The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva

By Stein Schjolberg
Chief Judge
December, 2008

1. Introduction

This paper presents a summary of the story of the global harmonizing of computer crime and cybercrime legislation,[1] from the very first efforts in the late 1970ties to the initiatives in Geneva in 2008.

As computers have developed, so have also criminal offences associated with their use. Mankind will always have to live with criminal activity, and as a result of the conversion to the use of computer networks in the online society in Cyberspace, new methods of perpetrating crimes have been developed.

Traditional penal laws were not written with the on-line society in Cyberspace in mind. The main problem is the applicability of this legislation on cybercrime and to what extent. The information structure in Cyberspace represents values that should be protected, also by criminal law measures. Provisions in traditional criminal law describe qualified unethical behaviours that the societies have decided to be criminal offences. These qualified unethical behaviours have developed over hundreds of years, as criminal offences against individuals and property have developed. Codes of ethics and public sentiment of justice have been the main resources in this development, together with the human, financial and technological development. Cyberspace has been reality only since the mid 90-ties, and the impact has been so fast and enormous that criminal laws have not kept pace.

In order to establish criminal offences for the protection of information and communication in Cyberspace, provisions must be enacted with as much clarity and specificity as possible, and not rely on vague interpretations in the existing laws. When cybercrime laws are adopted, perpetrators will be convicted for their explicit acts and not by existing provisions stretched in the interpretations, or by provisions enacted for other purposes covering only incidental or peripheral acts.

One of the most important purposes in criminal legislation is the prevention of criminal offenses. A potential perpetrator must also in cyberspace be given a clear warning with adequate foreseeability that certain offences are not tolerated. And when criminal offences occur, perpetrators must be convicted for the crime explicitly done, satisfactorily efficient in order to deter him or her, and others from such crime. These basic principles are also valid for cybercrimes.

Cybercrime, including massive and coordinated cyber attacks against countries critical information infrastructure, and terrorist misuse of the Internet, are global crimes. Cyberspace has made a new environment for criminal offenses. Through international organizations, efforts must be taken to ensure the similarity of provisions in the individual countries. This harmonization may be achieved by means of conventions, recommendations or guidelines.

Cyberspace is today one of the great legal frontiers. From 2000 to 2008, the Internet has expanded at an average rate of 305 % on a global level, and currently an estimated 1,46 billion people are "on the Net."[2] The increase in Asia has been 406% and in Africa 1031%.

In order to reach a global harmonization of cybercrime legislation, and a common understanding of cybersecurity and cybercrime among countries at all stages of economic development, a global agreement

[1] See Stein Schjolberg and Amanda M. Hubbard: Harmonizing National Legal Approaches on Cybercrime (2005), www.itu.int/cybersecurity/gateway/laws_legislation.html

[2] See World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm (June, 2008).

or Protocol at the United Nations level should be established that includes solutions aimed at addressing the global challenges.

A convention or a treaty is normally a more binding agreement, where parties to the treaty may be held liable under international law for breaches of the agreement. A Memorandum of Understanding (MoU) is normally a more loosely agreement. It usually indicates a common line of action between multilateral parties. A MoU is normally used in situations where parties either do not imply a legal commitment or in situations where the parties cannot create a legally enforcement agreement. It is a more formal alternative to a gentlemen's agreement.[3]

Even if a MoU is not binding under international law, it should be registered in the United Nations treaty database.

The most active UN-institution in reaching harmonization on global cybersecurity and cybercrime legislation is the International Telecommunication Union (ITU). ITU in Geneva is uniquely positioned for developing a global agreement or protocol on cybersecurity and cybercrime. It may be then called the Geneva Protocol, since the importance to the global society is almost equally as important as the Kyoto Protocol.

2. The History

2.1.The Pioneers

Several individuals were engaged in the fight against computer crime from the early development. The founder and father of the knowledge of computer crime is by many observers considered to be Donn B. Parker, USA. He was involved in the research of computer crime and security from the early 1970ties.[4] He served as a Senior Computer Security Consultant at the SRI International (Stanford Research Institute), and was the main author of the first basic federal manual for law enforcement in USA: "Computer Crime – Criminal Justice Resource Manual" (1979).[5] This manual became soon an encyclopedia also for law enforcement outside US.

Other authors in USA that contributing in the fight against computer crime in the early days were August Bequai[6] and Jay Bloombecker.[7]

Outside USA, Stein Schjolberg, a police attorney and prosecutor in Norway[8] was involved as a practitioner from 1976. He assisted Interpol from 1979 in the development of knowledge of this new phenomenon. In Germany, Ulrich Sieber, was involved as an academician at the University of Freiburg.[9] He assisted early on many international organisations, such as OECD from 1983 and United Nations. In The Netherlands, H. W. K. Kaspersen another academician, was early involved and became later the "father" of the Council of Europe Cybercrime Convention, through his initiative in 1997.

In Australia, K. E. Brown, a detective chief inspector at the Victoria police in Melbourne was early involved in the fight against computer crime.[10]

2.2. 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.[11] Several categories of computer crime were introduced.

---

[3] See http://en.wikipedia.org/wiki/MoU/

[4] See an overview of his archives, www.cybercrimelaw.net. His first book on the subject was: "Computer Crime" (1976).

[5] This manual was made for the National Criminal Justice Information and Statistics Service, by the Law Enforcement Assistance Administration LEAA (370 pages).

[6] August Bequai: Computer Crime, Lexington Books, USA (1978)

[7] Ulrich Sieber: Computercriminalitat und strafrecht, Carl Heymanns Verlag KG (1977)

[8] Stein Schjolberg was 1977 appointed as an assistant police commissioner in Oslo, and as a judge in 1983, and chief judge in Moss tingrett Court in 1994.

[9] Ulrich Sieber was later appointed as a professor at the Max Planck University. He has assisted many international organizations: The OECD as a consultant for the guidelines published in 1986, United Nations in 1989, and the Council of Europe for the Organised Crime Report (2004).

[10] K.E. Brown: Toward an International Convention on Computer-related Crime. (1982).

[11] A Paper for the 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15-18 November 1976, page 225-229.

2.3. The Ribikoff Bill

In the United States a staff study by the U.S. Senate Government Operations Committee in February 1977 was the first comprehensive initiative on computer crime The staff study addressed several problems associated with computer programs, and recommended that legislation should be considered that would prohibit unauthorized use of computers. The Chairman of this committee was Senator Abe Ribicoff.[12]

Later in 1977 Senator Ribicoff introduced the Ribikoff Bill. 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 (95th Congress) was cited the "Federal Computer Systems Protection Act of 1977".[13] 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.[14]

Senator Joe Biden, made a statement in a Senate hearing about Senator Abe Ribikoff in 1977:

> .... for hearing those voices in the wilderness and focusing the Senate´s and this committee´s attention on the crime of the future – computer fraud.

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.

2.4. Interpol

Interpol was the first international organization addressing computer crime and penal legislation at a Conference in Paris in 1979.[15] In a presentation on computer frauds it emphasized as follows:

> The nature of computer crime is international, because of the steadily increasing communications by telephones, satellites etc., between the different countries. International organizations, like Interpol, should give this aspect more attention.[16]

Interpol initiated a discussion, and a project[17] was approved by the General Assembly in 1980/81. A Questionnaire on computer crime was circulated to the Interpol member countries. It was followed by The First Interpol Training Seminar for Investigators of Computer Crime, in Paris, December 7-11, 1981.[18]

In conjunction with this Conference a summary of answers from Interpol member countries on computer crime and penal legislation identified several legislative areas with unsatisfactorily existing penal legislation, such as:

a. modification and erasure of data, or otherwise affecting data processing with destructive intent,
b. appropriation or obtaining data belonging to another with intent to gain the perpetrator,
c. obtaining, without authority, computer services for one's own purpose, using a computer belonging to another,
d. modification of data with fraudulent intent, or with intent to be used in legal transactions,
e. disclosure of data without authority.

