EVOLVING STRATEGIES FOR THE ENFORCEMENT OF CYBERLAWS

By

Karnika Seth*

ABSTRACT

The Information Technology age has led to the emergence of a dynamic and highly specialized field of law, namely 'Cyber laws'. The unique features of the internet, particularly, its borderless expanse, rapid technological advancements, anonymity, speed of communication & data transfer have posed multiple challenges to legislators of different countries who strive to adapt their existing laws for application in cyberspace or develop new laws to govern the virtual world. One of the most perplexing issues are determining Jurisdiction when a cybercrime is committed in one or more jurisdiction and the effect of it is felt in one or more other jurisdictions. Other issues include concerns of privacy, data protection and Intellectual property infringements, rising cybercrimes, cyber terrorism , child pornography. While some countries have developed laws to regulate these pertinent issues in cyberspace, the law is fraught with intrinsic lacunae and countries have faced serious law enforcement problems in their efforts to enforce cyberlaws. This is particularly felt in the context of combating cybercrimes which may involve more than a single Jurisdiction and consequently more than one set of cyberlaws , or in other words, inevitably a conflict of laws between the laws of two or more sovereign nations. This paper discusses briefly the impediments in the enforcement of cyberlaws and highlights the possible effective strategies that will lead to an effective enforcement of cyberlaws from a global standpoint.

At the outset, I would like to express my gratitude to the Hon'ble Members of the National Project Committee on Enforcement of Cyberlaw for giving me the opportunity to present this paper in the One day High Level Consultation Meeting of Judges for formulation of a National Policy and Action plan for Enforcement of Cyberlaw at New Delhi on 31, Jan 2010. I hope this paper will fulfill the intended purpose.

* Karnika Seth is a practicing cyberlawyer & Managing Partner of Seth Associates, a Law firm based in India. She is the Chairperson of the Cyberlaws Consulting Centre and the Author of the book titled "Cyberlaws in the Information Technology Age" published in 2009 by Butterworths lexisnexis that discusses the evolution of Cyberlaws across different jurisdictions including India, USA, U.K and Europe.

INTRODUCTION

William Gibson in the early 1980s , wrote a science fiction novel named *Neuromancer* which involved a large corporation that replaced governments and computer hackers that waged war against secure data. The setting described in *Neuromancer* had no physical existence. Gibson named this space as *Cyberspace.* This virtual world of 'Cyberspace' in today's information technology age is not only a practical reality but also our daily necessity. Devoid of physical boundaries, cyberspace is dynamic, undefined and rapidly changes with new technological advances in information technology. The expression 'Cyberlaws' encompasses the legal matrix of cases, statutes, regulations & legal principles that affect persons and institutions to control entry to cyberspace, provide such access, use this space and create hardware and software which enable people to go online to experience this world. To put it simply, Cyberlaws constitutes rules and regulations that govern the cyberspace .

Different countries have had their own experiences while framing and implementing cyber laws. Some early adopters in the US and the West in general, had come up with their own legislations in this regard by either adapting their existing laws in the context of cyberspace or creating new laws in respect thereof. Following their footsteps, the developing countries such as India, Pakistan, Dubai, Singapore, Malaysia, Japan, Korea, and Philippines have also enacted cyberlaw legislations . By and large, there are many complex legal issues that the law enforcement agencies of different countries have witnessed from time to time and still remain unresolved. The legislators of cyberspace law have faced peculiar obstacles in adapting the legal principles of the traditional legal systems in context of cyberspace. The borderless space, anonymity of users online, dynamic e-commerce and rapid digital transmission pose a real challenge to the application of traditional laws in cyberspace. On one hand, the proponents of Cyberlaws voice the need for States to put up informational borders in cyberspace through deploying technological and legal measures. On the other hand, there are also critics who strongly advocate that the Society should accept the Internet

and its developing social practices on "as is" basis and with minimal government interference[1].

Before we proceed to discuss the complications faced in enforcing cyberlaws and recommend strategies to combat these problems , it is important to highlight the fact that on a global scenario there are some substantive issues in cyberspace for which effective solutions have been recognized and accepted through enacting legislations or caselaws on which certain degree of universal acceptance has been conferred. While some are contractual, the others are non contractual.

Contractual issues in cyberspace

On the contractual front, jurisdiction and formation the e-contracts are two key issues on which traditional legal principles have been largely applied by Courts worldwide. There is a now a general consensus that in the e-world, electronic signatures and electronic documents are equally legally valid as the hand-written signatures or hard copy paper documents. In U.S. alone 57 new electronic bills were introduced in the state legislature during the first two months of 1999 after the enactment of the UTAH Digital Signature Act 1995.The United Nations Commission on International Trade law working group on electronic commerce completed its work on Model law on Electronic Commerce in 1996. The purpose of Model law is to offer national legislators a set of internationally acceptable rules which detail how a number of legal obstacles to the development of electronic commerce may be removed and how a more secure environment may be created for electronic commerce. The Model law achieves its purpose through the principle of "*functional equivalence*". This approach involves analyzing the purposes and function of the traditional paper based requirements such as handwritten signature and original documents and considering the criteria necessary to enable electronic data to achieve the same level of recognition as a paper document.

India enacted its first law of IT through the IT Act, 2000 based on the principles elucidated in the UNCITRAL model law of e-commerce. The Indian Evidence Act 1872 has also been

---

1 John Perry Barlow's "Declaration of the Independence of the cyberspace" at www.eff.org~barlow/declaration-Final.html, *See* David G. Post, *The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed*, 5 IND. J. GLOBAL LEGAL STUD. 521, 539 (1998) (arguing that the unregulated Internet naturally guarantees consent of the governed).

amended to adopt legislative provisions dealing with the admissibility and evidential weight of electronic documents / data messages.

Non contractual issues in Cyberspace

Among the non contractual issues that have emerged in cyberspace before the courts of different jurisdictions is the situation where in the absence of a contract which establishes jurisdiction, a claim is made that something happened in the course of internet commerce which constitutes a business tort[2]. The extent to which someone who allegedly causes tortious injury in cyber space is subject to jurisdiction in a remote location may well depend on the extent to which this tort is intentional. The jurisdictional issues arise also from consumer protection disputes in the world of online marketing and transactions where the bargaining power disparity originates. The consumer protection laws of individual states in the United States, modelled on the Federal Trade Commission Act [3]have been interpreted to apply to the internet. In *People vs. Lipsitz* [4], an in-state seller of magazine subscription over the Internet, violated consumer protection laws of New York by falsifying statements in emails, and by failing to deliver promised magazines. It was made subject to personal jurisdiction in New York due to active contacts and business solicitation it had in the State. Different countries are making attempts to interpret, adapt and apply their local laws to resolve cyberspace jurisdictional and enforcement issues based on new found principles such as ***Zippo sliding scale test***[5](based on interactivity of a website), ***Effects test***[6](based on where effects of an illegal act are felt), and of late the ***Targeting approach principles***[7](based on whether accused solicited business in a particular jurisdiction). By far, the effects test has gained much consensus followed by the target approach principle[8].

