CHAPTER VI
LEGAL & TECHNOLOGICAL MEASURES TO COMBAT CYBER CRIME
CHAPTER VI

LEGAL & TECHNOLOGICAL MEASURE’S TO COMBAT CYBER CRIME

Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is cyber crime by the use of Internet. The term cyber crime can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represent the cyber crime as Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data. Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses. It has proved a challenge for governments because different domains are typically administered through respective ministries and departments. The task is made all the more difficult by the inchoate and diffuse nature of the threats and the
inability to frame an adequate response in the absence of tangible perpetrators.¹

The rapidity in the development of information technology (IT) and the relative ease with which applications can be commercialized, has seen the dramatic expansion of cyber space in its brief existence. From its initial avatar as a Network (NW) created by academics for the use of the military, it has now become a global social, economic and communications platform.

The increasing centrality of cyberspace to human existence is exemplified by facts and figures brought out recently by the International Telecommunications Union (ITU), according to which the number of Internet users has doubled between 2005 and 2010 and surpasses two billion. Users are connecting through a range of devices from the personal computer (PC) to the mobile phone, and using the Internet for a variety of purposes from communication to e-commerce, to data storage.²

The rise in the Internet population has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown a pace with the rise in the number of users. While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and

stability of cyberspace in terms of their own security. Governments are constrained in their responses by pressures exerted by politico-military-national security actors at one end and economic-civil society actors at the other.3

6.0 Impacts of Cyber-Crime

Lunda Wright, a legal researcher specializing in digital forensic law at Rhodes University, has an interesting research finding on a blog posted in October 2005. It states that there has been an increase in the rate of prosecutions of cyber-criminals. There has been an increase in clamping down on cyber-piracy related to the film and music works. There are novel lawsuits and strategies for litigation. There is a greater dependence on the skills of computer forensic experts in corporations and government. Finally, there is an increase in inter-government cooperative efforts.4

Organized crime groups are using the Internet for major fraud and theft activities. There are trends indicating organized crime involvement in white-collar crime. As criminals move away from traditional methods, internet-based crime is becoming more prevalent. Internet-based stock fraud has earned criminals millions per year leading to loss to investors, making it a lucrative area for such crime.

3 Ibid.
Police departments across the nation validate that they have received an increasing number of such crimes reported in recent years. This is in sync with the national trend resulting from an increase in computer use, online business, and sophisticated criminals. In the year 2004, cyber-crime generated a higher payback than drug trafficking, and it is set to grow further as the use of technology expands in developing countries.\(^5\)

Scott Borg, director of the U.S. Cyber Consequences Unit (an agency supported by the U.S. Department of Homeland Security), recently indicated that denial-of-service attacks won't be the new wave of future. The worms, viruses are considered not quite mature as compared to the potential of attacks in future.

i. **Potential Economic Impact**

The 2011 Norton Cyber crime disclosed that over 74 million people in the United States were victims of cyber crimes in 2010. These criminal acts resulted in $32 billion in direct financial losses. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cyber crime resulting in 1 million cyber crime victims a day. Many people have the attitude that cyber crime is a fact of doing business online.\(^6\)

\(^5\) Ibid.

As today's consumer has become increasingly dependent on computers, networks, and the information they are used to store and preserve is at risk due to the cyber crimes. Some of the surveys, conducted in the past have indicated that 80% of the company's surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was $450 million. Each week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. This could range from the theft of personally identifiable information to denial of service attacks.

As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

The disruption of international financial markets could be one of the big impacts and remains a serious concern. The modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one region of the world will have ripple effects in other regions. Hence any disruption of these systems would send shock waves outside of the market which is the source of the problem.

---


8 Ibid.
Productivity is also at risk. Attacks from worms, viruses, etc take productive time away from the users. Machines become perform slowly; servers might be in accessible, networks might be jammed, and so on. Such instances of attacks affect the overall productivity of the users and the organizations. It has customer service impacts as well, where the external customer sees it as a negative aspect of the organization.

In addition, user's concern over potential fraud prevents a substantial cross-section of online shoppers from transacting business. It is clear that a considerable portion of e-commerce revenue is lost due to shopper's hesitation, doubt, and worry. These types of consumer trust issues could have serious repercussions and are described in detail.

ii. Cyber Crime's Impact on Market Value

The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget as well as for insurance companies that provide cyber-risk policies. For example, a ruling in favor of Ingram Micro stated that physical damage is not restricted to physical destruction or harm of computer circuitry but includes loss of use and functionality. This new and evolving view of damage becomes even more important as many firms rely on information systems in general and the

---

9 Supra note 4.

Internet in particular to conduct their business. This precedent may force many insurance companies to compensate businesses for damage caused by hacker attacks and other security breaches. As the characteristics of security breaches change, companies continually reassess their IS environment for threats. In the past, Chief Investigation Officer’s (CIOs) have relied on FUD—fear, uncertainty, and doubt to promote IS security investments to upper management. Recently, some insurance companies created actuarial tables that they believe provide ways to measure losses from computer interruptions and hacker attacks. However, these estimates are questionable mostly due to the lack of historical data. Some industry insiders confess that the rates for such plans are mostly set by guesswork. Industry experts stress on the need for improved return on security investment (ROSI) studies that could be used by insurance companies to create hacking insurance, with adjustable rates based on the level of security employed in the organization and by the organization to justify investments in security prevention strategies.

Depending on the size of the company, a comprehensive assessment of every aspect of the IS environment may be too costly and impractical. IS risk assessment provides a means for identifying threats to security and evaluating their severity. Risk assessment is a process of choosing controls based on the

11 Ibid.
12 Supra note 4.
probabilities of loss. In IS, risk assessment addresses the questions of what is the impact of an IS security breach and how much will it cost the organization.\textsuperscript{14} However, assessing the financial loss from a potential IS security breach is a difficult step in the risk assessment process for the following reasons:

1. Many organizations are unable or unwilling to quantify their financial losses due to security breaches.\textsuperscript{15}

2. Lack of historical data. Many security breaches are unreported. Companies are reluctant to disclose these breaches due to management embarrassment, fear of future crimes,\textsuperscript{16} and fear of negative publicity. Companies are also wary of competitors exploiting these attacks to gain competitive advantage.

3. Additionally, companies maybe fearful of negative financial consequences resulting from public disclosure of a security breach.

\textsuperscript{14} Supra note 10.


