A PAPER PRESENTED ON:

CYBER LAWS IN PAKISTAN;

A SITUATIONAL ANALYSIS AND WAY FORWARD

June 24, 2006

Presented by:

Zibber Mohiuddin

President and CEO
ERICSSON PAKISTAN (PVT.) LTD.
# TABLE OF CONTENTS

1 Abstract..................................................................................................................3
2 Background .............................................................................................................4
  2.1 Internet Origin....................................................................................................4
  2.2 The World Wide Web (WWW)............................................................................4
3 Cyber Crime..........................................................................................................6
  3.1 Emergence of Cyber Crime....................................................................................6
  3.2 Disputes in the Cyber World .............................................................................6
  3.3 Cyber Crime v/s Conventional Crime..................................................................6
  3.4 Complexity of Cyber Disputes .........................................................................7
  3.5 Types of Cyber Crime.......................................................................................7
  3.6 Targets of Cyber Crime.....................................................................................8
4 Cyber Law.............................................................................................................10
5 International Aspects of Cyber Law .................................................................11
6 Role of Pakistan in the Cyber World .................................................................17
7 Conclusion...........................................................................................................19
8 Recommendations..............................................................................................20
9 Bibliography ......................................................................................................22
1 Abstract

The revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future. Where originally only some specific sectors of society had rationalized their working procedures with the help of information and communication technology, now hardly any sector of society has remained unaffected. They have changed our society profoundly.

These developments have given rise to unprecedented economic and social changes, but they also have a dark side: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Moreover, the consequences of criminal behavior can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries.

Along with encouraging the use of Information and Communication technologies from their inception, countries have been looking at ways to counteract the negatives simultaneously. Technical measures to protect computer systems are being implemented along with legal measures to prevent and deter criminal behavior.

Pakistan has seen an adequate increase in the use of Information and Communications Technologies over the past half decade. We now have 75,00,000¹ internet users, grown by 5,501.2% from 2000-2005. The technology is currently less penetrated, 4.6%², and yet to compete with international standards.

This paper tends to probe into the networked economy, its impact on society in general and economic wellbeing of states along with the parallel and anticipated downsides. We analyze the increased and far increasing dependency on the networked economy impacting individuals, companies and nations both nationally and globally. The loop holes in the cyber space leading to cyber crimes pressurize countries to look for jurisdictions. A situational analysis of the international aspects of cyber law is carried out to analyze how China, USA, European Union among others have achieved a level of control over cyber activities while trying to minimize the negative impact on their societies.

Finally, the Electronic Transactions Ordinance 2002 and the Electronic Crime Act 2004 as a basis, for the way forward for Pakistan is discussed.

¹ Nielsen//NetRatings, 2005
2 Background

From their modest beginnings some 20 years ago, computer networks have become a critical element of modern society. These networks not only have global reach but they also have impact on virtually every aspect of human endeavor. Networked systems are principal enabling agents in business, industry, government, and defense. Major economic sectors, including defense, energy, transportation, telecommunications, manufacturing, financial services, health care, and education, all depend on a vast array of networks operating on local, national, and global scales.

Internet has changed the very perceptions of mankind. Internet today represents and embodies the single most important development in the history of civilization. On-line culture has become an integral part of modern existence.

2.1 Internet Origin

In 1969 the U.S. government undertook an experiment, today known to people all around the world as the 'Internet'. The purpose of this experiment was to create a way of preserving communications in the event of a nuclear war. Through the collaboration of ARPA (Advanced Research Project Agency) and some academic institutions involved in joint research on defence technologies via interconnected networks ARPANET, the earliest version of the Internet was created.

As time passed the popularity of the Internet grew and what was originally a network of a small handful of computers in the United States was now a growing phenomenon amongst educational establishments and enterprising entrepreneurs who were beginning to see the potential in selling Internet access into people’s homes.

In the 1980’s the UK and Europe realized the potential of the Internet and an academic network called CSNET, which enabled the computer science departments of some universities to be connected, was established.

The CSNET further established the Internet with TCP/IP with the support of the country’s major networking companies.

Even though the Internet clearly existed since the 1980’s it was not until the early 1990’s that the corporate world were able to make use of it instead of just the academic community and government sponsored organizations. This limited use was due to the ‘user unfriendly’ nature of the system, which led to the need for an interface to be designed to make the Internet easier to use. This interface is what is now known as the WWW (World Wide Web).

2.2 The World Wide Web (WWW)

In 1993 a researcher called Tim Berners-Lee with the aim of making the Internet a user-friendly environment introduced the WWW. Designers had the task of designing
and formatting web pages with the use of HTTP (Hypertext Transport Protocol) and HTML (Hypertext Mark-up Language) to link documents together electronically. This new technology enabled a world wide web of information to be provided.

However real usability came shortly after the introduction of the WWW when in 1993 a team led by Marc Anderson at the University of Illinois developed a browser called Mosaic which was a graphical user interface for the Internet to facilitate point and click navigation, more commonly referred to as browsing. N.Bandyopadhyay cites Reid (1997) who states that by July 1996, 150,000 server computers were 'web-enabled'. In 1994, the same team developed Netscape, which is today the most commonly used browser. Netscape was equipped with a search engine to type keywords into and was created using advanced HTTP.

