



INTERNATIONAL TELECOMMUNICATION UNION

**WSIS Thematic Meeting on Cybersecurity**

Geneva, 28 June – 1 July 2005



**Document: CYB/04**  
**10 June 2005**

---

# **HARMONIZING NATIONAL LEGAL APPROACHES ON CYBERCRIME**

**JUDGE STEIN SCHJØLBERG & AMANDA M. HUBBARD**

© ITU  
June 2005

The paper was prepared by Judge Stein Schjolberg, Moss District Court, Norway and Amanda Hubbard, Computer Crime and Intellectual Property Division, Department of Justice, United States of America, for the ITU WSIS Thematic Meeting on Cybersecurity.

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>3</b>
<b>2</b>	<b>BACKGROUND OF ISSUES FOR DISCUSSION.....</b>	<b>3</b>
<b>2.1</b>	<b>WHAT IS CYBERCRIME?.....</b>	<b>4</b>
<b>2.2</b>	<b>CYBERCRIMES ARE GLOBAL CRIMES.....</b>	<b>5</b>
<b>3</b>	<b>BUILDING TRUST IN CYBERSPACE THROUGH IMPLEMENTING STANDARD AND LEGAL OBLIGATIONS DRAWN FROM INTERNATIONAL CONVENTIONS AND RECOMMENDATIONS .....</b>	<b>5</b>
<b>3.1</b>	<b>UNITED NATIONS EFFORTS .....</b>	<b>6</b>
<b>3.1.1</b>	<i>General Assembly Resolutions .....</i>	<i>6</i>
<b>3.1.2</b>	<i>World Summit on the Information Society.....</i>	<i>6</i>
<b>3.1.3</b>	<i>Group of Government Experts on Information Security.....</i>	<i>7</i>
<b>3.1.4</b>	<i>International Telecommunications Union (ITU) Standards and Working Groups .....</i>	<i>7</i>
<b>3.1.5</b>	<i>United Nations Crime Congresses .....</i>	<i>7</i>
<b>3.1.6</b>	<i>Other UN Efforts .....</i>	<i>7</i>
<b>3.2</b>	<b>GROUP OF EIGHT .....</b>	<b>7</b>
<b>3.3</b>	<b>COMMONWEALTH MODEL LEGISLATION .....</b>	<b>7</b>
<b>3.4</b>	<b>ORGANIZATION OF AMERICAN STATES.....</b>	<b>8</b>
<b>3.5</b>	<b>EUROPEAN UNION .....</b>	<b>8</b>
<b>3.6</b>	<b>ASIAN PACIFIC ECONOMIC COOPERATION.....</b>	<b>8</b>
<b>3.7</b>	<b>ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT .....</b>	<b>8</b>
<b>3.8</b>	<b>THE COUNCIL OF EUROPE.....</b>	<b>8</b>
<b>3.9</b>	<b>EDUCATIONAL AND RESEARCH BODIES .....</b>	<b>10</b>
<b>4</b>	<b>AREAS FOR POTENTIAL INTERNATIONAL LEGAL COORDINATION EFFORTS.....</b>	<b>10</b>
<b>4.1</b>	<b>LEGISLATION.....</b>	<b>10</b>
<b>4.1.1</b>	<i>Substantive Criminal Law .....</i>	<i>10</i>
<b>4.1.2</b>	<i>Procedural Law .....</i>	<i>15</i>
<b>4.1.3</b>	<i>Mutual Legal Assistance Agreements.....</i>	<i>17</i>
<b>4.1.4</b>	<i>Protection of Individual Rights.....</i>	<i>18</i>
<b>4.2</b>	<b>JUDICIAL REVIEW .....</b>	<b>19</b>
<b>5</b>	<b>SUMMARY AND DISCUSSION TOPICS FOR THE THEMATIC MEETING.....</b>	<b>20</b>



## **1 INTRODUCTION**

“Those who fail to anticipate the future are in for a rude shock when it arrives.”  
Professor Peter Grabosky, Australia.

Cyberspace is one of the great legal frontiers of our time. From 2000 to 2005, the Internet has expanded at an average rate of 146.2 percent and currently an estimated 6.4 billion people are “on the Net.”<sup>1</sup> Individuals, groups, and states depend on cyberspace for an unprecedented level of services. Maintaining the confidentiality, integrity, and availability of the networks and the data they carry increases the trust individuals and groups place in their information infrastructures to take advantage of those services. Increasing trust allows greater levels of traditionally non-electronic services to be made available, and encourages stable development and innovation of new services. Only through developing compatible standards and laws can such innovation continue to grow. How we shape standards and legal norms of conduct on the Internet now will affect millions of people in the future. The standards and laws created must include greater flexibility to account for exponential growth in technology and innovations.

However, with this exponential growth in technology and services, bad actors have found and exploited weaknesses for their own selfish interests, eroding the levels of trust in the electronic system. Several organizations collect statistics on the levels of misuse of Internet resources. Though many countries or industry groups within countries collect statistics, no report yet has managed to capture the full scope of Internet misuse internationally.

In response to the growth in misuse, States have responded in many different ways. The two principle responses are criminalizing specific types of conduct, and creating civil or private rights of enforcement violation of protected interests. This background paper deals mainly with harmonizing criminal enforcement mechanisms for a few reasons. First, all countries have criminal justice systems and not all countries have yet recognized private rights of property or of enforcement for cyberspace. Second, the world has a long history of cooperation and harmonization in criminal matters, which gives rise to the concepts of extradition of accused perpetrators, evidentiary assistance, and other matters. Such a tradition is not as readily available for comparison. Lastly, standardization and harmonization of laws for cyberspace is still relatively new in the world of law, having only come about in the last twenty-five years of centuries-old legal systems. As such, the authors believe the simplest way to make the greatest advances is to focus on creating a baseline of laws that protect the population from the worst offences, and build on that base over time, as States develop greater standardization and legal capacity. The paper may briefly note some of the trends in civil or private enforcement actions, where appropriate and relevant to the larger discussion, but leaves thorough discussion of those issues to experts who practice law in that field.

The text that follows this introduction provides a brief history of relevant issues and legislative enforcement actions to preserve security in cyberspace. Section three highlights some of the efforts regional and international groups have taken to harmonize legislation between States. Section four provides background information on four areas where greater standardization and harmonization work could be beneficial: legislation, criminal enforcement and judicial review. The final section summarizes some of the central themes in the paper, and provides a number of discussion topics for the Thematic Meeting.

## **2 BACKGROUND OF ISSUES FOR DISCUSSION**

As with most technological innovations, the race begins early between law-breakers and law-enforcers. Cybercrime legislation has been evolving since the late 1970s, when private personal use of the Internet was still in the early stages of the growth curve. Even these early efforts recognized the potential for the globalization of certain types of malicious behaviours on the Internet and sought to bring States together to

create compatible laws and investigation cooperation. The paragraphs that follow provide a brief overview chronology of some of the important achievements that serve as the basis for current work.

The first comprehensive initiative on computer crime in the United States, where the Internet was born, was a staff study by the U.S. Senate Government Operations Committee in February 1977. This staff study addressed several problems associated with computer programmes and recommended that legislation should be considered that would prohibit the unauthorized use of computers. The Chairman of this committee was Senator Abe Ribicoff.<sup>2</sup> Senator Ribicoff introduced the Ribikoff Bill later in 1977. This Bill was the first proposal for Federal computer crime legislation in the U.S. that would specifically prohibit misuse of computers. The Bill S. 1766 (95<sup>th</sup> Congress) was cited the “Federal Computer Systems Protection Act of 1977”.<sup>3</sup> Senator Ribikoff stated in his presentation, still valid today:

Our committee investigation revealed that the government has been hampered in its ability to prosecute computer crime. The reason is that our laws, primarily as embodied in title 18, have not kept current with the rapidly growing and changing computer technology. Consequently, while prosecutors could, and often did, win convictions in crime by computer cases, they were forced to base their charges on laws that were written for purposes other than computer crime. Prosecutors are forced to “shoe horn” their cases into already existing laws, when it is more appropriate for them to have a statute relating directly to computer abuses.<sup>4</sup>

The Bill was not adopted, but this pioneer proposal raised awareness around the world as to the potential problems that unauthorized computer usage could cause and the need to define the scope of the topic, in order to adequately address the problems in a comprehensive but flexible way.