Previous research suggests that public news of an event that is generally seen as negative will cause a drop in the firm's stock price.\(^\text{17}\)

Risk assessment can be performed using traditional accounting based measures such as the Return on Investment (ROI) approach.\(^\text{18}\) However, ROI cannot easily be applied to security investments. To justify investment in IS security, Chief Investigation Officers (CIOs) will need to (1) present evidence that the costs of a potential IS security problem outweigh the capital investment necessary to acquire such a system and, (2) prove the expectation that the IS security system's return on investment will equal or exceed that of competing capital investment opportunities. This is difficult to accomplish because if the security measures work the number of security incidents are low and there are no measurable returns. Accounting-based measures such as ROI are also limited because of the lack of time and resources necessary to conduct an accurate assessment of financial loss. Instead, companies IT resources are devoted to understanding the latest technologies and preventing future security threats.\(^\text{19}\) in addition, potential intangible losses such as loss of


competitive advantage that result from the breach and loss of reputation\textsuperscript{20} are not included because intangible costs are not directly measurable.

Therefore, there is a need for a different approach to assess the risk of security breaches. One such approach is to measure the impact of a breach on the market value of a firm. A market value approach captures the capital market's expectations of losses resulting from the security breach. This approach is justifiable because often companies are impacted more by the public relations exposure than by the attack itself\textsuperscript{21}. Moreover, managers aim to maximize a firm's market value by investing in projects that either increase shareholder value or minimize the risk of loss of shareholder value.

iii. Impact on Consumer trust

Since cyber-attackers intrude into others' space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer losing confidence in the said site and in the internet and its strengths.


According to reports presented by the Better Business Bureau Online (BBBO), over 80% of online shoppers cited security as a basic concern when conducting business over the Internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information. The perception, that the Internet is rife with credit card fraud and security hazards, is growing. This has been a serious problem for e-commerce.

Complicating the matter, consumer perceptions of fraud, assess the state to be worse than it actually is. Consumer perception can be just as powerful or damaging as fact. Hence users' concerns over fraud prevent many online shoppers from transacting business. Concern over the credibility of an e-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business. Even the slightest perception of security risk or amateurish commerce seriously jeopardizes potential business.

6.1 Areas Ripe for Exploitation: National Security

Modern military of most of the countries depends heavily on advanced computers. Information Warfare (IW) including network attack, exploitation, and defense, is not a new national security challenge, but since 9/11, it has gained some additional importance. IW appeals because it can be low-cost, highly effective and provide deniability to the attacker. It can easily spread malware, causing networks to crash and spread misinformation. Since the emphasis is more on non-information warfare, information warfare is definitely ripe for exploration.
The Internet has 90 percent junk and 10 percent good security systems,\textsuperscript{22} when intruders find systems that are easy to break into, they simply hack into the system. Terrorists and criminals use information technology to plan and execute their criminal activities. The increase in international interaction and the widespread usage of IT has facilitated the growth of crime and terrorism. Because of the advanced communication technology people need not be in one country to organize such crime. Hence terrorists and criminals can find security loopholes in the system and can function from unusual locales instead of the residents of their own country.

Most of such crimes have been originating in developing countries. The widespread corruption in these countries fuel these security hacks. The internet has helped fund such crimes by means of fraudulent bank transactions, money transfer etc. Greater encryption technology is helping these criminal activities.

\textbf{6.2 Future Trends}

One of the biggest concerns is that if there is a hack into the critical systems in government, companies, financial institutions etc? This could lead to malware in critical systems leading to data loss, misuse or even killing the critical systems. Since the communication flow is easy via the internet, the

crime organizations might merge and cooperate even more than they are currently.

The Internet is increasingly likely to be used for money laundering. As the Internet becomes the medium through which more and more international trade takes place, the risk of money laundering through over-invoicing and under-invoicing is likely to grow. Online auctions offer similar opportunities to move money through apparently legitimate purchases. Online gambling also makes it possible to move money especially to offshore financial centers.

Recruitment into crime agencies over internet will be easier than before. Secret messages can be transferred over the internet to a large group of people very easily without being conspicuous.

Because mainly information technology companies are privately owned, the focus would be on making customer happy as opposed to worry about the transnational crime. In addition, legitimate civil liberties could argue in favor of not monitoring the information technology. All of these things make it more difficult to deal with cyber-crimes.

Some of the future trends predicted by Stephen Northcutt & Friends are briefly summarized in the following words.

---

Improved Social Engineering Attacks will be the trend for the coming era. Attackers will increasingly make use of social-engineering tactics to bypass technological security controls, fine-tuning their techniques to exploit natural human predispositions. This will bring us closer to merging the line between external and internal threat agents, because social engineering will allow external attackers to quickly gain an internal vantage point despite traditional parameter security measures.

Social Media will provide the platform for the cyber crimes. More organizations will adopt social media as a core aspect of their marketing strategy. They will struggle to balance the need to be active as part of on-line social communities while balancing compliance and litigation risks associated with such activities. Similarly, organizations will have a hard time controlling online social networking activities of their users. Attackers will continue to take advantage of the still-evolving understanding of online social networking safety practices to defraud people and organizations. Security vendors will position their products, solving all these problems; some of them will stand out by allowing organizations to gradually control and monitor on-line social networking activities, while being mindful of users' privacy expectations.

Humans are the weakest link, irrespective of the change in technology attackers know that they can always hack employees. In the year 2012 and 2013 these human attacks will only grow in sophistication and numbers. Cyber attackers will always take the path of least resistance. Organizations
Legal & Technological Measures to Combat Cyber Crime

and management will finally start doing something about it to secure the human.

It is the sensitive issue for the people relying on iPhones for their day-to-day works that without issuing a warning that some worm will eat all the iPhones and convert the Androids to bricks. However, the biggest issue seems to be applications with spyware. Even the apps that come loaded on the phones, are likely to phone home, it is a sure thing with third party apps.

Memory scraping will become more common in the coming times. This has been around for a long time, but is more aggressively targeting data such as credit card records, passwords, PIN's, keys. The reason they are successful is that they get around Payment Card Industry, Gramm-Leach-Bliley Act, Health Insurance Portability And Accountability Act, (PCI, GLBA, HIPAA, etc.), Security requirements that data must be encrypted while in transit and at rest. Data in transit is decrypted on the system and often stored in memory during the lifetime of a process, or at least during a decryption routine. Depending on how a process cleans up after itself, it may stay resistant even after the fact. The data is encrypted on the hard disk, but again, the RAM likely maintains the clear-text version of the data. Browsers are notorious for leaving things sitting around in memory during web sessions. The RAM Scraping malware also targets encryption keys in memory to decrypt anything for session data to encrypted files. As far as the emerging security threat part, we are seeing RAM scraping more
commonly now as attackers focus on client-side attacks, shifting away from server-side attacks. Browsers are often misconfigured, allowing malware to get into a user's system, stealing credit card data and passwords. They are mostly an annoyance where if a customer or fraud department detects fraudulent transactions, the account must be credited and changed. This requires the banks to write-off these transactions, which can add up quickly. Audio Visual (AV) products can't keep up with the aggressive rate and polymorphic characteristics of this type of malware. We discover a ton of new malware every week, reverse it to some extent, and send the details to AV vendors to be added as a new signature. The other emerging component is the threat of RAM scraping malware targeting Point of Sale (POS) systems.