---

[2] See Legal implications of offering online financial services , Stephen Revill, Bell Gully at http://www.bellgully.com/resources/resource_00254.asp

[3] 15 U.S.C Section 5

[4] 663 N.Y.S. 2d468 (Sup. Ct. N. Y. Co. 1997)

[5] *Zippo Manufacturer v. Zippo Dot Com* 952 F. Supp. 1119 (D.C.W.D. Pa. 1997)

[6] *Calder v. Jones465 U.S. 783 (1984).*

[7] *People v. World Interactive Gaming*714 N.Y.S. 2d 844 (N.Y.Sup. 1999), 1999 N.Y. Misc. LEXIS 425 (S.C. N.Y.1999).[hereinafter *World Interactive Gaming*].

[8] Darrel C Menthe, *'Jurisdiction in Cyberspace: A Theory of International Spaces'*, Michigan Telecommunications Technology Law Review, vol 4, 1998, p 69, at http://www.mttlr.org/ volfour/menthe.pdf.

However ,it may be noted herein that there is no uniform, international jurisdictional law of universal application, and such questions are generally a matter of conflict of laws, particularly private international law. An example would be where the contents of a web site are legal in one country and illegal in another. In the absence of a uniform jurisdictional code, legal practitioners are generally left with a conflict of law issue.

Another area that poses a major legal issue is that of data protection[9]. Many countries have already introduced comprehensive legislation to deal with data protection issues in the context of online activity. For example, EU has introduced Data Protection Directive which allows consumer of EU members States to view and update their personal information held by other entities which places an immense burden on websites operators who may have infrequent contact with residents of the members states. United Kingdom also has a UK Data Protection Act[10] in force since 1998.India has incorporated Data Protection provisions in its Information technology law regime through incorporating specific provisions, in particular, Section 43,66,43A ,72 of the IT Act,2000.

In addition, Intellectual property infringements over the internet are quite frequent due to the ease which copyrighted and trade mark materials may be copied, published, and transmitted in the e-world. Copyrighted material may be copied from websites and placed on another website. Registered Trade marks may be used in domain names, in meta tags as a cue for search engines or be sold as search word to buyers other than the trade owner. Courts have applied the innovative Minimum Contacts Test analysis of *International Shoe*[11] *and the Zippo*[12] *sliding scale approach based on interactivity of a website with a user t*o decide such cases. Further , a global acceptance has been received by the ICANN Domain Name Dispute Resolution Policy that is being effectively utilized to resolve domain name disputes[13].

---

[9] The world first computer specific statutes was enacted in 1970 by the German State Hesse, in the form of data protection act. Prompted in large major by memories of the misuse of records under the Nazir regime the legislation sought to assuage public concern about the use of the computers to store and process large amount of personal data.

[10] A detailed discussion paper can be found at - HTTP://www.KENTLAW.edu/cyberlaw/docs/rfc/ad2rtx

[11] *Washington v International Shoe co* 326US310(1945),317

[12] *Zippo Manufacturer v Zippo Dot com* 952FSupp 1119 (DCWD Pa 1997)

[13] www.icann.org

While there may be a global consensus with respect to legal enforcement and internet censorship against certain offences such as Child pornography, Cyberwarfare, threat to national security and cyber terrorism, different countries may completely differ in treatment of certain other serious issues such as Gambling, hatespeech, political propaganda, defamatory matter, pornography on internet where these may be protected by the right to freedom of speech and expression. Hence despite some homogeneity in law , the substantive laws are heterogeneous to a great extent.

CHALLENGES IN THE ENFORCEMENT OF CYBERLAWS & RECOMMENDED STRATEGY FOR EFFECTIVE ENFORCEMENT.

A major challenge in enforcement of cyberlaws is posed by the fact that there are no territorial boundaries in the Cyberspace and there are heterogenous laws across the globe A very radical and direct way to solve the question would be giving an entity supra-national powers on cybercrime matters, thereby abolishing borders and creating a single, global, cyber-jurisdiction. However, this seems to be highly unrealistic and a virtual myth.

This dilemma in Cyberspace is rightly commented by Johnson and Post in their paper on *'Law and border - The rise of law in cyber space*[14]' when they stated that -

> "Cyber space radically undermines the relationship between legally significant online phenomena and physical location. The rise of the global computer network is destroying link between geographical locations and (i) the power of the local government to assert control over online behavior (2) The effects of online behavior in individual or things (3) the legitimacy of the efforts of local sovereign to enforce rules applicable to global phenomena (4). the ability of physical location to give notice of which sets of rules apply."

> From a practical standpoint there are a number of challenges posed by the cyberspace interalia, lack of general awareness on the subject, technical complexities due to anonymity element and ease of committing crimes online, difference in procedural and substantive laws, difficulties in storage and preservation of digital

[14] See www.temple.edu/lawschool/dpost/Borders.html

evidence, lack of training of law enforcement personnel , international cooperation and coordination hurdles to name a few key challenges. I intend to now discuss each of these challenges and recommend strategies to combat these law enforcement problems.

Challenge 1: Lack of awareness of the cyberlaws among general public

Strategy 1: Educate the people about their rights and obligations in cyberspace and legal remedies in cyberspace law

The first and foremost initiative recommended is to educate the people and inform them about their rights and obligations in Cyberspace. The practical reality is that most people are ignorant of the laws of the cyberspace. Over 80% of our population may not know what are Viruses, Trojans, Malware . The gullible victims may be a part of a botnet , the infamous zombie computer networks at the core of a criminal activity.As a matter of fact, most people may not know that their PCs are infected or may not know or have the confidence to report such detected criminal activity.

The ' **2008 Computer Crime and Security survey** ' of the Computer Security Institute reports that when they were victims of cybercriminal offences, only 27% of organizations (both from the private and public sector) reported them to a law enforcement agency. A statement made by *John Kane,* manager of the IC3 (the US platform for reporting cybercriminal offences online) about the number of reports processed by the IC3 in 2008 seems to indicate that the situation may not be any better when it comes to individual users: 'It's our belief that these numbers, both the complaints filed and the dollars, represent just a small tip of the iceberg' . He estimates that 'only about 15% of Internet fraud cases ever get reported'.[15]

There are plethora of cyber crime activities that have germinated in the last two decades, the most rampant ones in today's world being hacking, MMS scams, phising attacks, virus attacks, credit card frauds, piracy of music, or software programs. Computer crime encompass a broad range of potentially illegal activities. Generally, however, it may be divided into one of two types of categories: (1) crimes that target computer networks or

[15] http://profmgmt.wordpress.com/2007/04/16/ is-google-money-laundering/.

devices directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

Examples of crimes that primarily target computer networks or devices would include,

- Malware (malicious code)
- Denial-of-service attacks
- Computer viruses

Examples of crimes that merely use computer networks or devices would include,

- Cyber stalking
- Fraud and identity theft
- Phishing scams
- Information warfare

Convicting cybercriminals is necessary for effective legal enforcement of cyberlaws as they may pose a direct threat to a user's reputation, finances, physical integrity, data and privacy and also because cybercrime has economic consequences and indirectly promotes traditional violent crimes, terrorism and moneylaundering scams. Spreading awareness of simple best practices on the internet such as installation of antiviruses (i.e McAfee, Norton), installation of firewalls, practicing safe shopping and clicking, avoiding disclosure of sensitive information , system updations and strong passwords can effectively assist in reducing the number of cybercrimes and even add evidentiary value to assist in convicting cybercriminals. Also people need to be made aware of the legal enforcement procedure and infrastructure in place in their countries to report the cybercrimes and effectively prosecute cybercrime cases. In India, not many people are aware of the office of Adjudicating Authority that is empowered under the IT Act, 2000 to try cases of cyber contraventions and pass orders imposing penalties by way of damages and compensation.

