RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF JURIDICAL SCIENCES

COURSE:BA.LL.B

Semester : VIII th

SUBJECT: Cyber Law

SUBJECT CODE:BAL-805

NAME OF FACULTY: Dr.Puja Paul Srivastava

RAMA UNIVERSITY

Lecture-27

- **LECTURE 27:** Cyber crimes under International law,

Introduction

Traditionally, crime and punishment are largely local, regional, or national. Today, many differences confronting us are associated with the transnational character of cybercrimes. It is therefore important to have international legal instruments ready to serve anti-crime efforts.

This article looks at international harmonizing efforts to fortify the legal battle against cybercrime, categorizing the actions into four aspects: professional law-enforcement efforts, regional efforts, multi-national efforts, and global international efforts. Subsequently, the article also categorizes the international actions according to the subject-matters into additional aspects, including the promotion of security awareness at both international and national levels, the harmonization of legislation, coordination and cooperation between law-enforcement agencies, and direct anti-cybercrime actions. The article will also examine the nations' attitudes toward the Convention on Cybercrime. Based on the analysis, the article will briefly evaluate the effectiveness of previous attempt at international harmonization.

From domestic legislation to international harmonization

People usually are impressed by the illusory overlap between Internet space and international space. Notwithstanding the fact that information systems are linking continents, islands, residents and communities into a giant virtual network, states and areas preserve their traditional sovereignty. McConnell International's metaphor (2000, p. 8) said that: "In the networked world, no island is an island." At this turning point, the globally connected Internet has made cybercrime a trans-border problem. The "international dimension" (Wasik, 1991, pp. 187-201), "trans-national dimension" (Sofaer & Goodman, 2005) or "global dimension" (Grabosky, 2004, pp. 146-157) of cybercrime is universally perceived. While law is always territory-based, the tool, the scene, the target, and the subject of cybercrime are all boundary-independent. Domestic measures will certainly be of critical importance but not sufficient for meeting this worldwide challenge. International coordination and cooperation are necessary in fighting offences commonly prohibited by every country.

Many international organizations have been making efforts to harmonize actions within their forums. Many authors have also been pursuing research on international harmonization from different standpoints and for different goals; for example, Sieber (1996, 1998), United Nations Crime and Justice Information Network (UNCJIN, 1999), Police Commissioners' Conference Electronic Crime Working Party (2000), Sofaer et al. (2000), Putnam and Elliott (2001), Schjølberg & Hubbard (2005), and so on. Although information about the basic facts of international harmonization that these research studies deal with is the same, different knowledge can

be drawn from different thinking. For the purpose of convenient summarization within this article, we categorize the international harmonization actions into the following groups: professional organizations, regional organizations, multi-national organizations, and global organizations. Many other valuable international actions have simply not been considered due to the limit of this study (it is hardly possible to assume that studies on cybercrime can cover all useful international actions of international organizations at all levels).

Professional efforts of International Criminal Police Organization (Interpol)

Many international organizations qualify for professional organizations, because their goals and activities are focused on certain specific issues; these organizations include Interpol, the International Telecommunications Union, etc. However, professional efforts here primarily mean substantial actions in the field of cybersecurity protection and cybercrime prevention. Although some other organizations also greatly contribute to coordinating cybersecurity protection, their emphasis is not necessarily on the law. By this standard, this section only analyzes the actions of the International Criminal Police Organization (Interpol).[1]

As an international law-enforcement organization with 184 members, Interpol started to tackle computer crime very early, coordinating law-enforcement agencies and legislations, in regard to which Interpol made efforts to improve counter-cybercrime capacity at the international level. A 1981 survey of members on cybercriminal law recognized dilemmas in application of existing legislation (Schjølberg & Tingrett, 2004). Based on the recognition of the legal gaps between countries, and gaps between the legal framework and criminal phenomena, Interpol expanded its task to both law enforcement and legal harmonization.

Currently, there are four working parties within the framework of Interpol, comprising African, American, Asia-South Pacific and European Working Parties on Information Technology Crime. Besides these groups, a Steering Committee for Information Technology Crime was established in order to harmonize the different regional working-party initiatives.[2] Considering the already-harmonized legislation as the prerequisite for the coordinated law enforcement, the African Working Party agreed upon "the project on legislation and comparative law existing in the Africa with a view to having more African states co-signing and/or ratifying the Council of Europe Cybercrime Convention."[3] Apparently, legal harmonization is one of Interpol's important tasks in working towards an effective law-enforcement environment.

In regard to law enforcement, Interpol has provided a technical guidance in cybercrime detection, investigation and evidence collection. The Interpol Information Technology Crime Investigation Manual was compiled by the European Working Party on Information Technology Crime.[4] Compared with the substantive and procedural law harmonization of today's Convention on Cybercrime, the Manual developed a technological law-enforcement model to improve the efficiency of combating cybercrime.

Along with efforts in law enforcement on cybercrime, Interpol also takes distinct actions to prevent cybercrime, cooperating with credit-card companies to combat payment fraud by building a database on Interpol's web site (Police Commissioners' Conference Electronic Crime Working Party, 2000, p. 64). As one of the necessary cooperation projects at the international level of law-enforcement, cybercrime and other trans-border crimes are specially dealt with by Interpol in gathering and sharing information. In addition, Interpol is making efforts to establish a network to for harvesting information relating to activities on the Internet.[5]

Regional efforts

There are many regional international organizations, with a narrow or broad coverage of states, more or less making efforts to maintain cybersecurity and harmonize international measures to combat cybercrime. This section will introduce only four of these organizations, which have taken typical actions in combating cybercrime.

