Chapter 11

Necessity of international legal control and cooperation to combat the Cyber crime
Chapter 11

NECESSITY OF INTERNATIONAL LEGAL CONTROL
AND COOPERATION TO COMBAT THE CYBER CRIME

11.1 Introduction

The inevitability for international cooperation in dealing with the transnational criminality and more specifically Cyber crime is overdue. The Cyberspace demonstrates the growing threat of Cyber crime. It involves almost all nations clubbed together with optic fibers by Internet networking. Generally, the debate currently use to be undertaken over the form and scope of such international cooperation, modality in the Cyberspace, and level of compatibility of developed, developing, and underdeveloped nations on scale of technological advancement should rely upon such multilateral, multidimensional effort to enhance Cyber security.

The basis for international cooperation rests, most fundamentally, on the combination of a demonstrable need for international agreement to combat harmful Cyber conduct and the existence of an international consensus on what conduct should be considered criminal. A review of existing statutory law and proposed international arrangements reflects widespread consensus on prosecuting as criminal activity.

While commenting on the need for international instruments, Fausto Pocar comments,

"It is almost banal to remark that crime follows human technological progress: as cyberspace was established as a new medium of communication, criminal activity followed in parallel. In addition, this kind of criminal activity takes advantage[s] of and expands as a result of all the opportunities offered by the Internet, i.e. the evolution of e-commerce, the growth of multinational companies, the ease and speed with which information can be passed around the world, the security and anonymity provided by this technology, and, above all, the territorial dimension of traditional legal approaches."


295
Finally, for organized crime "[t]he spoils (....) are significant and the risk must appear very low and this situation leads to great vulnerability for any member of the international community."

It is necessary that a review of existing statutory law and proposed international arrangements should be made to reflects widespread consensus on prosecuting as criminal, the conduct, and particularly those criminal attacks aimed at disrupting or damaging computer operations, deliberate and unauthorized intrusions, interference with computer-security measures, maliciously altering content, intentionally and materially facilitating the commission of prohibited conduct, using a Cyber system in committing violations of any of several widely adopted antiterrorist conventions, and using a Cyber system to attack critical infrastructures. In preceding chapters the incidences for voluntary international cooperation has already been discussed and analyze how it is being implemented.

The principle element of proposals so advanced in the direction of international cooperation in the area of harmonizing Cyber Laws consists of two basic elements -

i. to educate, prepare and train the enforcement agencies of law

ii. instruct and inform the officials to manage and combat Cyber crime

iii. to create and generate quick emergency response team

iv. to established the Internet Alliance

However, though several efforts has been displayed at international scene to compile the national system in the direction of International common consensus, and no

---


3 See for discussion advanced in Chapter 5 of this research writing specifically with respect to UNCITRAL's 'Model Law' on e-commerce and its impact on the Information Technology Act, 2000.

bout that the various groups recognize that international cooperation is essential, they have yet to accept the idea that an international treaty should be negotiated establishing legally mandated standards and obligations.

11.2 Two approaches: Voluntary support OR Legal Mandate

The international cooperation can be sought by two ways.

i. First by voluntary cooperation of all the concerned entity and another

ii. by way of developing common legal mandate by all member country seeking harmonizing system to combat over the problems arising in Cyberspace.

If examine the first approach to develop international cooperation though voluntary support amongst those dealing in Cyberspace though sound good, pose several arguments. First, as it is discussed in preceding chapters, most of the Cyber crime is conventional crime. Speaking with examples, frauds, drug dealing, defamation, money laundering, sexual exploitation of minors, are merely the crime if happened in Cyberspace, are the crime in which Cyber technology happens to be used (or more precisely misused).

The voluntary support in the area of International cooperation can be seen into the existing treaties and international arrangements, in which either bilateral or multilateral treaties, the member nations has reiterated the on extradition and other legal assistance to member nations. However, the attempt to secure the Cyberspace by international agreement merely on the existing foundation with new versions will again create the difficulties.\(^5\) The reason for this arguments lies in the vast differences exist among different national systems regarding

appropriate regulations, content, the different in criminal procedures, the notion of transnational investigations, and mainly different in the forms of tracking information and messages should be subject to seizure and scrutiny.