Speaking at the opening of the 16 th session of the Commission on Crime Prevention and Criminal Justice, UNODC Executive Director Antonio Maria Costa said countries lacked

sufficient information on criminal activities such as money-laundering, corruption, identity-theft, counterfeiting, cyber-crime and environmental destruction.

"Despite the fact that trans-national crime is one of the greatest threats to security, we operate in an information fog," Mr Costa said. "We do not know the scope of the threats we face and we cannot gauge global crime trends."

He urged countries to track organized crime more effectively and provide information of the type already collated by UNODC on illicit drugs so that governments have the data they need to generate an effective global response[16].

Greater awareness can be imparted through specialized professional courses, organizing seminars, workshops , through print and electronic media, mass campaigns, involvement of Industry specialists, cyberlawyers, forensic associations amongst other means for spreading cyber education. International organizations should be involved in seminars and workshops conducted with members of Judiciary, Police and legal experts and Industry Associations so that cyberlaws is discussed from an international perspective and Policy makers learn about new technical , policy and legal measures (substantive & procedural) being adopted in other jurisdiction to harmonize cyberlaws and its enforcement.

Challenge 2: Our law enforcement officials lack proper training in cyberlaws

Strategy 2: Adequate training to law enforcement officials must be imparted to equip them with legal knowledge and required technical knowledge to enforce cyberlaws.

There is an imperative need to impart the required legal and technical training to our law enforcement officials, including the Judiciary and the Police officials to combat the Cybercrimes and to effectively enforce cyberlaws. Because of the speed at which communications technologies and computers evolve, even experts must receive regular and frequent training in the investigation and prosecution of high-tech cases.

[16] see http://www.unodc.org/unodc/en/press/releases/2007-04-23.html

At the judiciary level, the lawyers, judges and judicial officers both of civil court and criminal courts may also be involved in discussions on Cyberlaw and at the National Judicial Academy specialized workshops on cyberlaws could be organized to develop better understanding of the law and to bring about speedy delivery of justice. Due to the peculiar characteristics of the cyberspace and fragility and vulnerability of e-evidence, it is important for law enforcement officers to pass search and seizure orders to procure mirror images of the systems at the earliest instance. Since the majority of cyber crime offences defined under the amended IT Act are punishable with imprisonment for three years, the net effect of all amendments is that a majority of these cybercrimes are bailable. This means that the moment a cybercriminal is arrested by the police, barring a few offences, in almost all other cyber crimes, he has to be released on bail as a matter of right, by the police. A cyber criminal, once released on bail, will immediately attempt at destroying or deleting all electronic traces and trails of his having committed any cyber crime. This makes the task of law enforcement agencies extremely complicated.

The reporting and access points in police department require immediate attention. In domestic territory, every local police station should have a cybercrime cell that can effectively investigate cybercrime cases . Accessibility is one of the greatest impediments in delivery of speedy justice. Only 4 cybercrime crime cells in Metropolitan cities and a handful of police officers is highly inadequate in light of growing cybercrimes in India. EOW cell only handles Economic crime cases that involve a sum of INR 1 crore and above and the local police stations have neither trained officers nor equipment to handle the problem. It is a welcome move that the IT Act 2000 has been recently amended and investigation powers have been conferred on Inspectors and above (as opposed to DSP and above provided earlier). Further, two batches of police officers have been recently trained at the IP University on cyberlaw and legal enforcement. We need to encourage such imparting of specialized training and establish cybercrime cells in each local police station. Also we have only one Government recognized forensic laboratory in India at Hyderabad which prepares forensic reports in cybercrime cases. We need more such labs to efficiently handle the increasing volume of cybercrime investigation cases.

In addition to domestic training, countries should participate in coordinated training with other countries, so transnational cases can be pursued quickly and seamlessly. Trained and

well-equipped law enforcement personnel - at local, state, and global levels can ensure proper collection of evidence, proper investigation, mutual cooperation and prosecution of cybercases. Such initiatives to train its law enforcement officials are being taken at various levels by different organizations. For instance, as part of its growing number of activities to tackle cybercrime, UNODC recently hosted a one-week training workshop for law enforcement officers on live data forensics, a subject area which looks at ways in which data can be seized from a suspect's computer while it is still running, thus avoiding the need to seize the computer and take it to a laboratory for analysis. UNODC is working closely with the Irish Police Service, which was recently awarded funding under the European Commission Prevention of and Fight against Crime (ISEC) programme to develop and deliver cybercrime training for all 30 European Union and candidate countries. Experts from Europol and INTERPOL, representatives of Internet service providers and academics are also involved in the programme[17]

Challenge 3: Anonymity on the internet poses serious issues in tracing cybercriminals as tracing an IP can be complicated due to use of proxy servers and other spoofing tools.

Strategy 3: It is recommended that adequate manpower and resources are dedicated to developing & promoting technologically sound applications to trace IPs and imparting of forensic science education

When a cyber-stalker sends a threatening emails, or when credit card numbers are stolen from a company engaged in e-commerce, investigators must first locate the source of the communication. To accomplish this, they must trace the electronic trail leading from the victim back to the perpetrator. Actual IP address of a cybercriminal may be extremely difficult to trace. With technical ways to circumvent correct display of IP addresses, such as use of proxy Ips and spoofing techniques, it is a challenging task for law enforcement agencies to track cybercriminals. Fast Flux is one example of such a large scale use of zombie machines as proxies. Fast Flux is a technology used by cybercriminals to make a website resistant both to firewall website filtering(when it is IP address based) and to trace and ' Take down" attempts by law enforcement and malware fighters. It is even more

[17] see http://www.unodc.org/unodc/en/frontpage/2009/June/law-enforcement-officers-trained-in-tackling-cybercrime.html

complex to trace an IP if it involves an Onion routing[18] . The People's Republic of China has had a very hard time preventing people from bypassing its 'Golden Shield Project' (a national Internet control and censorship project [19], sometimes referred to as 'The Great Firewall of China'), that it has announced a new directive: as of 1 July 2009, all personal computers sold in mainland China, including those imported from abroad, must feature the *Green Dam* software (either installed/pre-installed, or on CDs). *Green Dam* restricts access to a secret list of sites, and monitors users' activity[20] .Such a move highlights the fact that in the same way as it is difficult to trace connections, it is even difficult to prevent access to information on the internet with definiteness. For instance, access to terrorist based websites and child pornography cannot be blocked for techie users who may use a proxy,a private network,onion routing or proxy programs such as *freegate and ultrasurf* . Similarly, "anonymous re-mailer" services, which are services that strip the address information from email messages before passing them along to their intended recipients, raise difficult privacy and law enforcement policy issues. Further, wireless access can either be easily stolen (a survey conducted by *Sophos* in December 2007 revealed that out of 560 computer users, 54 per cent had stolen WiFi connectivity[21]. Moreover, even identifying the owner of a particular mobile phone can be difficult, because mobile phones can be altered to transmit false identifying information. As the costs of mobile phones and mobile telephony service drop, we can expect to see the marketing of "disposable phones," which will further complicate the ability of law enforcement agencies to gather evidence linking a perpetrator to the communication.