(i) The Asia-Pacific Economic Cooperation (APEC)

In the Asia-Pacific region, the APEC coordinates its 21 member economies to promote cybersecurity and to tackle the risks brought about by cybercrime (APEC, 2003). The APEC has conducted a capacity-building project on cybercrime for member economies in relation to legal structures and investigative abilities, where the advanced APEC economies support other member-economies in training legislative and investigative personnel.[6]

After the 9/11 attacks on the U. S., the APEC Leaders issued a Statement on Counter-Terrorism, condemning terrorist attacks and considering it urgent to reinforce collaboration at different layers to fight against terrorism. The Leaders called for reinforcing APEC activities to protect critical infrastructure.[7]

The Telecommunications and Information Ministers of the APEC economies issued the Statement on the Security of Information and Communications Infrastructures and a Programme of Action in 2002,[8] supporting measures taken by members to fight against misuse of information. The Senior Officials' Meeting has made a recommendation which designates six areas that can serve as the foundation for the APEC's endeavor for cybercrime prevention, comprising legal development, information sharing and cooperation, security and technical guidelines, public awareness, training and education, and wireless security.[9] The Ministers and Leaders of APEC have made a commitment 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 the UN General Assembly Resolution 55/63 and Convention on Cybercrime by October 2003."[10]

In response to this call from the leaders, a survey of laws was carried out and a summary was made of the responses from member economies received in 2003 (see E-Security Task Group, 2003). The economies proposed corresponding projects in information-security task groups. For example, the U.S. proposed a project in the E-Security Task Group of the Telecommunications and Information Working Group. The first phase of this project was a meeting of cybercrime experts from around the region. The meeting was

held from 21-25 July, 2003 in Bangkok, Thailand, and was attended by over 120 delegates from 17 economies. The objectives of the meeting were to assist the economies to develop the necessary legal frameworks; to promote the development of law-enforcement capacity; and to strengthen cooperation between private and public sectors in addressing the threat of cybercrime.[11] In the conference, the experts present agreed that every economy needed a legal framework including one for substantive and procedural law, and for the law and policies of inter-economies cooperation. They confirmed the role of international instruments, particularly the Convention on Cybercrime. They also emphasized jurisdictional cooperation, law-enforcement construction, and the capacity building of the investigators.[12]

In 2005, The sixth APEC Ministerial Meeting on the Telecommunications and Information Industry passed the Lima Declaration, "encouraging all economies to study the Convention on Cybercrime (2001) and to endeavor to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with international legal instruments, including UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001)."[13] However, due to the great difference between member economies within the APEC, the development toward unified legal instruments has not been too satisfactory. Although some economies have claimed that their laws have been completely consistent with the Convention, and some other economies were taking actions to implement provisions similar to the Convention, many other countries have quite different legal systems or have no law criminalizing cybercrime.

Efforts are still to be made in the forum of the APEC to address cybercrime. The U.S. proposed the Judge and Prosecutor Cybercrime Capacity Building Project in 2006 in order to develop a curriculum devised by government and private sector experts; to translate the curriculum into domestic languages; and to train the trainer (judges and prosecutors).[14]

(ii) The Council of Europe (COE)

The Council of Europe has been working to tackle rising international anxiety over the risks brought about by the automatic processing of personal data since the early 1980s.[15] In 1981, the Council of Europe implemented the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108, 26 January 1981), which was revised according to the Amendment to Convention ETS No. 108 Allowing the European Community to Accede, 15 June 1999, and the Additional Protocol to Convention ETS No. 108 on Supervisory Authorities and Trans-border Data Flows, 8 June 2000. The Convention recognized the desirability "to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing," and the necessity "to reconcile the fundamental values of the respect to privacy and the free flow of information between peoples" (Preamble). The Convention covers the protection of personal data in both the public and private sectors.

Chapter II of the Convention established basic principles for data protection, one of which is data security (Article 7), covering the prohibition of accidental or unauthorized access, alteration and dissemination.

The expert committee appointed in 1985 published Recommendations of 1989 and 1995, addressing the issues of substantive laws and procedural law in this area respectively (See Recommendation No. R. (95) 13).

Recommendation R. No. (89) 9 recognized the importance of an adequate and quick response to the new challenge of computer-related crime, which often has a trans-border character, and recommended the governments to consider the Report on Computer-Related Crime drawn up by the European Committee on Crime Problems.

Then there is Recommendation No. (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology. The Recommendation recognized that information systems may also be used for committing criminal offences, evidence of criminal offences may be stored and transferred by these systems, while the criminal procedure law of member states often do not provide for appropriate powers to search and collect evidence in these systems during a criminal investigation. The appendix to the Recommendation lays down the principles for criminal procedure laws on search and seize, technical surveillance, obligations to co-operate with the investigating authorities, electronic evidence, use of encryption in research, statistics and training, and international cooperation.

In 1997, the Council of Europe began drafting the Convention on Cybercrime, which was open for signature in 2001 and took effect in 2004.[16] In 2003, the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer System (ETS NO. 189) was implemented. The Convention addresses substantive law, procedural law, jurisdiction, and international law in the field of cybercrime. The Convention is a historic landmark in the combat against cybercrime. It is expected that the Convention will have a deep impact on the legal reform relating to cybercrime in its 46 member states and one candidate state.

In the 2004 Conference on Cybercrime, the Council of Europe called for "wide and rapid" access to and "effective implementation" of the Convention on Cybercrime, raising awareness in the highest political level, and encouraging cooperation between public and private sectors.[17]

In the 2005 Conference on Cybercrime, the Council of Europe expressed concern about the fast-increasing threats and serious social and economic results of cybercrime including terrorist activity on the Internet, noting that most cybercrime is international cybercrime, recognized the need for effective and compatible laws and tools to enable efficient cooperation to combat cybercrime, calling upon public and private cooperation, and encouraging access to the Convention on Cybercrime.[18]

In 2006, the Council of Europe launched a Project against Cybercrime, intended to grant assistance to the development of national legislation in line with the provision of the

Convention, training of judges, prosecutors and law-enforcement officers, and training of criminal justice officials and 24/5 contact points in international cooperation.