Being able to perform keyword searches was a huge factor in the increased popularity of the Internet. Other browsers such as Internet Explorer by Microsoft soon followed and shortly after that several websites dedicated to producing keyword searches such as Yahoo and Lycos appeared. These are today known more popularly as search engines. The WWW also contributed to providing increased levels of security on the Internet by encrypting the messages that moved between servers. Security on the Internet is today a huge cause of debate.
## 3 Cyber Crime

### 3.1 Emergence of Cyber Crime

The first recorded cyber crime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime!

Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers, cyber crime has assumed rather sinister implications.

### 3.2 Disputes in the Cyber World

Disputes are not new to our existence but disputes relating to on-line transactions and culture are extensively different in their nature, scope and treatment.

The pervasive societal dependence on networks magnifies the consequences of intrusions, accidents, and failures, and amplifies the critical importance of ensuring network survivability. A new network paradigm is emerging. Networks are being used to achieve radical new levels of organizational integration. For example, commercial organizations are integrating operations with business units, suppliers, and customers through large-scale networks that enhance communication and services. This new paradigm represents a shift from bounded networks with central control to unbounded networks.

Thus, the extremely important feature of today's unbounded networks is the emergence of tremendous disputes, differences, fights and controversies on the Internet relating to varied aspects of 'on-lineism'.

### 3.3 Cyber Crime v/s Conventional Crime

CONVENTIONAL CRIME

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into
punishment." The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkin “the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences”.

**CYBER CRIME**

Cyber crime is the most complicated problem in the cyber world. “Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime.” Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.

A generalized definition of cyber crime may be “unlawful acts wherein the computer is either a tool or target or both.” Thus, crimes are unlawful acts wherein the computer is either a tool or a target or both.

### 3.4 Complexity of Cyber Disputes

Cyber disputes are complex in nature due to the following reasons:

- The world itself becomes a big courtroom when cyber crimes across geographic boundaries take place.
- Because of the global nature of the internet, the clarity as to which court would have the exclusive jurisdiction to try the case is missing.
- Thirdly litigation and the legal systems in different countries are different and can be extremely expensive and threaten to wipe out millions of legal entities into oblivion.
- And there is considerable doubt relating to the efficacy of decisions given by the courts of one jurisdiction on a global level and the sanctions are questionable.

### 3.5 Types of Cyber Crime

Let us examine the typical types of cyber crimes:

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial crimes</td>
<td>Cheating, credit card frauds, money laundering etc.</td>
</tr>
<tr>
<td>Cyber pornography</td>
<td>Pornographic websites etc.</td>
</tr>
<tr>
<td>Sale of illegal articles</td>
<td>Sale of narcotics, weapons and wildlife etc., through websites or email communication.</td>
</tr>
<tr>
<td>Online gambling</td>
<td>Online gambling, money laundering etc.</td>
</tr>
<tr>
<td>Intellectual Property crimes</td>
<td>Software piracy, copyright infringement, trademarks violations, theft of computer source code etc.</td>
</tr>
<tr>
<td>Email spoofing</td>
<td>Sending e-mails that appear to originate from one source but actually has been sent from another source.</td>
</tr>
</tbody>
</table>

---

6 Granville Williams  
7 Proprietary Articles Trade Association v. A.G. for Canada (1932)  
8 Author of CYBER CRIME by Parthasarathi Pati (naavi.org)  
9 Duggal Pawan  
10 Nagpal R. – What is Cyber Crime?
<table>
<thead>
<tr>
<th>Forgery</th>
<th>Counterfeit currency notes, postage and revenue stamps, mark sheets etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Defamation</td>
<td>Publishing/distributing defamatory matter about someone.</td>
</tr>
<tr>
<td>Cyber stalking</td>
<td>Victimizing someone online.</td>
</tr>
<tr>
<td><strong>Unauthorized access to computer systems or networks</strong></td>
<td>Hacking.</td>
</tr>
<tr>
<td><strong>Theft of information contained in electronic form</strong></td>
<td>Stealing information on computer hard disks, removable storage media etc.</td>
</tr>
<tr>
<td>Email bombing</td>
<td>Sending a large number of emails crashing email accounts or servers.</td>
</tr>
<tr>
<td>Data diddling</td>
<td>Altering data.</td>
</tr>
<tr>
<td>Salami attacks</td>
<td>Commissioning financial crimes.</td>
</tr>
<tr>
<td><strong>Denial of Service attack</strong></td>
<td>Flooding systems by sending excessive demands etc.</td>
</tr>
<tr>
<td>Virus / worm attacks</td>
<td>Spread of viruses and worms.</td>
</tr>
<tr>
<td>Logic bombs</td>
<td>Triggering programs at events.</td>
</tr>
<tr>
<td>Trojan attacks</td>
<td>Unauthorized programs.</td>
</tr>
<tr>
<td>Internet time theft</td>
<td>Stealing internet hours.</td>
</tr>
<tr>
<td>Web jacking</td>
<td>Stealing control over websites.</td>
</tr>
<tr>
<td><strong>Theft /damaging of computer system</strong></td>
<td>Theft of a computer, peripherals etc.</td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td>The cyber crime of “gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network”¹¹ known as access has the greatest impact Packet sniffing, tempest attack, password cracking and buffer overflow etc. are some techniques for gaining access.</td>
</tr>
</tbody>
</table>

### 3.6 Targets of Cyber Crime

Cyber crimes are targeted and have an impact at three levels: Individuals, Organizations, Society at large. Examples of crimes targeted at the three levels mentioned is as follows:

<table>
<thead>
<tr>
<th>Against Individual Property</th>
<th>Against Organization</th>
<th>Against Society at large</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. Computer vandalism</td>
<td>i. Unauthorized</td>
<td>i. Pornography (basically child pornography)</td>
</tr>
<tr>
<td>ii. Transmitting virus</td>
<td>control/access over</td>
<td>ii. Polluting the youth through indecent exposure</td>
</tr>
<tr>
<td>iii. Unauthorized control/access over</td>
<td>computer system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ii. Possession of</td>
<td></td>
</tr>
</tbody>
</table>

¹¹ Section 2(1)(a) of the US Information Technology Act
¹² Author of CYBER CRIME by Parthasarathi Pati (naavi.org)
<table>
<thead>
<tr>
<th>Computer system crimes</th>
<th>Unauthorized information crimes</th>
<th>Other crimes</th>
</tr>
</thead>
<tbody>
<tr>
<td>v. Internet time thefts</td>
<td>iv. Distribution of pirated software etc.</td>
<td>v. Sale of illegal articles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vi. Online gambling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vii. Forgery</td>
</tr>
</tbody>
</table>
4 Cyber Law

In an increasing networked economy, safeguarding cyberspace as well as Information and Communication Technology systems (ICTs) and infrastructure have taken on real urgency. It is essential to instill confidence in online trade, commerce, banking, telemedicine, e-governance and host of other applications. It is also critical for the future social and economic development of the world, said ITU secretary general Yoshio Utsumi\textsuperscript{13}.

Achieving cyber-security depends upon the security practices of each and every networked country, business and citizen.

To guard against the sophisticated skills of cyber-criminals, a global culture of cyber-security needs to be developed. This will require not only good policing and legislation but also acute threat awareness and development of tough ICT-based counter measures.

Cyber law is the intersection of technology and law. Controversy exists in that one school of thought thinks that the technology should not (or can not) be regulated.

Cyber law encompasses a wide variety of political and legal issues related to the Internet and other communications technology, including intellectual property, privacy, freedom of expression, and jurisdiction.

Cyber law has been a vibrant field in which numerous developments took place in the year 2001 on the global level. Cyber law tends to addresses a more definitive, regulated and orderly cyberspace and towards evolving the regulated code of conduct for online activities in the context of electronic mediums around it.

\textsuperscript{13} ITU secretary general Yoshio Utsumi International Telecom Union (ITU) 141st Anniversary 2006
5 International Aspects of Cyber Law

Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. This causes difficulty, as the internet-based society has no physical boundaries and thus much traffic escapes national supremacy. Criminals are increasingly located in places other than where their acts produce their effects.

Over the past thirty years, developed nations’ transit from the industrial era to the new information age has enabled them to develop the nascent technology and produce ever greater quality in standards and value. Between 2000 and 2005, the average internet user growth rate was of 183.4%, the highest rate being in the Middle East with 454.2%. Not far behind was Africa with 423.9% and Latin America and the Caribbean collectively with 342.5%14. It is clear from these statistics that these regions, in which most developing countries subsist, are eager to implement and exploit the advantages of ICTs and the internet superhighway.

<table>
<thead>
<tr>
<th>World Regions</th>
<th>Population (2006 Est.)</th>
<th>Population % of World</th>
<th>Internet Usage, Latest Data</th>
<th>% Population (Penetration)</th>
<th>Usage % of World</th>
<th>Usage Growth 2000-2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>915,210,928</td>
<td>14.1 %</td>
<td>23,649,000</td>
<td>2.6 %</td>
<td>2.3 %</td>
<td>423.9 %</td>
</tr>
<tr>
<td>Asia</td>
<td>3,667,774,066</td>
<td>56.4 %</td>
<td>364,270,713</td>
<td>9.9 %</td>
<td>35.6 %</td>
<td>218.7 %</td>
</tr>
<tr>
<td>Europe</td>
<td>807,289,020</td>
<td>12.4 %</td>
<td>291,600,898</td>
<td>36.1 %</td>
<td>28.5 %</td>
<td>177.5 %</td>
</tr>
<tr>
<td>Middle East</td>
<td>190,084,161</td>
<td>2.9 %</td>
<td>18,203,500</td>
<td>9.6 %</td>
<td>1.8 %</td>
<td>454.2 %</td>
</tr>
<tr>
<td>North America</td>
<td>331,473,276</td>
<td>5.1 %</td>
<td>227,303,680</td>
<td>68.6 %</td>
<td>22.2 %</td>
<td>110.3 %</td>
</tr>
<tr>
<td>Latin America/Caribbean</td>
<td>553,908,632</td>
<td>8.5 %</td>
<td>79,962,809</td>
<td>14.4 %</td>
<td>7.8 %</td>
<td>342.5 %</td>
</tr>
<tr>
<td>Oceania / Australia</td>
<td>33,956,977</td>
<td>0.5 %</td>
<td>17,872,707</td>
<td>52.6 %</td>
<td>1.7 %</td>
<td>134.6 %</td>
</tr>
<tr>
<td><strong>WORLD TOTAL</strong></td>
<td><strong>6,499,697,060</strong></td>
<td><strong>100.0 %</strong></td>
<td><strong>1,022,863,307</strong></td>
<td><strong>15.7 %</strong></td>
<td><strong>100.0 %</strong></td>
<td><strong>183.4 %</strong></td>
</tr>
</tbody>
</table>

As developing countries are jumping onto the bandwagon, penetration of Internet and awareness is on an overall low level. Different National Governments in Asia have yet to galvanize themselves into action vis a vis Internet and cyberspace. The future holds tremendous promise for Asia and Asian countries have to respond to the same with lightening speed. The problem is nonetheless that many have neither the expertise nor the experience to deal with the legal and policy issues necessary.