Therefore, technically advanced tools and softwares to detect spoofing and to trace the correct IP addresses is therefore essential to detect and identify Cybercriminals on the internet. Proper training and education in cyberforensics is equally essential for collection , storage, and preservation of digital evidence which can otherwise be easily tampered or

[18] Onion routing, popularized by the surge of Tor, is an extremely powerful means of anonymization over the Internet. In an onion routing scheme, information transmitted between two relay nodes (including the client and the first relay) is encrypted, and from origin to destination each relay only has knowledge of the previous and the next relay. In other words, when the nodes relay information, they don't know

[19] See http://en.wikipedia.org/wiki/Golden_Shield_Project

[20] See http://en.wikipedia.org/wiki/Green_Dam_Youth_Escort.

[21] See http://www.itpro.co.uk/165633/users-will-steal-wi-fi -to-bypass-fi le-sharing-crackdown.

erased. There is a definite need to define, design, produce, and implement efficient security tools and measures of protection and reaction to support availability, integrity and confidentiality of ICT infrastructures and develop confidence into e-services. Security Technologies should be Cost effective; User friendly; Transparent; Auditable; and Third party controllable.

Challenge 4: *lack of adequate legal provisions to maintain internet usage files and records makes combating cybercrimes a complex task*

Strategy 4 : Enacting Stricter laws on maintaining logs and Registers for internet usage

The IP can be traced by checking the logs derived from the Internet Service provider . At times, the access to the user details may be denied by Internet Service Provider on jurisdictional grounds or its logs may have simply expired or overwritten. The police may need to secure appropriate legal orders in each jurisdiction where a relevant carrier or ISP is located. The tracing of cybercriminal becomes difficult when no logs are maintained for reasonable duration of time by companies and ISPs or they are overwritten frequently. Also the cybercafés may not maintain the required Registers for recording personal details and keep records of identity verification of any customers who may use their internet services.

Adequate legal mechanisms will need to be developed to tackle these intricate issues. At present only Police orders mandate in India that Cybercafes should maintain in a Register the personal details and identity proof of its internet users. However, very rarely any inspections by Police are made to effectively check enforcement of this law. Further under Section 79 of the IT Act ,2000 no guidelines exist for ISPs to mandatorily store and preserve logs for a reasonable period to assist in tracing IP addresses in Cybercrime cases.

Voice over Internet Protocols (VoIP) and other new technologies may be a challenge for law enforcement in the future. It is important that law enforcement, government, the VoIP industry and ICT community consider ways to work together to ensure that law enforcement has the tools it needs to protect the public from criminal activity and decrease the number of vulnerabilities of digital environments.

Challenge 5: Electronic data is sensitive and can be easily tampered or destroyed.

Strategy 5: Providing cyber forensic science education to law enforcement personnel will assist in protecting sensitive e-evidence admissible in court of law

Electronic data generated by computers and networked communications such as the Internet can be easily destroyed, deleted, or modified. Digital photographs are but one example of digital information that can be altered in ways that may be difficult to detect. As a result, law enforcement officials must be cognizant of how to gather, preserve, and authenticate electronic evidence in a authentic manner that will be completely admissible in a court of law. When computers are used to store information, law enforcement agents generally can, upon securing a warrant, search the computer in the same way that they would a briefcase or file cabinet. The difference is that a computer can store a tremendous amount of information, including evidence that might not be known to the computer's owner.

This feature of computer information can be both a benefit to and a challenge for law enforcement. It can benefit law enforcement by providing information (sometimes in a readily searchable way) that might not have existed in the non-computer world. But it can obviously present law enforcement challenges by highlighting the need for training and time for the information to be recovered. This will not only require substantial training of law enforcement personnel, but also sufficient experience with such evidence by investigators, prosecutors, defense counsel, courts, and others until clear rules and standards are established. Cyber-specific equivalents of traditional investigation measures include-

- expedited preservation of stored computer and also traffic data, the so-called "quick freeze procedure" to ensure that cybercrime investigations do not fail simply because data were deleted during the (often lengthy and complex) investigation process,
- search and seizure of stored computer and also traffic data, and
- real-time collection of traffic data and interception of content data (provided that the general requirements of an interception of telecommunications are fulfilled).

Challenge 6: Law enforcement agencies often find it difficult to keep abreast of the dynamic technical knowhow & tools

Strategy 6: Effective Public private partnership is recommended to circumvent this problem.

A further legal challenge results from the fact that the State is, vis-à-vis the internet, an actor of limited power and capacity so that there is a need of public-private partnerships in fighting cybercrime. The development of modern information and communication technologies has been and is largely controlled by private actors. The internet has been constructed as a private and non-hierarchical global network without specific location and definitely not under state control.

The sheer volume of today's internet communication makes it an impossible task for state authorities with limited resources to "check the web". And "normal" police and prosecution authorities often lack the technological experience and capacity to investigate and prosecute efficiently in a complex data-processing environment. Therefore, criminal justice systems depend on the private sector – the civil society and the economy, in particular the information and communication technology industry and service providers of all kinds — for an efficient investigation and prosecution of cybercrimes. Without active participation of the private sector, it is hardly possible, for example, to detect the whole spectrum of child pornography in the internet and trace it to its distributors and, in the end producers.

State authorities and private companies carry out threat assessments, establish prevention programs and develop technical solutions. On the other hand, it is true that private actors are naturally reluctant to share information, expertise and best practices with state authorities because they want to protect their business models, secrets and also the customer trust. Nevertheless, certain types of voluntary public-private partnerships against cybercrime have been developing during the last years. They include-

- operational cooperation in specific cases,
- blocking of websites containing illegal content such as child pornography or hate speech,
- private self-regulation through codes of conduct,
- sharing of necessary and relevant information across the private and public sector,
- setting up networks of contact points in both the private and the public sector.

An instructive example of a voluntary private-public partnership is the so-called "***Mikado operation***" which took place in Germany in 2006: In 2004, a German TV station had identified a website offering the download of child pornography following payment of 79,99 US-$ through an internet credit card transaction into a specific account. In order to investigate and prosecute persons who downloaded and, consequently, possessed child pornography (which is a criminal offence under German law), a public prosecutor asked 22 German credit card firms to scan all their clients' credit card transactions from 2004 and identify those clients who had transferred 79,99 US-$ into the specific account. The credit card firms cooperated on a voluntary basis, and billions of credit card transactions by millions of credit card holders were checked without their consent. Indeed, 322 persons were identified who had transferred the exact amount into the specific account. The authorities applied for search and seizure orders against these persons, and in fact many of them had downloaded child pornography.