Wireless adoption will continue, branching out into a larger number of purpose-focused protocols that fit the needs of individual technology. Wi-Fi technology will continue to grow, but other protocols will also emerge with widespread adoption suiting the needs of embedded technology with a variety of focus areas including ZigBee, Wireless HART and Z-Wave, as well as proprietary protocols. With this growing alternate wireless adoption, we are already seeing some of the past mistakes from earlier failed protocols repetition. Based on this exposure, and the trend of Wi-Fi failure and improvement, we will see history repeating itself where vendors are quick to the market to capitalize on new opportunities, failing to critically examine the lessons from earlier wireless technologies.
More cloud computing issues will be at the eye of the cyber attackers. While there are many possible benefits to cloud computing, the honeymoon will end. Many organizations will soon discover that they do not have the flexibility they need for their businesses, and many others will discover that any security issues (from audit to compromise) are far more complex in the cloud. Many security professionals will come to terms with security risks of cloud computing. They will do so under pressure from the businesses they support, as companies will continue to migrate to cloud platforms. The information security community will better understand cloud environments, while the technologies implementing cloud platforms will reach an acceptable level of maturity. Security professionals will continue to apply extra scrutiny to scenarios that involve processing sensitive or regulated data in shared cloud environments.

Security Continues to become the part of Virtual Infrastructure. As more and more organizations add virtualization technologies into their environment, particularly server and desktop virtualization, security will be more embedded in the native technologies, and less of an "add-on" after the implementation is complete. For server virtualization, new firewalls and monitoring capabilities are being integrated into some of the leading platforms now. For desktop virtualization, native integration with remote access technologies and client-side sandbox capabilities are common. Vendors will continue to push the envelope and offer new tools to enhance
virtual environments, but virtualization platforms will evolve to easily allow existing security technologies to interoperate more natively, as well. In addition, security architecture design will be a "must have" element of virtual infrastructure planning and deployment, not a "nice to have".

6.3 Internet Governance Challenges and Constraints

The success of the Internet has partly been attributed to its relative openness and low barriers (including minimal security features) to entry. However, the same Internet Corporation for Assigned Names and Numbers (ICANN), it has done so very reluctantly.

Though it has been a participant in multilateral forum, the United States' agenda invariably has been to ensure that its dominant position is not disturbed.

More recently, approaches to cyberspace have taken ideological hues, with countries ultimately seeking to gain effective control over deciding the form and shape of cyberspace within their national boundaries. The jockeying to influence Internet governance issues has seen increased actively in recent times. Most of these have taken place at the multilateral level, with countries forming coalitions and introducing resolutions at multilateral forum. While Russia has been introducing resolutions on cyber security at the United Nations since 1998, it recently joined hands with China, Tajikistan and Uzbekistan to introduce an "International Code of Conduct for Information Security" (ICCIS). Some of the clauses within this resolution have been criticized as an attempt to increase control over content and information in the
guise of securing cyberspace. Proposals by the IBSA forum (India, Brazil, South Africa) have also been seen with similar skepticism. One of the noted goals of the recent Cyber Security Summit held by the British government would be seen as an effort on the part of the advanced economies to regain the initiative in drawing up norms for cyberspace that highlight core Western values.²⁴

6.4 The Indian Cyberspace

The National Informatics Centre (NIC) was set up as early as 1975 with the goal of providing IT solutions to the government. Between 1986 and 1988, three NWs were set up: INDONET connecting the IBM mainframe installations that made up India's computer infrastructure, NICNET (the NIC Network) being a nationwide very small aperture terminal, (VSAT) NW for public sector organizations as well as to connect the central government with the state governments and district administrations and the Education and Research Network (ERNET), to serve the academic and research communities.

Policies such as the New Internet Policy of 1998 paved the way for multiple Internet service providers (ISPs) and saw the Internet user base grew from 1.4 million in 1999 to over 125 million users by 2013 end.²⁵ Though the rate of growth has slowed subsequently, with Internet users now approximately above 100 million, exponential growth is again expected as

Internet access increasingly shifts to mobile phones and tablets, with the government making a determined push to increase broadband penetration from its present level of about 6%. The target for broadband is 160 million households by 2016 under the National Broadband Plan.

Despite the low numbers in relation to the population, Indians have been active users of the Internet across various segments. The two top email providers, Gmail and Yahoo, had over 34 million users registered from India. Similar figures have also been seen in the social networking arena, which is the most recent entrant to the cyber platform. India currently has the fastest growing user base for Facebook and Twitter, the two top social networking sites. An indication of the rapid pace of adaptation to the Internet in India is that Indian Railways, India’s top e-commerce retailer. It saw its online sales go up from 19 million tickets in 2008 to 44 million in 2009, with a value of Rs. 3800 crore ($875 million).

Even though the Indian government was a late convert to computerization; there has been an increasing thrust on e-governance, seen as a cost-effective way of taking public services to the masses across the country. Critical sectors such as Defence, Energy, Finance, Space,

---

26 According to the Report for 2010 of the Telecom Regulatory Authority of India (TRAI), over 381 million mobile subscribers possessed the ability to access the Internet through their mobiles, with 35 million having accessed at least once.

27 According to Internet research firm Comscore, 62% of Internet users in India use Gmail.

28 A report compiled by the Indian Market Research Bureau (IMRB) projects domestic e-commerce to be in the region of $10 billion by the end of 2011.
Telecommunications, Transport, Land Records, Public Essential Services and Utilities, Law Enforcement and Security all increasingly depend on NWs to relay data for communication purposes and for commercial transactions.

The National e-governance Program (NeGP) is one of the most ambitious in India and seeks to provide more than 1200 governmental services online. Looking to the future, the Cisco Visual Networking Index estimates that India’s Internet traffic will grow nine-fold between now and 2015, topping out at 13.2 Exabytes in 2015, from 1.6 Exabytes in 2010. That will be the equivalent of the data contained in 374,372 DVDs being carried every hour through these NWs.

In terms of contribution to the economy, the ICT sector has grown at an annual compounded rate of 33% over the last decade. The contribution of the IT-ITeS industry to GDP increased from 5.2% in 2006-7 to 6.4% in 2010-11. Much of the activities of the IT/BPO sector, which was responsible for putting India on the services export map, would not have been possible but for the cost-efficiencies provided through the expansion of global data NWs.

The government has ambitious plans to raise cyber connectivity. There has been a boom in e-commerce, and many activities related to e-governance are now being carried out over the Internet. As we grow more dependent on the internet for our daily activities, we also become more vulnerable to any disruptions caused in and through cyberspace. The rapidity with which this sector has grown has meant that governments and private companies are still
trying to figure out both the scope and meaning of security in cyberspace and apportioning responsibility. As in other countries, much of the infrastructure related to cyberspace is with the private sector, which also provides many of the critical services, ranging from banking, to electricity to running airports and other key transportation infrastructure.