(iii) The European Union

The EU took a series of actions to tackle cybercrime through impelling a coordinated law enforcement and legal harmonization policy. Civil liberty has also been a focus in the anti-cybercrime field.

In 1995, the European Parliament and the Council endorsed Directive 95/46/EC of 24 October 1995 on the protection of Individuals with regard to the Processing of Personal Data and on the Movement of Such Data. Section VIII of the Directive specifically deals with confidentiality and security of processing of personal data. The Directive applied to protection of natural persons (Article 2(a)). The scope of the Directive was limited to the processing of personal data entirely or partially by automatic means (Article 3-1). The Directive required that appropriate technical and organizational measures have to be implemented to protect personal data against illegal destruction, alteration, access and other illegal forms of processing (Article 17-1).

The Directive required the Member States to provide administrative and judicial remedies for the victim (Article 22), and provided for the compensation liability of (Article 23) and sanctions on (Article 24) the transgressor.

In 1997, the European Parliament and the Council endorsed Directive 97/66/EC of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. The Directive was aimed at furthering the protection implemented in Directive 95/46/EC, and providing for the harmonization of the member states' provision to attain an equivalent level of protection (Article 1-1). The Directive extended the protection of legitimate interests to legal persons (Article 1-2).

The application scope of the Directive was limited to the processing of personal data relating to the provision of publicly available telecommunications services in the public telecommunications networks; particularly via the ISDN (Integrated Services Digital Network), and public digital mobile networks (Article 3-1). As the Directive 95/46/EC is concerned with automatic processing systems, Directive 97/66/EC has emphasized the linkage with the telecommunications network. The Directive provides requirements directly targeted at the service providers (but not member states) "to take appropriate technical and organizational measures to safeguard the security of its services." (Article 4-1). The Directive requires the Member States to implement the regulations ensuring the confidentiality of communications, prohibiting listening, tapping, storage or other kinds of interception or surveillance of communications by unauthorized natural and legal persons (Article 5). The Directive limited unsolicited communications (Article 12), which covers automatic calling systems or facsimile machines, but not e-mails.

On 27 November 2001, a plenary session took place in Brussels of the EU Forum on Cybercrime, organized by the EC,[19] and where the primary discussion was about the retention of traffic data (EU Forum on Cybercrime, 2001).

In April 2002, the Commission of the European Communities presented a proposal for a Council Framework Decision on Attacks against information systems, and this proposal constitutes the case of the Decision of 24 February 2005.[20] The Framework Decision criminalized the offences of illegal access to information systems (Article 2), illegal system interference (Article 3), illegal data interference (Article 4), and instigation, aiding and abetting of these offences or attempt at them (Article 5). The Framework Decision only dealt with attacks through unauthorized access to or interference with information systems or data. According to the Decision, illegal access can only be constituted when the illegal activities are targeted intentionally against an "information system with specific protection measures in place and [the attacks] must be for economic gain." (Article 2)

The Commission further considered the future possibility of "specific protection measures" (Proposal for a Council Framework Decision on Attacks against information systems) to broadband networks, saying that, "it is necessary that criminal law covers unauthorized access to their systems even though there may not be adequate technical protection for their systems." (ibid.) Thus, concerning the interference with information systems, it is constituted by serious "hindering" or "interrupting" of the functioning of information systems by "inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data" (Article 3).

This Framework Decision does not specify penalties for illegal access to information systems and instigation, aiding and abetting and attempting of these offences, but requires member states to take the necessary measures to ensure that they are punishable by effective, proportional and dissuasive criminal penalties (Framework Decision, Article 6.1). The Decision specifies the penalties for illegal system interference and illegal data interference as punishable by criminal penalties to a maximum of at least one to three years of imprisonment (Article 6.2). As for the "aggravating circumstances", the criminal draws a maximum of at least two to five years imprisonment (Article 7.1). These aggravating circumstances include an organized attack, and an attack that has "caused serious damages or has affected essential interests" (Article 7.2). Criminal organization is defined as a "structured association, established over a period of time, of two or more persons, acting in a concerted manner with a view to committing offences."[21]

It is worth noting that the matters mentioned in the Framework Decision can also be found in the Convention on Cybercrime.[22] After revision of the legislation required by the Convention, the national law (of Finland) will also meet the demand of the Framework Decision.[23] Today, comprised of 27 member states and three candidate countries, the EU remains active in addressing cybercrime.

(iv) The Organization of American States (OAS)

As other regional organizations, the Organization of American States (OAS) with 35 member states is also highly concerned about the issue of cybercrime. Through its forum for the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA), the OAS has long recognized the central role that a sound legal framework plays in combating cybercrime and protecting the Internet. Such recognition has prompted the REMJA to recommend the creation of the Group of Governmental Experts on

Cybercrime (The Group of Experts) in March 1999.[24] The Group of Experts has been devoted to analyzing cybercrimes, to inspecting the domestic cybercrime law, and to finding ways of cooperating in the Inter-American system of combating cybercrime. The Group of Experts has held four meetings.[25]

The Meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA III)[26] has urged member states to take steps to endorse cybercrime law; harmonize cybercrime laws to make international cooperation possible. The Meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA V) [27] has recommended that member states evaluate the advisability of implementing the principles of the Convention on Cybercrime, and consider the possibility of acceding to that Convention.