## **2.1 What is cybercrime?**

As experiences and technology have developed, so also have the definitions of computer crimes or cybercrimes. Historically, in the search for a definition one argued that since computer crimes may involve all categories of crimes, a definition must emphasize the particularity, the knowledge or the use of computer technology.

In the first comprehensive presentation of computer crime, *Computer Crime: Criminal Justice Resource Manual* (1979),<sup>5</sup> the definition of computer-related crime was defined in the broader meaning as: “any illegal act for which knowledge of computer technology is essential for a successful prosecution”.<sup>6</sup> In a study on the international legal aspects of computer crime in 1983, computer crime was consequently defined as: “encompasses any illegal act for which knowledge of computer technology is essential for its perpetration”.<sup>7</sup>

The OECD Recommendations of 1986<sup>8</sup> included a working definition as a basis for the study: “Computer-related crime is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data.”

The Council of Europe Recommendation of 1989<sup>9</sup> adopted a functional approach and computer-related crime was simply described as the offences enumerated and defined in the proposed guidelines or recommendation for national legislators. The Council of Europe Recommendation of 1995<sup>10</sup> on Criminal Procedural Law, has a definition of offences connected with Information Technology (IT offences) as follows: “encompassing any criminal offence, in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer systems, or electronic data processing systems.” The Council of Europe Convention on Cyber-crime of 2001<sup>11</sup> defines cybercrime in the Articles 2-10 on substantive criminal law in four different categories: (1) offences against the confidentiality, integrity and availability of computer data and systems; (2) computer-related offences; (3) content-related offences; (4) offences related to infringements of copyright and related rights. It is a minimum consensus list not excluding extensions in domestic law.<sup>12</sup>

The proposal for a European Union Council Framework Decision on attacks against information systems of 19 April 2002, the Commission also includes a functional definition: “computer-related crime should be understood as including attacks against information systems as defined in this Framework Decision”.<sup>13</sup>

Content-related offences, such as copyright infringements, racism, xenophobia and child pornography may, by many observers normally not be understood to be cybercrimes. Copyright infringements are based upon civil agreements and contracts and are not traditionally criminal offences in many countries. Copyright infringements will very often be enforced through civil remedies due to many the complicated issues. Child pornography has always been a criminal offence in the paper-based version.

Therefore, it could be argued that the term “cybercrime” may be understood as attacks against the infrastructure of the computer systems and networks itself on the Internet, in addition to the Internet forgery and fraud. Consequently cybercrimes may be defined as defined in the Council of Europe Convention of Cybercrime Articles 2-8: Illegal access, Illegal interception, Data interference, System interference, Misuse of devices, Internet forgery and Internet fraud

## **2.2 Cybercrimes are global crimes**

Cyberspace has developed since the 1990’s and the impact on societies has been so fast and enormous, that codes of ethics and the common sense of justice and penal laws have not kept pace. In order to establish ethical standards in cyberspace, penal laws must be enacted with as much clarity and specificity as possible, and not rely on vague interpretations in the existing legislation. With cybercrime laws, perpetrators will be convicted for their explicit acts and not by existing provisions stretched in the interpretation, or by provisions enacted for other purposes covering only incidental or peripheral conduct.

Any regulation of unlawful conduct involving the use of the Internet should be analyzed through a policy framework that ensures that online conduct is treated in a manner consistent with the way offline conduct is treated, in a technology-neutral manner that accounts for other important societal interests such as privacy and protection of civil liberties.<sup>14</sup> Cybercrime laws will also ease the evidentiary burden for law enforcement and prosecutors, and the courts will be able to participate in the process of establishing precedents and ethical standards more significantly through their ruling and sentencing.

The nature of cybercrime and the legal issues are global. Through international organizations, such as the G-8 Group, OAS, APEC and the Council of Europe, efforts have been taken to ensure the harmonization of provision in the individual countries. Ensuring that the dual criminality requirement is fulfilled may provide for an efficient global prosecution of cybercrimes. Such an approach is especially vital in the investigation and prosecution of attacks against the infrastructure of computer systems and networks.

Countries must be able to prosecute cybercrimes committed by national individuals or any person domiciled in that country, whenever the acts are committed abroad. And each country should also be able to prosecute a foreigner present in the country, whenever it does not extradite the person after a request for extradition for cybercrimes committed abroad.

## **3 BUILDING TRUST IN CYBERSPACE THROUGH IMPLEMENTING STANDARD AND LEGAL OBLIGATIONS DRAWN FROM INTERNATIONAL CONVENTIONS AND RECOMMENDATIONS**

International and regional governmental organizations have been active in defining the scope of the problems and attempting to create ways to harmonize domestic legislation. This section describes those efforts in several regional and International bodies.

### **3.1 United Nations Efforts**

The United Nations has long been a leader in looking at issues with a global scope and has engaged in multiple efforts that are relevant to the discussion on this issue. Various bodies within the U.N. have provided significant research and negotiation efforts to reach consensus on a number of cyberspace topics, including setting standards on providing security for networks, establishing a dialogue on a number of problematic issues, such as spam and information security, and as the sponsor of the World Summit on the Information Society (WSIS). This Thematic Meeting has the benefit of all of those resources when developing recommendations and observations for the final round of the WSIS.

#### **3.1.1 General Assembly Resolutions**

The First, Second and Third Committees of the General Assembly have looked into cyberspace issues and have passed a number of resolutions over the last five years. Some of the relevant UNGA resolutions include:

- Resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002 and 58/32 of 18 December 2003 on “Developments in the Field of Information and Telecommunications in the Context of International Security”.
- Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on “Combating the Criminal Misuse of Information Technology”.
- Resolution 57/239 of 20 December 2002 on “Creation of a Global Culture of Cybersecurity”.
- Resolution 58/199 of 23 December 2003 on “Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures”.

The first six resolutions addressed concerns that information technology could be used for purposes inconsistent with the goals and principles of the United Nations. Each successive resolution noted relevant developments in the field and encouraged States to continue such work. These resolutions also authorized the creation of a Group of Experts to further examine the issue. Greater information about that Group, convened in 2004, appears in a subsequent section below.

The second set of resolutions adopted by the General Assembly in 2000 and 2001<sup>15</sup> addressed various ways States could strive to combat the criminal misuse of information technologies. States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies. Among the measures to combat criminal misuse, it was recommended that law enforcement cooperation in the investigation and prosecution should be coordinated, legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized, and that legal system should permit the preservation of and quick access to data in the investigation of such crimes.

Resolutions 57/239 in 2002 and 58/199 in 2003 both dealt with changes in cultural perceptions necessary to achieve greater information and network security. The first resolution focused mainly on the need for States to take action domestically to fulfil nine goals.<sup>16</sup> The second resolution noted the interdependence on information infrastructures with other sectors of the global infrastructure critical for public services.<sup>17</sup> The Annex to 58/199 provides eleven ways States can provide greater protection to critical information infrastructures.

#### **3.1.2 World Summit on the Information Society**

Throughout the process leading up to the first World Summit on the Information Society, experts from around the world have shared ideas and experiences in order to build documents that can facilitate States’ building of compatible standards and laws. One area the experts concentrated on is information and network security. Delegates and representatives from business and civil society contributed many ideas that eventually resulted in drafting two documents at the Phase I Summit in Geneva in 2004, and are in the process of crafting documents for the 2005 Summit in Tunis.



*Geneva Declaration and Plan of Action.* Through many hours of discussion, and many disagreements, the small drafting group in Geneva crafted language for the Geneva Declaration of Principles and Plan of Action that reached consensus. The three paragraphs in the Declaration of Principles that comprise Section Five summarize the critical concerns of the WSIS participants. The Action Plan provides ten elements that all participants felt were the most critical elements of building confidence and security in the use of ICTs.<sup>18</sup>

*Ongoing Negotiations for the Tunis Phase of the Summit.* Negotiations have begun for developing language for follow on documentation that builds on the foundation created in Geneva. The current drafts of the Tunis Phase documents are available at <http://www.itu.int/wsis/documents/index2.html>. In addition to the Preparatory Conferences convened to build consensus for documentary texts, the time leading up to the Summit is full of other preparatory meetings on specific topics (such as this Thematic Meeting on Cybersecurity). The Working Group on Internet Governance has also drafted a preliminary paper on cybersecurity and cybercrime to facilitate discussion.<sup>19</sup>

### **3.1.3 Group of Government Experts on Information Security.**

As mentioned above, the UN General Assembly passed several resolutions on the topic of Information Security and appointed a fifteen-member Experts Group to study the issue further and file a report with the 60th Session of the General Assembly. The Group met first in New York in 2004 and met again in Geneva early in 2005. The Group will conclude its work in July of this year with a two-week session to finalize the report.

