THE RULE OF LAW IN THE GLOBAL VILLAGE

ISSUES OF SOVEREIGNTY AND UNIVERSALITY

SYPOSIUM ON THE OCCASION OF THE SIGNING OF THE
UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL
ORGANIZED CRIME

PANEL ON "THE CHALLENGE OF BORDERLESS CYBER-CRIME"

Introductory Remarks and
Concluding Remarks
by
The Moderator of the Panel

Mr. Hans Corell
Under-Secretary-General for Legal Affairs
The Legal Counsel of the United Nations

Palermo, Italy, Palazzo dei Normanni
14 December 2000

Introductory Remarks

Ladies and Gentlemen,

The topic given to the Fourth Panel at this symposium on The Rule of Law in the Global Village is: “The Challenge of Borderless Cyber-Crime”. I have been asked to be the Moderator of this Panel.

In a few moments, I will introduce our three distinguished panelists, Peter Grabosky, Tan Ken Hwee and Cormac Callanan, but before I do that, I would like to make a few introductory remarks – to set the scene, as it were.

In the invitation to this symposium it is said that eminent theorists will explore the utility of the *Rule of Law* concept as a possible framework for further harmonization of national laws while practitioners will relate the concept to particular areas of crime which are in urgent need of a global approach. This is also the explanation of the title of the symposium: *The Rule of Law in the Global Village*.

The three other panels have examined, respectively:

- The idea of Rule of Law;
- Towards Universal Jurisdiction: Promise or Threat? and
- Coping with Transnational Crimes: Need for a Common Response.

Allow me for the record to state that the idea of rule of law in international relations and at the national level has been the subject of much attention in the United Nations lately. The Secretary-General has addressed it in many of his statements over the past few years. Part of his Annual Report to the General Assembly this year is devoted to enhancement of the rule of law. In his Millennium Report “We the peoples: the role of the United Nations in the twenty-first century” there are several references to this concept.

Also, the General Assembly and the Security Council have addressed the topic. In order to translate fundamental values essential to international relations in the twenty-first century into actions, the Millennium Declaration, adopted by the Summit Meeting of the General Assembly on 8 September 2000, identified certain key objectives, including those in the legal field. Let me quote the following four elements:

- To strengthen respect for the rule of law in international as in national affairs and, in particular, to ensure compliance by Member States with the decisions of the International Court of Justice, in compliance with the Charter of the United Nations, in cases to which they are parties.

- To make the United Nations more effective in peaceful resolution of disputes.

- To ensure the implementation by States Parties of treaties in areas such as arms control and disarmament and of international humanitarian law and human rights law, and to consider signing and ratifying the Rome Statute of the International Criminal Court.

- To take concerted action against international terrorism, and to consider acceding, as soon as possible, to all the relevant international conventions.

In the Declaration, Member States also made the following pledge, followed by a number of detailed commitments (paragraphs 25 and 26):

« We will spare no effort to promote democracy and strenghten the rule of law, as well as respect for all internationally recognized human rights and fundamental freedoms, including the right to development. »

Let us now look at the concept we are to discuss : What do we mean by cyber crime?

First, we must note that there is no agreed definition of “cyber crime”, though experts do speak of “high-tech and computer-related crime”.

Cyber crime – and I am now referring to the material for the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in Vienna in April this year - is any crime capable of being committed in an electronic environment, where crime refers to behavior generally defined as illegal or likely to be criminalized (not all States criminalize the same acts). A cyber crime can be committed by means of a computer system or network, in a computer system or network or against a computer system or network.

Sometimes reference is made to subcategories of cyber crime.

They could be new crimes in a narrow sense: “computer crime”. This crime would be any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Examples of such crimes are:

- Hacking or gaining unauthorized access;
- Unauthorized use of computer systems;
- Computer vandalism.

Within this category there may be secondary or indirect offenses, such as preparation for the more serious offences: transferring computer passwords, encryption keys, access codes, etc.