Taking telecommunications as a case in point, CII in India comprises around 150 Internet and telecom service providers, offering Internet, mobile and wireless connectivity to a user base of nearly 800 million. A major portion of data communication is facilitated by submarine cables. India has landing points for major submarine cable systems which are minimally protected. A preview of what could happen by way of these cables being disabled took place in 2008 when a series of outages and cable cuts in undersea cables running through the Suez Canal, in the Persian Gulf and Malaysia caused massive communications disruptions to India and West Asia.

Other sectors that could be subjected to serious threats include the financial sector, which has largely transferred operations online. Stock exchanges in the United States and Hong Kong have reportedly been subject to cyber attacks. The electricity grid is also vulnerable with the inevitable move towards a smart grid, given the economic and efficiency factors. The protection of critical infrastructure is a complex task requiring forethought, planning, strong laws, technologies, PPP and resources. For all these reasons it needs to be given top priority by the government. The country cannot afford
to wait indefinitely for a robust policy to protect this critical infrastructure. Above all, the policy makers will need to take the challenge head on.

The government would necessarily have to work closely with the private sector, particularly in promoting cyber security practices and hygiene.

**Cyber Threats**

Cyber threats can be disaggregated, based on the perpetrators and their motives, into four baskets: cyber espionage, cyber warfare, cyber terrorism, and cyber crime.

Cyber attackers use numerous vulnerabilities in cyberspace to commit these acts. They exploit the weaknesses in software and hardware design through the use of malware. DDoS attacks are used to overwhelm the targeted websites. Hacking is a common way of piercing the defenses of protected computer systems and interfering with their functioning. Identity theft is also common. The scope and nature of threats and vulnerabilities is multiplying with every passing day.

**Cyber Warfare**

There is no agreed definition of cyber warfare but it has been noticed that states may be attacking the information systems of other countries for espionage and for disrupting their critical infrastructure. The attacks on the websites of Estonia in 2007 and of Georgia in 2008 have been widely reported. Although there is no clinching evidence of the involvement of a
state in these attacks, it is widely held that in these attacks, non-state actors (e.g. hackers) may have been used by state actors. Since these cyber attacks, the issue of cyber warfare has assumed urgency in the global media.

The US has moved swiftly and set up a cyber command within the Strategic Forces Command and revised its military doctrine. In the latest official military doctrine, the US has declared cyberspace to be the fifth dimension of warfare after land, air, oceans and space, and reserved the right to take all actions in response, including military strikes, to respond to cyber attacks against it. It is almost certain that other countries will also respond by adopting similar military doctrines. The issue whether cyber attacks can be termed as acts of warfare and whether international law on warfare applies to cyber warfare is being hotly debated. Multilateral discussions are veering around to debating whether there should be rules of behavior for state actors in cyberspace.

The issue becomes extremely complicated because attacks in cyberspace cannot be attributed to an identifiable person and the attacks traverse several computer systems located in multiple countries. The concept of cyber deterrence is also being debated but it is not clear whether cyber deterrence can hold in cyberspace, given the easy involvement of non-state actors and lack of attribution.

There is, however, ongoing debate between those who believe that cyber warfare is over-hyped and those who believe that the world is heading
towards a cyber armageddon. Both sides have valid arguments, but even as that debate continues, cyber warfare as a construct has become inevitable because the number of countries that are setting up cyber commands is steadily growing. These commands have been accompanied by efforts at developing applicable military doctrines. There is, therefore, a pressing need to think about norms for cyber warfare, whether the laws of armed conflict (LOAC) can be adapted to cyber warfare, and how principles like proportionality and neutrality play out in the cyber domain. Current rules of collective security such as Art 41 of the UN Charter and Chapter 7 are found wanting in the context of cyber warfare, particularly when it comes to the rapidity of cyber attacks, and the inordinate time it takes for decision making and action under these rules.

Cyber Crime

The increasing online population has proved a happy hunting ground for cyber criminals, with losses due to cyber crime being in billions of dollars worldwide. While other countries are reporting enormous losses due to cyber crime, as well as threats to enterprises and critical information infrastructure (CII), there are hardly any such reports coming out of India other than those relating to cyber espionage. Though the report of the National Crime Records Bureau (NCRB) for 2010 reported an increase of 50% in cyber crime over the previous year, the numbers were quite small in absolute terms. The total

number of cases registered across various categories was 698, but these low numbers could be because cyber laws have proved ineffective in the face of the complex issues thrown up by Internet. As a case in point, though the cyber crimes unit of the Bengaluru Police receives over 200 complaints every year, statistics show that only 10% have been solved; a majority of these are yet to be even tried in the courts; and the cases that did reach the courts are yet to reach a verdict since the perpetrators usually reside in third countries. Even though the Information Technology Act (IT Act) 2000 confers extraterritorial jurisdiction on Indian courts and empowers them to take cognizance of offences committed outside India even by foreign nationals provided “that such offence involves a computer, computer system or computer network located in India”, this has so far existed only on paper.

Similarly, there are relatively few reports of Indian companies suffering cyber security breaches of the sort reported elsewhere. Companies attribute this to the primacy placed on information assurance in the outsourcing business. Industry bodies such as the National Association of Software and Services Companies (NASSCOM) also attribute this to the fact that they have been at the forefront of spreading information security awareness amongst their constituents, with initiatives such as the establishment of the Data Security Council of India (DSCl) and the National Skills Registry. The Indian government has also aided these initiatives in a variety of ways, including
deputing a senior police officer to NASSCOM to work on cyber security issues, keeping the needs of the outsourcing industry in mind.

Cyberspace is increasingly being used for various criminal activities and different types of cyber crimes, causing huge financial losses to both businesses and individual’s Organized crime mafia have been drawn to cyberspace, and this is being reflected in cyber crimes gradually shifting from random attacks to direct (targeted) attacks. A cyber underground economy is flourishing, based on an ecosystem facilitated by exploitation of zero-day vulnerabilities, attack tool kits and botnets. The vast amounts of money lubricating this ecosystem are leading to increased sophistication of malicious codes such as worms and trojans. The creation of sophisticated information-stealing malware is facilitated by toolkits such as ZueS, which are sold on Internet for a few thousands of dollars. At the other extreme, components of critical infrastructure such as Programmable Logic Control (PLC) and Supervisory Control and Data Acquisition (SCADA) systems were targeted by the stuxnet malware that attacked supposedly secure Iranian nuclear facilities. Stuxnet exploited five distinct zero-day vulnerabilities in desktop systems, apart from vulnerabilities in PLC systems, and exposed the grave threat to critical infrastructure such as nuclear plants and other critical infrastructure. Cyber criminals are using innovative social engineering

---

10 A botnet is a collection of internet-connected computers whose security defenses have been breached and control ceded to a 3rd party.