### **3.1.4 International Telecommunications Union (ITU) Standards and Working Groups**

One of the most active bodies in reaching harmonization is the ITU, also the sponsor of this background paper and the Thematic Meeting. Several of the working groups are worthy of notice, however, since a separate workshop on the schedule is devoted to the work of the expert groups, the authors defer to the background paper for that session.

### **3.1.5 United Nations Crime Congresses**

The UN Crime Congresses have looked at technical issues and criminal enforcement of computer misuse for at least the last four Congresses. The United Nations adopted in 1990 a resolution<sup>20</sup> on computer crime legislation at the 8<sup>th</sup> U.N. Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba. The most recent Congress in Bangkok, Thailand, focused on issues of computer-related crime in a special workshop. The Congress report and background paper of workshop six are both available from the United Nations Office on Drugs and Crime.<sup>21</sup>

### **3.1.6 Other UN Efforts**

The United Nations has sponsored other projects within this topic area as well. One of note is the Manual on the Prevention and Control of Computer-related Crime, published in 1994. While this publication is in great need of revision to account for developments in the last decade, it does serve as a baseline document from which great progress could be made.

## **3.2 Group of Eight**

In 1997, the Group of Eight (G-8) countries established the Subgroup of High-Tech Crime (the Leon Group). At a meeting in Washington D.C. in 1997,<sup>22</sup> the G8 countries adopted Ten Principles in the combat against computer crime. The goal was to ensure that no criminal receives “safe havens” anywhere in the world. At the last Meeting of G-8 Justice and Home Affairs Ministers in Washington D.C., on 10 and 11 May 2004,<sup>23</sup> a joint communiqué stated that with the Council of Europe Convention of Cybercrime coming into force, the States should take steps to encourage the adoption of the legal standards it contains on a broad basis.

## **3.3 Commonwealth Model Legislation**

In an effort to harmonize computer-related criminal law in the Commonwealth countries, experts gathered and presented a model law to the conference of ministers in 2002. That law, entitled the Computer and Computer Related Crimes Act<sup>24</sup> shares the same framework as the Convention on Cybercrime to limit

conflicting guidance. The model law serves as an example of common principles each country can use to adapt framework legislation compatible with other Commonwealth countries.

### **3.4 Organization of American States**

The Ministers of Justice or Ministers or Attorneys General of the Americas in the Organization of American States (OAS) recommended in Peru, in 1999, the establishment of a group of governmental experts on cybercrime. The Fifth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas in Washington D.C. on from 28 to 30 April 2004,<sup>25</sup> approved conclusions and recommendations. The recommendations included that Member States should evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime (2001) and consider the possibility of acceding to that convention.

### **3.5 European Union**

In the European Union, the Commission of the European Communities presented on 19 April 2002, a proposal for a Council Framework Decision on attacks against information systems.<sup>26</sup> The Council of the European Union adopted the proposal on 27 February 2003. The Framework Decision includes illegal access to information systems, illegal system interference and illegal data interference.<sup>27</sup>

### **3.6 Asian Pacific Economic Cooperation**

The Asian Pacific Economic Cooperation (APEC) has at a meeting in Mexico in October 2002<sup>28</sup> leaders collectively committed to endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and Convention on Cybercrime (2001), by October 2003.

In a joint statement at the Ministerial Meeting in Santiago, Chile, 17-18 November 2004, APEC<sup>29</sup> leaders agreed to strengthen the respective economies ability to combat cybercrime by enacting domestic legislation consistent with the provisions of international legal instruments, including the Convention on Cybercrime (2001) and relevant United Nations General Assembly Resolutions.

### **3.7 Organization for Economic Cooperation and Development**

In 1983, the OECD in Paris appointed an expert committee to discuss computer-related crime and the need for changes in the penal codes. This committee made a proposal that could constitute a common denominator between the different approaches taken by the member countries.<sup>30</sup> The list consisted of computer fraud, computer forgery, damage to computer data and programmes, unauthorized infringement of a protected computer programme and unauthorized access to, or interception of a computer system.<sup>31</sup>

### **3.8 The Council of Europe**

The first international initiative on computer crime in Europe was the Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976.<sup>32</sup> Several categories of computer crime were introduced.

In 1985, the Council of Europe appointed another expert committee, in order to discuss the legal issues of computer-related crime. A summary of the guidelines for national legislatures, with liability for intentional acts only, was presented in the Recommendation of 1989.<sup>33</sup> It included a minimum list of computer fraud, computer forgery, damage to computer data or computer programmes, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of a protected computer programme and unauthorized reproduction of a topography.<sup>34</sup> The Recommendation included an optional list for consideration when planning new legislation.<sup>35</sup>

On 11 September 1995, the Council of Europe adopted another Recommendation concerning problems of procedural law connected with Information Technology. This Recommendation introduces 18 principles, categorized in seven chapters: search and seizure; technical surveillance; obligation to co-operate with the investigating authorities; electronic evidence; use of encryption; research; statistics and training; international co-operation.<sup>36</sup>

The Council of Europe Convention on Cybercrime was opened for signatures at a Conference in Budapest, Hungary, on 23 November 2001.<sup>37</sup> This Convention is a historic milestone in the combat against cybercrime, and entered into force on 1 July 2004; it has been signed by 37 States and currently (June 2005) has been ratified by ten States. An Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems of January 2003 has been signed by 22 States.

The Convention contains four chapters:

Chapter one, includes use of terms (computer system, computer data, service provider and traffic data).

Chapter two, includes measures to be taken at the national level and covers substantive criminal law, procedural law and jurisdiction. Substantive criminal law contains details of offences against the confidentiality, integrity and availability of computer data and systems,<sup>38</sup> computer-related offences such as computer-related forgery and fraud, offences related to child pornography, and offences related to infringements of copyright and related rights. The provisions of procedural law shall apply on any criminal offence committed by means of a computer system, and to the collection on evidence in electronic form of a criminal offence. The provisions contain expedited preservation of stored computer data, production order, search and seizure of stored computer data, real-time collection of computer data.

Chapter three, on International co-operation, includes principles relating to extradition, general principles relating to mutual assistance, procedures pertaining to mutual assistance requests in the absence of applicable international agreements, mutual assistance regarding provisional measures, mutual assistance regarding investigative powers and a 24/7 network.

Chapter four, on final provisions, contains the final clauses, mainly in accordance with standard provisions in the Council of Europe treaties. In accordance with Article 40, any State may declare that it avails itself the possibility of requiring additional elements as provided for under certain Articles. Similarly, for reservations in accordance with Article 42, any State may declare that it avails itself of the reservations provided for in certain Articles.

The establishment, implementation and application of the powers and procedures provided for on procedural law require the States to provide for the adequate protection of human rights and liberties. Some common standards or minimum safeguards are required, including international human rights instruments. The principle of proportionality shall be incorporated. The power or procedure shall be proportional to the nature and circumstances of the offence. Each State shall also consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties, including service providers and the interests of the public and victims.

As stated above, the Council of Europe Convention on Cybercrime is a historic milestone in the combat against cybercrime; Member States of the Council of Europe should complete the ratification of the Council of Europe Convention on Cybercrime of 2001, and other States should evaluate the advisability of implementing the principles of the Convention and consider the possibility of acceding to that Convention. Based on the Council of Europe Convention on Cybercrime and the recommendations from G8, OAS and APEC, we may reach our goal of a global legal framework against cybercrime.

In order to make a proposal for the ratification or acceding to the Council of Europe Convention on Cybercrime, we recommend establishing a Cybercrime Expert Committee. An Expert Committee commission may be split in two reports: the first report should consist of a proposal for the necessary amendments in the penal code and the criminal procedural law only for the ratification or acceding to the

Convention; the second report should cover a broader approach, with an overview of all possible amendments in the domestic penal and procedural provisions needed in the information and communication technology of computer systems and networks. The strategy for a Committee may, therefore, be using declarations according to article 40 and reservations according to article 42, whenever it is possible.