In 2004, the Fourth Plenary Session of the Organization of American States General Assembly passed the resolution on "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity," proposing that "An effective cybersecurity strategy must recognize that the security of the network of information systems that comprise the Internet requires a partnership between government and industry."[28]

Multi-national efforts

Unlike professional organizations that are limited to a more specific field of concern, and unlike regional organizations that are limited to a more specific location of states, the multi-national international organizations care for affairs of a broader range and take actions in a broader territorial environment. This section recounts the efforts of three of the multi-national organizations.

(i) The Commonwealth of Nations

The Commonwealth of Nations took a direct and timely action in the harmonizing laws of its member states. In October 2002, the Commonwealth Secretariat prepared the "Model Law on Computer and Computer Related Crime" (Bourne, 2002, p. 17). Within the Commonwealth's 53 member countries, the "Model Law" has had a wide influence on domestic legislation. Through this model law, the Convention on Cybercrime has become one of the legislative choices in substantive criminal law, covering the offences of illegal access, interfering with data, interfering with computer systems, illegal interception of data, illegal data, and child pornography.

Compared with the Convention on Cybercrime, the Model Law expanded criminal liability - so as to include reckless liability- for the offences of interfering with data, interfering with computer systems, and using illegal devices. The Model Law also covered the problem of dual criminality by stating that the act applied to an act done or an omission made by a national of a state outside its territory, if the person's conduct would also constitute an offence under a law of the country where the offence was committed. This may lead to prosecution or extradition based on dual criminality, but not extradition as it is provided in the Convention on Cybercrime.[29]

Some of the member countries of the Commonwealth have made efforts to draft domestic law according to the model law, such as Bahamas and St. Lucia.[30] In Barbados, Belize, and Guyana, the Model Law is being considered as a guide to the enactment of similar legislation.[31] However, in many other countries of the Commonwealth, there is still no special legislation for cybercrime.[32]

Besides impelling legislation within the forum, another focus of the Commonwealth is on mutual assistance in law enforcement between Commonwealth member states and between Commonwealth member states and non-Commonwealth states. In the 2005 Meeting of Commonwealth Law Ministers and Senior Officials, the Expert Working Group proposed 10 recommendations for member states to adopt suitable measures for improving domestic law enforcement and trans-national assistance, and encouraged member states to sign, ratify, accede to and implement the Convention on Cybercrime as a basis for mutual legal assistance between Commonwealth member states and non-Commonwealth states.[33]

(ii) The Group of Eight (G8)

Since the mid-1990s, the Group of Eight (G8) has created working groups and issued a series of communiqués from the leaders and actions plans from justice ministers. At the Halifax Summit 1995, the Group of Seven recognized "that ultimate success requires all governments to provide for effective measures to prevent the laundering of proceeds from serious crimes, to implement commitments in the fight against trans-national organized crime."[34] The group released 40-point set of "recommendations to combat Trans-national Organized Crime efficiently" at the G7/P8 Lyon Summit. The recommendations urged the states to increase the level of criminalization, prosecution, investigation, and international cooperation, while acknowledging in their entirety human-rights protection.[35]

At the Denver Summit 1997, the Group of Eight proposed to strengthen their efforts to realize the Lyon recommendations, by concentrating on punishing high-tech criminals, and promoting the governments' technical and legal abilities to react to trans-territorial computer crimes.[36] The Group of Eight Meeting of the Justice and Interior Ministers of December 1997 responded to the increased international movement of criminals, organized crime, and terrorists and their use of the ICT.[37] Ministers noted, in a Statement of Principles Concerning Electronic Crime, that, while criminal legislation was a national responsibility, the character of the information networks obstructed countries from operating traditional power over this problem. Domestic legislations have to be complemented by international cooperation to criminalize the abuse of the networks and harmonize the investigative action.[38]

At the subsequent summits, the Group of Eight repeatedly expressed their concern about cybercriminality. At the Okinawa Summit, the Okinawa Charter on Global Information Society adopted the principle of international collaboration and harmonization of cybercrime. "In order to maximize the social and economic benefits of the information society", the Group of Eight agreed on principles and approaches for the protection of privacy, the free flow of information, and the security of transactions.[39] The Charter

recognized that the security of the information society necessitated coordinated action and effective policy responses.[40]

(iii) The Organization for Economic Cooperation and Development (OECD)

With its 30 member countries, the OECD addressed computer security for several decades. In 1983, an expert committee was appointed by the OECD to discuss computer crime phenomena and criminal-law reform (Schjolberg & Hubbard, 2005). Offences against confidentiality, integrity or availability listed in the 1985 OECD document included unauthorized access, damage to computer data or computer programmes, computer sabotage, unauthorized interception, and computer espionage.[41] In December 1999, the OECD officially approved the *Guidelines for Consumer Protection in the Context of Electronic Commerce* (Department of Justice, 2000, p. 27), representing member states' consensus in the area of consumer protection for e-commerce: consumers should be protected in e-commerce not less than the protection they enjoyed within traditional commerce (Department of Justice, 2000, p. 27). The OECD adopted Guidelines for the Security of Information Systems and Networks in July 2002, calling on member governments to "establish a heightened priority for security planning and management", and to "promote a culture of security among all participants as a means of protecting information systems and networks" (OECD, 2002a, Part I).

The guidelines established nine principles, including awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment (OECD, 2002a, Part III). Because of the nature of the guidelines and the distance from the legal actions, practical endeavors were left to the member countries to make.

Global international efforts by the United Nations (UN)

There are numerous global organizations. Nevertheless, the UN is capable of being identified as the only global organization that forms a forum of its 191 member states with fuller functions. Compared with professional organizations, the UN does not limit its activities to certain domains. Compared with regional organizations, the UN does not limit its activities to certain states (in the field of cybersecurity protection and cybercrime prevention). The actions of the UN have unique advantages in coordinating international positions.