31 Stuxnet is a highly sophisticated computer worm.
techniques through spam, phishing and social networking sites to steal sensitive user information to conduct various crimes, ranging from abuse to financial frauds to cyber espionage. While large enterprises are ploughing more resources into digital security, it is the small enterprises and individuals that are falling prey to cyber crime, as evinced by the increasing number of complaints on consumer complaint forums.

The low levels of computer security are also apparent in recurring statistics that show that India is the third-largest generator of spam worldwide, accounting for 35% of spam zombies and 11% of phishing hosts in the Asia-Pacific-Japan region. Over 6,000,000 computers were part of bot NWS. India ranked first in the Asia-Pacific region and contributed 21% to the regional total. A continuing trend for Internet users in India was that of the threat landscape being heavily infested with worms and viruses. The percentage of worms and viruses in India was significantly higher than the Asia-Pacific regional average. According to Computer Emergency Response Team India (CERT-In), India sees an average of 788 bot-infected computers per day. With regard to web-based attacks, India has seen a significant increase and has ranked seventh, with 3% of the world attacks, and second in the Asia-Pacific region.

Cyber terrorism

Cyberspace has been used as a conduit for planning terrorist attacks, for recruitment of sympathizers, or as a new arena for attacks in pursuit of the
terrorists' political and social objectives. Terrorists have been known to have used cyberspace for communication, command and control, propaganda, recruitment, training, and funding purposes. From that perspective, the challenge of non-state actors to national security is extremely grave. The shadowy world of the terrorist takes on even murkier dimensions in cyberspace where anonymity and lack of attribution are given. The government has taken a number of measures to counter the use of cyberspace for terrorist-related activities, especially in the aftermath of the terrorist attack in Mumbai in November 2008. Parliament passed amendments to the IT Act, with added emphasis on cyber terrorism and cyber crime, with a number of amendments to existing sections and the addition of new sections, taking into account these threats. Further actions include the passing of rules such as the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act. In doing so, the government has had to walk a fine balance between the fundamental rights to privacy under the Indian Constitution and national security requirements. While cyber hactivism cannot quite be placed in the same class, many of its characteristics place it squarely in the realm of cyber terrorism both in terms of methods and end goals.

**Cyber Espionage**

Instances of cyber espionage are becoming quite common, with regular reports of thousands of egabytes of data and intellectual property worth
millions being infiltrated from the websites and NWs of both government and private enterprises. While government websites and NWs in India have been breached, the private sector claims that it has not been similarly affected. It may also be that theft of intellectual property from private enterprises is not an issue here because R&D expenditure in India is only 0.7% of GDP, with government expenditure accounting for 70% of that figure.

Companies are also reluctant to disclose any attacks and infiltration of data, both because they could be held liable by their clients and also because they may suffer a resultant loss of confidence of the public.

As far as infiltration of government NWs and computers is concerned, cyber espionage has all but made the Official Secrets Act, 1923 redundant, with even the computers in the Prime Minister's Office being accessed, according to reports. The multiplicity of malevolent actors, ranging from state-sponsored to hactivists, makes attribution difficult; governments currently can only establish measures and protocols to ensure confidentiality, integrity and availability (CIA) of data. Law enforcement and intelligence agencies have asked their governments for legal and operational backing in their efforts to secure sensitive NWs, and to go on the offensive against cyber spies and cyber criminals who are often acting in tandem with each other, and probably with state backing. Offence is not necessarily the best form of defence in the case of cyber security, as seen in the continued instances of servers of the various government departments being hacked and documents exhilarated.
6.5 Need for a comprehensive Cyber Security Policy

As in most of the countries around the world, the cyber security scenario in India is one of relative chaos and a sense of insecurity arising out of the periodic reports of cyber espionage, cyber terrorism, cyber warfare and cyber crime. The complexity of the issue has resulted in a virtual paralysis. Legal and law enforcement mechanisms have not shifted gears fast enough to grapple with growing cyber crime.

Periodic newspaper reports indicate that a wide variety of protective measures are being contemplated by various agencies, but that is all. The lack of a coherent cyber security policy will seriously interfere with India’s national security and economic development.

It is essential that more attention at the highest levels is paid to ensuring that cyber-related vulnerabilities that can impact on critical sectors are identified and removed. A coherent and comprehensive cyber security policy will have several major elements, including accurate conceptualization of cyberspace threats; building of robust cyberspace through a variety of measures, including technical, legal, diplomatic, international cooperation; creation of adequate organizational structures; strengthening of PPPs; HR development; and implementation of best practices and guidelines. The list is only illustrative.

India’s approach to cyber security has so far been ad hoc and piecemeal. A number of organizations have been created but their precise roles have not
been defined nor has synergy been created among them. As it transcends a vast domain, this falls within the charter of the NSCS. However, there appears to be no institutional structure for implementation of policies. Neither the private sector nor government has been able to build information systems that can be described as reasonably robust. There has not been enough thinking on the implications of cyber warfare.

Meanwhile, many countries are seriously engaged in attending to their cyber security doctrines and strategies. The US, Russia, UK, France, Australia, Germany, New Zealand, South Korea, China, Brazil, South Africa, Denmark, Sweden, EU, Singapore, Malaysia the list is long and growing are actively engaged in ensuring a safe and secure cyber environment for their citizens. The international community is also engaged in a variety of discussions. NATO has taken the task of creating cyber security institutions in member countries. A group of governmental experts (GGE), set up by the UN Secretary General, gave a report in 2010 on “developments in the field of ICT in the context of international security”. The report noted that there was increasing evidence that states were developing ICTs as “instruments of warfare and intelligence, and for political purposes”. To confront challenges in cyberspace, the GGE recommended cooperation among like-minded partners, among states, between states, and between states and civil society and the private sectors.
The draft cyber security policy document put out by the DIT for public discussion is an important step but it is essentially a departmental effort, not taking a whole of government approach. DIT does not have jurisdiction over departments. The document lists a number of major stakeholders, including:

1. National Information Board (NIB); 2. National Crisis Management Committee (NCMC); 3. National Security Council Secretariat (NSCS); 4. Ministry of Home Affairs (MHA); 5. Ministry of Defense; 6. Department of Information Technology (DIT); 7. Department of Telecommunications (DoT); 8. National Cyber Response Centre (NCRC); 9. Computer Emergency Response Team India (CERT-In); 10. National Information Infrastructure Protection Centre (NIIPC); 11. National Disaster Management Authority (NDMA); 12. Standardization, Testing and Quality Certification (STQC) Directorate; and 13. sectoral CERTs. However, only CERT-In is mandated under the IT Amendment Act, 2008 to serve as the national agency in charge of cyber security. The Act also provided for a national nodal agency for protection of CII but it is not clear whether such an organization exists other than on paper; NDMA and some others play only a peripheral role; and many of the sectoral CERTs are yet to come up. In the meantime, real oversight over cyber security may be said to be distributed amongst the Ministries of Communication and Technology, Home Affairs and Defence, and the office of the NSA.
6.6 Need for a Nodal Authority