The Convention uses technology-neutral language, so that the offences may be applied to both current and future technology. States may exclude petty or insignificant misconduct from implementation of the offences. For criminal liability to apply, the offences must be committed intentionally. Intentionally may be understood as “wilfully” or “knowingly” but this is left to national interpretation. Only in certain offences does an additional, specific intentional element apply, for instance on computer-related fraud, with the requirement of fraudulent or dishonest intent of procuring an economic benefit. The offence must be committed without right. This may refer to conducts undertaken without authority or conducts not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The offences are not intended to criminalize legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices.

By ratifying or acceding to the Council of Europe Convention of Cybercrime, States agree to ensure that their domestic laws criminalize conduct described in the substantive criminal law section and establish the procedural tools necessary to investigate and prosecute such crimes. This is the harmonizing of national legal approaches on cybercrime.

### **3.9 Educational and Research Bodies**

Several large academic conferences over the years have provided ideas that later appeared in national legislation and regional recommendations. Examples of these academic contributions include the Wurzburg Conference, organized by the University of Wurzburg in 1992.<sup>39</sup> This conference introduced 29 national reports and recommendations for the development of computer crime legislations. Another example is the December 1999 Conference on International Cooperation to Combat Cybercrime and Terrorism, organized by Stanford University in California. In 2000, participants at this conference introduced a Proposal for an International Convention on Cybercrime and Terrorism.<sup>40</sup>

## **4 AREAS FOR POTENTIAL INTERNATIONAL LEGAL COORDINATION EFFORTS**

To stimulate discussion at this Thematic Meeting, the authors have divided possible coordination and harmonization efforts into three main areas: legislative efforts; criminal enforcement efforts; and judicial review. Within each section, subsections will address various specific elements of the three types of governmental action. These segregations are based on the concept that each legal system includes legislative, enforcement and judicial elements.

### **4.1 Legislation**

In this section we provide a brief overview of four types of legislation for discussion: substantive, procedural, mutual legal assistance and protection of individual rights. Each of these sections is only a brief introduction to the topic. Greater detail is available from a number of sources on each individual piece. For an overview of the laws of States that deal with cybercrime, see [www.cybercrimelaw.net](http://www.cybercrimelaw.net).

#### **4.1.1 Substantive Criminal Law**

To combat global cybercrime, States must create some degree of harmony in substantive offences. The following elements are drawn from some of the regional and international harmonization efforts mentioned in section III, above; they serve as a minimal listing of conduct that States should criminalize, in order to reach the most serious antisocial conduct in cyberspace.

*Illegal access*

Illegal access to the whole or any part of a computer system<sup>41</sup> without right should be considered as a criminal offence (Council of Europe Convention on Cybercrime Article 2).

Illegal access or unauthorized access to data<sup>42</sup> is the basic cybercrime. Data are a formal representation of concepts, facts or instructions. Information is the meaning that data has for human beings. Data have, therefore, two different aspects: it is potential information for human beings, or it consists of instructions meant for a computer.<sup>43</sup> States that updated their penal codes according to the Recommendations from the OECD of 1986, or the Council of Europe of 1989, may also be covered against illegal access in cyberspace.

Illegal access to computer systems and networks is also described as “computer trespass,” “cracking” or “hacking”<sup>44</sup> offences. It may constitute an offence even when the perpetrator did not obtain access to the data, but merely activated the computer security devices. It may also constitute an offence if data are accessed in a computer system without any understanding of the content or where the data is located and without any knowledge of the content.

This is the “mere” access to computer systems and networks. Obtaining or trying to obtain illegal access to data in a computer system is thus a criminal offence. Checking passwords covers obtaining information about data stored in the computer systems, whether or not the perpetrator succeed in gaining the information, whether or not it is factually possible to gain the information, whether his aim is merely to explore the system generally. It covers actively interfering with the system itself, in order to inspect its contents or test its access procedures. As long as the requirement of intentional securing of access to data is established it falls within an offence.<sup>45</sup> Or when the computer is being operated with the object of gaining access but no access is actually achieved.

The mere access provisions are strict trespass provisions, whether or not further harm is attempted or achieved. The mere sending of an e-mail or file to computer system is not considered as “access”. Access requires the entering of another computer system or network. Some States do not consider the “mere” access as a criminal offence, but require an additional element of obtaining information. It constitutes a criminal offence whenever a person intentionally and without authority “obtains access” to stored data. “Obtaining information” includes the mere observation and reading of the information,<sup>46</sup> i.e. there is no requirement that the information has to be downloaded.

Many countries find it difficult to punish illegal access without qualifying elements, such as infringing security measures, because it promotes enhanced security in cyberspace and it avoids over-criminalization. But it should be reconsidered with the introduction of broadband communication technology systems into public institutions and private homes. A State may require that the offence be committed with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

### *Illegal interception*

The interception, made by technical means, of non-public transmissions of computer data, including electromagnetic emissions, to or within a computer system should be covered (Council of Europe Convention on Cybercrime Article 3). Within a computer system, includes the computer itself or to or from its devices. It covers the interception of electromagnetic emission during the operation of the computer, such as cables when data is reconstructed from the emission.

The right of privacy in the electronic communication technology is protected in different ways and to different standards around the world. Service providers monitoring traffic on their own networks, undertaken to protect their rights, obligations and property, is not included as illegal interception. The conduct represents the same category of violation as traditional tapping and recording of oral telephone conversations. The offence must apply to all categories of electronic communication, by telecommunication, e-mail or file transfer.

The offence must cover the monitoring, surveillance, listening to the content of the transmission of computer data. The monitoring may be carried out either directly through access to or use of the computer system, or indirectly through the use of electronic eavesdropping or tapping devices. The offence requires technical means, in order to avoid over-criminalization. It includes all kinds of technical devices, also such as computer programmes, passwords or other access codes.

The term “non-public” covers the transmission of computer data, and not the content of the data. Even public accessible information may be “non-public”. If the parties involved in the transmission wish to communicate confidentially, the communication is “non-public”. Similarly, if the transmission is inaccessible until the receiver has paid for it, such as in Pay-TV, the signal will be “non-public”. A State may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. The mental intent is a critical portion of any law regarding illegal interception.

#### *Data interference*

A provision should cover the damaging, deletion, deterioration, alteration or suppression of computer data (Council of Europe Convention on Cybercrime Article 4). Computer data and programmes should be protected in the same manner as tangible objects. The protected interest is the integrity and availability through the proper functioning or use of stored data or computer programmes.

When a perpetrator unauthorized or without right, intentionally destroys, damages or renders useless tangible objects it is clearly a criminal offence. The purpose of cybercrime legislation is to provide computer data, traffic data or computer systems with similar legal protection. Erasure of data is only readable electronically and will not appear understandable to humans.

The traditional provisions assume the physical tangibility. In some States, the legal definition of “property” includes data. In other States, the traditional interpretation of “renders useless an object” may have included the erasure of data, since the object, i.e. the computer, is not operating in the same manner as before. In any circumstances, the differences in the physical concepts may create severe problems on the traditional applicability of vandalism or sabotage. Cybercrime laws should be enacted with as much clarity and specificity as possible, in order to provide adequate foresight of the type of conduct that will result in criminal sanction. The preventive and deterrent role of penal legislation is vital in the development of ethical standards in the information society.

The deletion of stored data occurs when data and programmes are obliterated from the original or previous legal appearance in their formalised manner, even if it is possible to restore the data after the attack. It may include data ranging from small amounts up to complete databases or computer programmes. Alteration requires any modification of the quality of the information to human beings, even if it is understandable, such as obscene words or website defacements. The same goes for adding data without erasure, thus changing the content of computer data. The term “suppression” covers conduct that prevents or terminates the availability of the data, such as when the perpetrator causes the computer data to disappear without being erased. Data is then removed from being accessed by the authorized individuals.

The terms “damaging” and “deterioration” are overlapping conducts, but also include rendering the computer data or traffic data useless or meaningless. Damage to the accumulation of passwords and subsequent corrective measures that computer owners must take to prevent unauthorized access, also qualifies as damage to the networks security data, even if no data is changed or erased.