At the same time, we cannot ignore the disparity that exists among states in terms of technological advancement, the extent of rights citizens of different nations equipped with, the constitutional objectives of each national laws that would either operate to limit an international agreement, or what is the level of compromise between state and citizens that limit the execution of national and international laws. In addition, till today, Internet as an instrument of mass media still outside the clutches of governmental control, where pre-censorship is still not application in most of the nation.

Under this circumstance, as the Internet that display wide scope for economic growth, trade prosperity, and communication potentiality only because of its control lies in private sector rather than government, the point remain under discussion that how so far the permissible limit for international legal requirement and regulation to encroach upon in the area.

By legal mandate, it is explicitly expected that the international consensus should be develop for a common system in some of the area like Cyber crime, Crime against humanity, War crime, Genocide, where the member country should adopt common system avoiding conflicts with the private international laws. Particularly in the area of these pre-declared priority issues, the preferences should be given to international legal mandate over the national issue.

This sound very powerful because in the era of globalization where the entire globe is reduced to just "village", such legal mandate is very essential. The arguments can also be supported by arguing that the jurisdiction of International Criminal Court should be made compulsory and development of International agency if law enforcement should be developed which will be authorized to combat with such type of criminality and other issues to protect larger interest of world community.

Today, if we analyze the legal response of various countries towards the set of Cyber crimes, we can see the disparities in the treatment given by the different national systems. Most of the countries either fail to response the most of the categories of Cyber crimes. Again the different in the various model of the
treatment by various legal systems also differ. In some of the countries the adversarial model is in existence and on some, either inquisitorial or communist model is present. This make the humanizing legal response to this trans-national criminality is difficult. Following graph may be illustrative in this regard.

**PERCENT OF COUNTRIES WHERE LAW ADDRESSES SUCH CONDUCT**

![Types of criminal conduct in cyberspace](chart.png)

Emerging international consensus on cyber crimes: Results of Global Cyber Law Survey of fifty countries in Africa, the Americas, Asia, Europe, the Middle East, and Oceania.

(Source: Ekaterina Drozdova, prepared for the Conference on International Cooperation to Combat Cyber Crime and Terrorism, December 6-7, 1999, Hoover Institution, Stanford University.)

The existing international norms, agreements are rather mute or quite helpless in dealing with crimes that are directly related to the information infrastructure, including attacks of viruses (such as "I Love You", "Melissa", "Stoned-Marijuana", "The Chernobyl, or PE CIIH" or "The VBS_LOVELETTER viruses"), denial of services attacks, defamatory information pastes by Cyber

---

*Quoted from, Putnam Tonya L. & Elliott David D., 'International Responses to Cyber Crime, Hoover Press : Cyber DP5 HPCYBE0600 06-09-11 18:11:49 rev1 P. 35*
stalkers on the websites registered in foreign country, and other destructive conduct.

Furthermore, the need for an international agreement to deal with Cyber crime rests not merely on the fact that such acts include new types of conduct but also on the need for new methods by which Cyber crime will have to be investigated and prosecuted to provide effective protection. Certainly it would be complicated to secure multilateral agreement on the precise wording of Cyber crime, but that effort need not be undertaken: a broad consensus exists with regard to certain conduct involving the information infrastructure that should be made criminal and a treaty could readily be drafted that describes such conduct and requires all States Parties to make such conduct criminal through any formula they choose to utilize. The differences that exist among states concerning several key issues in developing a treaty must be taken into account and will limit and shape the arrangements that are currently feasible. But differences concerning such issues as regulation of content, scope of extraterritorial investigation, standards of proof, and protection of privacy and other rights can be resolved, largely through a willingness to begin this effort by focusing on measures likely to secure universal agreement. The sharp differences that exist among states with regard to what can be done unilaterally demonstrate, in fact, the need to attempt to secure agreed, multilateral arrangements, rather than establishing a basis for making no effort to do so.\textsuperscript{7} The prohibition on illegal access, for example, would prohibit intentional access to any part of a computer system "without right."\textsuperscript{12} Acts "without right" may include conduct not deliberately undertaken to violate adequately communicated prohibitions on entry.