The NIB is tasked with national-level policy formulation and creation of suitable institutions and structures on Cyber and Information War (CIW). It is considered that the Secretariat of the NSC needs to be suitably structured and strengthened with the appointment of a Director General (DG) as head of CIW. To ensure the desired level of coordination, the DG must be suitably empowered and should be a person who combines a technical, operational and innovative mind with a proactive and decision-oriented approach. As structured about the functioning and meeting of NIB it feels that there are some hurdles in frequently meeting. So, it is therefore recommended that a smaller effective and flexible apex body be created to oversee and deliberate on policy and other issues in respect of CIW, with coordination and monitoring left to the DG. This apex body could constantly review the situation and institute remedial measures, where required. With experience, and confidence in delegation it could possibly take on the role of the NIB. As these include public and private agencies, the Planning Commission’s experience, which incorporates expertise from all fields, could serve as a guide. The success of the Indian BPO industry is based on ensuring demanding security requirements of clients. This experience can usefully be adapted and harnessed. Tasked as it is, the NIB could under its powers establish this apex body and DG CS&IW office as proposed. Permanence in functioning could be ensured by the allocation of business rules.
6.7 Need for an International Convention on Cyberspace

Cyber security is becoming an indispensable dimension of information security. The rapid growth of ICTs has contributed immensely to human welfare but has also created risks in cyberspace, which can destabilise international and national security. Global and national critical infrastructure is extremely vulnerable to threats emanating in cyberspace. Additionally, the growth of social media (Twitter, Facebook, Orkut etc.) has created a new medium for strategic communication that bypasses national boundaries and national authorities. The global data transmission infrastructure also depends critically on the NW of undersea cables, which is highly vulnerable to accidents and motivated disruptions.

The UNGA resolution of 8 December 2010 deals with the impact of ICT on international security. The underlying concern is that ICT should not be used to destabilize international peace and stability.

Given the positive as well as negative potential of cyberspace, there has been talk of devising an international convention on cyber security which would ensure that states behave responsibly in cyberspace.

There already exist several international conventions (chemical weapons convention, biological toxins and weapons convention, NPT, etc.) and a body of international humanitarian law (Geneva and Hague conventions) from which inspiration to draw up a cyber warfare convention can be drawn.
A pressing question to be considered in the current unpredictable cyber scenario is the following: should India actively engage itself in international efforts in framing a treaty or drawing up a framework of coherent cyber laws? Or, alternatively, should it wait till its own cyber capabilities mature to a level that they are beyond the ambit of control regimes that may evolve as subsidiaries of a proposed cyberspace treaty? Such a question has faced decision-makers right from the missile to nuclear technology control regime eras.

Opponents of a cyberspace-related treaty argue that even though the international efforts for harmonization of international legal frameworks for cyberspace do not refer to technology control regimes in their current manifestations, it would be just a matter of time before ancillaries/corollaries of such a treaty may emerge which would be based on technology control regimes; and signing such a treaty would result in undermining national sovereign interests.

Similar arguments are brought up in respect of the European Convention on Cyber crime, specifically Article 32, which, countries like Russia maintain, undermines their sovereignty.

The argument is that such treaties are biased in favour of the requirements of the major international players/powers and that India should stay aloof from such exercises till its own cyber capabilities mature to a level that they are beyond the ambit of control regimes. But this type of isolationist
approach is extensively dependent on capability maturity model; and derives little or no benefit of the opportunities that can be capitalized by following an engagement model towards these treaties and conventions. On the other hand, most of these cyber treaties are currently in their infancy and are undergoing development at various tiers 2 and tier 1 forums. If at this stage India proactively engages with the international community in drafting these cyber treaties and conventions, and capitalizes on this opportunity by molding these cyber treaties and conventions to suit its sovereign interests, then the benefits achieved by the engagement approach would, without doubt, outweigh the potential outcomes of an isolationist approach.

Can there be a convention to govern cyber warfare, cyber weapons, use of force in cyber warfare, prevent cyber crime, etc.? As debate on these issues goes on, there is as yet no convention governing cyberspace. One idea that has been mooted is that critical systems like those of schools and hospitals should be protected from attacks in cyberspace, as attacking them would be tantamount to violating international humanitarian law. It is a separate matter whether such information systems can be marked for protection and whatever source of attack can be identified and sanctioned.

A cyber convention would be unlike existing conventions in many ways. This is because in cyberspace attribution and identification is extremely difficult and identities can be easily masked. Cyber attacks also typically
involve systems located in many countries. Often, cyber attacks are silent and go unnoticed for long periods.

UNGA has regularly passed resolutions on information security. Information security summits have been held in which cyber security has also been discussed. Several regional initiatives like the European Convention on Cyber crime have been in existence for decades. These efforts can be consolidated in the form of a cyberspace convention. The key issues for consideration for a possible cyberspace convention would be:

**National critical infrastructures should not be harmed.**

- Secure, stable and reliable functioning of the Internet should be ensured.
- A common understanding of Internet security issues should be evolved.
- National governments should have the sovereign right to make national policies on ICT consistent with international norms.
- A global culture of cyber security based on trust and security should be encouraged.
- The digital divide should be overcome.
- International cooperation should be strengthened.
- PPP should be encouraged.
Legal & Technological Measure’s to Combat Cyber Crime

- CIA of information systems should be ensured.
- Balance between the need to maintain law and order and fundamental human rights should be maintained.

Such a convention would also define more precisely what constitutes threat in cyberspace and what would be the basic principles of information security. It would have many don’ts, as for instance the obligations on states not to take any overt or clandestine measures which would result in cyber warfare. It would also need to define what the use of force in cyberspace would mean and in what circumstances such force can be used, if at all. How would a state react if it is subjected to cyber attacks by a state, or a non-state actor, or by a combination of the two? Given the nature of cyberspace, where attribution is difficult, these prohibitions will be hard to define and even harder to agree upon.

Arriving at a cyberspace convention would prove highly contentious. Yet, in India we need to debate openly the merits and demerits of the international law on cyberspace. Is such a convention possible at all? An Indian view needs to be evolved.