Computer viruses are covered; any programme or code that does harm is correctly referred to as malicious, but it is not a virus if it does not have the means to propagate or replicate itself. A computer virus is actually a specific type of malicious code that replicates itself and inserts copies or new versions of itself into other programmes when it is executed with the infected programme.<sup>47</sup> One example is the “I LOVE YOU”<sup>48</sup> virus, which was estimated to have infected 45 million computers around the world and caused USD 10 billion in damage. There were no laws penalizing such acts in the Philippine at the time of its commission in

early 2000. But a new law was enacted one month after the virus attack, namely the Electronic Commerce Act of 2000, making it a crime whenever hackers attacked legal business transactions.

Another case is the “Melissa” computer virus. The Melissa virus appeared on thousands of e-mail systems on 26 March 1999, disguised as an important message from a colleague or friend and read: “Here is that document you asked for ... Don’t show anyone else.” Opening and downloading the message caused the Melissa virus to infect the victim’s computer. Such e-mails would only be sent if the computers used Microsoft Outlook for e-mail. Because each infected computer could infect 50 additional computers, which in turn could infect another 50 computers, the virus proliferated rapidly, resulting in substantial interruption or impairment of public communications or services. Its rapid distribution disrupted computer networks by overloading e-mail servers, resulting in the shutdown of networks and significant cost to repair or cleanse computer systems. The virus infected millions of computers, 1.2 million in U.S. alone, and caused more than USD 80 million in damage. In December 1999, David L. Smith pleaded guilty to sending the virus and was later sentenced to five years in prison.

Logic bombs are covered. A logic bomb is computer instruction coding in a programme that triggers the execution of a malicious act if and when certain criteria are met. Any change in value or state in a computer can trigger a logic bomb. For example, a specified time in a computer’s time-of-day or a day-of-year clock may trigger a time bomb.<sup>49</sup>

### *System Interference*

A provision should cover the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data (Council of Europe Convention on Cybercrime, Article 5).

It should constitute a criminal offence when the perpetrator is able to influence the activity of the computer system or make the system inoperative, e.g. crashing the system. Computer systems can thus be closed down for a short or extended period of time, or the system may also process computer data at a slower speed, or run out of memory, or process incorrectly, or omit correct processing. Hindering or interrupting the proper functioning of a computer system by using or influencing computer data should be a criminal offence.

Hindering the functioning of essential governmental or public computer systems may have the most serious consequences to society. Cybercrime targeting critical infrastructures, such as energy, broadcasting, transportation and telecommunications may cause comprehensive disturbance and represent a significant threat to public administration and society.

It does not matter if the hindering is temporarily or permanent, or partial or total. Hindering or interruption may occur as denial of service (DOS) attacks. Categories of such attacks include: blocking users from legitimate access by entering wrong passwords for correct user name, in order to block the access for that user name; or triggering a denial of service attack alert without the existence of any such attack at all, so that the computer system really restrict access to anyone. Spam is the most typical denial of service attacks and the term used to describe the technique of flooding computers with multitudes of e-mail messages or sending large numbers of unwanted messages (unsolicited e-mails) to many Internet users. It began in 1996, when a law firm sent e-mail advertisements to thousands of Internet sites.

In a case on 7-9 February 2000, several Websites, including Yahoo, CNN, Amazon.com, eBay and others, were the targets of distributed denial of service programmes that overwhelmed the sites with data. This bombardment caused the target site’s servers to run out of memory, and thus prevented general access to them from legitimate customers.<sup>50</sup>

Hindering the functioning of essential governmental or public computer systems may have the most serious consequences to society. Cybercrimes targeting critical infrastructures, such as energy, broadcasting,

transportation and telecommunications may cause comprehensive disturbance and represent a significant threat to public administration and the society.

#### *Misuse of devices*

A provision covering the misuse of devices for the purpose of committing illegal access or interception, or data and system interference should be considered a criminal offence (Council of Europe Convention on Cybercrime Article 6). These crimes are committed using computer programmes, such as computer virus or other malicious programmes, or computer password, access code or similar data. The possession, production, sale, procurement for use, import, distribution or otherwise making available of such items with the intent that it be used for the purpose of committing such crimes should be criminalized.

Computer viruses and other malicious programmes are tools in cybercrime offences. Computer viruses represent a dangerous and economic threat to Cyberspace and all societies dependent of the Internet, and no legitimate interest may be protected. The devices must be designed or adapted primarily for the purpose of committing such crimes. Devices that are designed for legal purposes are not covered. The mere possession of devices or access codes or a number of such items may be considered a criminal offence. Some States requires that a number of such items be possessed before criminal liability attaches.

A State may reserve the right not to apply misuse of devices as a criminal offence, provided that the reservation does not concern the sale, distribution or otherwise making available of passwords, access codes or similar data with the intent that they be used for committing illegal access or interception, or data or system interference.

#### *Computer-related forgery*

The input, alteration, deletion, or suppression of computer data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible, should constitute a criminal offence. A State may require an intent to defraud, or similar dishonest intent, before criminal liability attaches (Council of Europe Convention on Cybercrime Article 7)

The provision of the forgery recommendation requires in most countries visual readability of statements or declarations embodied in a document and therefore do not cover computer data. Computer data that is either of significance as evidence of any right, obligation or exemption there from or appears to be designed to serve as evidence, must be protected in the similar manner as paper-based documents. Manipulations of such data may have the same serious consequences and should be a crime in the same manner as traditional forgery of documents.

It is the security and reliability of computer data that may have consequences on legal transactions and are legally relevant that must be protected. Computer-related forgery involves unauthorized creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, subject to a deception.<sup>51</sup>

The unauthorized “input” of correct or incorrect data corresponds to the making of a false document. “Alterations” (modifications, variations, partial changes), “deletions” (removal of data from a data medium), and “suppression” (holding back, concealment of data) correspond, in general, to the falsification of a genuine document.<sup>52</sup> Internet forgery may include bogus websites that falsely present themselves as the sites of established companies for fraudulent purposes, or the assumption of a false identity in e-mail messages for fraudulent purposes, or the posting of false information on Internet bulletin boards to manipulate stock market prices.

The sale or distribution of false identification documents through computer files or computer templates are illegal. It is also illegal to place a template for making false identifications on a website or other online location available to others. A fake identification template is a computer file, usually in Adobe PhotoShop



format, which can be modified, printed and laminated, with the intent of resembling a real license, such as a driver's license. States may also require a specific intent to defraud or similar dishonest intent, before criminal liability attaches.<sup>53</sup>

#### *Computer-related fraud*

As with traditional fraud, computer-related fraud in Cyberspace involves causing a loss of property to another by:

- a. any input, alteration, deletion or suppression of computer data,
- b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another (Council of Europe Convention on Cybercrime Article 8).

Computer fraud is conduct that involves the manipulation of a computer, by whatever method, in order to obtain money, property or some other advantage of value dishonestly, or to cause loss.<sup>54</sup> In most countries the traditional provisions of fraud require a deception of a human being. It is not possible to deceive a computer within the meaning of deception in this required sense and consequently new provisions covering computer-related fraud have been enacted.

The traditional elements of committing fraud are still valid on computer fraud in Cyberspace. They are: (1) by the use of incorrect or incomplete information; (2) by altering data or programmes, or otherwise unlawfully influences the result of computer operations; (3) that causes a loss of property or a risk of loss to anyone; (4) with the intent of procuring an unlawful economic gain for himself or for another person.

Any input, alteration, deletion, suppression of computer data, or any interference with the functioning of a computer system is covered. The aim of the fraud provision is to "criminalize any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property."<sup>55</sup> The act must cause a loss of property, and in addition to money, it must be understood as anything of economic value.

Internet frauds have become a global issue due to the rapid development of the information technology. Internet fraud includes several categories of schemes. It may be false or misleading offerings involving all kinds of property, promises, unfounded financial projections. It may be credit card fraud, mail fraud or bank fraud. A typical fraud on the Internet is stock fraud or online securities fraud. Companies and individuals are using the Internet to artificially inflate the market value of stocks by creating demand for less traded, low priced stocks. Unsolicited e-mails, electronic newsletters, message boards and websites are used as tools to commit such frauds.