15 NOTES: (1) Internet Usage and World Population Statistics were updated for March 31, 2006. (2) CLICK on each world region for detailed regional information. (3) Demographic (Population) numbers are based on data contained in the world-gazetteer website. (4) Internet usage information comes from data published by Nielsen//NetRatings, by the International Telecommunications Union, by local NICs, and other other reliable sources. (5) For definitions, disclaimer, and navigation help, see the Site Surfing Guide. (6) Information from this site may be cited, giving due credit and establishing an active link back to www.internetworldstats.com. ©Copyright 2006, Miniwatts Marketing Group. All rights reserved.
INTERNET USERS AND POPULATION STATISTICS FOR ASIA\textsuperscript{16}

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Only</td>
<td>3,667,774,066</td>
<td>56.4 %</td>
<td>364,270,713</td>
<td>9.9 %</td>
<td>35.8 %</td>
<td>218.7 %</td>
</tr>
<tr>
<td>Rest of the World</td>
<td>2,831,922,994</td>
<td>43.6 %</td>
<td>653,786,676</td>
<td>23.1 %</td>
<td>64.2 %</td>
<td>165.0 %</td>
</tr>
<tr>
<td>WORLD TOTAL</td>
<td>6,499,697,060</td>
<td>100.0 %</td>
<td>1,018,057,389</td>
<td>15.7 %</td>
<td>100.0 %</td>
<td>182.0 %</td>
</tr>
</tbody>
</table>

International Telecommunications Union has helped certain developing countries to become actively involved in the deployment and use of services aimed at building security and trust, thereby extending the benefits of ICTs beyond commercial to societal applications such as government and health.

ITU-D (Development Bureau) has been mandated to:\textsuperscript{17}
- Enhance security and build confidence in the use of public networks for e-services/applications.
- Provide assistance to Member States in developing laws and model legislation for e-services/applications, prevention of cyber crime, security, ethical issues and data privacy.
- Identify security requirements and propose solutions for the development of secure IP infrastructure for e-services/applications on various types of networks using relevant technologies.
- Develop tools to facilitate the exchange of best practices on IT security, legal issues related to the areas of activity of this Programme.

The European Union, on the other hand, has enabled harmonized implementation of regulation on electronic commerce through directives in almost all European countries, with non-member countries aligning themselves with the EU movement. Similarly, the US has both important knowledge and experience in the legal field of cyber security, with significant influence in the area.

The U.S has a very well defined structure for reporting crimes. The primary federal law enforcement agencies that investigate domestic crime on the Internet include: the

\textsuperscript{16} Internet Usage Statistics
\textsuperscript{17} ITU-D: E-Strategies Unit website, www.itu.int/ITU-D/e-strategy/
Federal Bureau of Investigation (FBI), the United States Secret Service, the United States Immigration and Customs Enforcement (ICE), the United States Postal Inspection Service, and the Bureau of Alcohol, Tobacco and Firearms (ATF). Each of these agencies has offices conveniently located in every state to which crimes may be reported. Contact information regarding these local offices may be found in local telephone directories. In general, federal crime may be reported to the local office of an appropriate law enforcement agency by a telephone call and by requesting the "Duty Complaint Agent."

Each law enforcement agency also has a headquarters (HQ) in Washington, D.C., which has agents who specialize in particular areas. For example, the FBI and the U.S. Secret Service both have headquarters-based specialists in computer intrusion (i.e., computer hacker) cases.

Following federal investigative law enforcement agencies are responsible for reporting of crimes:

<table>
<thead>
<tr>
<th>Type of Crime</th>
<th>Appropriate federal investigative law enforcement agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer intrusion (i.e., hacking)</td>
<td>• FBI local office&lt;br&gt;• U.S. Secret Service&lt;br&gt;• Internet Fraud Complaint Center</td>
</tr>
<tr>
<td>Password trafficking</td>
<td>• FBI local office&lt;br&gt;• U.S. Secret Service&lt;br&gt;• Internet Fraud Complaint Center</td>
</tr>
<tr>
<td>Copyright (software, movie, sound recording) piracy</td>
<td>• FBI local office&lt;br&gt;• If imported, U.S. Immigration and Customs Enforcement&lt;br&gt;• Internet Fraud Complaint Center</td>
</tr>
<tr>
<td>Theft of trade secrets</td>
<td>• FBI local office&lt;br&gt;• If imported, U.S. Immigration and Customs Enforcement&lt;br&gt;• Internet Fraud Complaint Center</td>
</tr>
<tr>
<td>Trademark counterfeiting</td>
<td>• FBI local office&lt;br&gt;• If imported, U.S. Immigration and Customs Enforcement&lt;br&gt;• Internet Fraud Complaint Center</td>
</tr>
<tr>
<td>Counterfeiting of currency</td>
<td>• U.S. Secret Service&lt;br&gt;• If imported, U.S. Immigration and Customs Enforcement&lt;br&gt;• Internet Fraud Complaint Center</td>
</tr>
<tr>
<td>Child Pornography or Exploitation</td>
<td>• FBI local office&lt;br&gt;• If imported, U.S. Immigration and Customs Enforcement&lt;br&gt;• Internet Fraud Complaint Center</td>
</tr>
<tr>
<td>Child Exploitation and Internet Fraud matters that have a mail nexus</td>
<td>• U.S. Postal Inspection Service&lt;br&gt;• Internet Fraud Complaint Center</td>
</tr>
<tr>
<td>Internet fraud and SPAM</td>
<td>• FBI local office&lt;br&gt;• U.S. Secret Service (Financial Crimes)</td>
</tr>
</tbody>
</table>
The US Internet Crime Complaint Center (IC3): The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). IC3’s mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