6.8 Jurisdiction Issue

Territorial limitation on the internet becomes of peripheral nature in the virtual medium as the web pages on the net can reach almost every province in the nation and conceivably almost every nation on the globe. This is where
the point of friction between the cyber world and the territorial world begins as in the territorial world there are limitations set up by the sovereignty of the nation which is not the case in the cyber world.\(^2\)

A judicial system can function effectively if it is well regulated; it is these regulations that identify every functional aspect of the judicial system including the jurisdiction of the courts. A court in order to deliver effective judgments must have proper and well defined jurisdiction, as without a jurisdiction the court’s judgments would be ineffective. Jurisdictions are of two types namely, Personal and Subject Matter jurisdiction, and for a judgment to be effective both these types must exist contemporaneously. Further the conventional requirement as to a party can sue another is at the place where the defendant resides or where the cause of action arises. This itself is the problem with Internet jurisdiction as on the net it is difficult to establish the above two criteria with certainty. Issues of this nature have contributed to the complete confusion and contradiction that plague judicial decisions in the area of Internet jurisdiction.

The IT Act 2000 passed in India is a perfect example of the ambiguous law in the area of jurisdiction in the context of the Internet. Section 1(2) provides that the act 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. Similarly Section 75(2) provided that this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. Such a provision appears to be against the principle of justice. Going to the next level, let’s say even if the Indian court successfully assert jurisdiction and pass a judgment as per the above provisions of the IT Act 2000, the other question that arises will the foreign courts implement such a judgment? In case of the above predicament the only way to resolve such a dispute is by means of having an extradition treaty with the host nation and India. Further, it has been suggested that the Indian court develops justifiable ground on which the extra-territorial jurisdiction may validly be exercised as done by the American Judiciary.\(^3\)

From the above it becomes necessary to appreciate the complexities involved and thus it becomes indispensable to understand the nature of the Cyber crime, and whether the existing penal laws are sufficient.

When Macaulay introduced the Indian penal code in 1860 the notion of Cyber Crimes was completely unknown. Further until the IT Act 2000 was enacted there was no legal provision viz. Cyber Crimes; this was the sole rationale along with recognizing transactions carried on by means of

electronic communications to augment the e-commerce, with which the IT Act 2000 was enacted. Further a blanket provision was made under section 77 of the IT Act 2000 which provides that the penalties or confiscations provided under the IT Act 2000 will not release an offender from liability under any other law, in short the substantive provisions of the IPC are still applicable to Cyber Crimes committed in India.³⁴

Criminal Liability under Indian Criminal Law and the Information Technology Act 2000

The Indian Criminal Law hovers around the Indian Penal Code, though there are other statutes which provide for criminal liability, but the Indian Penal Code is the sole authority in regards of deciding the conditions required to fulfill criminal liability. Various expressions have been used in defining offences under the Indian Penal Code like ‘Intention’, ‘Knowledge’ etc but in spite of this clinical treatment of mens Rea experience has shown that the court have imported the Common law maxim of mens Rea in the process of interpreting the offence defined under the Indian Penal Code and other special statutes.³⁵ Thus the Courts in India have been treating the concept of mens Rea on offence to offence basis. Thus it can be said that the maxim “actus non facit reum nisi mens sit rea” as a maxim has no significance to the

---

³⁴ Penalties or confiscation not to interfere with other punishments: No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

³⁵ The Regina v. Prince Case 13Cox CC 138.
offences under the Indian Penal Code. Where the code has not indicated any peculiar guilty intent or knowledge etc, then the court presume, by considering the general definition that such an omission was made with some specific intention. In such case it would be unfair to import the maxim and arrive at a judgment declaring the offender guilty. The Indian Law Commission in its 47th Report has mentioned that as a result of the transition process that the society was going through i.e. from a simple to an industrialized society it has become incumbent to contain the malpractices that were prevailing in the society then as such malpractices were unknown before for instance Unfair Trade Practices, Adulteration in Food, drugs etc, thus to restrain the emerging situation the judiciary and the parliament played a pivotal role in introducing the concept of Strict Liability because it is difficult to prove guilty intention of the offender in such socio-economic crimes. The effect of this was that with the imposition of Strict Liability under Criminal Law the burden of proof shifted from the prosecution to the defendant, and the Guilty mind need not be proved example in crimes like hacking it is almost impossible to prove guilty mind.

In regards of the Cyber Crimes under the Information Technology Act 2000 the Liability is divided into three categories. This has been done in order to avoid broad criminalization of all the wrongful acts in the virtual medium. Firstly there are certain wrongful acts that do not attract criminal liability and mens rea is not applicable to them, such acts are subject to civil penalties and
strict liability is imposed on the wrongs of this category\textsuperscript{36} e.g. failure to maintain books of accounts, or contaminating the computer with viruses etc. Secondly there are certain acts where mens rea has been made and fundamental part of the definition of the offence, thus expressions like ‘Knowledge’, ‘intension’ etc are included in the definition of such offences\textsuperscript{37} e.g. tampering with the computer, publishing for fraudulent purposes etc. Lastly there are some acts or omissions that are made criminally liable with strict liability\textsuperscript{38} e.g. Penalty for breach of confidentiality and privacy, penalty for misrepresentation etc.

\textbf{Antiquated Criminal Procedural Laws}

The distinctive feature of the cyber crimes has also had their consequence on the criminal procedural laws which have become more obvious in the areas of prosecution and investigation of the cyber crimes. The significant feature of this ever widening space between the law enforcement agencies and the cyber criminals is that the law enforcement agencies of most of the nations are not oriented for the dexterity necessary for investigating the crime in the virtual medium to add to this complexity is the trans-national nature of the cyber crime. The result is that the traditional methods of crime investigation and the evidence collection have become obsolete partially. Following reasons can be attributed.

\textsuperscript{36} Sections 43,44,45 of the Information Technology Act 2000.
\textsuperscript{37} Sections 65,66, 67,74 of the Information Technology Act 2000.
\textsuperscript{38} Sections 71,72,73 of the Information Technology Act 2000.
As per the traditional criminal procedure as soon as the police officer come to know about the commission of the offence he/she is expected to visit the scene of the crime, and collect the first hand details about the crime. If the offence is of a cognizable nature then he must initiate investigation of the crime, but in case of a non-cognizable crime the officer is required to record the complaint and direct the informant to a Magistrate having power to try such case. The problem faced by the police officer is to begin with is that the victims are not aware of the fact that a crime has been committed against them or that the crime is being committed.

Further the police officer is empowered to ensure the attendance of the person who gives the information or who is acquainted with the facts and circumstance of the case. But in the context of cyber crime it has been noticed that there is very low reporting of the crime to the police, this factor must also be taken into consideration that the non-realization of the commission of the crime. The reasons cited for the Non-reporting of the crime are many, and many of them are of convincing nature e.g. fear of bad publicity, breach of security systems will affect the goodwill and confidence of the customers, fear of insurance cover of the companies been blown off, fear of transparency in the activities of the victim i.e. financial and other trade secrets will be required to be parted with to the investigation authorities etc.