In 1985, General Assembly Resolution 40/71 of 11 December called upon governments and international organizations to take action in conformity with the recommendation of the commission on the legal value of computer records of 1985, in order to ensure legal security in the background of the broadest possible use of information processing in international transactions.[42]

In 1990, the General Assembly of the UN adopted the Guidelines Concerning Computerized Personal Data Files. It proposed to take appropriate measures to protect the

files against both natural and artificial dangers. The guidelines extended the protection of governmental international organizations (Part B).

"*The International Review of Criminal Policy: United Nations Manual on the Prevention and Control of Computer-related Crime*" called for further international work and presented a proper statement of the problem. It stated that at the international level, further activities could be undertaken, including harmonizing substantive law, and establishing a jurisdictional base.[43]

The Background Paper for the Workshop on Crimes Relating to the Computer Network at the Tenth UN Congress on Prevention of Crime and Treatment of Offenders proposed two levels of definition of cybercrime: In the narrow sense, that is, the strict computer crime, had to refer to "any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them." In the broad sense, that is, computer-related crime denoted "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distribution information by means of a computer system or network."[44]

The UN General Assembly has endorsed several resolutions dealing with its desire to witness progress regarding this issue. According to information provided by Schjølberg and Hubbard (2005), checking Resolutions 55/63 (2000) and 56/121 (2001) on Combating the Criminal Misuse of Information Technology, the value of the Group of Eight Principles was noted, and states were urged to consider these principles; checking Resolutions 53/70 (1998), 54/79 (1999), 55/28 (2000), 56/19 (2001), 57/53 (2002), 57/239 (2002), 58/32 (2003), and 58/199 (2003), all calling on member states "to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats."[45] These resolutions have the same motive to improve the cybersecurity awareness at both the international and the national levels.

In Resolution 55/63, the General Assembly noted the value of the following measures to combat computer misuse:

a. To ensure the elimination of safe havens for cybercriminals;
b. To coordinate cooperation in the investigation and prosecution of cybercrime;
c. To exchange information for fighting cybercrime;
d. To train and equip law-enforcement personnel to address cybercrime;
e. To protect the security of data and computer systems from cybercrime;
f. To permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;
g. To ensure mutual assistance regimes for the timely investigation of cybercrime and the timely gathering and exchange of evidence;
h. To remind the general public of the requirement to prevent and combat cybercrime;
i. To design information technologies to help to prevent and detect cybercrime;
j. To take into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight cybercrime.

The General Assembly invited states to consider the measures in their endeavor to fight the criminal misuse of information systems, and decided to maintain the question of the criminal misuse of information technologies on the agenda of its future session.

In Resolution 56/121, the General Assembly invited states to consider the work and achievements of the Commission on Crime Prevention and Criminal Justice and of their international and regional organizations when developing national law, policy and practice to prevent cybercrime.

The resolution emphasized the value of the measures set forth in Resolution 55/63, and again invited states to take them into account in their efforts to combat the criminal misuse of information technologies. However, the General Assembly decided to postpone consideration of this subject, pending work considered in the plan of action against high-technology crime of the Commission on Crime Prevention and Criminal Justice.

It is necessary to mention that, besides the advantages, the disadvantages of the UN's actions are also striking. The UN is a multifunctional international organization, which in some sense has malfunctioned over the years. Focusing on the current topic, it can be said that the consensus on cybercrime in this forum remains a preliminary one. The diversified legal systems of members of this gigantic organization hinder the conclusion of a fruitful agreement.

The focuses of international harmonization

From the above presentation on international actions in anti-cybercrime areas, we can further summarize the major themes of these international organizations. These aspects mainly include the promotion of security awareness at both the international and national levels, the harmonization of legislation, coordination and cooperation in law enforcement, and direct anti-cybercrime actions.

(i) Promotion of security awareness at the international level

The typical actions in this aspect have been taken by the UN. The UN's two Resolutions (55/63 (2000) and 56/121 (2001)) on Combating the Criminal Misuse of Information Technology recalled the importance of the Group of Eight principles, and urged states to take these principles into account. Some other resolutions also called on member states to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as promising measures to limit these threats. Other international organizations also made efforts to promote security awareness at the international level. For example, after the 9/11 incidents, the APEC Leaders called for a reinforcing of APEC activities to protect critical infrastructure.

(ii) Promotion of security awareness at the state level

All international organizations have made efforts to promote security awareness at the domestic level. For example, the APEC guided its member states and regions to promote cybersecurity and tackle the threats of cybercrime. The APEC also conducted a project for

developed states to support other states in training personnel. The Shanghai Declaration of 2002 supported measures to fight against misuse of information.

(iii) Harmonization of legislation

Legal harmonization has been a major emphasis on the work of various international organizations. Harmonization in Europe started in the 1980s and a recent achievement was the Convention on Cybercrime. Other international organizations have also endeavored to attain legal harmonization. Early in 1981, Interpol surveyed the criminal laws of member states so as to explore defects in the existing legislation, and made efforts to harmonize the laws. Today, Interpol's African Working Party on Information Technology Crime Projects is trying to persuade the African states to sign and ratify the Convention on Cybercrime. APEC also took steps to survey the laws and to encourage economies to enact comprehensive laws consistent with the Convention on Cybercrime and the pertinent UN resolutions. The EU Framework Decision of 2002 specifically granted the member states the responsibility of criminalizing the offences of illegal access to and illegal interference with information systems. The REMJA urged states to criminalize cybercrime and harmonize the member states' laws, and consider the possibility of joining the Convention on Cybercrime. The Commonwealth Model Law on Computer and Computer Related Crime expanded the criminal liability of the Convention on Cybercrime so as to include reckless liability. Through this Model Law, the Commonwealth made efforts to criminalize cybercrime in the member countries. The Group of Eight Paris Conference discussed the public and private interact with the objective of implementing an international penal code for fighting cybercriminality. The Okinawa Charter on Global Information Society further consented to international collaboration and harmonization concerning cybercrime.

