&lt;sup&gt;84&lt;/sup&gt;</td>
<td>Following a user’s “footsteps on the Internet.</td>
</tr>
<tr>
<td>24.</td>
<td>Cyber squatting&lt;sup&gt;85&lt;/sup&gt;</td>
<td>Taking over an IP address to host your own information thus preventing the real owner from using “their” cyberspace.</td>
</tr>
<tr>
<td>25.</td>
<td>Cybercrime&lt;sup&gt;86&lt;/sup&gt;</td>
<td>Any type of criminal activity conducted over cyberspace, typically refers to financial scams such as phishing, pharming and other 419 type scams</td>
</tr>
</tbody>
</table>

Cyber crime is a social phenomenon involving people, places and institutions. To curb crime in cyberspace vigorous, timely, coordinated and effective policing is urgently needed.

a) **Problem of Cross border illegal activities**

The criminal activities in cyberspace are in permanent evolution and have cross border character. Legislation and operational law enforcement have obvious difficulties in keeping pace. The intrinsic cross-border character of this new type of crime also creates a need for improved cross-border law enforcement cooperation. A continuing situation of uncoordinated policy among nations would increase the problem by leading to fragmented anti cyber crime actions, a state of affairs which could potentially be exploited by criminals<sup>87</sup>. Thus there is need for better

---

<sup>84</sup>Ibid.
<sup>85</sup>Ibid.
<sup>86</sup>Ibid.
coordination of criminal policies for regulating cyberspace. This is true in particular for the field of fight against cyber crime.

b) **Problem of Terrorism in Cyberspace**

Cyberspace brings efficiency to all who use it. The cyberspace has revolutionized not only human communication but also means of waging war\(^88\). Criminal and terrorist groups have taken advantage of the cyberspace to their own ends. Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents. Terrorists do the following things in cyberspace\(^89\):

i) **Planning:**

Cyberspace is used to plan terrorist operations. This generally includes intelligence gathering, analysis, coordination of personnel and equipment, and other aspects of operations\(^90\).

ii) **Finance:**

Cyberspace is one of the keys in the financial system of terrorist organizations. They use Cyberspace to get funding, track books, move money around, coordinate financial actions, and make purchases. Funding often goes through so-called charitable donations, through computer crimes like credit card theft, through solicitations of any sort, and naturally, through the drug trade\(^91\).

iii) **Coordination and operations:**

Many activities are coordinated through Cyberspace. This ranges from the transmission of ‘go’ signals for the coordinated start of operations, to

---


\(^{90}\)Ibid.

\(^{91}\)Ibid.
Chapter 3  
Cyberspace and Need for its Policing

synchronization of global activities, to arrangements to meet incoming shipments, to digital versions of dead drops\(^92\).

iv) Political Action:

One of the key efforts or terrorist groups is the use of information technology to gain political action and attention. This ranges from high profile websites that urge supporters to contact their congress people to sites that give detailed instructions on how to hold protests for maximum media effect\(^93\).

v) Propaganda:

Many websites are used by terrorist organizations as part of their propaganda machines. These sites actively promote the ideals of the movements, provide selected facts and lots of misleading statements. Therefore the emerging terrorist activities in cyberspace need policing\(^94\).

c) Cyber attack on National Security

The cyberspace has revolutionized not only human communication but also means of waging war.

- In October 2007, Chinese hackers defaced over 143 Indian websites\(^95\).
- In 2010 during an attack which reportedly lasted for two months, the Chinese attackers gained access to a number of official websites including Prime Ministers Office\(^96\).
- Recently in June 2013, it came to light that National Security Agency had gathered call log records of millions of U.S. phone subscribers and targeted the cyberspace data of foreign websites. Technology giants cooperated in

\(^{92}\)Ibid.
\(^{93}\)Ibid.
\(^{94}\)Ibid.
\(^{95}\)The Times of India, November 16, 2007.
\(^{96}\)The Times of India, August 8, 2011.
Prism, a top-secret system at the U.S. N.S.A. that collects emails, documents, photos and other material for secret service agents to review\textsuperscript{97}. America’s security agencies employ some 1.4 million people with “top secret” clearances to mine data collected for U.S. National security. The facts were brought into light by Edward Snowden, the former CIA employee who turned whistleblower and fled to Hong Kong\textsuperscript{98}. Thus America is using a secret data mining programme to monitor worldwide internet data and India is the fifth most tracked country by the American Intelligence\textsuperscript{99}.