39 Sections 154,156, 157 of the Cr.PC.
40 Section 155 of the Cr.PC, committal of the case for trial.
Few steps\textsuperscript{41} that have been recommended by Dr. S. V. Joga Rao in order to facilitate reporting and investigation of cyber crimes are:

1. Establish an incident response policy.
2. Maintain an up-to-date human resource record.
3. Archive systems logs.

The next stage of investigation is of Search and Seizure by the Police officers and the collection of incriminating evidence connected with the crime. Again in the present context of cyber crimes the investigation process requires collection of the data, which further needs to be evaluated, which may be stored in a computer system located in some other country in case of a trans-national computer crime. The police authorities find getting access to such data in other country difficult and time consuming. Further the investigation agencies need to be careful as the possible evidence in a computer system can be altered and the genuineness of such evidence is often challenged in the courts of law. The Indian Information Technology Act 2000 has addressed such issues by making amendments to the Indian Evidence Act 1872; the term electronic records have been included in the definition of the term evidence.\textsuperscript{42}


\textsuperscript{42} The Second Schedule of the Information Technology Act 2000.
The Degree of power of search is also one important aspect which needs to be addressed. The problem mainly arises in the area of Public International law with respect to search and seizure of databases via an international telecommunications network systems, as any unauthorized penetration in such databases would amount to infringement of the sovereignty of that State where the data is stored, further such unauthorized access to any computer system is an offence in India. Further the major hindrance that is caused in the investigation of cyber crimes is the level of expertise on the cyber forensics, as they must have extensive knowledge of the hardware, software, operating systems and the data-processing systems. Further the security software's, encryption software's limit the process of deciphering the data stored on the computer system. This is despite of the provision made in the criminal procedure code for the surrender of the documents or objects which are necessary for the investigation purpose either before the court or to the investigation officer on his written order. Along with the above provision there is also a duty cast on the person in-charge of the premises to grant access to the investigation authorities.

Another aspect which needs to be highlighted in light of the search and seizure of data is the tapping of telephone communications lines. This becomes inevitable especially in the case of Internet crimes as data is only

---

43 See Section 43 and Section 65 of the Information Technology Act 2000.
44 See Section 91 of the Cr.PC.
45 See Section 100 of the Cr.PC.
transmitted and not stored permanently on the computer system. This may necessitate real time monitoring system to make possible collection of evidence and make possible catching the suspect ‘red handed’. But in order to make such provisions in law, care need to be taken about the Right to privacy as unlike in the case of search and seizure, which amounts to perceptible interference which is of a limited nature, interception of the communication amount to gross invasion of the right to privacy. At the moment the power of wiretapping have been provided under section 5 of the Indian Telegraph Act 1885, which lays down a complex procedure and so that this power is not misused. The Information Technology Act 2000 provided for a specific power to intercept transmitted information through any computer resource under section 69. Comprehensive provisions with detailed procedures were made in the Convergence Bill introduce in year 2000 viz. interception of all kinds of communication like wire, electronic communications etc, however this in due course lapsed and failed to become a law.46

6.9 Cyber Crimes and the nature of Evidence

The nature of evidence in the real world and the virtual world is different. This disparity is conspicuous in all the stages of evidence detection, gathering, storage and exhibition before the court. The critical part is that all the investigation authorities that are responsible right from the stage of collection of the evidence to the presentation of the evidence before the court

46 Supra Note 36, p 182.
must understand the distinguishing attributes of the evidence so that they can preserve the evidence collected by them. In this regard the role of the judiciary also becomes vital as the judiciary must also be in the position to appreciate the computer evidence presented before them. Contrary to the real world crimes where any tangible evidence in the form of fingerprints, weapon of crime, blood stain marks etc can be traced, in the virtual world such traces become very difficult to find. The science of computer forensics is gaining significance in the investigation departments, corporate world, government departments etc. Let us understand some of the challenges that are involved in the process of cyber evidence detection, gathering, storage and exhibition before the court.  

It is considered difficult to expunge the information from the computer system than what is generally contemplated. This can be done with the help of computer forensics who are able to gather evidence or even recover information which may have been deleted intentionally. It is vital that the victim report the law enforcement agencies about the crime as early as possible. The process of preservation of cyber crime evidence lies within the understanding of an efficient and knowledgeable computer forensics expert because any carelessness in the process can lead to diminutive value of the evidence. The most often faced impediment is that the victim–companies are

47 Supra Note 31.
48 Supra note 28, p16.
more concerned with restoration of their systems to full operational status rather than allowing proper evidence collection. Thus the timely assistance of the computer forensics expert can help collect evidence from the system within shortest time possible.

Cyber evidence is of physical or logical nature. It is the physical evidence that can be traced easily as the investigator just has to visit the scene of crime and search for and take into his custody computer hardware, which may constitute main frame computers to pocket sized personal assistants, floppy diskettes, electronic chips etc. The facets of the logical component of the cyber evidence are of different nature. This entails a process described as ‘Information Discovery’ wherein the investigator scrutinizes through the log files, and tries to salvage the data from a computer system which has been affected.

Once the required evidence is identified, then the investigator must ensure that the same is collected by adhering to the legal requirements, such as evidence is collected only after the requisite warrant for it is issued or if the information appears to be outside the scope of the warrant then additional warrant be issued. The evidence collected becomes valid in the courts of law only if the evidence is collected by legal means. At the moment only officers not below the rank of a Deputy Superintendent of Police and officers deputed by the central government can be authorized to enter public places.

\[^{29}\text{Supra note 36, p 197.}\]

and collects evidence and carry out search operations and arrest.\(^5^0\) This authority has been given to higher grade officers at the moment keeping in view the misuse of this power viz. right to privacy and ensuring the validity of the cyber evidence. As of now in India the concept of ‘Reasonable expectation of Privacy’ has not be developed. The issues involved in this are that whether an ‘individual’s demeanor reflects subjective expectation of privacy’ or ‘the individual’s subjective expectation of privacy is such that the society is ready to recognize it as reasonable’.\(^5^1\)

Another quarter which needs to be tested under cyber evidence and which is inevitable is the appreciation of the computer generated evidence by all the authorities associated with the process of administration of justice. Thus not just the judiciary\(^5^2\) but also the prosecutors, the defence lawyers must become familiar with the technicalities, this is so because till now these authorities were dealing with evidence in the tangible form but the nature of evidence undergoes complete change under the virtual medium, they will have to adjust themselves to appreciate the evidence in logical format.

\(^{50}\) See Section 80 of the Information Technology Act 2000.

\(^{51}\) Supra note 36, p.198.

\(^{52}\) Section 46 of the Information Technology Act 2000 empowers the Central government in appointing adjudicating officers having experience both in the information technology and the legal field.