Such types of issues, which have common focal point for all the nations having related transnational investigation, shared several common questions. The first and most important question in this regard is concerned with Technology. What would be level of technological sharing and measure that are possible on account of international cooperation? Does a common level of technological compatibility will possible?

This seems to be difficult because we have already seen in forgoing chapters that there is vast difference in the pace of technological development

across the globe in developed, developing and underdeveloped nations. Again, what would be the modality of such technological support among the nations what how so far the member nation will go beyond the conventional steps to materialize such cooperation? Such issues are always here while giving a thought for the technological cooperation at international level.

However, this does not mean that the national government should give up the idea of ‘soverign’, but it has to play vital role indeed.

“National governments remain the dominant authority for regulating criminal behavior in most places in the world. One nation already has struggled from, and ultimately proved, its legal authority after a confrontation with the unique challenges presented by cyber crime. It is crucial that other nations profit from this lesson, and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals. In many cases, nations will find that current laws ought to be updated. Enactment of enforceable computer crime laws that also respect the rights of individuals are an essential next step in the battle against this emerging threat.”

These arguments against the creation of an international legal regime to deal with Cyber security are cogent, but they are based on difficulties and dangers that are avoidable. Not only is the case for a multilateral agreement to combat Cyber crime and terrorism strong, the need to undertake the effort of negotiating one is becoming clearer with the increasing costs of such activity. Though it may indeed be true that most crimes in which computers and networks are involved are conventional and potentially covered by international agreements, these are not the crimes against which a new treaty is needed. The notion that the all the national by their own should act unilaterally when necessary to protect its interests is in principle sound.

In addition to the technological dimension there are certain questions of principle concerning the right of States Parties to defend against or to investigate Cyber crime. May a State Party, for instance, deliberately initiate investigative actions or countermeasures for law enforcement purposes that could involve

---

sending transmissions into Cyber systems located in other, sovereign territories? Based on experience to date, fast-spreading computer viruses and other Cyber attacks demand prompt efforts to track down attackers, and it is difficult if not impossible to know in advance all the places to or through which any part of any Cyber transmission might travel.\textsuperscript{10}

The next questions will arise with respect to jurisdiction. If international cooperation and consensus would be anticipated, then the conduct it covers will have effects potentially conferring jurisdiction on multiple States Parties for the same offense. It would provide a set of priorities that Parties would agree to follow in performing their duties and pursuing their rights, to the extent practicable, given the difficulty of anticipating all the possible contingencies. A State Party must establish jurisdiction to try offenders who commit offenses in its territory, who are its nationals, or who are stateless residents in its territory and whose extradition from its territory is refused. A State Party may establish jurisdiction to try offenders who attempt to harm it or its nationals, or to compel it to perform or abstain from performing an act, or whose offenses have substantial effects within its territory.\textsuperscript{11}

The problem of multiple-state jurisdiction over crime is by now commonplace in international law. Transnational fraud, for example, has led to decisions by national courts assuming jurisdiction on the basis of any significant connection to the conduct involved. Among these are the states where a fraud was planned, where an effort to defraud was initiated, where individuals worked at implementing the fraud, where or through which communications were made that were intrinsic to the fraud, where the victims were located, and where the fraud had material and intended effects.\textsuperscript{12}


\textsuperscript{11} However, the COE Draft provides less comprehensive coverage, and fails to provide any guidance with regard to priorities, requiring only "consultation" aimed at determining the "most appropriate" jurisdiction for prosecution.