Other categories of fraud in Cyberspace include price tag frauds and online auction frauds. Electronic price tag alterations on websites are a growing concern in e-commerce. And the most common of all frauds in Cyberspace is online auction fraud. "Shell bidding" is a practice of false bidding by the seller and/or conspirators designed to drive up the price of an item and force unknowing bidders to increase their bids to acquire the item.<sup>56</sup>

#### **4.1.2 Procedural Law**

##### *General principles*

Adopting procedural laws necessary to establish powers and procedures for the prosecution of criminal conduct against the information technology infrastructure of computer systems and networks is essential for a global investigation and prosecution of cybercrime. But such powers and procedures are also necessary for the prosecution of other criminal offences committed by means of a computer system, and should apply on the collection of evidence in electronic form of all criminal offences.

Such powers and procedures are covered in the section on procedural law in the Council of Europe Convention on Cybercrime. The section is, to a great extent, based on the Council of Europe Recommendation of 1995 concerning problems of criminal law connected with information technology<sup>57</sup>.

The powers are: expedited preservation of stored computer data; expedited preservation and partial disclosure of traffic data; production order; search of computer systems; seizure of stored computer data; real time collection of traffic data; interception of content data.

Common provisions on rules on procedural powers, and procedures for collecting, preserving and presenting evidence in electronic form should be established, in order to provide for an efficient investigation and prosecution on a global level. Only the investigation and prosecution of specific criminal cases, not routine, should be included.

Mandatory data retention for service providers on retaining traffic data for a certain fixed period of time has been discussed in many States. In the European Union (EU), countries such as UK, France, Sweden and Ireland have proposed that telecommunication companies are obliged to store electronic communications for the law enforcements investigation of terrorism in the aftermath of the Madrid terror attacks. But the EU may instead submit a separate data retention legislative proposal for a period of one year, after having studied a cost analysis of a proposal.

#### *Powers of expedited preservation of stored data and expedited preservation and partial disclosure of traffic data*

Each State should adopt measures necessary for law enforcement to order or obtain expedited preservation of stored computer data and expedited preservation and partial disclosure of traffic data<sup>58</sup>. Both principles apply to computer data, including traffic data, that has been stored by means of a computer system and has already been collected, and not to the real-time collection of future data. It means that by ordering a service provider existing data shall not be altered or deleted until its disclosure is obtained. The person or the service provider shall be required to preserve and maintain the integrity of the computer data for a period up to a maximum of 90 days (and to be subsequently renewed). It may be required that the obliged person shall keep the undertaking of the procedures confidential for the same period of time.

It may be obtained by obliging the data-holder to preserve and expeditiously disclose a sufficient amount of traffic data to enable the identification of the service providers and the path through which the communication was transmitted. Traffic data may otherwise be lost and would not enable law enforcement to trace a communication back to its source, especially where several service providers were involved.

#### *Production order*

Each State<sup>59</sup> should adopt measures that enable the authorities to order a person on its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium. Or a service provider to submit stored subscriber information relating to such services in that service provider's possession or control. Subscriber information means information on subscribers in the form of computer data, as well as in any other form, including paper records. Information on traffic data and content data is not included.

#### *Search and seizure of stored computer data*

Each State<sup>60</sup> should adopt measures that relate to the search and seizure of stored computer data in the same manner as with traditional tangible property. The preconditions and the degree of belief required for the legal authorization are similar, but the environment is different. Stored computer data in computer systems or computer data storage mediums, may only be accessed or searched with the use of computer equipment or through electronic communication systems. If the data sought is stored in another computer system, the search shall be extended to the other computer system.

Measures should be adopted to seize or similarly secure the computer data that has been searched or accessed; this includes seizing or similarly securing the computer system or a part of it, or the computer data storage medium itself. Law enforcement shall be able to make and retain a copy of the computer data, and maintain the integrity of the stored computer data. And at the same time render inaccessible or remove the computer data in the accessed computer system.

Provisions should also enable the authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information to enable the undertaking of the search and seizures. But it should be understood as limited to submit the information.

#### *Real time collection of traffic data<sup>61</sup> and interception of content data*

Each State<sup>62</sup> should adopt measures to empower its competent authorities on the real-time collection of traffic data and the real-time interception of such data. The real-time collection of traffic data requires the collection or recording of data with respect to any offence associated with specified communications at the time of the data communication. But reservations may be allowed to offences or categories of offences specified in the reservation.

The real-time interception of content data may be limited to a range of serious offences to be determined by domestic law. A State would be able to reserve the right to apply provisions on the interception of content data only to those serious offences. Content data<sup>63</sup> is not especially defined. The measures adopted on the real-time collection of traffic data and the real-time interception of content data are similarly required to a) collect or record through the application of technical means, b) compel a service provider, within its existing technical capability, either to collect or record through the application of technical means, or to cooperate and assist the competent authorities in the collection or recording of such data. On both categories of data measures may be taken to oblige a service provider to keep confidential the fact of the execution of any power provided for.

#### *Jurisdiction*

Each State<sup>64</sup> should adopt measures to include the traditional jurisdiction provisions in criminal law. Jurisdiction should be established over cybercrime offences, when the offence is committed on its territory, or on board a ship flying the flag of that State, or on board an aircraft registered under the laws of the State, or by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. A State may enter a reservation not to apply or to apply only in specific cases or conditions in the jurisdiction rules. States should be able to prosecute cases where an alleged offender is present in its territory and the State does not extradite the person to another State, solely on the basis of the person's nationality, after a request for extradition. When more than one State claims jurisdiction over an alleged cybercrime offence, the States involved shall, where appropriate, consult with each other to determine the most appropriate jurisdiction for prosecution.

### **4.1.3 Mutual Legal Assistance Agreements**

Mutual Legal Assistance is crucial in international cybercrime investigations, or in civil investigations. The rapid growth of networks and the increase in connection speeds allows criminals to hop between States much more quickly and easily than investigators are able to follow the trail through traditional investigative techniques. Early on, investigators realized the need to establish contacts and procedures in other countries that could produce quick, efficient and reliable results.

Mutual Legal Assistance is not new; the concepts and methodologies have been around for over a century. However, the speed and degree of cooperation between States has changed over the years. Whole works have been written on the topic of mutual legal assistance and this paper does not aim to re-create those works. This section will provide a brief overview of the types of mutual legal assistance arrangements needed for combating cyber offences. Mutual legal assistance of the type discussed in this section is only available in criminal cases; in most instances involving civil cases, parties must file request for evidence using different procedures such as letters rogatory.

In cybercrime cases, one of the most important attributes of digital evidence is the speed in which it travels and the fragility of the data whilst at rest. Data is easily deleted, altered, copied, saved, transferred and destroyed. In order for an investigator to follow leads along an electronic path to lead to a suspect, the leads

must be preserved; obtained in a way that preserves their evidentiary integrity and shared between the requesting State and the State that holds the data. Speed is one of the single most important factors in the success or failure of an international cyber investigation. Additionally, not all investigations require formal assistance or complex chains of admissible evidence; in some cases, one country merely needs a lead for where to look for the next link in the search for a suspect. Using a hacking case as an example, an investigator in Norway could trace an IP address from a computer log of a compromised computer to a service provider in the United States. Because the U.S. service provider is the first computer connection away from the compromised computer, it is unlikely that the perpetrator is the owner of the account at that service provider. The more likely explanation is that the U.S. service provider, or the user account used to intrude into the Norwegian computer, has also been compromised. In such a case, rapid cooperation from the U.S. service provider is crucial for the Norwegian investigators to trace the connection back one more step along the communication path toward the perpetrator. The Norwegian investigator needs a lead to find the next step in the electronic transmission, rather than admissible evidence for court of the logs that simply show the next connection, that is also likely only a hop point to yet another computer in yet another country. Investigators should not overlook the possibility of informal investigative cooperation in order to share, develop, and provide leads.