Some of the other initiatives based on public private partnership are -

- A criminal referral by Microsoft lead to the arrest of 8 Bulgarian members of the MBAM Phishing gang for the phishing of a Microsoft billing website
- NCFTA is an alliance between the FBI, US Postal Inspection Service and private industry.
- Digital PhishNet: public-private cooperation to drive enforcement against phishing websites hosted by NCFTA
- Signal-Spam was initiated as a public-private organization to identify spammers for enforcement cases
- London Action Plan, a cooperation between industry and Telecom and Consumer Public Authorities to fight spam
- European Financial Coalition is a cooperation between law enforcement and IT and financial industry to fight child exploitation
- The NHN Corporation of the Republic of Korea has made a donation of $500,000 to the United Nations Office on Drugs and Crime to help establish a Virtual Forum against Cyber-crime. This strengthens the Office's work in this area and is the first time that a private company has granted money to UNODC[22]

[22] http://www.unodc.org/unodc/en/press/releases/2007-12-03.html

Challenge 7: - Institutionalizing the contact points for reporting cybercrimes that affect National sovereignty and public good and safeguard Critical Information Infrastructure of a country is absent or weak in many countries. Statutorily recognized accreditation agencies are also absent in few countries rendering online security at risk.

Strategy 7: Computer Emergency Response team to be strengthened financially technically and by infrastructure to aptly serve as national agency for incident response. Establishing statutorily recognised accreditation agencies, creating certification policies, office of Controller of Certifying authority,and other security measures will be indispensable in securing the online environment.

Statutory authority must be given to institutions responsible to maintain Critical Information Infrastructure security and depute Computer Emergency Response teams empowered to take immediate interception, filtering, blocking and other measures against offending material that endangers national security , integrity of a State, or public good. In many countries such agency is either not statutorily institutionalized or is not well equipped to meet the challenges in cyberspace.

Continued development of national CERTS (Computer Emergency Response Teams) around the world, and their liaison with the international FIRST (Forum of Incident, Response and Security Teams) community is essential to prevent and combat cybercrimes, cyber warfare, damage to critical infrastructure and cyberterrorism. Their activities should include not only information sharing, analysis of case studies and warning roles, but also a response capability operated by ICT security professionals. This will protect against cyber attacks and also improve end-user awareness and responsibilities with respect to safeguarding information, security and privacy. To make these organizations stronger greater financial , manpower and technical resources must be allocated to the CERT to perform its role effectively in combating cybercrimes.

For better security in online environment, establishing statutorily recognised accreditation agencies, creating certification policies, office of Controller of Certifying authority, and creating procedures of information security enhancing measures will also play a vital role.

Challenge 8: The Corporate world is not seriously paying the deserved attention to adopting strong ICT culture and best practices

Strategy 8: At a corporate level, bringing ICT policy into action is important for enhancing information security practices

Different countries have adopted stringent provisions in their cyber legislation to make Corporate entities responsible and accountable for failure to protect data . India inserted Section 43A in the IT Act,2000 whereby any corporate entity that deals in or possesses sensitive personal data or information in a computer resource it owns,controls or operates and is negligent in implementing reasonable security practices that causes wrongful loss or gain to a person , such corporate entity shall be liable to pay damages to the person so affected. The reasonable security practices may be contractually declared, or specified by law or industry standards . At this juncture it is imperative to clearly form the security standards which professional/industry Association can assist in framing or to develop a law that seeks to achieve the 'data security' objective.

Besides framing the best security practices , better enforcement of cyberlaws can be achieved through an internal approach of Integrated Privacy and Security management of information that embodies several components in a cycle of continual vigilance and improvement:

i. Assessments of risks and liabilities in the context of business function,

ii. Top management review of risks and formulation of policy objectives

iii. Design of policy, procedural and technological tools and evaluation of the associated costs,

iv. Top management review and endorsement of mitigation tools and costs,

v. Training commitment at all levels within the organization,

vi. Implementation of tools including test and evaluation of tools

vii Monitoring of compliance and enforcement,

viii Annual reviews and audits,

ix. Adjustments to the security program. Employees must comply with security policies and procedures, and management must take enforcement action taken in instances of violations. Both employee monitoring and audits are important compliance tools.

Challenge 9: *There are heterogeneous laws and no one universal cyberlaw.*

Strategy 9: Unification of Cyberlaw through multilateral treaties and other international initiatives

Solving the problem of transnationality and involvement of multiple jurisdictions involves multilateral treaties, establishing which jurisdiction to apply and defining the ensuing legal procedure. The investigation of cybercrimes and prosecution of cybercriminals and execution of court orders requires efficient international cooperation regime and procedures.

Organization for Economic Co-operation and Development (OECD) first studied the legal issues raised by cybercrime in 1983. Recommendations were made in an attempt to harmonize qualification of the same cybercrimes amongst the varied national legal systems [23]. Later, in 1997, the G8 instigated the creation of a Contact Points Network, meant to become the reference directory for international cooperation actions on cybercrime. Crimes against peace and security in cyberspace should be established as crimes under international law through a Convention or Protocol on the United Nations level.

A Convention or a Protocol on the United Nations level on cybersecurity and cybercrime should be a global proposal for the present times that is based on a potential for consensus. The final draft code may be prepared by the International Law Commission. Mankind will in the future be completely dependent on information and communication technologies. Serious crimes in cyberspace should be established and punishable under international law, whether or not they are punishable under national law.

A combined global initiative on the United Nations level by organizations such as United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU) should be established. This initiative could have as a final goal a Draft Convention that should be submitted to the International Law Commission for considering a United Nations Convention on Peace and Security in Cyberspace. The work which is being done under the aegis of the ICT Task Force of the United Nations to prepare draft

[23] Verdelho, P. The effectiveness of international co-operation against cybercrime: examples of good practice. For the Project on Cybercrime of the Council of Europe, 2008

proposals for a Law of Cyberspace is welcome. Deliberations of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice (Bangkok, 18-25 April 2005)[24], in particular those of its Workshop on Measures to Combat Computer-related Crime and its underlying background paper are important steps in this process.

Further, ITU launched in May 2007 the Global Cybercrime Agenda (GCA) for a framework where the international response to growing challenges to cybersecurity could be coordinated.[25] In order to assist the ITU in developing strategic proposals , a global High-Level Experts Group (HLEG) was established in October 2007. This global experts group of almost 100 persons made a report through its Chairman in August 2008 with recommendations, including on cyber crime legislations. The Global Strategic Report was delivered in November 2008, including strategies in five work areas: Legal measures, Technical and procedural measures, Organizational structures, Capacity building, and International cooperation.

Council of Europe Convention on Cybercrime (2001) is another substantial initiative. The Convention on Cybercrime is an international treaty initially drafted by the Council of Europe (CoE), with the addition of the USA, Canada and Japan; however signature and ratification are by no means limited to member states of the CoE, and are open to all countries. It aims at providing the basis of an effective legal framework for fighting cybercrime, through harmonization of cybercriminal offences qualification amongst the legal systems of member states, Provision for laws empowering law enforcement or/and prosecutors with cybercrime investigation capabilities in each member state and provisions for laws and procedures enabling international cooperation amongst member States during investigation and prosecution of transborder cybercrimes[26].