Thus cyberspace is another arena of warfare which is being used against India which needs urgent policing\textsuperscript{100}.

d) Threat and Vulnerability: A Five-Level Problem

The problem of cybercrime and threat to security can arise at various levels such as:-

*Level 1, The Home User/Small Business*

Though not a part of a critical infrastructure the computers of home users can become part of networks of remotely controlled machines that are then used to attack critical infrastructures. Undefended home and small business computers, particularly those using digital subscriber line or cable connections, are vulnerable to attackers who can employ the use of those machines without the owner’s knowledge. Groups of such “zombie” machines can then be used by third-party

\textsuperscript{97}The Hindu, June 14, 2013.
\textsuperscript{98}Hindustan Times, June 14, 2013.
\textsuperscript{99}The Hindu, June 14, 2013.
\textsuperscript{100}Available at https://www.uscert.gov/sites/default/files/.../cyberspace_strategy.pdf.
actors to launch denial-of-service (DoS) attacks on key Internet nodes and other important enterprises or critical infrastructures\textsuperscript{101}.

\textit{Level 2, Large Enterprises}

Large-scale enterprises (corporations, government agencies, and universities) are common targets for cyber attacks. Many such enterprises are part of critical infrastructures. Enterprises require clearly articulated, active information security policies and programs to audit compliance with cyber security best practices\textsuperscript{102}.

\textit{Level 3, Critical Sectors/Infrastructures}

According to the U.S. intelligence community, Critical Sectors/Infrastructures will be increasingly targeted by malicious actors both for the data and the power they possess\textsuperscript{103}.

\textit{Level 4, National Issues and Vulnerabilities}

Some cyber security problems have national implications and cannot be solved by individual enterprises or infrastructure sectors alone. All sectors share the Internet. Accordingly, they are all at risk if its mechanisms (e.g., protocols and routers) are not secure. Weaknesses in widely used software and hardware products can also create problems at the national level, requiring coordinated activities\textsuperscript{104}.

\textit{Level 5, Global}

The worldwide web is a planetary information grid of systems. Internationally shared standards enable interoperability among the world’s

\textsuperscript{102}Ibid.
\textsuperscript{103}Ibid, at 8.
\textsuperscript{104}Ibid.
Chapter 3  
Cyberspace and Need for its Policing

computer systems. This interconnectedness, however, also means that problems on one continent have the potential to affect computers on another. Therefore there is need for international cooperation to solve cyber issues and, further, to prosecute cyber criminals. Without such cooperation, our collective ability to detect, deter, and minimize the effects of cyber-based attacks would be greatly diminished.  

Thus individual and collective consciousness of a community, as well as that of a global culture is essential to the formulation and success of cyber crime control strategies. If a community has a clear and strong view about what constitutes cyber crime, and what is the appropriate and essential cyber crime control agenda, then the potential for crime and law enforcement to fragment society is minimised.

3.11 Case Laws

In number of cases the Honorable Courts have also felt need for policing of cyberspace:

- ‘A’ committed fraud to the extent of Rs. 2.27 crores by opening fictitious accounts in his own name and manipulated the credit entries in the said accounts without depositing any amount, by tampering with the computer data in the computers, and he has withdrawn amounts from the said accounts and thus defrauded the Bank.

- ‘A’ manipulated draw by using simple queries including change of font and by producing flaw in the software, thus manipulating the draw itself.

- ‘A’ exploited certain men and women for making pornographic photos and selling them to foreign websites.