Where formal assistance is needed, such as where evidence must be collected in such a way that the requesting State could admit the information into a court, States must rely on one of two means for requesting Legal Assistance. The Convention on Cybercrime provides an extensive review of the types and conditions of formal mutual legal assistance efforts needed between countries to trace criminals through cyberspace. These elements appear in Chapter III and include extradition, disclosure of information on a voluntary basis, confidentiality and the limitations on the use of shared information, communications between central authorities, requests for preservation, access and disclosure of stored data, interception of data and trans-border access to stored computer data. This last category of cooperation was particularly problematic during the drafting of the Convention and could serve as one topic for discussion at this workshop. How and when should States access data stored within the geographic borders of another State? The Convention on Cybercrime provided only two instances where cross-border searches would be allowed: a) where the data was available to the public, i.e. posted on a public website; and b) where the party searching for data in one State has the lawful consent of the data owner for data stored in another State.<sup>65</sup>

In most cases, countries will rely on treaties that outline the procedures each State must follow. Where treaties are not in place, however, the States must rely on traditional means, including formal requests for assistance between central authorities. In many ways, mutual legal assistance is the least problematic of the topics addressed in this workshop. Where compatible, substantive and procedural laws exist, mutual legal assistance often naturally develops. The greater need is to build the capacity for improving the speed and efficiency of requests made pursuant to mutual legal assistance treaties or mechanisms that already exist for traditional crimes.

Interpol was the first international organization to address computer crime and penal legislation<sup>66</sup> and act as an organized structure for providing mutual legal assistance. To build rapid response capabilities and expand on the original Interpol model, several countries set out to create a network of computer investigative resources available on a twenty-four hour a day, seven day a week basis. This new 24x7 network began with the Group of Eight countries and has rapidly spread to include, as of today, forty countries worldwide.<sup>67</sup> These countries provide points of contact available around-the-clock, trained in computer investigations and able to initiate the administrative procedures necessary to preserve and acquire computer evidence.

#### **4.1.4 Protection of Individual Rights**

One of the great American statesmen and scholars, Benjamin Franklin, once said: “They that give up essential liberty to obtain a little temporary security deserve neither liberty nor safety.”<sup>68</sup> Security and freedom are both important principles for the growth and development of States. How governments balance the two interests and factors that affect those interests are at the centre of many debates regarding cyberspace. Because the workshop includes a panel devoted to privacy interests, this paper will address only the legal harmonization issues regarding individual rights, such as privacy.

Three of the principle sources of these fundamental individual rights are the Universal Declaration on Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. These documents support the right of every person to exercise the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any medium regardless of frontiers, as set forth in Article 19 of the Universal Declaration of Human Rights.

In conducting cyber investigations, States must ensure that the procedural elements mentioned above include measures that preserve these rights. One method States use to ensure proper procedural safeguards is to require judicial review of intrusions into an individual's personal information or independent oversight of investigations. A second method is to limit the access of personal information to that which is reasonable or necessary in scope or duration of an investigation. Article 15 of the Convention on Cybercrime addresses the requirements for safeguards on individual rights and provides categories where procedural protections are most necessary.

**Box 1.1: The applicable paragraphs of the UDHR include:**

*Related rights enumerated in the UDHR:*

**Article 12:** No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

**Article 18:** Everyone has the right to freedom of thought, conscience and religion.

**Article 19:** Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

**Article 27:** Everyone has the right to freely participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits. Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author

**Article 29:** Everyone has duties to the community in which alone the free and full development of his personality is possible. In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations

*Source:* UDHR.

## 4.2 JUDICIAL REVIEW

The next logical step would be to include the judicial interpretations. An appropriate international legal instrument for the standardization and integration of Supreme Court decisions on the Internet should be established. The Supreme Court or High Court decisions on cybercrimes should, when posted in their native language on the Internet, have a short case summary with possibilities of a multilingual retrieval systems based on structured classifications or keywords.

The second level would be the retrieval system; by using tested search technology global surveillance, structuring, and presentation/distribution of relevant information should be organized. The end-user would, through a website, then be presented with an easy-to-use interface, where all search-parameters regarding cybercrime courts case laws are pre-defined.

## **5 SUMMARY AND DISCUSSION TOPICS FOR THE THEMATIC MEETING**

Cybercrime is a complex topic that requires countries to act domestically and cooperate internationally, in order to protect our vital information infrastructures. The development of international standards and frameworks for implementing network security protocols is one way to increase the safety and stability of networks. Harmonizing national and regional legal regimes for substantive, procedural, and mutual assistance efforts is another way States can cooperate. In order to assist this workshop with discussion on the topics included in this background paper, the authors have developed a few discussion questions to highlight areas where greater work could be useful.

**Discussion Question 1:** What additional topics in cybercrime law are not already covered in current international frameworks?

**Discussion Question 2:** What levels of technical assistance are available under current frameworks? Are those technical assistance means sufficient?

**Discussion Question 3:** What additional procedural areas require greater harmonization to meet today's needs?

**Discussion Question 4:** How can countries reach cooperate in areas where they have very different legal traditions and no basis for substantive cooperation?

- <sup>1</sup> See World Internet Usage and Population Statistics, [Hhttp://www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm) (9 June, 2005).
- <sup>2</sup> Staff Study of Computer Security in Federal Programmes; Committee on Governmental Operations, the 95<sup>th</sup> Congress 1 Session, United States Senate, February 1977
- <sup>3</sup> Congressional Record, 95<sup>th</sup> Congress, Vol. 123, No. 111, 27 June, 1977
- <sup>4</sup> *Id.*
- <sup>5</sup> The Criminal Justice Resource Manual on Computer Crime was prepared by SRI International, Menlo Park, California, USA, for the U.S. Department of Justice in 1979.
- <sup>6</sup> *Ibid.*, p. 3.
- <sup>7</sup> See Stein Schjolberg: Computers and Penal Legislation – A Study of the Legal Politics of a new Technology; CompLex 3/86, Universitetsforlaget, Norway (1983)
- <sup>8</sup> Computer-related criminality: Analysis of Legal Politics in the OECD Area (1986)
- <sup>9</sup> Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on 13 September 1989 and Report by the European Committee on Crime Problems: Computer-related crime. See [Hhttp://cm.coe.int/ta/rec/1989/89r9.htm](http://cm.coe.int/ta/rec/1989/89r9.htm)
- <sup>10</sup> Recommendation No. R (95) 13, approved by the European Committee on Crime Problems (CDPC) at its 44<sup>th</sup> plenary session 29 May – 2 June, 1995: Concerning problems of criminal procedural law connected with information technology. See [Hhttp://cm.coe.int/ta/rec/1995/95r13.htm](http://cm.coe.int/ta/rec/1995/95r13.htm)
- <sup>11</sup> See [Hhttp://conventions.coe.int/Treaty/en/Treaties/Html/185.htm](http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm)
- <sup>12</sup> *Ibid.* See Explanatory Report no. 34.
- <sup>13</sup> See [Hhttp://europa.eu.int](http://europa.eu.int)
- <sup>14</sup> The Electronic Frontier: The Challenge of Unlawful Conduct involving the use of the Internet – A Report of the President’s Working Group on Unlawful Conduct on the Internet. (US March 2000)
- <sup>15</sup> The resolution was adopted by the General Assembly on 4 December, 2000 (A/res/55/63).  
See [Hhttp://www.unodc.org/unodc/crime\\_cisp\\_resolutions.htm](http://www.unodc.org/unodc/crime_cisp_resolutions.htm)
- <sup>16</sup> Resolution 57/239 available from [Hhttp://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/57/239&Lang=EH](http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/57/239&Lang=EH)  
The specific actions are organized under the headings: Awareness; Responsibility; Response; Ethics; Democracy; Risk assessment; Security design and implementation; Security management; and Reassessment.
- <sup>17</sup> Resolution 58/199 available from [Hhttp://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/58/199&Lang=EH](http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/58/199&Lang=EH)
- <sup>18</sup> See [Hhttp://www.itu.int/wsis/docs/geneva/official/poa.html](http://www.itu.int/wsis/docs/geneva/official/poa.html)
- <sup>19</sup> The working paper is available at [Hhttp://www.wgig.org/docs/WP-cybersec.pdf](http://www.wgig.org/docs/WP-cybersec.pdf).
- <sup>20</sup> The resolution was adopted by the General Assembly on 14 December, 1990
- <sup>21</sup> The Crime Congress website is located at: [Hhttp://www.unodc.org/unodc/crime\\_congress\\_11/documents.html](http://www.unodc.org/unodc/crime_congress_11/documents.html)
- <sup>22</sup> The Washington Communiqué of 10 December, 1997
- <sup>23</sup> See [Hwww.usdoj.gov/ag/events/g82004/index.html](http://www.usdoj.gov/ag/events/g82004/index.html)
- <sup>24</sup> Legal and Constitutional Affairs Division, Commonwealth Secretariat, available at: [Hhttp://www.thecommonwealth.org/shared\\_asp\\_files/uploadedfiles/{DA109CD2-5204-4FAB-AA77-86970A639B05}\\_Computer%20Crime.pdf](http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/{DA109CD2-5204-4FAB-AA77-86970A639B05}_Computer%20Crime.pdf).
- <sup>25</sup> See [Hwww.oas.org](http://www.oas.org)
- <sup>26</sup> See [Hhttp://europa.eu.int/information\\_society/topics/telecoms/internet/crime/index\\_en.htm](http://europa.eu.int/information_society/topics/telecoms/internet/crime/index_en.htm)
- <sup>27</sup> Article 2. Illegal access to Information systems
1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases, which are not minor.
  2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.
- Article 3  
Illegal system interference  
Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.
- Article 4  
Illegal data interference  
Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.
- <sup>28</sup> See [Hwww.apectelwg.org](http://www.apectelwg.org)
- <sup>29</sup> See [Hwww.apecsec.org.sg/apec/ministerial\\_statements/annual\\_ministerial/2004\\_16th\\_apec\\_ministerial.html](http://www.apecsec.org.sg/apec/ministerial_statements/annual_ministerial/2004_16th_apec_ministerial.html)
- <sup>30</sup> Computer-related criminality: Analysis of Legal Politics in the OECD Area (1986)