---

[24] see www.**un.org**/events/11th**congress**/docs/programme.pdf

[25] See http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf

[26] Critics of the Cybercrime Convention are of the view that it is based on criminal cyber activities in the late 1990s. New methods of conducts in cyberspace with criminal intent must be covered by criminal law, such as phishing, botnets, spam, identity theft, crime in virtual worlds, terrorist use of Internet, and massive and coordinated cyber attacks against information infrastrutures. In addition, the terminology included in the Convention is a 1990s terminology, and is not necessarily suitable for the present times

Countries ratifying it must implement the provisions made by the Convention within their local legal system and designate points of contact for the cooperation procedures, so as to initiate them expediently upon request from another member state. India has not so far ratified the Convention and needs to think seriously on this issue . Also, India has not ratified the UN Convention Against Transnational Organized Crime, 2003.The Convention represents a major step forward in the fight against transnational organized crime and signifies the recognition by Member States of the seriousness of the problems posed by it, as well as the need to foster and enhance close international cooperation in order to tackle those problems. In light of these facts, although Section 1(2) read with Section 75 of the IT Act,2000, India assumes prescriptive jurisdiction to try accused for offences committed by any person of any nationality outside India that involves a computer, computer system or network located in India, on the enforcement front, without a duly signed extradition treaty or a multilateral cooperation arrangement, trial of such offences and conviction is a distant dream!

Another method to promote uniform international responses would be to come forward with model prescription by independent cyber experts from across the globe . Such texts could form a positive body of cyberlaw or code of conduct around which multilateral treaty-making could take place. This, in my view, will also assist in closing loopholes and increasing the approximation to a universal legal framework.

Alternatively, a '*self help*' approach would call on States to undertake efforts at updating their cyberlaws suo moto, along legal standards "as stringent" as existing legislation elsewhere. This process would work by emulation. Cyberlaw in this way would increasingly be harmonized. One important criterion for nations would certainly be that their work be compatible with emerging global consensus.

All these methods are not mutually exclusive, but indeed mutually supportive. Irrespective of which forum takes up this exercise of harmonizing cyberlaws the following parameters are extremely essential to bring out effective enforcement of cyberlaws-

(a) *It is important to have a unification in recognizing the offences that qualify as cybercrimes from a global consensus* . The Convention on Cybercrime is one of the strategies that achieves such

harmonization by Art. 2 to 11. These offences are illegal access, illegal interception, data interference (i.e. alteration or destruction of data), system interference (ex: DoS attacks), misuse of devices (production, distribution and use of hacking tools), computer-related forgery, computer-related fraud, child pornography (producing, distributing, procuring, possessing), infringements of copyright 'on a commercial scale', and aiding/abetting thereof.
In addition to the fact that laws of a country may differ from the other in categorization of offences and punishments in respect thereof, many countries may even consider an illegal activity such as Gambling or prostitution as legal and its laws in turn may even protect the same. This creates complications where for instance an activity is legal in one Jurisdiction but has its effect in another jurisdiction where such activity is considered illegal. Harmonizing the substantive laws, to this extent, becomes perplexing and entangles conflict of law principles , principles of sovereign rights and jurisdictional issues.

(b) Without *empowering domestic authorities with cybercrime investigative abilitie*s and international cooperation , enforcing cyberlaws may not be possible .Art. 16 to 21 of the Cybercrime Convention recognizes this fact. These provisions provide for expedited preservation of stored computer data to preserve volatile data such as connection logs at Internet Service Providers), expedited partial disclosure of traffic data (means ISPs have to immediately disclose the fact that the data to be preserved shows that connection is routed to or from another provider), production order (to compel ISPs to give out subscriber information upon request from authorities, most likely based on an IP address), search and seizure of stored computer data, real-time collection of traffic data ('traffic data' has to be understood as connection logs), interception of content data (sniffing at ISP level, provided the latter has the technical capacities to). In conducting cybercrime investigation and prosecution, countries should ensure that their procedural elements include measures that preserve the fundamental rights to privacy and human rights, consistent with their obligations under international human rights law. Preventive measures, investigation, prosecution and trial must be based on the rule of law, and be under judicial control.

•*International Cooperation amongst law enforcement agencies is a prerequisit*e- Since cybercrimes generally involve more than one jurisdiction (for example, a crime may be committed in one jurisdiction and the effect of it is felt in another jurisdiction) law enforcement agencies

need to cooperate internationally during investigation and prosecution of cybercrime cases. This strategy is an intrinsic part of an effective cyberlaw enforcement regime[27]. Art. 23 to 34 of the Cybercrime Convention confers power to a member state to quickly and efficiently request another member state to make use of its investigative abilities as defined above (Art. 16 to 21) for the purpose of a transborder investigation or prosecution. It must be noted that 'dual criminality' (i.e. action considered as a crime in both countries) shall not be required for a request of expedited preservation of stored computer data, while it may be required for accessing

preserved data (pertaining to the aforementioned preservation or not).

• *Designation of a permanent point of contact-*

At the international level, the Convention on Cybercrime provides for the '24/7 Network' by virtue of Art. 35. **I**n an effort to foster cooperation of law enforcement agencies around the world against cybercrime, Interpol has also created a contact point network, currently featuring 111 'National Central Reference Point' (NCRP).CERT is also playing an important role and increases receptivity and accessibility as point of contact for a country to aid investigation of cybercrimes that involve multiple jurisdictions. Both Interpol and the G8 countries offer a 24/7 network. The G8 24/7 network is offered to countries outside member countries, and includes today more than 40 countries.

- *Continuous Striving for removal of pitfalls*

There is truly no utopian strategy for effective enforcement of Cyberlaws. Even Cybercrime Convention which has a reasonably sound legal infrastructure needs constant endeavours to improvise its effectiveness. At the time of writing, 46 countries have signed the Convention, of which 26 countries have ratified it and effectively put it into force . For instance, a country like Romania, although at the edge of cybercrime fighting with about 900 cases processed per year by a specific prosecution service and all provisions fully implemented,

[27] In Art 29,30,31 of the Cybercrime Convention ,International cooperation, for instance, may be refused if: 'the request concerns an offence which the requested party considers a political offence or an offence connected with a political offence,' or 'the requested party considers that execution of the request is likely to prejudice its sovereignty, security,public order or other essential interests.' (Art. 29, 30, 31)

only receives a dozen international requests per year via its 24/7 network contact point (as defined by Art. 35).Estonia has received no queries till date and France from 10 to 20 per year. As a matter of fact, over the 26 countries that ratified the Convention, only four of them have designated a cybercrime-specific unit (whether a police unit or a Dept of Justice service) as the 24/7 network point of contact of Art. 35 (France, Romania, USA, Norway).[28] Hence, better implementation procedures needs to be infused to effectively enforce Cyberlaws .Also, continuous efforts ought to be made for removal of operational and cross border coordination difficulties .

Challenge 10- Creating cyberlaw does not equate with "No cybercrimes "

Strategy 10: Attention to Sociological aspect is recommended as role of a strong political and governance will cannot be undermined.