Cyber crime could also be crimes in a broader sense, that is to say older crimes facilitated by new technologies: "computer-related crime". This crime would be any illegal behaviour committed by means of, or in relation to, a computer system or network. This would include such crimes as illegal possession and offering or distributing information by means of a computer system or network. Examples of such crimes are:

- Property and economic crimes (misdirecting funds or distorting financial data, extortion, manipulation of stock records, etc);
- Information or privacy-related crimes (access to protected databases, sale of information);
- Telecommunications crimes (avoiding charges, "wiretapping");
- Criminal communications (transmitting threats);
- "Offensive content" offenses;
- Gambling offenses.

In this context it should also be noted that telecommunications systems are grouped in the same category as computer systems and networks, possibly broadening the scope of the topic.

The question that we should ask now is: What are the problems posed?

First, we note that the scope of international cooperation is currently limited by international agreements and by the national law of the requested State.

There are also differing priorities between developed and developing countries. These differences complicate international cooperation and also expand the technological gap between the two groups. Lack of consultation with the developing countries might also pose additional problems when they are asked to adopt policies based on agreement among developed countries.

Just as when legislation on data protection was introduced in the late 1970's, there is a need to harmonize substantive criminal law to reduce "data havens", which allow criminals to carry out their activities in a State where the conduct is not criminalized.

Different legislation that criminalizes material relating to the incitement of hate or discrimination varies among States and poses problems in presenting a global policy.

Furthermore, dissemination of prohibited material presents a problem. This encompasses material that is illegal per se and material where the content is not necessarily illegal but becomes criminal under the circumstances of its distribution. The question is whether existing national laws apply to the new electronic environment.

In addition, data is sometimes stored, sometimes in a state of flow, posing difficulty in treating it legally as a tangible object.

Finally, Internet service-providers represent a particular problem. Generally, they are given the same treatment of telecom operators. This means that there is no legal obligation to monitor or block traffic on their computer systems. Questions arise, however, with respect to their possible civil liability and the extent to which they might be obliged to cooperate with law enforcement authorities.

Another area, where problems present themselves is criminal investigations. Such investigations go beyond cyber crime per se, because they might encompass cases where evidence needs to be secured in an electronic environment. Problems posed are:

- Limited availability of specialized computer crime units;
- Possible lack of powers to investigate the content of a computer system against the will of a right holder;
- Encryption policies: tension between those favoring law enforcement and crime control and those concerned about privacy and commercial interests;
- Legal concerns on distinctions between stored data and interception of data flowing through a network, since the latter are generally subject to stricter standards;
- Formal requirements vary among States regarding the use of electronic data as evidence (sound or images might not be admissible);
- Verification of authenticity of evidence.

Against this background you may ask: What is done by way of international cooperation?

Cyber crime is increasingly crossing national boundaries. But the question is: Is sufficient attention given to these transnational crimes? International police cooperation might be enhanced by international agreements. In 1997, the G-8 adopted a number of legal principles and a common action programme against “high-tech crime”. This included the establishment of a system of contact points

available 24 hours a day. Furthermore, INTERPOL has established working groups on information technology.

What about mutual legal assistance, you may ask?

Here several problems present themselves: lack of dual criminality (the acts may not necessarily be criminalized in the requested State); the law may not make available all powers that would be available if the matter was purely domestic; there could be time consuming formalities, which – even if they may be appropriate for regular cooperation – do not offer the necessary support for securing ephemeral evidence as in case of cyber crimes.

Difficulties might also arise when law enforcement activities may have extraterritorial effects. Examples are:

- Interception of data flowing between two other jurisdictions;
- Undercover operations might be legal under laws in one State, but not the others;
- Searching, copying and deleting data located in another State may constitute a criminal act in that other State and a violation of national sovereignty.

International cooperation can, however, be reinforced via harmonization of substantive criminal law provisions and attainment of international consensus on conditions under which activities with extraterritorial effects can be conducted.

This brings me to my last point in this context: What are the prospects for an international legal instrument in this particular field?