The summary was the first step on the development of harmonizing penal laws dealing with computer crime around the world. The summary concluded as follows:

---

[12] Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977

[13] Congressional Record, 95th Congress, Vol. 123, No. 111, June 27, 1977

[14] *Id.*

[15] The Third Interpol Symposium on International Fraud, Saint-Cloud, Paris, France, December 11-13, 1979.

[16] Stein Schjolberg, then Assistant Commissioner of Police in Oslo, Norway.

[17] Approved by Secretary General A. Bossard on April 30, 1980

[18] The Conference was organized by Interpol in co-operation with Stein Schjolberg, It was attended by 66 delegates from 26 countries. The keynote speaker at the Conference was Donn B. Parker, SRI International, Menlo Park, California, USA, the "founder" of the combat against computer crime.

> On the international level the transborder data flow through telephones and radio systems, satellites and microwave facilities, could create bilateral or multilateral problems if perpetrators are using such communications in criminal activities. If more than one country is involved, it emphasize the need to harmonize penal codes through guidelines or recommendations to assure proper prosecution, which otherwise could be prevented by international jurisdictional problems.[19]

2.5. The OECD Recommendation of 1986.

In 1982[20] the OECD in Paris decided on appointing an expert committee[21] to discuss computer-related crime and the need for changes in the Penal Codes. As a result of the expert committee proposals[22], the ICCP-Committee of the OECD in 1986 highly recommended:

> With respect to the transnational aspects of computer-related criminal activity, important issues have been noted which point to the desirability for international cooperation in repressing and controlling such activity. And that all member countries consider the extent to which acts committed knowingly in this field should be covered by national penal legislation. These acts may be expressed as far as possible in terms of functions rather than technology.[23]

A list of acts which could constitute a common denominator between the different approaches taken by the member countries was suggested. The list consisted of computer fraud, computer forgery, damage to computer data and programs, unauthorized infringement of a protected computer program and unauthorized access to or interception of a computer system as follows:

a. the input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully 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 programs made willfully with the intent to commit a forgery;
c. the input, alteration, erasure, and/or suppression of computer data and/or computer programs, or other interference with computer systems, made willfully 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 program with the intent to exploit commercially the program and put it on the marked:
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.

2.6. The Council of Europe Recommendations of 1989.[24]

The Council of Europe appointed in 1985 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.[25] It included a minimum list of computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of a protected computer program and unauthorized reproduction of a topography:

> Computer fraud. The input, alteration, erasure or suppression of computer data or computer programs, 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

---

[19] Stein Schjolberg: EDP and Penal Legislation, A presentation at the Interpol Conference in December 1981. In cooperation with SRI International, USA, The Norwegian Research Center for Computers and Law, University of Oslo, and Interpol, Paris, he was working on a model law for computer crime laws that could be used as a remedy, or guideline for other countries.

[20] Stein Schjolberg meeting with Paul Kenneth, OECD, September 1982.

[21] A group of experts met at the OECD in Paris on May 30, 1983: Mme C.M.Pitrat, France, Mr. M. Masse, France, Mr.A. Norman, United Kingdom, Mr. S. Schjolberg, Norway, Mr. B. de Schutter, Belgium, and Mr. U. Sieber, Germany. These" founders " of the harmonization of European computer crime legislation recommended that the OECD should take an initiative. An expert committee was established, and recommended in September 18, 1986 through the ICCP Committee a common denominator between the different approaches taken by the Member countries.

[22] Ulrich Sieber, Germany, served as a consultant in preparing the analysis.

[23] Computer-related criminality: Analysis of Legal Politics in the OECD Area (1986)

[24] Computer-related crime: 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. (Published in Strasbourg 1990)

[25] Computer-related crime: Recommendation No. R. (89) 9.

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 programs, 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 programs. The erasure, damaging, deterioration or suppression of computer data or computer programs without right.

Computer sabotage. The input, alteration, erasure or suppression of computer data or computer programs, 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 program. The reproduction, distribution or communication to the public without right of a computer program 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.

The Recommendation included an optional list for consideration when planning new legislation:

The optional list:

Alteration of computer data or computer programs. The alteration of computer data or computer programs 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 program. The use without right of a computer program 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.

The Council of Europe adopted this Recommendation on September 13, 1989. It contains a minimum list of offences necessary for a uniform criminal policy on legislation concerning computer-related crime, and an optional list.

2.7. The Council of Europe Recommendations of 1995

The Council of Europe adopted on September 11, 1995, another Recommendation concerning problems of procedural law connected with Information Technology.

This Recommendation introduces 18 principles categorized in 7 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.[26]

[26] 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,

2.8. G-8 Group of States[27]

The High Tech Subgroup of the G-8's Senior Experts on Transnational Organized Crime, developed and established in 1998 a 24-hour, seven day network of experts to assist in high-tech crime investigation. The goal was to ensure that no criminal receives safe haven anywhere in the world, and that the law enforcement authorities have the technical ability and legal process to find criminals who abuse technologies and bring them to justice. Other countries have joined the network and are participating in the co-operation.

The G-8 Group has also agreed upon principles that should apply when law enforcement agents employed by law enforcement agencies are investigating criminal offenses and require assistance in other countries. Such principles should be implemented through treaties and through national laws and policies.[28]

Principles On Transborder Access To Stored Computer Data
Principles On Accessing Data Stored In A Foreign State

Preservation of stored data in a computer system.

1. Each state shall ensure its ability to secure rapid preservation of data that is stored in a computer in particular data held by third parties such as service providers, and that is subject to short retention practices or is otherwise particularly vulnerable to loss or modification, for the purpose of seeking its access, search, copying, seizure or disclosure, and ensure that preservation is possible even if necessary only to assist another State.
2. A State may request another State to secure rapid preservation of data stored in a computer system located in that other State.
3. Upon receiving a request from another State, the requested State shall take all appropriate means, in accordance with its national law, to preserve such data expeditiously. Such preservation shall be for a reasonable time to permit the making of a formal request for the access, search, copying, seizure or disclosure of such data.

   Expedited mutual legal assistance
4. Upon receiving a formal request for access, search, copying, seizure or disclosure of data, including data that has been preserved, the requested State shall, in accordance with its national law, execute the request as expeditiously as possible, by:
   a) Responding pursuant to traditional legal assistance procedure; or
   b) Ratifying or endorsing any judicial or other legal authorization that was granted in the requesting State and, pursuant to traditional legal assistance procedures, disclosing any data seized to the requesting State; or
   c) Using any other method of assistance permitted by the law of the requested State.
5. Each State shall, in appropriate circumstances, accept and respond to legal assistance requests made under these Principles by expedited but reliable means of communications, including voice, fax or e-mail, with written confirmation to follow where required.

   Transborder access to stored data not requiring legal assistance.
6. Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of:
   a) accessing publicly available (open source) data, regardless of where the data is geographically located;
   b) accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data. The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State.