In *Finance Criminelle* Marie-Christine Dupuis-Danon notes that-

> '*for the sociologist and the criminologist alike, it is not because there is a law against corruption that corruption disappears*'[29]

The same logic could be applied to cybercrime. In simple words, the view that once all the countries have ratified the Convention on Cybercrime or similar treaty, there will be no 'cyber-havens' any more is a myth. To be efficient, ratification and implementation must be connected with a strong political and governance will.

One such factor, largely used by the Financial Action Task Force on Money Laundering (a.k.a. GAFI, by its French acronym) in the domain of money laundering, is pressure from the international community: in 2000 and 2001, the GAFI issued its famous list of 'Non-Cooperative Countries or Territories' (commonly referred to as the GAFI Blacklist)
featuring 23 countries. It has proved to be effective, since at the time of writing all but one of the 23 original blacklisted countries have implemented legal and institutional changes

[28] Verdelho, P. The effectiveness of international co-operation against cybercrime: examples of good practice. For the Project on Cybercrime of the Council of Europe, 2008

[29] Dupuis-Danon, M.-C. Finance Criminelle.

(such as creating Financial Intelligence Units) in order to be de-listed . As a consequence, 21 countries have been cleared off the blacklist, and only eight countries have been added since the initial lists.[30]

On a similar note, the case of Romania may be cited as an example. With a nominal GDP of $7,773 per capita, Romania is listed by the IMF as an emerging country[31]. Yet, as mentioned earlier, with nearly 900 cybercrime cases prosecuted per year, a very extensive legal framework, a cybercrime-specific police unit and a cybercrime-specific prosecution service attached to the High Court of Cassation and Justice, Romania seems to be a leading party in combatting cybercrime. Romania became an 'acceding' country to the European Union in 2004, which is the year it ratified the Convention on Cybercrime. It became an actual member of the EU in 2007. Numerous reforms of the Romanian society stemmed from the will to gain access to the EU[32], and it is not senseless to speculate that addressing the cybercrime issue was one of those, and that amongst other considerations, Romanian officials felt that gaining access to the EU would yield a greater benefit for the local economy than a flourishing cybercrime haven.

POINTS OF CAUTION

Caution 1- Internet Censorship may transgress globally acceptable parameters -

In the urge to effectively enforce Cyberlaws, we will need to understand that internet censorship may lead to politically motivated and moral policing. The technology may be misused for bringing out or shielding/blocking political debate and freedom of opinion, and to reinforce authoritarian or repressive governments.

[30] See http://en.wikipedia.org/wiki/Financial_Action_Task_Force_on_Money_Laundering.

[31] See http://www.imf.org/external/pubs/ft/weo/2009/01/weodata/groups.htm#oem.

[32] See http://en.wikipedia.org/wiki/Accession_of_Romania_to_the_European_Union.

Since 2006, Reporters without Borders has been maintaining a list of countries it calls 'enemies of the Internet'[33] (at the time of writing: Burma, China, Cuba, Egypt, Iran, NorthKorea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan and Vietnam) based on their use of censorship on the Internet. In those countries, censorship is to a great extent used as a means of policing and controlling political opinion, but not only that: pornography , gambling and any other theme that may be considered licentious or threatening to civil order is subject to censorship. The border between protecting moral values and exercising oppressive censorship and mind control is very thin and one can easily transgress the reasonable boundaries of censorship. Such censorship can hinder free flow of information and its availability online. This contravenes or infringes Article 19 of the United Nations' Universal Declaration of Human Rights which explicitly guarantees the freedom to "receive and impart information and ideas through any media and regardless of frontiers".

Caution 2: Internet Surveillance without technical or institutional restraint may infringe one's Right to Privacy

The new Internet filtering techniques allow for unlimited screening and are employed by governments without any technical or institutional restraint. Most prominent has been the OpenNet Initiative (ONI), a collaborative partnership between three leading academic institutions[34]. ONI monitors the development and application of filtering techniques, elaborates country reports and legal analyses[35]. The Yale Center for the Study of Globalization [36]or the watchdog group Reporters Without Borders (Paris) have equally been documenting their concern and raised the problematic nature of the involvement of international technological companies.

---

[33] See http://www.rsf.org/List-of-the-13-Internet-enemies.html.

[34] The initiative is a collaborative partnership between the Citizen Lab at the Munk Centre for International Studies, University of Toronto; the Berkman Center for Internet & Society at Harvard Law School, and the Advanced Network Research Group at the Cambridge Security Programme at the University of Cambridge

[35] In this regard, see also the Berkman Center's study Zittrain and Edelman, *Documentation of Internet Filtering Worldwide* (last update Oct. 2003), http://cyber.law.harvard.edu/filtering

[36]see www.yaleglobal.yale.edu

Another example is that of the '*Technological Trojan*'. The protection of privacy may battle with global surveillance techniques and question its alleged reasonable imposition in cyberspace. The 'Magic Lantern' Trojan horse project, initiated on occurrence of the 9/11 events in the USA is one such case. Public knowledge suggests that it was abandoned – although the FBI uses a 'light' monitoring tool called CIPAV [37]. Back in 2007, the German federal police came up with their own 'Bundestrojaner' (federal trojan) project, but faced mitigation by the Federal Constitutional Court: the latter stated in February 2008 that trojanizing a suspect's computer was 'constitutionally permissible only if actual evidence of a concrete danger' existed, and that it was to be conducted only under judicial authorization (i.e. requiring a warrant) [38].The French government inculcated that judge-control factor in their own law project[39] . Due to the extremely invasive nature of Trojan horses, the ethical issue of privacy protection becomes important in context of increased global surveillance measures, communications surveillance; weakened data protection regimes; increased data sharing; and increased profiling and identification.[40]

There is to date no global consensus on internationally accepted surveillances practices on internet. On a global level, it is advisable to create or initiate an international monitoring or surveillance laws & procedure to clarify internet filtering practices, thus promoting the principles of transparency and accountability that should govern them, and permitting their evaluation against changing international standards.

In addition, one could also explore the possibility of setting up a complaint procedure available to all Internet stakeholders to enable the monitoring and evaluation of Internet censorship Practices.

---

[37] http://en.wikipedia.org/wiki/Cipav.

[38] http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

[39] http://www.interieur.gouv.fr/sections/a_la_une/toute_l_actualite/securite-interieure/loppsi/downloadFile/attachedFile_1/Loppsi_projet_loi.pdf.

[40] *A Starting Point: Legal Implications of Internet filtering* : A publication of Open Net Initiative Sept 2004 at http://opennetinitiative.net/docs/Legal_Implications.pdf

CONCLUSION

Effective Legal enforcement of Cyberlaws requires a multipronged approach. No one strategy by itself is self sufficient or mutually exclusive to create effective enforcement results. To devise a well integrated action plan for cyberlaw enforcement is the need of the hour. It is imperative to spread greater awareness on the subject amongst general public and impart continuous training to the law enforcement personnel and forensic experts. Due measures to establish means and processes of evaluating new ICT developments and products including establishing accreditation agencies, certification policies, CERT, and procedures to enhance information security in the online world require strategic adoption . In addition to specific consumer protection initiatives, the private sector's dedication and support for a secure Internet system is crucial to curbing unlawful conduct on the Internet. The public private participation and increased Corporate accountability and responsibility in maintaining security practices can assist in improved enforcement of cyberlaws. In addition, global initiatives to harmonise cyber laws (in substantive and procedural spirit) will play a vital role in removing existing lacunae by crystallizing the laws of cyberspace.