\textsuperscript{12} Libman v. The Queen [1985] 2 S.C.R. 178, a leading decision of the Canadian Supreme Court providing in-depth description of modern developments with regard to jurisdiction to prosecute conduct involving extraterritorial elements. See also Laurent Belsie, "Cops Narrow Gap on Web Criminals: This Week's Arrest of a Teen Hacker Shows That Law Enforcement Is Getting More Savvy," Christian Science Monitor, April 21, 2000, available at 2000 WL 4427576, reporting on the arrest in Montreal after investigations by the Royal Canadian Mounted Police and the FBI of "Mafiaboy" for allegedly sabotaging the CNN.com website in February 2000.
The widespread recognition of fraud as criminal activity leads states readily to find jurisdiction over such activity, despite the significant relationship particular frauds may have to other states. They tend to assume that punishing fraud will be supported by other affected states, rather than opposed as violating their sovereignty. Cyber crime is quintessentially transnational, and will often involve jurisdictional assertions of multiple states. To avoid the conflict such assertions of jurisdiction could cause, enforcement under the common agreement by all international community on issues that is limited to some agree area like Cyber activities that are universally condemned. Such Draft reflecting International consensus for cooperation may not accede to a state’s jurisdiction merely because someone within its territory is able to access a website in another state; to confer jurisdiction, someone in control of the website must deliberately cause one of the covered crimes, with effects in the state seeking to assert jurisdiction. It seems likely, therefore, that states will in general accept all of the reasonably based jurisdictional claims approved in the Draft.

Furthermore, even before a multilateral treaty is complete, the developed nations like USA or any continental country or even European country may be able to reach less comprehensive arrangements with other states to enhance legal protections. Unilateral conduct that offends other states, and leads them to reject or delay negotiating a desirable treaty, would harm the interest of these develop nation.

Concerns expressed by the private sector over establishing legally mandated norms and obligations stem from the fear that law enforcement considerations will adversely affect (and greatly burden) Internet businesses and freedom of expression. Government control of the information infrastructure could well have detrimental effects, and international regulation could be especially damaging if political objectives and bureaucratic requirements are allowed to interfere with the present, privately dominated Internet regime.

National governments of these developed nations have sought or imposed potentially damaging restrictions on Internet users, including limitations on the use and sale of advanced encryption, demands for the power to intrude upon, hear, and record Internet traffic, and suggestions that private entities assume quasi-
prosecutorial responsibilities in criminal investigations. These policies and suggestions have, however, unjustifiably evoked suspicion of all efforts to establish legally mandated obligations. If, as we believe, voluntary efforts will not provide adequate security, legal obligations to cooperate can be devised that are consistent with continued private creativity and control. An international regime can be fashioned to satisfy the full range of Cyber-security needs, in a manner that ensures continued private-sector control of Internet technology and practices. Most of the developed nations are party to several international regimes encompassing the creation of consensus-based, non-mandatory measures crafted by public and private-sector experts, which a treaty for Cyber security could draw on in providing a comprehensive and lasting system for international cooperation.

The strong case for a legally mandated, international regime has led to several significant developments. Treaty provisions are being proposed to close loopholes in existing multilateral commitments in the specific area of civil aviation. This approach may be feasible in other areas, particularly to protect critical infrastructures from criminal and terrorist attacks, and it seems likely to cause little controversy. The next example can be given that of the Council of Europe (COE), which has taken a more comprehensive approach, publishing and refining a draft treaty on Cyber crime. This proposal includes definitions of Cyber activities that must be made criminal by all States Parties, as well as other features and forms of cooperation. The COE's draft assumes, correctly, that substantial consensus exists with respect to what Cyber activities should be considered criminal, and that substantial benefits can be derived from a multilateral arrangement with common standards, investigative cooperation, and extradition. This chapter seeks to demonstrate the advantages and feasibility of an even more comprehensive regime by proposing a draft international convention (the Stanford Draft) and discussing its principal elements. The Stanford Draft differs from the draft COE Convention on Cyber-crime in several important respects. Most significantly, the Stanford Draft would limit the acts it covers to