Other US Government Initiatives to Combat Cyber crime:

- Department of Homeland Security’s National Infrastructure Coordinating Center: (202) 282-9201 (report incidents relating to national security and infrastructure issues).
- U.S. Computer Emergency Readiness Team (U.S. CERT) (online reporting for technicians)
- Internet Fraud Complaint Center (IFCC) (online reporting for Internet related crime).
- National Association of Attorney General’s Computer Crime Point of Contact List (all state related cyber questions).
- Digital Millennium Copyright Act - the epidemic law that outlaws not only software piracy but also the activities that help it.
- Online Copyright Infringement Liability Limitation Act technically a part of the DMCA but distinct from it.
- Uniform Computer Information Transactions Act
- Can Spam Act of 2003
- Proposed EU Directive on the patentability of computer-implemented inventions

Most domestic laws for the developed countries are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments.

Shenzhen, China and Saudi Arabia are two more examples of nations that have achieved high degrees of success in regulating their citizens’ access to the internet.
China boasts of 111 million internet users, the world's second largest number after the United States. But the lack of police supervision has caused rampant spread of pornographic information, slanders and gambling on the Internet.

China's booming special economic zone of Shenzhen is leading the way in curbing online crimes and the spread of hazardous information with the use of cyber police. Shenzhen has about 4 million users and more than 5,000 major websites, 400 of which support cyber forums and chat rooms. With rapid website development, online crimes, such as on-line stealing, cheating and gambling, have become rampant.

The local police authorities said that since the cyber police appeared this year, the amount of hazardous information at the city's major portal websites have reduced by 60 percent.18

Since January, cyber policeman and cyber policewoman have performed their duties at major portal websites. Both have cartoon icons on Internet.

Cyber police in China have been at work in three areas:
- Firstly, the police folks patrol areas where crimes frequently occur to warn cyber criminals.
- Secondly, users can find, by clicking on icons of police folk, information on rules and regulations of cyber space management and typical online criminal cases. In a few months, the police icons have received an accumulated 100,000 clicks, provided more than 600 legal consultations and received more than 1,600 reports on online crimes, 235 of which have been proved effective.
- The virtual reality cops are also responsible for receiving online crime reports from users and providing legal consultations concerning cyber crimes.

Considering the success of the cyber space in Shenzhen, the Ministry of Public Security in early May decided to establish cyber police in another eight major cities.

For developing countries to trade with the developed ones, they must ensure that their national legislation ensures the same level of protection granted by other countries regarding storage and processing of personal data. This is imperative if these countries want to trade with European Union countries, which have very strong data protection laws.

Following are the stronger International Fora for Cyber Crime:

Two treaties, negotiated under the auspices of the World Intellectual Property Organization (WIPO), the Copyright Treaty of 1996 and the Phonograms and Performers Treaty of 1996 attempt to interpret traditional rules of copyright in the new internet environment. These are implemented in the US, the European Union (EU), Canada and other countries.

The Council of Europe Convention on Cyber Crime in 2001 was the first international initiative on computer crime. It has been signed by 37 States and entered into force in July 2004. This Convention helps to foster international

18 Xinhua News Agency 2006.
cooperation by criminalizing the basic cyber crimes. The ideal is that all signatory states have the same legislative foundation, regardless of further domestic laws in this area, which will enable prosecution of crimes committed in one country but which have an effect on several different countries.19

The UN Guidelines concerning computerized personal data files list a few principles for the elaboration of legislation in States. Initiatives are, however, left to the States regarding implementation of such legislation.

The United Nations Resolutions 55/63 and 56/121 on Combating the Criminal Misuse of Information Technology tried to address the problem of safe havens for those who criminally misuse information technology by requesting that States put into place laws to eliminate such havens. Two further Resolutions were adopted, Resolutions 57/239 and 58/199 on the Creation of a Global Culture of Security and the Protection of Criminal Information Infrastructure.

The US Department of Justice is working with foreign governments through many channels to address global threats related to computer crime.

**OECD-APEC Global Forum: Policy Frameworks for the Digital Economy**

The Organization for Economic Cooperation and Development (OECD) announced on August 7, 2002 the completion of "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security." These guidelines, which replace the original guidelines published in 1992, provide a set of principles to help ensure the security of today's interconnected communications systems and networks.

---

6 Role of Pakistan in the Cyber World

The Pakistan market has now grown manifolds with the largest majority of internet users in Karachi and then Lahore and Islamabad. These three cities jointly provide over 90% of the customer base and expansion in activity is also likely to remain primarily confined to these cities because of the concentration of economic activity in these cities.²⁰

It is no surprise that Pakistan is not free from the cyber space dilemma. The availability of computers and Internet connections provides unprecedented opportunities to communicate and learn in Pakistan. However, certain individuals do exploit the power of the Internet for criminal purposes as well.

Pakistan has a legal framework in place to address cyber crimes. The Electronic Transaction Ordinance 2002 was passed by Pakistan Government with the objective to recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers. With this legal framework we do have legal backing for electronic information and communication, as any written and signed document. With ETO in place, Pakistan has joined an exclusive band of countries that provide necessary framework and an impetus for growth of electronic commerce in Pakistan.