2.9. The Stanford Draft Convention of 2000.

Stanford University, Hoover Institution, in California, organized in December 6-7, 1999, a Conference on International Cooperation to Combat Cyber Crime and Terrorism.

Based on the experience at this conference Stanford University introduced in 2000 a Proposal for an International Convention on Cyber Crime and Terrorism.[29]

---

[27] G-8 consists of the following States: Canada, France, Italy, Japan, Russia, United Kingdom, Germany and USA. See www.g7.utoronto.ca

[28] Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow October 19-20, 1999, Annex 1.

[29] See http://cisac.stanford.edu/publications/11912

Article 3 on offences reads as follows:

1. Offences under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent:
   a) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or programs in a cyber system with the purpose of causing, or knowing that such activities would cause, said cyber system or another cyber system to cease functioning as intended or to perform functions or activities not intended by its owner and considered illegal under this Conventions;
   b) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data in a cyber system for the purpose and with the effect of providing false information in order to cause substantial damage to persons or property;
   c) enters into a cyber system for which access is restricted in a conspicuous and unambiguous manner;
   d) interferes with tamper-detection or authentication mechanisms;
   e) manufactures, sells, uses, posts, or otherwise distributes any device or program intended for the purpose of committing any conduct prohibited by Article 3 and 4 of this Convention;
   f) uses a cyber system as a material factor in committing an act made unlawful or prohibited by any of the following treaties:.....
   g) engages in any conduct prohibited under Articles 3 and 4 of this Convention with a purpose of targeting the critical infrastructure of any State Party.
2. Purpose, intent, or knowledge with respect to the crimes set forth in paragraph 1 of this section may be inferred from objective factual circumstances.

Other Articles includes: jurisdiction; mutual legal assistance; prosecution; cooperation in law enforcement; agency for information infrastructure protection; protection of privacy and other human rights.

2.10. The Electronic Frontier

The U.S. President established in 1999 a Working Group in order to provide an initial analysis of legal and policy issues surrounding the use of the Internet to commit unlawful acts. The Working Group's[30] report was called *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet,* and published in March 2000. The report recommended three approaches for addressing unlawful conduct on the Internet:

1) 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, and in a manner that accounts for other important societal interests such as privacy and protection of civil liberties.
2) Law enforcement needs and challenges posed by the Internet should be recognized as significant, particularly in the areas of resources, training, and the need for new investigative tools and capabilities, coordination with and among federal, state, and local law enforcement agencies, and coordination with and among our international counterparts.
3) There should be continued support for private sector leadership and the development of methods - such as "cyber ethics" curricula, appropriate technological tools, and media and other outreach efforts - that educate and empower Internet users to prevent and minimize the risks of unlawful activity.

2.11. Research

The first academic study of computer crime in Europe was presented in Germany 1977 by Ulrich Sieber, Germany.[31]

Several academic conferences have over the years provided ideas that later appeared in national legislation and regional recommendations. The most important was the Wurzburg Conference, organized by the University of Wurzburg in 1992.[32] This conference introduced 29 national reports, and recommendations for the development of computer crime legislations. Another example was the December 1999 Conference on International Cooperation to Combat Cyber Crime and Terrorism, organized by Stanford University in California.

---

[30] See www.cybercrime.gov

[31] Ulrich Sieber: Computercriminalitat und strafrecht, Carl Heymanns Verlag KG (1977)

[32] Ulrich Sieber (ed): Information Technology Crime – National Legislations and International Initiatives, Carl Heymanns Verlag KG (1994).

3. What is cybercrime? The history of definitions

As experiences and technology have developed so have also 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),[33] 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.[34]

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.[35]

The OECD Recommendations of 1986[36] included a working definition as a basis for the study:

> Computer-related crime is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data.

The Council of Europe Recommendation of 1989[37] 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.

In the Council of Europe Recommendation of 1995[38] on Criminal Procedural Law, the term *"offences connected with Information Technology"* (IT offences or IT crimes) is used. In this Recommendation, IT offences are described as: *"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."*

In a Communication from the Commission of the European Union in 2001 a single definition is once again introduced. In this Communication, "computer-related crime is addressed in the broadest sense as:

> any crime that in some way or other involves the use of information technology.[39]

In addition the Communication follow up with the traditional distinction between "computer specific crimes" and "traditional crimes performed with the aid of computer technology."

In the Proposal for an International Convention on Cyber Crime and Terrorism by the Stanford University (2000)[40], cyber crime means:

> conduct with respect to cyber systems that is classified as an offense punishable by this Convention.

A cyber systems means in this proposal "any computer or network of computers used to relay, transmit, coordinate, or control communications of data or programs."

The proposal for a European Union Council Framework Decision on attacks against information systems of April 19, 2002, the Commission includes also a functional definition:

> computer-related crime should be understood as including attacks against information systems as defined in this Framework Decision.[41]

The Council of Europe Convention on Cyber-crime of 2001[42] defines cybercrime in the Articles 2-10 on substantive criminal law in four different categories: (1) offences against the confidentiality, integrity and

---

[33] 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.

[34] Ibid. p. 3.

[35] See Stein Schjolberg: Computers and Penal Legislation – A Study of the Legal Politics of a new Technology; CompLex 3/86, Universitetsforlaget (1986)

[36] Computer-related criminality: Analysis of Legal Politics in the OECD Area (1986)

[37] Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on September 13 1989 and Report by the European Committee on Crime Problems: Computer-related crime. See http://cm.coe.int/ta/rec/1989/89r9.htm

[38] Recommendation No. R (95) 13, approved by the European Committee on Crime Problems (CDPC) at its 44th plenary session May 29 – June 2, 1995: Concerning problems of criminal procedural law connected with information technology. See http://cm.coe.int/ta/rec/1995/95r13.htm

[39] See the Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, January 26. 2001. http://europa.eu.int

[40] Center for International Security and Cooperation (CISAC), Stanford University: A Proposal for an International Convention on Cyber Crime and Terrorism, August 2000. See http://cisac.stanford.edu/publications/11912

[41] See http://europa.eu.int

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.

Content-related offences such as copyright infringements, racism, xenophobia, and child pornography may by many observers normally not be understood as 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 criminal offences in the paper-based version.

Today, we must include identity theft, spam, and phishing and other preparatory acts prior to attempted acts.

Cybercrime may also be understood as including massive and coordinated attacks against the information infrastructure of a country. Even the distinction to terrorism has been blurred, especially for terrorist misuse of the Internet in public provocation, recruitments and training for terrorist acts.

*

The massive and coordinated cyber attacks against critical information infrastructure.in Estonia from April 27 to May 18, 2007 may be an example. Toomas Viira, Estonian Informatics Center, has in January 2008 described the attacks as follows:[43]

> In phase I most of the attacks were relatively simple Denial of Service (DoS) attacks against government organizations web servers and Estonian news portals.
>
> In phase II much more sophisticated, massive (use of larger botnets) and coordinated attacks appeared. Most dangerous were Distributed Denial of Service (DDoS) attacks against some of the critical infrastructure components – against data communication network backbone routers and attacks against DNS servers. Some of these DDoS attacks were successful for a very short time period – we had few less than 5 minutes interruptions in data communication backbone network.
>
> Cyber attacks (mostly DDoS) continued also against government organizations web servers. Since May 10, DDoS attacks against two Estonian biggest banks started. For one of them the attack lasted for almost two days and Internet banking services were unavailable for one hour and thirty minutes. For several days, restrictions were applied for accessing Internet banking services from foreign countries.
>
> Several attacks were also performed against media company web sites, e.g. DDoS against web servers and comment spam against media portals. There were periods were media companies limited the commenting in media portals and when it was not possible to access web pages from foreign countries."