---

attacks on the information infrastructure and violations of antiterrorist conventions, whereas the COE Draft includes conventional crimes in which computers are used as well as content-related offenses but do not include violations of antiterrorist conventions. The Stanford Draft also would establish an international agency, modeled along the lines of successful, specialized United Nations agencies, to prepare and promulgate — on the basis of advice from nonpolitical experts — standards and recommended practices (SARPs) to enhance the effectiveness of protective and investigative measures, whereas the COE proposes detailed forms of cooperation without such a process.\textsuperscript{16}

It is necessary therefore, and in order to avoid the conflicting the various national interest of participating nations that a common standard should be agreed upon which recognizes and attempts to deal with the fact that states have different standards in statutes that cover the conduct it proscribes. Instead of attempting to list specific, commonly defined “offenses,” as in most extradition treaties, the proposed Draft would refer to types of conduct, and secures commitments from all States Parties to enforce any applicable law against every form of covered conduct, or to adopt new laws necessary to create authority to prosecute or extradite for such conduct. This approach overcomes the problem of attempting to develop precise, agreed-upon definitions of offenses, and therefore the requirement that every State Party adopt particular formulations as national crimes. In addition to requiring criminal enforcement against conduct specifically aimed at the information infrastructure, the Stanford Draft requires criminal enforcement against the use of computers in the commission of offenses under certain widely adopted multilateral treaties.

These include clearly defined crimes against aircraft, ships, and diplomats, and terrorist bombings. Computers can greatly enhance the potential damage caused by crimes, and can make them especially difficult to investigate. Therefore, since most states are parties to these multilateral treaties, they should be prepared to impose more stringent punishment for the use of Cyber capacities in committing the targeted offenses.\textsuperscript{17} Other widely recognized forms of criminal conduct may also become more aggravated through the use of computers, such as


\textsuperscript{17} For e.g. The COE Draft, No. 24, Rev. 2, does not include such provisions.
forgery, fraud, theft, and conversion. These crimes are not included in the so far as carried out international agreements or conventions, however, since they are in general already encompassed in extradition treaties, to the extent States Parties want such coverage. The Cyber dimension of such activities, moreover, would generally involve conduct covered in the Stanford Draft, irrespective of the crimes such conduct may have facilitated.\(^{18}\) Other types of conduct, when related to the information infrastructure, have been prohibited in some states, including copyright violations and sexual exploitation of minors. Such types of conduct are not covered in the Stanford Draft because their inclusion may prove controversial. These areas are covered by the COE Draft, however, as “Content-related offences.”\(^{19}\) In fact, a sufficient consensus for including some of these offenses, specially the use of computers for sexual exploitation of minors, may exist, and the Stanford Draft’s coverage could be expanded to include such offenses. The COE Draft covers offenses related to child pornography, as well as “copyright and related rights,” but whether the scope of copyright coverage should be coterminal with treaties in the area, such as the Berne Convention and other copyright treaties administered by the World Intellectual Property Organization, is left unsettled, and Parties are explicitly allowed to “reserve the right not to impose criminal liability” for copyright violations, “provided that other effective remedies are available.”\(^{20}\)

Thus there is dire need of developing the common consensus amongst the nations at international level.