The Electronic Transaction Ordinance is an essential prerequisite for e-commerce growth and termed as "a landmark decision for the IT development of the country"²¹.

The Ordinance aimed to achieve:
- Great economic impact.
- E-commerce and projecting Pakistan’s products such as textile, leather goods, sports goods and surgical items to the world.
- Increased e-transactions.
- Major benefits for the small and medium business enterprises as the cost of transactions are greatly reduced electronically.
- Legal and safe trading to take place as the necessary laws to protect the interests of both the buyers and the sellers in the process of electronic sales and purchases are protected through the promulgation of the Electronic Transaction Ordinance 2002.

The Federal Government, by notification in the official Gazette, makes rules to carry out the Purposes of the Ordinance.

The ordinance has laid down clauses for the following offenses related to electronic transactions:

- Provision of false information

²⁰ Internet Service Providers Association of Pakistan (ISPAK)
²¹ Electronic Transaction Ordinance to help e-commerce growth- The News, 13/7/2002
- Issue of false certificate
- Damage to information system

Furthermore, the **Electronic Crime Act 2004** was prepared by the Ministry of Information Technology, Pakistan with the Electronic Transaction Ordinance 2002 as the basis.

The Act addresses and lays down legislative terms for the following cyber crimes:

- Criminal access
- Criminal data access
- Data damage
- System damage
- Electronic fraud
- Electronic forgery
- Misuse of devices
- Misuse of encryption
- Malicious code
- Cyber stalking
- Spamming
- Spoofing
- Unauthorized interception
- Cyber Terrorism
- Waging cyber war
- Enhanced punishment for offences involving sensitive electronic systems
- Attempt and aiding or abetting

Other initiatives taken by GoP include the formation of a **National Response Center** to stop internet misuse and trace those involved in cyber crimes. The **Accreditation Council**, in line with the National IT Policy and the Electronic Transactions Ordinance 2002, was also formed for Certificate Authorities by the Ministry of Information Technology. This voluntary licensing program aims at promoting high integrity licensed CAs that can be trusted. A CA wishing to get licensed will have to meet stringent licensing criteria in various aspects, including financial soundness, personnel integrity, strict security controls and procedures.


7 Conclusion

It is not possible to eliminate cyber crime from the cyber space in its entirety. However, it is quite possible to check it. Any legislation in its entirety might be less successful in totally eliminating crime from the globe. The primary step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime.

Developing nations must learn from the experiences of developed nations and leap forward to prepare against the inevitable cyber crime. In order to strengthen the overall infrastructure, efforts by each country must be made at an international level to cooperate and coordinate with each other so as to come to harmonized terms on matters regarding security. In this regards, international instruments such as the Council of Europe’s Convention on Cyber Crime 2001, could prove extremely valuable in fighting cyber crime at an international level.

However, in any draft legislation it is important that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive.
8 Recommendations

Cyber crime is a global phenomenon and therefore the initiative to fight it should come from the same level. The need of the hour is a worldwide uniform cyber law to combat cyber crime.

Following is the proposed way forward and recommendations to equip the country to counteract cyber crimes at the national and global levels.

i. Fostering Linkages
- Creating liaison with the international community will further create sharing of experiences and good practices in the field of information security and network security and encourage their use by all parties concerned.

- Given the cross-border nature of information and communication technologies, a concerted international effort is needed to deal with misuse. A binding international instrument can ensure the necessary efficiency in the fight against these new phenomena. In addition to measures of international co-operation, such a framework should also address questions of substantive and procedural law, as well as matters that are closely connected with the use of information and communication technologies.

- The value of fostering co-operation internationally with other countries/regions and parties needs to be enhanced. This includes fostering international cooperation in the areas of internet, information technology, e-business, e-commerce, and cyber crime. Liaison with national governments, local, national and international bodies, organizations and other groups in order to demand immediate and necessary national legislations is vital.

- Co-operation between governments and the private sector in combating cyber crime and the need to protect legitimate interests in the use and development of information and communication technologies is essential.

- Furthermore, strengthening of the trust and security of the governing framework among nationals is essential to enhance usage. Encouraging development of secure and reliable applications to facilitate online transactions will also generate trust in the systems. Define processes for all cyber crimes, including illegal access, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringements of copyright and related rights, which would contribute to the overall trust and security process.

ii. Building National level Partnerships and Creating Awareness
- Create specialized forums for exchange of experiences and information which would entail initiating and promoting literary, technical and scientific activity; research; education; and training pertaining to cyber laws. These activities should be catered to law enforcement agencies, government departments, bar associations, judiciary, institutes, universities, corporations and other private organizations.
- Setting up a cyber crime cell consisting of experts to deal with cyber-crime will encourage reporting and evolve into a process inline with the legislature. These cyber crime cells should be constituted in all metropolitan and other important cities.

**iii. Training and Awareness Raising**

- It is essential to educate and empower youth to safely and responsibly take control of their Internet experience.

- Disseminate general awareness of cyber crimes and user laws/rights by arranging symposia, seminars, lectures, classes, demonstrations, presentations, briefings, to educate the society and gain their comfort level.

- Creating awareness of the Electronic Transaction Ordinance 2000 and Electronic Crime Act 2004 of 2000 among the target groups will prove successful and inform the concerned about their rights. People need to be aware of the appropriate law enforcement investigative authorities at the local, state, federal, or international levels.