4. The Road to Geneva

The nature of cybercrime and the legal issues are global. Through international organizations, such as ITU, INTERPOL, United Nations Office on Drugs and Crime (UNODC), G 8 Group of States, Council of Europe, Organization of American States (OAS), Asia Pacific Economic Cooperation (APEC), The Organization for Economic Cooperation and Development (OECD), The Commonwealth, European Union, efforts have been taken to ensure the harmonization of legislation in the individual countries.

4.1. United Nations

The United Nations General Assembly has adopted a number of resolutions. General Assembly Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on "Combating the criminal misuse of information technologies", are most important.

The Resolution 55/63 includes as follows:

> (a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies.
>
> (b) Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized"

The Resolution 56/121 invites Member States, when developing national laws, policy and practices, to combat the criminal misuse of information technologies, to take into account, inter alia, the work and achievements of the Commission on Crime Prevention and Criminal Justice.

---

[42] See http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[43] See Toomas Viira: Meridian, Vol.2 No 1 (January 2008)

4.1.1. International Telecommunications Union (ITU)

The most active UN-institution in reaching harmonization on global cybersecurity and cybercrime legislation is the International Telecommunication Union (ITU) in Geneva.[44]

The UN General Assembly recognized in 2001 the need for a multi-phase World Summit on the Information Society (WSIS) and asked the ITU to take the lead role in coordinating robust, multi-stakeholder participation in these events. Phase one of WSIS occurred in Geneva in December 2003, and Phase two took place in Tunisia in 2005. Following the WSIS summits and the 2006 ITU Plenipotentiary Conference, ITU assumed an important role in coordinating to build confidence and security in the use of information and communication technologies (ICTs).

At the World Summit on the Information Society (WSIS) in Tunis in 2005, the ITU was entrusted as a facilitator for Action Line 5: "Building confidence and security in the use of information and communication technologies (ICTs)."

A Global Cybersecurity Agenda (GCA)[45] was launched in May 2007 by the Secretary General as a global framework for dialogue and international cooperation aimed at proposing strategies for solutions to enhance security in the Information Society. The GCA is made up of seven main strategic goals, including the main strategic goal for the legislative measures: the elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.

In order to assist the ITU's Secretary-General in developing strategic proposals to Member States, a High Level Experts Group (HLEG) was established in October 2007. This global expert group of more than 100 experts, has in June 2008 made the advices on strategies in the following five work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation.

The role of ITU is to seek consensus on a framework for international cooperation in cybersecurity, in order to reach for a common understanding of cybersecurity threats among countries at all stages of economic development, that includes developing and putting into action solutions aimed at addressing the global challenges to cybersecurity and cybercrime.

GCA is the framework for proposing strategies for solutions to enhance confidence and security in the information society, under the umbrella of cybersecurity. The principles of this framework was adopted by the 2005 Tunis Agenda of WSIS.

The Tunis Agenda, paragraph 42 and 40, reads as follows:

> We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles. (paragraph 42)
>
> We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe´s Convention on Cybercrime. (paragraph 40)

The main strategic goal in the Global Cybersecurity Agenda for legislative measures, is the elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.

4.1.2. United Nations Crime Congresses

The UN Crime Congresses[46] 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[47] on computer crime legislation at the 8th 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

---

[44] See also page 2-3

[45] See www.itu.int/osg/csd/cybersecurity/gca

[46] See www.unodc.org

[47] The resolution was adopted by the General Assembly on December 14, 1990

six are both available from the United Nations Office on Drugs and Crime.[48] The Bangkok Declaration no. 16 reads as follows:

> We note that, in the current period of globalization, information technology and the rapid development of new telecommunication and computer network systems have been accompanied by the abuse of those technologies for criminal purposes. We therefore welcome efforts to enhance and supplement existing cooperation to prevent, investigate and prosecute high-technology and computer related crime, including by developing partnerships with the private sector. We recognize the important contribution of the United Nations to regional and other international forums in the fight against cybercrime and invite the Commission on Crime Prevention and Criminal Justice, taking into account that experience, to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations.

4.2. The Council of Europe

The Council of Europe Convention on Cybercrime was opened for signatures at a Conference in Budapest, Hungary, on November 23, 2001.[49]This Convention is a historic milestone in the combat against cybercrime, and entered into force on July 1, 2004. The number of signatures not followed by ratifications are 23 States and the number of ratifications/accessions are 23 States (December 2008). An Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems of January 2003 has also been adopted.

The Convention contains four chapters. Chapter 1 includes use of terms (computer system[50], computer data, service provider and traffic data).

Chapter 2 includes measures to be taken at the national level and covers substantive criminal law, procedural law and jurisdiction. Substantive criminal law contains of offences against the confidentiality, integrity and availability of computer data and systems,[51] 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. 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.

---

[48] See www.unodc.org/unodc/en/commissions/crime-congresses-11.html

[49] See http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[50] The definition is sufficiently flexible to address technology that go beyond traditional computer systems. It includes mobile telephones that have the capability to produce, process and transmit data, such as accessing Internet, sending e-mail, and transmitting attachments.

[51] 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 program, 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.

Chapter 3 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 4 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.

The Convention on Cybercrime is a historic milestone in the combat against cyber crime. Based on the Convention and the recommendations from regional organizations we may in the future reach our goal of a global legal framework against cybercrime.

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. The offences must be committed intentionally for criminal liability to apply. Intentionally may be understood as wilfully or knowingly, but it is left to national interpretation. Only in certain offences additional specific intentional element applies, for instance on computer-related fraud with the requirement of fraudulent or dishonest intent of procuring an economic benefit. Negligence or gross negligence would not be satisfactory.

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 criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices.

On terrorism, a Council of Europe treaty "The European Convention on the Suppression of Terrorism" was adopted in 1977 as a multilateral treaty. The treaty was in 2005 supplemented by the Council of Europe Convention on the Prevention of Terrorism,[52] and entered into force on June 1, 2007. In this convention a terrorist offence is merely defined as meaning any of the offences as defined in the attached list of 10 treaties in the Appendix.

According to the 2005 Council of Europe Convention on the Prevention of Terrorism, Articles 5-7, parties to the Convention are required to adopt certain preparatory conducts that have a potential to lead to terrorist acts as criminal offences.[53]

Public provocation to commit a terrorist offence is a criminal offence if the distribution of a message to the public, "whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed" (Article 5). Presenting a terrorist offence as necessary and justified is a criminal offence.[54] A specific intent is required *to incite the commission of a terrorist offence.* The provocation must in addition be committed unlawfully and intentionally.

Recruitment for terrorism is also a criminal offence if a person is solicited "to commit or participate in a commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group" (Article 6). The recruitment for terrorism may be carried out through the use of Internet, but it is required that the recruiter successfully approach the person. The recruitment must be unlawfully and intentionally.

Training for terrorism is a criminal offence if instructions are provided for "making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques" (Article 7). The purpose must be to execute the terrorist offence or contribute to it. The

[52] See conventions.coe.int
[53] See http://conventions.coe.int
[54] See Explanatory Report note 98.

trainer must have knowledge of that skills or "know-how" and intended to be used for the carrying out of the terrorist offence or for a contribution to it.[55] The training must be unlawfully and intentionally.