### 11.3 The need of model law for developing nations

It is observed that the developing nations, particularly which were under colonial rule has adopted the habit of following the “Model law” pattern from western nations particularly America or England. Most of the legislation in modern days are American ethnocentric and India is not exceptions to it. Generally, as these nations are at the second stage in the developmental race, they

---

\(^{18}\) The definition of forgery, for example, leaves members free to require or dispense with any dishonest intent, and that of fraud requires neither a false representation nor reliance. See “Draft Convention on Cyber-Crime,” Arts. 7 and 8.


want to get benefited by the experiments and experience carried out and gained by these western countries. It is worth to comment,

"[M]ost countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for e-commerce. But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public-private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cyber crime havens." 21

11.4 Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security

It would be misunderstood belief that crime is only concerned for state, particularly in modern age, where crime become so complex phenomenon, it is difficult to remain aloof from it. Therefore, while discussion, about the international harmonisation of Cyberspace at legal as well as social level, it is essential to verify the role that can be assign to various NGOs, firms, civil societies to strengthen the legal framework to make Cyberspace more secure for habitat. The following point worth to noted down.

"To be prosecuted across a border, an act must be a crime in each jurisdiction. Thus, while local legal traditions must be respected, nations must define cyber crimes in a similar manner. An important effort to craft a model approach is underway in the Council of Europe comprising 41 countries. The Council is crafting an international Convention on Cyber Crime. The Convention addresses illegal access, illegal interception, data interference, system interference, computer-related forgery, computer-related fraud, and the aiding and abetting of these crimes. It also addresses investigational matters related to jurisdiction, extradition, the interception of communications, and the production and preservation of data. Finally, it promotes cooperation among law enforcement officials across national borders. Late in its

process, the Council began to consider the views of affected industry and civil society.

This process is making the Council's product more realistic, practical, efficient, balanced, and respectful of due process that protects individual rights. At this point, most observers support provisions to improve law enforcement cooperation across borders. However, industry, through the World Information Technology and Services Alliance\textsuperscript{23} argues that the requirements on service providers to monitor communications and to provide assistance to investigators, as outlined in the Draft Convention, would be unduly burdensome and expensive. Another provision considered objectionable could criminalize the creation and use of intrusive software, or hacking programs, which are designed for legitimate security testing purposes.

This action could stifle the advances in technology vital to keep up with evolving cyber threats. Privacy and human rights advocates\textsuperscript{24} object to the Draft Convention's lack of procedural safeguards and due process to protect the rights of individuals, and to the possibility that the ensuing national laws would effectively place restrictions on privacy, anonymity, and encryption.

The Council plans to release a final draft of the Convention in December 2000. In 2001, a political process involving national governments will determine the scope and coverage of the final Convention. Because of cyber crime's international potential, all countries, and all companies, are affected. Interested parties, including national governments from outside Europe, and businesses and non-governmental organizations from around the world, should participate vigorously in a consensus process to develop measures that support effective international law enforcement and foster continued growth and innovation.\textsuperscript{25}
11.5 Analysis of Cyber laws of various nations

It is essential here to analyze the position of legal response by various nations across the world.  

![Figure 2: Countries with Updated Laws](image)

<table>
<thead>
<tr>
<th>Country</th>
<th>Data Crimes</th>
<th>Network Crimes</th>
<th>Access Crimes</th>
<th>Related Crimes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Access</td>
</tr>
<tr>
<td>Integrity</td>
<td>Interception</td>
<td>Modification</td>
<td>Theft</td>
<td>Unauthorized Access</td>
</tr>
<tr>
<td>Australia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Brazil</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Canada</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Chile</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>China</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Denmark</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Estonia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Finland</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>France</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Germany</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Japan</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Korea</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Malaysia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Netherlands</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>New Zealand</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Philippines</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Poland</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Portugal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Russia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Singapore</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>South Africa</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Spain</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sweden</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Switzerland</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>United States</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Key for Figure 2:
- **Data Integrity**: Interception of data in transmission.
- **Data Modifications**: Alteration, destruction, or erasing of data.
- **Data Theft**: Taking or copying data, regardless of whether it is protected by other laws, e.g., copyright, privacy, etc.
- **Network Integrity**: Impeding or preventing access for others.
- **Unauthorized Access**: Unauthorized access to a computer or network.
- **Computer-Related Forgery**: Alteration or destruction of data or systems.
- **Computer-Related Fraud**: Alteration of data with intent to derive economic benefit from its misrepresentation.