- Introducing Cyber Crimes awareness in schools and adding it to curriculum will create the required awareness amongst the youth.

- Disseminate information for consumers and businesses on computer security and safeguarding personal information. Along with this contact numbers of authorities, the process etc. should be explicitly stated.
9 Bibliography


Trademarks, domain names and patents, by M. Viljoen, G.M. du Plessis, G. Vivier Beng, Partners at Adams and Adams, Pretoria.

Cyberlaw India: To Link or Not to Link-The Judicial View by Shri Pavan Duggal, Cyberlaw Consultant, President Cyberlaws.net, MAC, ICANN http://www.cyberlaws.net/cyberindia/linking.html.

www.virtulaw.com/e-law.htm, Virtulaw, L.L.C. Copyright © 1999 Virtulaw, L.L.C. All rights reserved. Revised: June 04, 1999.


Electronic Communications Act 2000 (ECA).

Electronic Signatures Regulations 2002 (ESR).

Electronic Signatures in Global and National Commerce Act 2000 (E-Sign Act).


Nagpal R. – What is Cyber Crime?.

Nagpal R- Defining Cyber Terrorism.

Duggal Pawan – The Internet: Legal Dimensions.

Kumar Vinod – Winning the Battle against Cyber Crime.
China focus: China's cyber police curbs online crimes: Xinhua News Agency 2006.

Computer-related crime, Report by the European Committee on Crime Problems.

Code and Other Laws of Cyberspace, The Future of Ideas, and Free Culture by Lawrence Lessig.


Cyberlaw for Non-Lawyers - an archive of articles on cyberlaw compiled by the Electronic Frontier Foundation.

Law And Borders-The Rise of Law in Cyberspace.

Electronic Transaction Ordinance to help e-commerce growth- The News, 13/7/2002


http://www.pakcon.org

http://www.cnn.com

http://www.isbpak.com

Nielsen//NetRatings Dec/2005

International Telecommunications Union 2005- http://www.itu.int

Internet World Stats http://www.internetworldstats.com/stats3.htm#asia

Internet Service Providers Association of Pakistan (ISPAK)http://www.ispak.com.pk

Asian School of Cyber Laws Resources http://www.asianlaws.org/cyberlaw/library.htm

Proprietary Articles Trade Association v. A.G.for Canada (1932)

Author of CYBER CRIME by Parthasarathi Pati (naavi.org)

Nagpal R. – What is Cyber Crime?

Computer Misuse and the Criminal Law, www.cosgrave.com/courses/ProfIssues/Computermisuseandthecriminallaw.html