Participation of International organizations, professional & industry associations, law enforcement agencies, cyberlaw experts and other relevant bodies in creation of multilateral Treaties/Conventions and formulation of Code of Conduct for Cyberspace will assist in evolution of clear principles that will govern the cyberspace. The Interpol will also play a considerable role in coordinating and supplementing investigation and prosecution requests and processes amongst different jurisdictions and contribute towards achieving the goal of effective enforcement of cyberlaws. While we prepare and implement the Strategic Action Plan for cyberlaw enforcement, we will, however, need to ensure that all privacy and internet censorship issues have been properly addressed. To sum up, a sincere & concerted effort in implementing the strategies discussed in this paper can prove useful in accomplishing effective enforcement of cyberlaws .

BIBLIOGRAPHY

Inventory of relevant instruments:

 United Nations Office on Drugs and Crime: www.unodc.org

 International Telecommunication Union (ITU): www.cybersecuritygateway.

org/

 Interpol: www.interpol.int/Public/TechnologyCrime/

 Council of Europe: www.conventions.coe.int

 G8 Group of States: www.g7.utoronto.ca

 European Union: " www.europa.eu

 Asia Pacific Economic Cooperation (APEC): www.apectelwg.org

 Organization of American States: www.oas.org/juridico/english/cyber.htm

 The Commonwealth: www.thecommonwealth.org

 Association of South Asian Nations (ASEAN): www.aseansec.org

 Organization of Economic Cooperation (OECD): www.oecd.org

 The Arab League: www.arableagueonline.org

 The African Union: www.africa-union.org

 NATO: www.nato.int

 Shanghai Cooperation Organization (SCO) www.sectsco.org

Books & Research papers:

1. *Cyber Laws in the Information Technology Age*-By Karnika Seth , Butterworths Lexis Nexis Publications, 2009

2. Verdelho, P, *The effectiveness of international co-operation against cybercrime: examples of good practice*, Project on Cybercrime of the Council of Europe, 2008

3. Berkman Center's study Zittrain and Edelman, *Documentation of Internet Filtering Worldwide* (last update Oct. 2003) at http://cyber.law.harvard.edu/filtering

4. Darrel C Menthe*, 'Jurisdiction in Cyberspace: A Theory of International Spaces'*, Michigan Telecommunications Technology Law Review, vol 4, 1998, p 69

5 *A Starting Point: Legal Implications of Internet filtering* : A publication of Open Net Initiative, Sept 2004

6 *Western Frontier or Feudal Society: Metaphors and Perceptions of Cyberspace* ,Berkley Technology Law Journal, [Vol. 17]

Web- Resources:

1. Legal implications of offering online financial services, By Stephen Revill, Published on July, 2000 ; Bell Gully at http://www.bellgully.com/resources/resource_00254.asp

2. Jurisdiction in Cyberspace: A Theory of International Spaces; By Darell C. Menthe, Published on 4th Michigan Tech. Law Journal (1998) ; www.mttlr.org/volfour/menthe.pdf

3 Law and Borders, *The Rise of Law in Cyberspace* , David G. Post & David R. Johnson, 48 Stanford Law Review 1367 **(**1996) at www.temple.edu/lawschool/dpost/Borders.html

4 Is Google Money-Laundering, by Robin Allenson, Published in Professional Management Blog, (2007) at http://profmgmt.wordpress.com/2007/04/16/is-google-money-laundering/.

5 UNDOC calls for more effective global crime control regime, Published in UNDOC, April 23, 2007.at http://www.unodc.org/unodc/en/press/releases/2007-04-23.html

6 Law Enforcement officers trained to tackle cybercrime, UNDOC webpage, June 19, 2009 at http://www.unodc.org/unodc/en/frontpage/2009/June/law-enforcement-officers-trained-in-tackling-cybercrime.html

7 Golden Shield Project , Wikipedia Web Encyclopedia at http://en.wikipedia.org/wiki/Golden_Shield_Project

8 Green Dam Youth Escorts, Wikipidiea Web Encyclopedia at http://en.wikipedia.org/wiki/Green_Dam_Youth_Escort.

9 Proposed UK piracy legislation suggest tough penalties for ISP's as well as users that download pirated Media, By Asavin Wattanajantra, Feb 12 , 2008 at http://www.itpro.co.uk/165633/users-will-steal-wi-fi - to-bypass-fi le-sharing-crackdown.

10 Eleventh United Nations Congress on Crime Prevention and Criminal Justice, March 3rd , 2005 at

www.**un.org**/events/11th**congress**/docs/programme.pdf

11 A Global Protocol on Cybersecurity and Cybercrime: An Initiative for Peace and security in Cyber Space. , Stein S. & Solange G. Helie' at http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf

12 Financial Action Task Force on Money Laundering , Wikipidiea Web Encyclopedia at http://en.wikipedia.org/wiki/Financial_Action_Task_Force_on_Money_Laundering

13 Documentation of Internet Filtering World Wide, By Jonathan Zittrain and Benjamin Edelman, Berkman Centre for Internet & Society, Harvard Law School , Published on October 28, 2003 at http://cyber.law.harvard.edu/filtering

Legal Citations:

1. *People vs. Lipsitz*, 663 N.Y.S. 2d468 (Sup. Ct. N. Y. Co. 1997)
2. *Zippo Manufacturer v. Zippo Dot Com* 952 F. Supp. 1119 (D.C.W.D. Pa. 1997)
3. *Calder v. Jones* 465 U.S. 783 (1984).
4. *People v. World Interactive Gaming* 714 N.Y.S. 2d 844 (N.Y.Sup. 1999), 1999 N.Y. Misc. LEXIS 425 (S.C. N.Y.1999)
5. *Washington v International Shoe* co 326US310(1945),317

TABLE OF ABBREVIATIONS

Case- Citations:

1. U.S. C.	United States Code
2. N.Y.S.	New York State
3. U.S.	US Supreme Court
4. N.Y. Misc. Reports	New York Miscellaneous

5. D.C. WD Division — United States District Court, Western

Others:

1. CERT — Computer Emergency Research Team
2. COE — Council of Europe
3. EOW — Economic Offences Wing
4. G8 — Group 8 Nations
5. GCA — Global Cybercrime Agenda
6. ICANN — Internet Corporation for Assigned Names and Numbers
7. ISEC — European Commission on Prevention of and Fight Against Crime
8. ISP — Internet Service Providers
9. Interpol — International Criminal Police Organisation
10. ICT — Information and Communication Technology
11. NCFTA — National Cyber Forensics and Training Allaince
12. OECD — Organisation for Economic Co-operation and Development
13. UNODC — United Nations Office on Drugs and Crime
14. UNCITRAL — United Nations Commission on International Trade Law
15. WiFi — Synonym for IEEE 802.11 technology

****