Source: [www.mcconnellinternational.com](http://www.mcconnellinternational.com)

Finally, of the 33 countries with no updated laws in place, 13 indicated that progress toward the adoption of updated legislation to combat cyber crime is underway. Seven of these 13 countries are in Africa or the Middle East, indicating that, although these regions have not yet adequately addressed the issue of cyber crime, many countries are aware that action is needed.

---

Figure 1: Extent of Progress on Updating Cyber Crime Laws

Figure 3: Progress Underway in 13 Countries Without Updated Laws

- Albania
  - The Authority for the Regulation of Telecommunications began discussions earlier this year on the topic of cyber laws, with the aim of preparing protocols of collaboration and exchanging information.

- Cuba*
  - A working group at the Ministry of Justice has planned modifications to the Penal Code.

- Gambia
  - Gambia is planning a national information technology initiative, although the capacity for the drafting up a legal framework is limited. Gambia may look towards international organizations to specify this effort so that it could replicate or amend the needed laws.

- Iran
  - For the past six years, Iran has examined various aspects of cyber law, although no law or regulations in regard to computer offenses have been implemented. The areas that have been considered are: computer offenses, intellectual property issues, privacy, data protection, and freedom of information.

- Kazakhstan
  - State bodies in Kazakhstan are currently developing a law regarding cyber offenses. Also in development is a special state program on the protection of information resources, including technical and software protection.

- Latvia*
  - Amendments to the Criminal Code have been drafted envisaging considerable punishment for computer-related criminal acts. Corresponding additions would be made to the Administrative Offense Code.

- Lebanon
  - Lebanon has established special interest groups to look at the various aspects of information security relating to e-commerce.

- Malta*
  - In May 2000, Malta announced its goal of providing a strong legal framework for e-commerce, data protection, and computer misuses. The relevant Bills to develop a legislative framework for information practices were published in September 2000 and will be discussed in parliament in the coming months.

- Morocco
  - In Morocco, there is an inter-ministerial commission sponsored by the Prime Minister working on security issues.

- New Zealand*
  - At present, there are no general computer crime offenses in New Zealand. However, the country is currently drafting a Crimes Amendment Bill (No. 6).

- Sudan
  - The Sudan intends to invite lawyers, legislators and computer professionals to a workshop where ideas on the nature of computer crimes and the ways of dealing with them by means of appropriate legal codes will be exchanged.

- Vietnam
  - Vietnam is in the process of gathering information to make proposals for amendments to its laws.

- Zambia*
  - Zambia has made available a draft of its Telecommunications and Information Technology Council Act.

*Copies of relevant drafts are available at www.mcconnellinternational.com

Source: www.mcconnellinternational.com

11.6 Conclusion

Thus the common network is being shared by the entire globe and it is warranted that international cooperation should exist. In this circumstance it is necessary that nations should either develop a common infrastructure to deal with Cyber crime or at least develop their own rules having harmonizing legislative construction with legal system of other nations. At the same time there must be procedural cooperation among the nations. The ultimate objective of existence of legal rules in Cyberspace is not to escape the criminals. Criminals should not feel free to commit any sort of crime in the Cyber space. The Computer technology has shown great opportunity. Lack of cooperation in Cyber space may cause substantial damage to common interests. Which may, ultimately, out weight than the return derived from it.

It is true that due to difference in the pace of development, the international cooperation is seems to be difficult, though not impossible, in this sphere at least for the present moment. The reality cannot be ignored that present world is having three differ types of nations. These are Developed, Developing and Under-developed. The harmonized environment in the Cyber space requires upholding the standard of our own national system up to the level of member nations. How can poor underdeveloped nation bear the cost off?

Thus, presently by international treaties, conventions, commissions, the efforts are going on to develop common agenda harmonizing atmosphere to combat Cyber crime. UNCITRAL model law and joint effort of European nations are some of the examples where different corner of the world already initiated the process according to suitability and viability.