4.3. The G-8 Group of States

The G-8 Group of States[56] countries established in 1997 the Subgroup of High-Tech Crime (the Leon Group). At a meeting in Washington D.C. in 1997, 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 Meeting of G-8 Justice and Home Affairs Ministers in Washington D.C., on May 10-11, 2004,[57] 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. In a statement from the G8 Meeting in 2005 a goal was emphasized:

> To ensure that law enforcement agencies can quickly respond to serious cyber-threats and incidents.

At the Moscow Meeting in 2006 for the G8 Justice and Home Affairs Ministers discussed cybercrime and issues of cyberspace. In a statement it was emphazised:

> We also discussed issues related to sharing accumulated international experience in combating terrorism, as well as comparative analysis of relevant pieces of legislation on that score. We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that it is necessary to device a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors."

The G8 Summit in 2006 was held in St. Petersburg and a Summit Declaration on Counter-Terrorism included as follows:

> We reaffirm our commitment to collaborative work, with our international partners, to combat the terrorist threat, including:
>
> Implementing and improving the international legal framework on counter-terrorism;
>
> Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists;

At the Meeting of G8 Justice and Interior Ministers in Munich on May 23-25, 2007, the delegates also agreed "to work towards criminalizing, within national legal frameworks, specific forms of misusing the Internet for terrorist purposes."

The G-8 Group had their last meeting at the Hokkaido Tokyako Summit on July, 7-9, 2008. A report to the G8 Summit leaders from the G8 experts on International Terrorism and Transnational Organized Crime was presented.

4.4. The Commonwealth

In an effort to harmonize computer related criminal law in the Commonwealth[58] countries, experts gathered together and presented a model law to the conference of ministers in 2002. That law, titled the Computer and Computer Related Crimes Act,[59] 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.

A Meeting of Senior Officials of Commonwealth Law Ministers was held in October 2007. The meeting addressed laws to combat terrorism and money laundering.

---

[55] See Explanatory Report note 122.

[56] G-8 consists of the following States: Canada, France, Italy, Japan, Russia, United Kingdom, Germany and USA. See www.g7.utoronto.ca

[57] See www.usdoj.gov/ag/events/g82004/index.html

[58] See www.thecommonwealth.org

[59] Legal and Constitutional Affairs Division, Commonwealth Secretariat.

4.5. Organization of American States (OAS)

The Ministers of Justice or Ministers or Attorneys General of the Americas in the Organization of American States (OAS)[60] recommended in Peru in 1999 the establishment of a group of governmental experts on cybercrime. At a Meeting in Trinidad and Tobago in 2002 recommendations were adopted giving the Group of Experts the following mandate:

> To consider the preparation of pertinent inter-American legal instruments and model legislation for the purpose of strengthening hemispheric cooperation in combating cybercrime, considering standards relating to privacy, the protection of information, procedural aspects, and crime prevention.

The Fifth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas in Washington D.C. on April 28-30, 2004,[61] approved conclusions and recommendations. The recommendations included as follows:

> 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.

The General Assembly of the Organization of American States requested at the Meeting on June 7, 2005, the Permanent Council to convene the meeting of the Group of Governmental Experts on Cybercrime.

The Organization of American States, in cooperation with the Council of Europe and Spain, organised a conference in Madrid on December 12-13, 2005. This conference was titled: *Cybercrime: A Global Challenge, A Global response.* Among the conclusions was adopted:

> Acknowledge the importance of the only international treaty in this field: the Convention on Cybercrime which is open to all States as well as the importance of strengthening the international legal framework;
>
> Strongly encourage States to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level and on behalf of international cooperation;
>
> Recognise the need of pursuing cooperation, providing technical assistance and organising similar events in other regions of the world.

The Permanent Council of the Organization of American States resolved on December 15, 2005, that the Group of Governmental Experts on Cybercrime should meet on February 27-28, 2006 for the purpose of carrying out the mandates referred to in the conclusions and recommendations of the Fifth Meeting of Ministers of Justice of April 28-30, 2004.

The Group of Governmental Experts on Cybercrime met in Washington D.C. February 27-28, 2006. The Agenda included also:

> Challenges on accessing, drafting and amending legislation consistent with the principles, substantive and procedural law of the Council of Europe Convention on Cybercrime (2001)

The Group of Governmental Experts on Cybercrime met in Washington D.C. February 27-28, 2006. The Agenda included also:

> Challenges on accessing, drafting and amending legislation consistent with the principles, substantive and procedural law of the Council of Europe Convention on Cybercrime (2001)

At the Sixth Meeting of Ministers of Justice in June 2006 it was made a statement as follows:

> …continue to strengthen cooperation with the Council of Europe so that the OAS member states can give consideration to applying the principles of the Council of Europe's Convention on Cyber-crime and to acceding thereto, and to adopting the legal and other measures required for its implementation. Similarly, that efforts continue to strengthen mechanisms for the exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, such as the United Nations, the European Union, the Asia Pacific Economic Co-operation Forum, the Organisation for Economic Co-operation and Development (OECD), the G-(, the Commonwealth, and Interpol, in order for the OAS member states to take advantage of progress in those forums.

The conclusions and recommendations were followed up at a plenary session in June 2007 and a resolution was adopted (AG/RES. 2266 (XXXVII-o/07)) A Seventh Meeting of Ministers of Justice was held in June 2008. In addition, an OAS- Council of Europe Workshop on cybercrime legislation was held in Bogota, Colombia, in September 2008.

---

[60] See www.oas.org/juridico/english/cyber.htm

[61] See www.oas.org/juridico/english/cyber_meet.html

4.6. The European Union (EU)

In the European Union,[62] the Commission of the European Communities presented on April 19, 2002 a proposal for a Council Framework Decision on attacks against information systems.[63] It was necessary to complement the work performed by international organizations, such as the Council of Europe's work on approximating criminal law and the G-8's work on transnational co-operation, by providing a common approach in the European Union.

The Council of the European Union adopted the proposal in 2003 and it entered into force in 2005. The Framework Decision includes illegal access to information systems, illegal system interference and illegal data interference.[64]

States shall, according to Article 6, ensure that illegal system interference and illegal data interference is punishable of a maximum at least between 1 and 3 years of imprisonment. But aggravating circumstances included in Article 7 may result in a maximum of at least between 2 and 5 years.

States shall establish jurisdiction described in Article 10. According to Article 10.3 a State which under its laws does not extradite its own nationals, shall establish jurisdiction over and prosecute conducts referred to in Article 2-4, when it is committed by one of its nationals outside its territory.

In the latest development, the EU Commission considered an initiative in May 2007 regarding to European legislation against identity theft, called *Towards a general policy on the fight against cyber crime*.

The Commission organized an European Union Expert Meeting on Cybercrime in November 2007. The meeting represented a next step for the European Union in implementing the general policy outlined by the Commission. A statement was made as follows:

> The increasing prevalence of cyber crime across Europe, spanning large scale attacks in Estonia, identity theft in Spain, illegal content and high-profile online child abuse incidents in Austria, Germany, Italy and the UK, highlights the need for concerted action. Indeed successful operations such as "Operation Koala" and the global hunt for the "Vico" paedophile depends on regional and international cooperation. The conclusions of today´s meeting represent an important step by the EU to establish the cooperative links upon which such success is built.

A Framework Decision amending the Framework Decision 2002/475 JHA on combating Terrorism has been prepared in 2008 in the European Union. It will include three new crimes in the EU legislation: public provocation to commit terrorist offences, recruitment for terrorism, and training for terrorism.