---

105 Ibid, at 8.
106 Ibid.
Chapter 3  
Cyberspace and Need for its Policings

- ‘A’ learned a software “Photo shop” and he along with his friends edited the photos using the software “photo shop”. ‘B’ happened to see the morphed photographs in the computer, while the petitioner was operating his computer.\textsuperscript{110}

- ‘A’ handed over a compact disc to a fruit vendor which contained pornographic material including photographs of a girl of the locality.\textsuperscript{111}

- ‘A’ committed fraud to the extent of Rs. 81 lacs by opening fictitious accounts in his own name and manipulated the credit entries in the said accounts without depositing any amount, by tampering with the computer data in the computers, and he has withdrawn amounts from the said accounts and thus defrauded the Bank.\textsuperscript{112}

- “A” hacked into e-mail id (shadocat scratch@yahoo.co.in) of C and into an account of Facebook and used it to send vulgar message to C’s friends and strangers claiming to be C. “A” loaded obscene pictures of C in a social networking site (Face book).\textsuperscript{113}

- ‘A’ and ‘B’ in collusion, had impersonated different individuals and had used forged electronic records, created false email accounts, sent false and offensive information causing loss to the Company “C” and had deceived the addressees.\textsuperscript{114}

- ‘A’ the husband uploaded the vulgar photographs, text image of B the wife on the website and had accordingly defamed her that she is a lady of easy virtue.\textsuperscript{115}

\textsuperscript{111}Abdul Hamid and Another vs C.B.I., (2007) PH MANU 1614.
\textsuperscript{113}Shiva Jatan Thakur (Dr.) vs. Union of India & Ors., (2011) 3 GLT 813.
Chapter 3  

Cyberspace and Need for its Policing

- ‘A’ by accessing the computer system and information without the permission of the owners/authorised users copied, caused publication and thereby diminished the value of information, utility and affected it injuriously.\textsuperscript{116}

- Company (‘A’ and ‘B’) has designed, developed, hosted the pharmaceutical websites and was using these websites, huge quantity of psychotropic substances (Phentermine and Butalbital) have been distributed in USA with the help of associates. The accused and its associates are not intermediary as defined under Section 79 of the said Act as their acts and deeds was not simply restricted to provision of third party data or information without having knowledge as to commission of offence under the NDPS Act.\textsuperscript{117}

- ‘A’ during his stint in the C’s company transferred such confidential information and trade secrets to the local PC and thereafter on to his personal email id. Mails were being sent frequently to the aforesaid email id and that these contained the plaintiff’s valuable confidential, including drawing for a backhole bucket, tanks, fender, post leg etc. A unlawfully appropriated the C’s trade secrets and confidential information and moreover, violated the plaintiffs’ copyright in the drawings and data.\textsuperscript{118}

- ‘A’ indiscriminately sending e-mails and has published a large number of blogs on the website which according to C is highly vulgar, disgusting and abusive references.\textsuperscript{119}

\textsuperscript{118}JCB India Ltd. vs. I.P. Address: 122.163.98.166 and Ors., (2008) DE MANU 2584.
Chapter 3  
Cyberspace and Need for its Policing

- A taking advantage of some snapping of link between the ATM and the computer maintaining the bank accounts and other transaction of the bank had drawn sums of Rs. 5,000/- on three days though there was no sufficient balance in the account.\(^{120}\)

- ‘A’ was informed that she has won a lottery of 2,50,000 (pound two lakh fifty thousand only), and she was advised to get in touch with B on his e-mail address to claim her money after deposit of money on a particular account number of I.C.I.C.I. Bank. A went on depositing the amount time to time asked by B but she did not get any prize money.\(^{121}\)

- “A”-“F” made and used forged electronic records, created false e-mail accounts to send information that they knew was false and grossly offensive to cause annoyance, inconvenience, danger, obstruction, injury etc., to the Company, its Directors, employees and other persons with the further mala fide and deliberate intention of causing annoyance and inconvenience and deceive the addresses and recipients about the origin of such information/messages.\(^{122}\)

- “A” committed offences in manipulating the computer system and thereby causing loss to the company.\(^{123}\)

- “A” perpetrated hacking on B’s computer system having data pertaining to its client.\(^{124}\)

---


\(^{121}\)Simon Dunolz and Others vs. State of Uttarakhand, (2011) UC MANU 1608.