(iv) Coordination and cooperation in law enforcement

Interpol's European Working Party on Information Technology Crime compiled the Computer Crime manual to provide technical guidance in law enforcement. The Convention on Cybercrime also covers cooperative mechanisms in law enforcement against cybercrime. The EU discussed about the retention of traffic data in 2001. The Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA)'s Group of Experts on Cybercrime have been devoted to discover cooperation ways in the Inter-American system to combat cybercrime. The Group of Eight reviewed existing cooperation mechanisms and gaps, and made attempt to discover ways to fill these gaps. The Group urged the states to increase criminalization, prosecution, investigation, and international cooperation. The Denver Summit proposed to promote governments' technical as well as legal abilities to act in response to trans-territorial computer crimes. The Birmingham Summit called for agreement on a legal framework for evidence preservation and protection of privacy, and for agreements on the international sharing of evidence so as to struggle more effectively against a broad scope of crimes, including cybercrime.

(v) Direct anti-cybercrime actions

The direct international anti-cybercrime actions comprise two fundamental aspects: cybercrime prevention and cybercrime investigation. They have been more valuable before international harmonization in legislation could come into being. Different organizations have taken individual measures with specific emphases. For example, Interpol directly cooperated with credit-card companies to fight against payment fraud. The OECD's *Guidelines for Consumer Protection in the Context of Electronic Commerce* 1999 emphasized the protection of consumers in e-commerce as well as that in traditional commerce. Guidelines for the Security of Information Systems and Networks 2002 called on member governments to "establish a heightened priority for security planning and management", and to "promote a culture of security among all participants as a means of protecting information systems and networks".

From conversation to the European Convention

As one of the most outstanding achievements, international actions bred a comparatively effective implementation: the Convention on Cybercrime and its Protocol. The general purpose of the Convention is laid down in the Preamble as to deter crimes against the confidentiality, integrity and availability of information systems and the misuse of such systems. The purpose of the Protocol is to supplement the provisions of the Convention on cybercrime on the criminalization of acts of a racist and xenophobic nature committed through information systems (Protocol, Article 1).

The Convention has been widely accepted as a landmark, providing for both the substantive and procedural legal frameworks, both the domestic and international level of countermeasures, so as to achieve higher effectiveness in fighting against cybercrimes.[46]

Articles 2-12 of the Convention have required nations to criminalize the activities of illegal access to data and computer systems; illegal interception; data and systems interference; misuse of devices that can be used to enact the aforementioned crimes; computer-related forgery and fraud; content-related offences including child pornography; copyright crimes; and attempt, aiding or abetting. Article 13 of the Convention also establishes corporate liability, and sanctions and measures for these offences. Articles 3-7 of the Protocol requires nations to criminalize the activities of disseminating racist and xenophobic information through information systems. Also to be criminalized is racist and xenophobic motivated threat, racist and xenophobic insult, and in respect of genocide or crimes against humanity, denial of their existence, gross criminalistic approval or justification of them, and the behavior of aiding and abetting them.

The Convention provides two constituent elements for cybercrimes. First, the Convention establishes criminal liability on the subjective element of intent. Sometimes, the constitution of certain offences requires elements such as intent to procure "economic benefit" in computer-related fraud provided by Article 8. Second, the Convention establishes criminal liability on the objective element on act "without right" in all offence provisions.[47] The problems of what is an act committed intentionally, what is an act with right and without right, are all left to national law interpretation.

The Convention allows domestic laws to provide additional constituent elements, and provides the possibility of a reservation.[48] Apparently, the Convention fully respects the

decision-making of member states on the matter of criminal policy. As a result, we have good reason to worry that this diversified implementation will decrease the consensus on the harmfulness of conducts and increase the possible obstacles to international actions. The negative effect of this kind of provision is expected to diminish the effectiveness of prolonged expensive international negotiation for an agreement, although the provision itself is exactly one of the contents negotiated and agreed upon.

The Convention has also been criticized by civil liberties groups concerned that it will undermine individual privacy rights and that it expands too greatly surveillance powers, and is fundamentally unbalanced. As Taylor (2004) pointed out, the Convention contains comprehensive, far-reaching powers of surveillance, search, and seizure, while lacking a criterion for the protection of privacy and limitation of power.[49] The basic concerns in the field of human rights are the over-expansion of the states' power of surveillance, and over-criminalization of citizens' behavior. Before information systems have been completely developed, the states would strictly take this borderless system under control; those who use information systems would voluntarily enter the tight legal encirclement. For those who use information systems before these legal instruments, they are to accept externally imposed constraints; while for those who use information systems after these provisions, they are born into an inherent limitation. Both these two groups of users may feel a loss of freedom of information.

Despite the anxiety mentioned above, the Convention has unquestionably had some influence on the worldwide consensus in relation to the predicament of cybercrime. We are capable of seeing that the Convention will become one of the important steps towards a broader international accomplishment.

Firstly, some countries have taken practical measures to ratify the Convention. The total number of ratifications and accessions is 19 countries, including one non-member state of the Council of Europe, the U. S., with 24 countries (including three non-member states of the European Council, Canada, Japan and South Africa) having signed the Convention, not followed by ratifications.[50] The treaty has entered into force in only a small number of countries, representing a small proportion in terms of land area and population. However, it is still an important step towards a broader consensus: "A little is better than none."