4.7. Asian Pacific Economic Cooperation (APEC)

The Asian Pacific Economic Cooperation (APEC)[65] has at a meeting in Mexico in October 2002 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 the Convention on Cybercrime (2001), by October 2003.

---

[62] See www.europa.eu

[63] See http://ec.europa.eu/information_society/topics/telecoms/internet/crime/index_en.htm

[64] 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.

[65] APEC consists of 21 States: Australia; Brunei Darussalam; Canada, Chile; People's Republic of China; Hong Kong China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papa New Guinea; Peru; Philippines; Russia; Singapore; Chinese Taipei; Thailand; United States; Viet Nam. See www.apecsec.org

In a joint statement at the Ministerial Meeting in Santiago, Chile, November 17-18, 2004, APEC 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.

At the APEC Telecommunications and Information Working Group Meeting[66] on September 5-9, 2005, in Seoul, Korea, a statement reads as follows:

> Economies are currently implementing and enacting cybersecurity laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project will support institutions to implement new laws.

At the Ministerial Meeting in November 2005, APEC Ministers approved an APEC Strategy to ensure a trusted, secure, and sustainable online environment. Member States was urged to:

> Address the threat posed by the misuse, malicious use and criminal use of the online environment by ensuring that legal and policy frameworks; Address substantive, procedural and mutual legal assistance arrangements.

The Ministers renewed their commitment in the Lima Declaration, stating that they:

> Encourage all economies to study the Convention on Cybercrime (2001) and endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001).

A joint APEC-OECD Workshop on Security of Information was held in Seoul in 2005. Several topics were discussed, including promoting global governmental incidents response. In April 2007 an APEC-ASEAN Workshop was held in Manila.

A Chair's Report of the Telecommunications and Information Working Group was presented to the Seventh APEC Ministerial Meeting in Bangkok on 23 April 2008.

4.8. Association of Southeast Asian Nations (ASEAN)

The Association of Southeast Asian Nations (ASEAN)[67] has established high level Ministerial Meeting on Transnational Crime (AMMTC). At the Meeting in Bangkok, January 8, 2004, a statement included cyber crime was recognized and the need for an effective legal cooperation to enhance the fight against transnational crime.

A Plan of Action to Implement the Joint Declaration on ASEAN-China Strategic Partnership for Peace and Prosperity, was signed on October 8, 2003, in Bali, Indonesia. ASEAN and China will pursue the following joint actions and measures:

> 2.5.7. Formulate cooperative and emergency response procedures for purposes of maintaining and enhancing cybersecurity, and preventing and combating cybercrime.

In a statement from ASEAN Regional Forum (ARF) on July 2006 it was emphasized that:

> Believing that an effective fight against cyberattacks and terrorist misuse of cyberspace requires increased, rapid and well functioning legal and other forms of cooperation.
>
> 1. ARF participating states and organization endeavour to enact, if they have not yet done so, and implement cybercrime and cybersecurity laws in accordance with their national conditions and by referring to relevant international instruments and recommendations/guidelines for the prevention, detection, reduction, and mitigation of attacks to which they are party, including the ten recommendations in the UN General Assembly Resolution 55/63 on Combating the Criminal Misuse of Information Technologies.
> 2. ARF participating countries and organization acknowledge the importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyber space and encourage the formulation of such a framework that may include…"

Ministers of ASEAN member countries and China with responsibility for cooperation in combating transnational crime met in Brunei Darussalam in November 2007. It was agreed that with the emerging

---

[66] See wwwapectelwg.org

[67] ASEAN Group consists of 10 States: Brunei Darussalam; Cambodia; Indonesia; Laos; Malaysia; Myanmar; Philippines; Singapore; Thailand; Viet Nam. See www.aseansec.org

challenges and increasing scope of transnational crime cooperation, the ASEAN-China Memorandum of Understanding (MoU) needed to be reviewed and revised accordingly. In a Joint Communique, including China, Japan and the Republic of Korea, a statement was adopted as follows:

> We held a retreat to exchange views on strengthening ASEAN + 3 cooperation in combating transnational crime focusing on the emerging challenges of cyber-crime and its strong linkages to other transnational crime for example terrorism and trafficking-in persons.

A joint communiqué from the ASEAN Chiefs of Police Conference in Brunei Darussalam in May 2008 included the adoption of resolutions on cybercrime.

4.9. The Organisation for Economic Co-operation and Development (OECD)

The Organization for Economic Cooperation and Development (OECD)[68] adopted in 2002 new guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. This approach to the critical information infrastructure protection is a guideline, and as such not binding for member States.

- An OECD Global Forum on Information Systems and Network Security was in 2003 held in Oslo, Norway. A Workshop on Cybercrime was organized in conjunction with this Forum.
- The OECD Task Force on Spam was established in 2004 and delivered a report in 2006.
- A joint APEC-OECD Workshop on Security of Information was held in Seoul in 2005. Several topics were discussed, including promoting global governmental incidents response.
- In April 2007 an APEC-OECD Malware Workshop was held in Manila.

The OECD was the first international organization that initiated guidelines for computer crime,[69] but do not today work directly on cybercrime per se. The organization focuses more on cybersecurity, and promotes a global coordinated policy approach building trust and confidence. The OECD Working Party on Information and Privacy (WPISP) develops international guidelines.[70]

4.10. NATO

NATO[71] has organized a Science for Peace and Security Advanced Research Workshop in Sofia, Bulgaria, in October 2006. The workshop focused on Cyber Terrorism – a serious threat to peace and security in the 21st century.

NATO has in 2008 opened a centre of excellence on cyber defence in Tallinn, Estonia, in order to conduct research and training on cyber warfare.

4.11. African Union

Some members of the African Union,[72] such as Mauritius, South Africa and Zambia have adopted cybercrime legislation. A cybercrime Bill in Botswana passed the Second Reading in the Parliament in December 2007, and is expected to go for third reading in the near future, before it is signed into law.

A draft Information and Communications Bill 2008 has been introduced in Gambia. The Bill includes provisions on computer misuse and cybercrime issues.

The East Africa region includes Tanzania, Kenya and Uganda. The progress on cybercrime legislation has been slow in this region, except for Uganda. The Computer Misuse Bill has been introduced in 2008 in Uganda and a legislative process has started. The East Africa countries are trying to coordinate efforts so that the legislations should be similar to the cybercrime laws in the Southern African region.

A Cybercrime Bill is being prepared in Algeria, and may be submitted to the Parliament by the end of 2008.

A draft report on the harmonization of telecommunication, information and communication technologies policies and regulation in Africa has been published. It also includes tracing and combating of cybercrime in all its forms.

---

[68] See www.oecd.org
[69] See Computer-related Criminality: Analysis of Legal Politics in the OECD-Area (1986)
[70] See www.oecd.org/sti/security-privacy
[71] See www.nato.int
[72] See www.africa-union.org

The Southern African Development Community (SADC) involving Zambia, Zimbabwe, South Africa, Malawi and Mozambique, initiated efforts on harmonizing cybercrime laws in 2005.

A Connect Africa Initiative was launched at a Summit of African leaders in October 2007. It is a global multi-stakeholders partnership aiming to assist and complement the development of ICT infrastructure in Africa.

4.12. The League of Arab States

Several countries in the League of Arab States[73] have adopted cybercrime legislation, such as Saudi Arabia and United Arabic Emirates (UEA). UEA was the first country in the region that adopted legislation, with the Cyber-Crime Law no 2, in February 2006.