\(^{123}\)S. Sekar Vs. the Principal General Manager (Telecom), (B.S.N.L.) Bharat Sanchar Nigam Ltd., The Sub Divisional Engineer (G), (B.S.N.L.) Bharat Sanchar Nigam Ltd. and Inspector of Police, District Crime Branch, (2007) TN MANU 9663.
“A” made false representation using computer to the complainant that if the complainant could give him a sum of Rs. 1,00,000/-, the complainant would get in return, a profit @ 1% of the said amount everyday. After taking the said sum of Rs. 1,00,000/-, from the complainant, he did not keep up the said promise. It is clear that these averments prima facie constitute the offence of cheating which is cognizable. Offence committed is punishable under Sections 420, 417, 465, 471, 467 of Indian Penal Code, 1860 and under Sections 74, 67 & 67A of Information Technology Act, 2000125.

“A” had illicit relationships with several young ladies. The said illegal activities were video graphed and photographed by A and by screening those videographs and photographs through Internet, he amassed several crores and thereby spoiled the life of many young ladies126. In another case “A” took photographs of “B”, in objectionable and threatened to circulate them. It was held that nobody should be permitted to blackmail a woman by taking her nude photograph127.

‘A’ created a separate telephone exchange network. Telephone calls to foreign countries were being made by his customers without recording any telephone bills128.

‘A’ removed some information from the computer lying with him which have contained information as to the correct number of the lot of seeds issued for distribution to B by the company, removal of such data resulted in wrongful loss to the farmers, by facilitating submission of wrong data129.

---

126M.Saravanan, Asir @ Asir Gunasingh, Vijayan @ Vijayakumar and Dr. L. Prakash vs. State, (2006) TN MANU 8296.

95
3.12 Conclusion

Only three decades ago, a few people had even heard of cyberspace. Since then, this former military computer network has gone global. Today, cyberspace is the buzzword which enables private citizens, corporate employees, university communities, and government users to communicate with each other. People around the world can exchange ideas and information as though they were right next door. Currently, tens of millions use the cyberspace and that number is said to be doubling every year. People depend upon cyberspace every day for communications, commerce, transportation, and national security. Along with its greater capacity, however, comes greater vulnerability. For all the good it does, cyberspace has its dark sides too.\(^{10}\)

Given the unrestricted number of free web sites, the cyberspace is undeniably open to exploitation. It has begun to provide criminal opportunities of which one would never have dreamed. Not only does the increasing connectivity increase the number of prospective victims of computer related crime, it increases the number of prospective offenders also. Unlike conventional communities though, there are no policemen patrolling the information superhighway, leaving it open to everything from Trojan horses and viruses to cyber stalking, trademark counterfeiting and cyber terrorism. As the cyberspace becomes increasingly a medium of commerce, it will become increasingly a medium of fraud. Cyberspace has made it possible to invade privacy by monitoring and recording behavior of netizens. Computer crime or cyber-crime, i.e. unlawful conduct committed over the Internet, is spilling over national borders and causing a huge legal headache.\(^{11}\) Further cyber space creates a plethora of moral, civil and criminal wrongs.

---

\(^{10}\) J. Patel, K. Soni, M. Prashar, et al., Information technology act rather than information and technology giving rise to more cyber crime, 5 (2008).

Life is about a mix of good and evil. So is the Cyberspace. The integrity of the global cyberspace is critical not only to the day-to-day functioning of the world economy, but also to the security and well-being of governments, organizations and people: public bodies can be attacked, commercial interests can be defrauded and individuals can be subject to a range of assaults. Cyberspace is a system whose security is largely based on mutual trust and cooperation. Unfortunately, mutual trust and cooperation are not enough to ensure that, in this increasingly interconnected world, our computer networks remain unsafe from unauthorized intruders. With the ever rising number of people connecting to, and Cyberspace has the potential to be the most fully, and extensively, unregulated space that is not known — anywhere, at any time in history. 

Managing threat and reducing vulnerability in cyberspace is a particularly complex challenge because of the number and range of different types of users. Cyberspace security requires action on multiple levels and by a diverse group of actors because literally hundreds of millions of devices are interconnected by a network of networks. To tackle the present situation Cyberspace must be treated like a failed state, and that the world community must acknowledge what is happening in cyberspace and it must act – in coordination and on many levels. The situation is alarmingly out of control, and it may soon threaten economies and political stability in ways that are not yet understood fully. Therefore, there is urgent need to develop regulatory strategies to avoid misuse or abuse of cyberspace.