Secondly, besides successful endeavors, countries, including most signatory countries, are still on their way to ratifying the treaty. The Council of Europe Conference on "Cybercrime: a Global Challenge, a Global Response" in 2005 "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 co-operation."[51] The treaty has come into force in some of the Nordic countries, including Denmark, Iceland, and Norway, but Finland and Sweden are still seeking ratification though they were both countries of signature on the date opening for signature in 2001.[52]

However, this process has proved hard without the expected number of countries ratifying in the five-year period after the Convention was open to signature. The pressure against not ratifying the treaty coming from inside the countries seems to be a greater obstacle

than the differences over the drafting of the document. A significant obstacle comes from the difference of legislative styles between the Convention and the individual countries. Many of the valid provisions in current Finnish law do not need revision.[53] Whether the original Finnish Penal Code (which includes quite a few revisions concerning offences relating to data processing) is capable of dealing with *all* of the offences provided by the Convention has not been tested in judicial practice. But the Finnish legislature will have to add some new provisions to the Penal Code, if it wants to cope with the Convention. Expressly, provisions concerning the offence of interference with and gross interference with the information processing systems, the offence of possession of instruments for cybercrime (covering the computer viruses), the liability for inchoate cybercrime, and for corporate liability, and so forth must be taken in.[54]

The critical challenge of the Convention on Cybercrime to conventional international legal cooperation lies in the absence of a demand for the double criminality criterion. Since this criterion is in decline, individual countries are far from implementing it in domestic law, either. In accepting the Convention, individual countries will therefore have to revise domestic laws in the relevant area.[55]

Some other countries are seeking to remodel the Convention so as to provide a prohibition on the types of conducts and to create procedural and international mechanisms for serving successful investigations and prosecutions of crimes. The flexibilities of the Convention may have a positive effect in leaving to member states the alternative of using different methods and languages in their domestic law. This may actually lead to a wider application of the Convention so as to cover more and diversified legal systems. While the U.S. has asserted that its own domestic law dos not need revision, South Africa has implemented substantial criminal provisions in line with the Convention. Japan is considering filling the gap between its domestic law and the Convention. At least, among the APEC economies, Taiwan, the Philippines, and Hong Kong are considering taking the Convention as the basis on which they will carry out their own legislative amendments.

Some international organizations are propelling cooperation in promoting the member states' access to the Convention. As mentioned above, in the framework of Interpol, the African Working Party on Information Technology Crimes is working to promote domestic legislation and adherence to the Convention. APEC, the EU, and the REMJA V of the OAS have also taken measures to spread the Convention to its member states.

There are also efforts to develop cybercrime legislation beyond the Convention. As mentioned above, the Commonwealth's model law represents a breakthrough in extending criminal liability to the *mens rea* of offences of interfering with data, interfering with computer systems, and illegal devices so as to include reckless liability. Some of the Commonwealth's member states are also on their way towards legislation that will model the Convention and model domestic law.

Finally, in fact, most countries, particularly countries where cybercriminals are usually left at large, have taken no action in spite of the importance of the Convention. These countries have very specific interests in maintaining what may be considered "criminal" in other countries but are "legal" in their own countries, as far as web sites, services, or even

sales of goods online are concerned. The potential cybercrime perpetrators, regardless of whichever nationality they belong to, also seek asylum in such countries in order to escape punishment by countries that are seeking to extend their judicial arms to deal with cases committed inside their sovereign territory and committed by their citizens outside their territory.

Although the Convention on Cybercrime has been attracting increasing attention at both the domestic and international levels, it is necessary to point out that, once the Convention was in documentary form, the enthusiasm and efforts of other international entities towards a higher degree of international harmonization of legislation have been to some extent weakened. This situation reflects neither the purpose, nor the intended side effect of the Convention. However, a ready instrument must have its negative influence on the otherwise unsettled disputes of the problems of cybercrime deterrence. Regrettably, both the advantages and disadvantages of the Convention will bring about a more cautious discussion and a better plan will be discouraged from being implemented. At least, the similar but different schedules for international treaties, in either broader or narrower scope, have seen an interruption with the passing of the Convention. The Convention thus becomes not only a mutual compromise of member states, but also a turning-point in the knowledge and experiences of cybercrime punishment and prevention.

Traditionally, new legal instruments have usually been the subject of academic annotation immediately after its implementation, while the legislature is usually reluctant to change existing legal instruments. These two factors further determine the unfortunate fate of the better and newer proposals, particularly proposals having more or less better elements than the implemented one. In a word, we can say that classics were good, but classics hinder better classics; consensus is good, but consensus always hinders better consensus: and the Convention is good, but it potentially hinders a better convention.

Although the Convention was also appraised by politicians, such as the U. S. President George W. Bush, as "providing for broad international cooperation in the form of extradition and mutual legal assistance", and containing "safeguards that protect civil liberties and other legitimate interests" (Bush, 2003), the effectiveness of the Convention's cooperative framework is subject to reasonable doubt without a majority of countries' access to the agreement (Goldsmith, 2005, p. 4). Authors such as Archick (2004) have proposed that the Convention's arm would not be long enough to reach the countries that are regarded as a "haven" for cybercriminals: attacks are launched from those countries, but the countries do not join the agreement. Consequently, the countries with law and without law, or being the member and being non-member of the Convention, have to encounter mutual conflicts. The situation confronting international society is obviously still one of the tardiness of the acceptance of existing instruments and the lack of a universal agreement.