## Appendix 1  ASIA INTERNET USAGE AND POPULATION

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Afganistan</td>
<td>26,508,694</td>
<td>-</td>
<td>25,000</td>
<td>0.1 %</td>
<td>0.0 %</td>
<td>n/a %</td>
</tr>
<tr>
<td>Armenia</td>
<td>2,967,116</td>
<td>30,000</td>
<td>150,000</td>
<td>5.1 %</td>
<td>0.0 %</td>
<td>400.0 %</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>8,388,479</td>
<td>12,000</td>
<td>408,000</td>
<td>4.9 %</td>
<td>0.1 %</td>
<td>3,300.0 %</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>136,138,461</td>
<td>100,000</td>
<td>300,000</td>
<td>0.2 %</td>
<td>0.1 %</td>
<td>200.0 %</td>
</tr>
<tr>
<td>Bhutan</td>
<td>796,314</td>
<td>500</td>
<td>20,000</td>
<td>2.5 %</td>
<td>0.0 %</td>
<td>3,900.0 %</td>
</tr>
<tr>
<td>Brunei Darussalem</td>
<td>393,568</td>
<td>30,000</td>
<td>56,000</td>
<td>14.2 %</td>
<td>0.0 %</td>
<td>86.7 %</td>
</tr>
<tr>
<td>Cambodia</td>
<td>15,017,110</td>
<td>6,000</td>
<td>41,000</td>
<td>0.3 %</td>
<td>0.0 %</td>
<td>583.3 %</td>
</tr>
<tr>
<td>China</td>
<td>1,306,724,067</td>
<td>22,500,000</td>
<td>111,000,000</td>
<td>8.5 %</td>
<td>30.5 %</td>
<td>393.3 %</td>
</tr>
<tr>
<td>East Timor</td>
<td>947,401</td>
<td>-</td>
<td>1,000</td>
<td>0.1 %</td>
<td>0.0 %</td>
<td>0.0 %</td>
</tr>
<tr>
<td>Georgia</td>
<td>4,435,046</td>
<td>20,000</td>
<td>175,600</td>
<td>4.0 %</td>
<td>0.0 %</td>
<td>778.0 %</td>
</tr>
<tr>
<td>Hong Kong *</td>
<td>7,054,867</td>
<td>2,283,000</td>
<td>4,878,713</td>
<td>69.2 %</td>
<td>1.3 %</td>
<td>113.7 %</td>
</tr>
<tr>
<td>India</td>
<td>1,112,225,812</td>
<td>5,000,000</td>
<td>50,600,000</td>
<td>4.5 %</td>
<td>13.9 %</td>
<td>912.0 %</td>
</tr>
<tr>
<td>Indonesia</td>
<td>221,900,701</td>
<td>2,000,000</td>
<td>18,000,000</td>
<td>8.1 %</td>
<td>4.9 %</td>
<td>800.0 %</td>
</tr>
<tr>
<td>Japan</td>
<td>128,389,000</td>
<td>47,080,000</td>
<td>86,050,000</td>
<td>67.2 %</td>
<td>23.7 %</td>
<td>83.3 %</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>14,711,068</td>
<td>70,000</td>
<td>400,000</td>
<td>2.7 %</td>
<td>0.1 %</td>
<td>471.4 %</td>
</tr>
<tr>
<td>Korea, North</td>
<td>23,312,595</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>n/a %</td>
</tr>
<tr>
<td>Korea, South</td>
<td>50,633,265</td>
<td>19,040,000</td>
<td>33,900,000</td>
<td>67.0 %</td>
<td>9.3 %</td>
<td>78.0 %</td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>5,377,484</td>
<td>51,600</td>
<td>263,000</td>
<td>4.9 %</td>
<td>0.1 %</td>
<td>409.7 %</td>
</tr>
<tr>
<td>Laos</td>
<td>5,719,497</td>
<td>6,000</td>
<td>20,900</td>
<td>0.4 %</td>
<td>0.0 %</td>
<td>248.3 %</td>
</tr>
<tr>
<td>Macao*</td>
<td>490,696</td>
<td>60,000</td>
<td>201,000</td>
<td>41.0 %</td>
<td>0.1 %</td>
<td>235.0 %</td>
</tr>
<tr>
<td>Malaysia</td>
<td>27,392,442</td>
<td>3,700,000</td>
<td>10,040,000</td>
<td>36.7 %</td>
<td>2.8 %</td>
<td>171.4 %</td>
</tr>
<tr>
<td>Maldives</td>
<td>298,841</td>
<td>6,000</td>
<td>19,000</td>
<td>6.4 %</td>
<td>0.0 %</td>
<td>216.7 %</td>
</tr>
<tr>
<td>Mongolia</td>
<td>2,568,204</td>
<td>30,000</td>
<td>200,000</td>
<td>7.8 %</td>
<td>0.1 %</td>
<td>566.7 %</td>
</tr>
<tr>
<td>Myanmar</td>
<td>54,021,571</td>
<td>1,000</td>
<td>63,700</td>
<td>0.1 %</td>
<td>0.0 %</td>
<td>6,270.0 %</td>
</tr>
<tr>
<td>Nepal</td>
<td>25,408,817</td>
<td>50,000</td>
<td>175,000</td>
<td>0.7 %</td>
<td>0.0 %</td>
<td>250.0 %</td>
</tr>
<tr>
<td>Pakistan</td>
<td>163,985,373</td>
<td>133,900</td>
<td>7,500,000</td>
<td>4.6 %</td>
<td>2.1 %</td>
<td>5,501.2 %</td>
</tr>
<tr>
<td>Philippines</td>
<td>85,712,221</td>
<td>2,000,000</td>
<td>7,820,000</td>
<td>9.1 %</td>
<td>2.1 %</td>
<td>291.0 %</td>
</tr>
<tr>
<td>Singapore</td>
<td>3,601,745</td>
<td>1,200,000</td>
<td>2,421,000</td>
<td>67.2 %</td>
<td>0.7 %</td>
<td>101.8 %</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>19,630,230</td>
<td>121,500</td>
<td>280,000</td>
<td>1.4 %</td>
<td>0.1 %</td>
<td>130.5 %</td>
</tr>
<tr>
<td>Taiwan</td>
<td>22,896,488</td>
<td>6,260,000</td>
<td>13,800,000</td>
<td>60.3 %</td>
<td>3.8 %</td>
<td>120.4 %</td>
</tr>
<tr>
<td>Tajikistan</td>
<td>6,620,008</td>
<td>2,000</td>
<td>5,000</td>
<td>0.1 %</td>
<td>0.0 %</td>
<td>150.0 %</td>
</tr>
<tr>
<td>Country</td>
<td>Population</td>
<td>Internet Users</td>
<td>Usage Rate</td>
<td>Population %</td>
<td>Internet Users %</td>
<td>Usage Rate %</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>----------------</td>
<td>------------</td>
<td>---------------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Thailand</td>
<td>66,527,571</td>
<td>8,420,000</td>
<td>12.7 %</td>
<td>2.3 %</td>
<td>266.1 %</td>
<td></td>
</tr>
<tr>
<td>Turkmenistan</td>
<td>6,723,715</td>
<td>36,000</td>
<td>0.5 %</td>
<td>0.0 %</td>
<td>1,700.0 %</td>
<td></td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>26,311,197</td>
<td>880,000</td>
<td>3.3 %</td>
<td>0.2 %</td>
<td>11,633.3 %</td>
<td></td>
</tr>
<tr>
<td>Vietnam</td>
<td>83,944,402</td>
<td>5,870,000</td>
<td>7.0 %</td>
<td>1.6 %</td>
<td>2,835.0 %</td>
<td></td>
</tr>
<tr>
<td>TOTAL ASIA</td>
<td>3,667,774,066</td>
<td>364,270,713</td>
<td>9.9 %</td>
<td>100.0 %</td>
<td>218.7 %</td>
<td></td>
</tr>
</tbody>
</table>

NOTES: (1) The Asian Internet Statistics were updated for December 31, 2005. (2) CLICK on each country name to see detailed data for individual countries and regions. (3) The demographic (population) numbers are based on data contained in world gazetteer. (4) The usage numbers come from various sources, mainly from data published by Nielsen//NetRatings, ITU, and other trustworthy sources. (5) Data may be cited, giving due credit and establishing an active link to Internet World Stats. (6) For definitions and help, see the site surfing guide.