The Gulf Cooperation Council (GCC) involving Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and United Arabic Emirates, has at a conference in June 2007 recommended that the GCC countries make a treaty on cyber crimes.

An ITU Regional Workshop for Cybersecurity and Critical Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop was held in Doha in February 2008. The Workshop stressed the importance of reviewing national cybercrime legislation to address threats in cyberspace, and develop appropriate tools to combat cyber attacks.

4.13. Shanghai Cooperation Organisation (SCO)

The Shanghai Cooperation Organisation (SCO)[74] was founded by The People's Republic of China, Russia, Kazakstan, Kyrgyzstan, Tajikistan, and Uzbekistan. The organization was established on June 15, 2001 by the Declaration of Shanghai Cooperation Organisation.

The Shanghai Convention on Combating Terrorism, Separatism and Extremism states that the members are:

> firmly convinced that terrorism, separatism and extremism, as defined in this Convention, regardless of their motives, cannot be justified under any circumstances, and that the perpetrators of such acts should be prosecuted under the law;

For the purpose of this Convention "terrorism" means:

> a. …..
> b. other acts intended…, as well as to organize, plan, aid and abet such act"

A seventh council meeting of the SCO heads of state was held in 2007. A document, *"SCO member countries action plan to safeguard international information security"* was signed by Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan and China. Facing new challenges and threats in the field of information security, the SCO members will work together to jointly cope with the growing network and information security threats.

4.14. Human Rights

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 media regardless of frontiers, as set forth in Article 19 of the Universal Declaration of Human Rights.

4.14.1. Investigation

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 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

[73] See www.arableagueonline.org
[74] See www.sectsco.org

Cybercrime addresses the requirements for safeguards on individual rights and provides categories where procedural protections are most necessary.

4.14.2. Prosecution

The role of prosecution in protecting the rule of law and human rights in the context of terrorism in cyberspace should apply also on all categories of cybercrime.

Attorney Generals or General Prosecutors from 30 European States made a statement at the Ninth Annual Eurojustice Conference in September 2006 as follows:

> All countries are struggling to adapt their criminal justice systems to the threat posed by terrorism. However, combating terrorism is fundamental in order to guarantee the security and freedom of all citizens. However, the fight against terrorism should not be seen as a "war". Terrorism must be regarded as a crime, albeit a particularly serious one, and should be commanded as such. Preventive measures, investigation, prosecution and trial must be founded on the rule of law, be under judicial control and based on the international recognized human rights principles as enshrined in the United Nations Human Rights Conventions and the European Convention on Human Rights.

4.14.3. Judicial Courts

The national Court of Justices is the main legal guarantee on promoting the national rule of law on criminal conducts in cyberspace. The role of judges in protecting the rule of law and human rights in the context of terrorism in cyberspace should apply also on all categories of cybercrime. The Consultative Council of European Judges (CCJD) has adopted in 2006 the following principles:[75]

> While terrorism creates a special situation justifying temporary and specific measures that limit certain rights because of the exceptional danger it poses, these measures must be determined by the law, be necessary and be proportionate to the aims of a democratic society.
>
> Terrorism cases should not be referred to special courts or heard under conditions that infringe individual rights to a fair trial.
>
> The courts should, at all stages of investigations, ensure that restrictions of individual rights are limited to those strictly necessary for the protection of the interests of society, reject evidence obtained under torture or through inhuman or degrading treatment and be able to refuse other evidence obtained illegally.
>
> Detention measures must be provided for by law and be subject to judicial supervision, and judges should declare unlawful any detention measure that are secret, unlimited in duration or do not involve appearance before established according to the law, and make sure that those detained are not subjected to torture or other inhuman or degrading treatment.
>
> Judges must also ensure that a balance is struck between the need to protect the witnesses and victims of acts of terrorism and the rights of those charged with the relevant offences.
>
> While States may take administrative measures to prevent acts of terrorism, a balance must be struck between the obligation to protect people against terrorist acts and the obligation to safeguard human rights, in particular through effective access to judicial review of the administrative measures.

5. A Geneva Framework

5.1. International Telecommunication Union (ITU) in Geneva

The most active UN-institution in reaching harmonization on global cybersecurity and cybercrime legislation is the International Telecommunication Union (ITU) in Geneva.

The Secretary-General of the ITU launched in May 2007 the Global Cybersecurity Agenda (GCA)[76] for a framework where the international response to the growing challenges to cybersecurity could be coordinated. GCA is the framework for proposing strategies for solutions to enhance confidence and security in the information society, under the umbrella of cybersecurity.

ITU in Geneva is uniquely positioned for developing a global agreement or protocol on cybersecurity and cybercrime. It may be then called the Geneva Protocol, since the importance to the global society is almost equally as important as the Kyoto Protocol. It may include all five pillars of the ITU Global Cybersecurity Agenda (GCA): Legal Measures, Technical and Procedural Measures, Organizational

[75] Adopted November 11, 2006 by the Consultative Council of European Judges (CCJE), a Council of Europe advisory body.
[76] See www.itu.int/osg/csd/cybersecurity/gca

Structures, Capacity Building, and International Cooperation. A Geneva Protocol may be a non-binding statement of mutual intentions.

In order to assist the ITU's Secretary-General in developing strategic proposals to Member States, a High Level Experts Group (HLEG) was established in October 2007. This global expert group of more than 100 experts delivered Reports and Recommendations in June 2008, and the Chairmans Report[77]was published in August 2008. The Global Strategic Report[78] was published on November 12, 2008, including strategies in the following five work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation.

5.2. The Chairmans Report

Although HLEG members did not achieve full consensus in every recommendation, most of the HLEG experts were nevertheless in broad agreement on many recommendations that set a clear direction for ITU's future work in the domain of cybersecurity. In particular, HLEG Members were in full agreement that vital action is needed to promote cybersecurity and ITU has an important role to play. In the Report of the Chairman of HLEG, Recommendations on legal measures were made as follows:

Overview:

Work Area one (WA1) sought to promote cooperation and provide strategic advice to the ITU Secretary-General on legislative responses to address evolving legal issues in cybersecurity. Some HLEG members considered that the scope of WA1 included prosecution of cybercrimes. One member suggested the following summary of WA1: "ITU's Secretary-General should promote cooperation among the different actors so that effective legal instruments are identified and characterized in building confidence and security in the use of ICTs, making effective use of ITU recommendations and other standards, in accordance with present international agreements".

Summary of Discussions:

Discussions covered how to build on existing agreements in this area: for example, the Council of Europe's *Convention on Cybercrime* and the *Convention on the Prevention of Terrorism of 2005*. Some members preferred omitting mention of the *Convention on Cybercrime*, although they recognized it as an available reference. One member stated that the *Convention on Cybercrime* could not be proposed as the only solution for all states and wished to acknowledge the status of the *Convention* as an example of legal measures realized as a regional initiative belonging to signatory countries, consistent with the status accorded to the Convention in paragraph 40 of the WSIS Tunis Agenda for the Information Society.

There was considerable discussion as to whether recommendations 1.1-1.3 should be merged. Some members supported the suggestion that Recommendations 1.1-1.3 should be merged (e.g. some members wished to delete Recommendation 1.3). One key recommendation emerging from WA1 was that ITU could organize a global conference to promote cybersecurity, but this was contentious for some HLEG members (recommendation 1.13).