The limited progress in the international harmonization

Over the years, the international co-operation on cybercrime "has been very active and comprehensive" (Pihlajamäki, 2004, p. 286). The international level of consensus on criminal law has, however, not been achieved. Previously, the criminalization of war

crimes, crime against peace, crimes against humanity, genocide, torture, and other crimes have been the successful examples. The application of pertinent agreements in specific courts has demonstrated that an international forum can acquire certain achievements prior to legislation at the national level. Traditional international criminal law has aimed at harmonizing substantive law and coordinating procedural law on offences that have existed in society since the coming into being of humankind.[56] Presently, what the countries are eager to realize is an international agreement on offences with a history of only several decades. The anxiety for success, the absence of trial practice, the lack of an accumulation of experience and knowledge, the alienation between the legislature and general public, and the different interests between the various countries, all deliver an international consensus in its lowest form. It is inevitable that during the drafting stage and particularly after the Convention on Cybercrime has been opened for signature, many commentators have published their evaluation and criticism.[57] Combined with other progress made in international harmonization, the most important unsolved problem may be the limited participation and the limited consensus.

Firstly, international harmonization has hitherto been primarily the forum of the developed countries. The working mechanism of an effective international treaty is for all of the signatory countries to take effective action and preserve a common theatre of operation. The treaty is not aimed at any third party and thus the third party is not restrained by it. The participating countries of the Convention on Cybercrime are limited, representing only a limited population. Along with the development of the Internet globally, the number of cybercrimes will be correlated with the population base of Internet penetration, and the global population base. Most of the present international harmonization measures have not been incorporating the countries with the largest population. This will make the measures less effective. Considering the characteristics of cybercrime, the "safe haven for criminals" can only be eliminated when almost all the sovereign states have access to one agreement and almost all the online users are subject to the power of law enforcement. Although an international document can be modeled by member states when making domestic laws, the expectations should not be raised too high in respect of a timely update at a similar pace when it comes to international measures.

Secondly, another limitation is that a lower level of consensus has been reached. Unlike traditional offences in international criminal law, which have rarely been penalized in domestic law, cybercrime was initially devised in the legislation at the national level. In many countries, domestic legislation on offences such as genocide, crime against peace and similar types of crime did not happen before the countries were subject to the obligation of international treaties. The situation of cybercrime is that countries that have already enacted laws assisted or forced the countries that have not enacted laws to enter a consensus. As a whole, international cooperation in preventing cybercrime is more sluggish than domestic legislation; its impact on domestic legislation is, nonetheless, undeniable. Domestic laws should be amended according to international instruments so that the measures provided in the international instruments can be effectively carried out. An agreement on a wider scope of issues in cybercrime is also necessary so as to ensure effective law enforcement. However, such an agreement is still lacking. The efforts of various international organizations should be integrated into a more unified action.

Thirdly, there is, strangely, a tendency towards pluralization on the international harmonization. In regulating or deregulating the information community, different interest groups stay at different standpoints. In criminalizing and decriminalizing the online activities, different players hold different opinions. Different organizations propose countermeasures for the benefit of a certain number of their member states. Yet other organizations oppose any kinds of plans for imposing constraints on the free use of information systems. The mechanism is that while one interest group is anxious about the misuse of information systems, another group may concentrate on the side-effect of anti-misuse actions. Various international harmonization measures are full of a trade-off of interests and a contrast of powers. This marathon process of negotiation has inherited the inherent style of international actions.

Fourthly, another tendency is the regularization of international harmonization. The effect of international harmonization is less significant compared with the efforts. The role of the UN as a universal international organization seems limited to arranging an international treaty in this area. If the United Nation's frequent "call" does not motivate member states to legislate on cybercrime, a universal agreement would be a better alternative in promoting consensus. The UN may have the opportunity to incorporate the consensus reached in other fields into the above-mentioned unified action.

Conclusion

Globalization does not mean globalized welfare at all. Globalized information systems accommodate an increasing number of trans-national offences. The network context of cybercrime makes it one of the most globalized offences of the present and the most modernized threats of the future. We can take actions in two different ways to resolve this problem. One is to divide information systems into segments bordered by state boundaries. The other is to incorporate the legal system into an integrated entity obliterating these state boundaries. Apparently, the first way is unrealistic. Although all ancient empires including Roman, Greece, and Mongolia became historical remnants, and giant empires are not prevalent in current world, the partition of information systems cannot be an imagined practice. Information systems become the unique empire without tangible territory.

Offences occurring in information systems are not likely to receive punishment from this system. Rather, they are punishable by the territory-based states that they cross. It is increasingly stringent and necessary to establish an international cooperation system for punishing cybercrime. Various international organizations have taken actions to resolve the problem in different forums and at different levels.

The Convention on Cybercrime is acknowledged as a landmark in the sphere of the international harmonization of cybercrime law.[58] However, apart from the fact that it represents a significant step forward, more states will have to sign the Convention and abide by its mandates in order to serve as a deterrent. International harmonization centered on the convention is obviously limited and must necessarily be extended to more participating member states with an even wider scope of issues. The final effect should be achieved only through a universal agreement on combating cybercrime. The UN may have

higher potential to implement such universal measures. However, we should not expect an instantaneous reaction from any of the international organizations, because not too much attention and interests of these international organizations are concentrated on the problem of crime or precisely, on cybercrime. While these organizations are devoted to dealing with the more important international affairs, threats against a critical information infrastructure will become more serious, until they are listed at the top of these organizations' schedule. Consequently, the development of an international level of consciousness and an international level call for a national level of consciousness are still the grounds for effective actions. The need is to reassess and renew as necessary the present international legal frameworks, offering a forum for broader international discussion expressing an outlook towards increasing and advancing international law-enforcement cooperation among the national authorities. This development should consider the influences of the novel and emerging issues in respect of international law-enforcement cooperation, with recommendations on capacity-building, which should show an equal concern for the situation in countries at different stages of development so as to avoid a futureless future of information chaos.

SELF-TEST QUESTIONS

S.NO	Question	Option (a)	Option (b)
1.			
2.			
3.			
4.			
5.			

Answers: 1-(),2-(), 3-(),4-(),5-()