- <sup>31</sup> a) the input, alteration, erasure and/or suppression of computer data and/or computer programmes made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;
- b) the input, alteration, erasure and/or suppression of computer data and/or computer programmes made wilfully with the intent to commit a forgery;
- c) the input, alteration, erasure, and/or suppression of computer data and/or computer programmes, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or telecommunication system;
- d) the infringement of the exclusive right of the owner of a protected programme with the intent to exploit commercially the programme and put it on the market; and
- e) the access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either by infringement of security measures or for other dishonest or harmful intentions.

<sup>32</sup> 12<sup>th</sup> Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15-18 November 1976, page 225-229.

<sup>33</sup> Computer-related crime: Recommendation No. R. (89) 9, see <http://cm.coe.int/ta/rec/1989/89r9.htm>

<sup>34</sup> Computer fraud. The input, alteration, erasure or suppression of computer data or computer programmes, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful gain for himself or for another person (alternative draft: with the intent to unlawfully deprive that person of his property).

Computer forgery. The input, alteration, erasure or suppression of computer data or computer programmes, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence.

Damage to computer data or computer programmes. The erasure, damaging, deterioration or suppression of computer data or computer programmes without right.

Computer sabotage. The input, alteration, erasure or suppression of computer data or computer programmes, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system.

Unauthorized access. The access without right to a computer system or network by infringing security measures.

Unauthorized interception. The interception, made without right and by technical means, of communications to, from and within a computer system or network.

Unauthorized reproduction of a protected computer programme. The reproduction, distribution or communication to the public without right of a computer programme, which is protected by law.

Unauthorized reproduction of a topography. The reproduction without right of a topography, protected by law, of a semi-conductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semi-conductor product manufactured by using the topography.

<sup>35</sup> The optional list:

Alteration of computer data or computer programmes. The alteration of computer data or computer programmes without right.

Computer espionage. The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with the intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person.

Unauthorized use of a computer. The use of a computer system or network without right, that either:

is made with the acceptance of a significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or

is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or causes loss to the person entitled to use the system or harm to the system or its functioning.

Unauthorized use of a protected computer programme. The use without right of a computer programme which is protected by law and which has been reproduced without right, with the intent, either to procure an unlawful economic gain for himself or for another person or to cause harm to the holder of the right.

<sup>36</sup> Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on 11 September 1995.

<sup>37</sup> See <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

<sup>38</sup> Article 2 - Illegal access:

...the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 - Illegal interception:

...the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 - Data interference:

...the damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 - System interference:

...the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data

Article 6 - Misuse of devices:

...the production, sale, procurement for use, import, distribution or otherwise making available of:



---

a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2-5;

a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Article 2-5, and;

b. the possession of an item referred to in paragraphs (a) (1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2-5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Each country may reserve the right not to apply Article 6, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph a.ii of this article.

<sup>39</sup> See Ulrich Sieber (ed): *Information Technology Crime – National Legislations and International Initiatives*, Carl Heymanns Verlag KG (1994).

<sup>40</sup> See <http://cisac.stanford.edu/publication/11912H>

<sup>41</sup> "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data;

<sup>42</sup> "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function; see Council of Europe art. 1 b).

<sup>43</sup> See Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, 2 October 1995, page 13

<sup>44</sup> A malicious hacker is someone who routinely executes programmes in other people's computers without their express or implied permission. Malicious hackers frequently engage in criminal acts while exploring others' computers, and violate the privacy of computer users and owners. They may also engage in software piracy, in spreading computer viruses, and in fraud, burglary, and theft. See Donn B. Parker: *Fighting Computer Crime* (1998) page 160.

<sup>45</sup> See The Law Commission (Law Com. No.186) *Criminal Law: Computer misuse*. Presented to Parliament by the Lord High Chancellor by Command of Her Majesty, October 1989. Reprinted 1994, page 16-22.

<sup>46</sup> The U.S. Senate Judiciary Committee on U.S.C. 1030(a)(2): "Because the premise of this subsection is privacy protection, the Committee wishes to make clear that obtaining information in this context includes mere observation of the data.

<sup>47</sup> See Donn B. Parker: *Fighting Computer Crime* (1998) page 82

<sup>48</sup> See *World Internet Law Report*, (2000) Vol I, Issue 13, page 8

<sup>49</sup> See Donn B. Parker: *Fighting Computer Crime* (1998) page 90

<sup>50</sup> See U.S. Department of Justice, <http://www.usdoj.gov:80/criminal/cybercrime.ccpolicy.html>

<sup>51</sup> Explanatory Report to the Convention on Cybercrime no. 81

<sup>52</sup> Explanatory Report to the Convention on Cybercrime no 83

<sup>53</sup> Explanatory Report to the Convention on Cybercrime, no. 85

<sup>54</sup> The Law Commission, Report No. 186, *Criminal Law-Computer Misuse*, 1989, England

<sup>55</sup> Explanatory Report to the Convention on Cybercrime, no 86

<sup>56</sup> See Paula Selis, Anita Ramasastry and Charles S. Wright: *Toward a fraud-free marketplace – best practices for the online auction industry*.

<sup>57</sup> See <http://cm.coe.int/ta/rec/1995/95r13.htm>

<sup>58</sup> See the Council of Europe Convention on Cybercrime Articles. 16 and 17

<sup>59</sup> See Article. 18

<sup>60</sup> See Article. 19

<sup>61</sup> Traffic data is defined in the Article 1 as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."

<sup>62</sup> See Articles 20 and 21

<sup>63</sup> Content data refers to "the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)

<sup>64</sup> See Article 22

<sup>65</sup> See Convention on Cybercrime, Article 32

<sup>66</sup> The Third Interpol Symposium on International Fraud, Saint-Cloud, Paris, France, 11-13 December, 1979. Interpol held the First Interpol Training Seminar for Investigators of Computer Crime, 7-11 December, 1981. The keynote speaker at the conference was Donn B. Parker, SRI International, USA, and the founder of the combat against computer crime.

<sup>67</sup> Australia, Austria, Brazil, Canada, Croatia, Denmark, the Dominican Republic, Finland, France, Germany, Hungary, India, Indonesia, Israel, Italy, Japan, Republic of Korea, Luxembourg, Malaysia, Mexico, Morocco, the Netherlands, New Zealand, Norway, Philippines, Romania, Russia, Singapore, South Africa, Spain, Sweden, Thailand, Tunisia, United Kingdom, United States, and the territories of Hong Kong, China and Taiwan, China.

<sup>68</sup> Benjamin Franklin, *Historical Review of Pennsylvania* (1759).