Recommendations:

1.1. ITU is a leading organisation of the UN system and could elaborate strategies for the development of model cybercrime legislation as guidelines that are globally applicable and interoperable with existing national and regional legislative measures.

1.2. Governments should cooperate with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks: for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional relevant initiatives including, but not limited to, the Council of Europe's *Convention on Cybercrime*.

1.3. Considering the Council of Europe's *Convention on Cybercrime* as an example of legal measures realized as a regional initiative, countries should complete its ratification, or consider the possibility of acceding to the Convention of Cybercrime. Other countries should, or may want to, use the Convention as a

[77]www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf
[78] www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice.

With regard to the Council of Europe's Convention on Cybercrime, some members suggested that countries could be encouraged to join and ratify the Convention and draw on it in drafting their relevant legislation. One member suggested that countries could, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. Other members preferred omitting mention of the Convention on Cybercrime, although they recognized it as an available reference, whilst one member stated that the Convention could not be proposed as the only solution for all states and wished to acknowledge that the Convention is an example of legal measures realized as a regional initiative belonging to those countries which are signatories, consistent with the status accorded to the Convention in paragraph 40 of the WSIS Tunis Agenda for the Information Society. Some members wished to delete recommendation 1.3, despite the insertion of text recognizing the Convention as a regional initiative. One member wished to delete the phrase "may want to" in recommendation 1.3.

1.4. It is very important to implement at least Articles 2-9 in the substantive criminal law section, and to establish the procedural tools necessary to investigate and prosecute such crimes as described in Articles 14-22 in the section on procedural law.

A few members wished to delete this recommendation.

1.5. Cybercrime legislation should be designed using existing international and regional frameworks as a reference or as a guideline, and the Convention on Cybercrime was designed in a way so that it could be adapted to technological developments, and laws using the Convention as a guideline should be able to address modern developments.

One member wished to delete the first phrase on how cybercrime legislation should be developed. A few other members wished to delete the text referring to the history of the design of the Convention and the normative statement as to what it might be able to achieve.

1.6. Discussions about how to address criminal activities related to online games have just begun. Currently, most states seem to focus on extending the application of existing provisions, instead of developing a new legal framework for activities in virtual worlds. Depending on the status of cybercrime-related legislation, most offences should be covered this way; otherwise, countries should consider an appropriate approach to cover such offences.

One member wished to delete this Recommendation.

1.7. Supplementing Articles in the Convention may however be necessary. Countries should especially consider legislation efforts against spam, identity theft, criminalization of preparatory acts prior to attempted acts, and massive and coordinated cyber attacks against the operation of critical information infrastructure.

A few members wished to delete the first sentence referring to the need for supplementing Articles in the Convention.

1.8. Countries should consider how to address data espionage and steps to prevent pornography being made available to minors.

One member considered that the term "data espionage" is ambiguous, and should be defined properly, whilst another member wished to remove this term. Two members wished to delete this recommendation.

1.9. The introduction of new technologies always presents an initial challenge for law enforcement. For example, VoIP and other new technologies may be a challenge for law enforcement in the future. It is important that law enforcement, government, the VoIP industry and ICT community consider ways to work together to ensure that law enforcement has the tools it needs to protect the public from criminal activity.

1.9.a. Given the responsibility of government authorities in protecting their consumers, special attention should be given to requirements enacted by government authorities that bear directly on the infrastructure-based and operational requirements imposed on those who provide and operate network infrastructures and services, or supply the equipment and software, or end-users. The concept of shared responsibilities and responsible partnership should be underscored in the development of legal measures on cybersecurity obligations in civil matters. A coordinated approach between all parties is necessary to

develop agreements, as well as provide civil remedies in the form of judicial orders for action or monetary compensation instituted by legal systems when harm occurs.

Two members wished to delete this recommendation. Some members wished to replace the specific references to VoIP with more general text recognizing that the introduction of a broad range of new technologies presents initial challenges for law enforcement. One member supported reference to "government, industry and ICT community", whilst another wished to make more general reference to "all relevant parties" [who] "should work together to ensure that law enforcement has the tools, resources and training needed". One member proposed the specific insertion of the additional text in 1.9(a).

1.10 Implementation of a data retention approach is one approach to avoid the difficulties of getting access to traffic data before they are deleted, and countries should carefully consider adopting such procedural legislation.

Two members wished to delete this recommendation. Another member proposed the alternative text: "the implementation of a data preservation approach has proven to be a key resource to law enforcement in investigations. Development of a balanced and reasonable data retention requirement should be carefully examined, taking into account expectations of privacy, security risks, etc., when considering adopting such procedural legislation".

1.11 In the fight against terrorist misuse of the Internet and related ICTs, countries should complete their ratification of the *Convention on the Prevention of Terrorism of 2005*. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. Article 5 on public provocation to commit a terrorist offence, Article 6 on recruitment for terrorism, and Article 7 on training for terrorism are especially important. In addition, the *Convention on Cybercrime* has been studied with relation to terrorist misuse of the Internet and has been found to be important for defense against it.

One member wished to delete the last sentence.

1.12 Given the ever-changing nature of ICTs, it is challenging for law enforcement in most parts of the world to keep up with criminals in their constant efforts to exploit technology for personal and illegal gains. With this in mind, it is critical that police work closely with government and other elements of the criminal justice system, Interpol and other international organizations, the public at large, the private sector and non-governmental organizations to ensure the most comprehensive approach to addressing the problem.

General consensus was achieved in respect of this recommendation.

1.13 There are several challenges facing prosecutors today in order to successfully prosecute cybercrime cases. These challenges include: 1) implementation of relevant cybercrime legislation; 2) understanding the technical evidence; 3) collecting evidence abroad; and 4) being able to extradite suspects located abroad. Thus, international coordination and cooperation are necessary in prosecuting cybercrime and require innovation by international organizations and governments, in order to meet this serious challenge. The *Convention on Cybercrime* Articles 23-25 address basic requirements for international cooperation in cybercrime cases.

One member wished to delete the last sentence, while several other members wished to extend the reference to the Articles mentioned, with the replacement of Article 25 with 35.

1.14 In conducting cybercrime investigation and prosecution, countries should ensure that their procedural elements include measures that preserve the fundamental rights to privacy and human rights, consistent with their obligations under international human rights law. Preventive measures, investigation, prosecution and trial must be based on the rule of law, and be under judicial control.

General consensus was achieved in respect of this recommendation.

The ITU, as the sole Facilitator for WSIS Action Line C5, should organize a global conference with the participation of [ITU Membership] for Members, regional and [international] organizations on cybersecurity and [relevant private organizations] in cybercrime. Participating organizations include, but are not limited to: INTERPOL, United Nations Office on Drugs and Crime (UNODC), G 8 Group of States, Council of Europe, Organization of American States (OAS), Asia Pacific Economic Cooperation (APEC), The Arab League, The African Union, The Organization for Economic Cooperation and Development (OECD), The Commonwealth, European Union, Association of South East Asian Nations (ASEAN), NATO and the Shanghai Cooperation Organization (SCO).

Many members supported the recommendation of a global conference to promote cybersecurity, whilst other members wished to remove this recommendation – one member voiced its strong opposition to this. One member emphasized that ITU conferences should be open in its membership, especially to developing countries, whilst another underlined the importance of ITU remaining open to collaboration. Several members included reference to ITU's mandate as Facilitator for WSIS Action Line C5 and proposed insertions in square brackets refining the scope of the stakeholders involved.