In view of the challenges that cyber crime poses to States and the peoples of the world, I think that it is fair to suggest that only a universal agreement would in the long run achieve practical results. If this is not attainable, there is the possibility of a model regulation or a non-binding instrument. The panelists will, I am sure, address this question.

Problems of a particular nature have come to the fore in negotiations limited to the G-8 and the Council of Europe. It has proven difficult for the members of these organs to agree on language to reconcile effective law enforcement powers with basic human rights protections.

Inextricably linked to international cooperation and international agreements is the question of universal jurisdiction.

This topic has been discussed in the Second Panel. But we are bound to touch upon it also in the present panel, and I have been asked specifically to

bring it to your attention in view of my work in relation to the international criminal tribunals.

The right of a State to exercise jurisdiction is determined in the first instance by international law. There are five principles of this law which are recognized by States to varying degrees as providing a basis for the exercise of criminal jurisdiction, namely: the territoriality principle, the nationality principle, the protective principle, the passive personality principle and the universality principle.

The principle of universal jurisdiction applies to “crimes under international law”. These crimes are of such exceptional gravity that they affect the fundamental interests of the international community as a whole. The conduct in question is prohibited and punishable as a matter of international law. The principle of universal jurisdiction authorizes all States to exercise their jurisdiction with respect to these crimes because of the strong interest of the international community in the deterrence, repression and punishment of these crimes.

However, there is no authoritative and comprehensive elaboration of the principle of universal jurisdiction. There are different views concerning the offences that constitute crimes under international law, which are subject to universal jurisdiction. There are also different opinions with respect to the significance of the obligation to prosecute or extradite contained in various treaties as evidence of universal jurisdiction. Whether States are not only permitted but also required to exercise jurisdiction with respect to crimes under international law is also subject to different opinions.

Let us, therefore, look at precedents concerning the exercise of universal jurisdiction.

The Nuremberg Tribunal referred to the making of the Nuremberg Charter as the exercise of the sovereign legislative power of the victorious countries as part of their right to legislate for the occupied territories. In contrast, the Commission of Experts on the former Yugoslavia referred to the Nuremberg Tribunal as an example of the possibility that States may vest their combined national jurisdiction under the universality principle in an international tribunal.

The Secretary-General’s report containing the draft Statute of the International Criminal Tribunal for the former Yugoslavia considered the legal basis for its establishment in relation to the powers of the Security Council rather than the principle of universal jurisdiction with respect to States.

In the negotiations leading to the adoption of the Rome Statute, some States argued for the exercise of jurisdiction by the International Criminal Court based on the universality principle. However, this was not acceptable to the majority of States. Consequently, the International Criminal Court can exercise jurisdiction

on the basis of either the territoriality principle or the nationality principle in accordance with article 12 of the Rome Statute. The referral of a situation to the Court by the Security Council is not subject to this jurisdictional requirement.

What conclusions can be drawn from these facts? In particular, what significance do they have for our work related to cyber crime?

Ladies and Gentlemen,

These were some reflections that, hopefully, could assist in our discussion this morning. Allow me now to introduce our panelists.[*]

Concluding Remarks

Ladies and Gentlemen,

This panel, and likewise this symposium on *The Rule of Law in the Global Village*, is now drawing to its close. I would, therefore, like to thank our distinguished panelists, Peter Grabosky, Tan Ken Hwee and Cormac Callanan for their interesting and thoughtful remarks on this very difficult and challenging topic. I would also like to thank all those present who have participated in this part of the symposium.

Before I close this panel, I would like to make an attempt to draw some conclusions. I stress that these are my own conclusions and that they may not be attributed to the United Nations as an Organization.

The following are the conclusions, as I see them:

- The focus of this symposium has been on the rule of law. It is interesting and maybe symptomatic that this issue has been brought to the forefront among Member States of the United Nations with such determination lately. Rule of law in international relations and at the national level and legal cooperation among States is the only way to protect peace and security in the future.

- Another issue that has been brought to the forefront in the discussion is state sovereignty. There is a growing understanding that state sovereignty today has to be viewed in a new light; the point of departure should not be the “sovereign”, but the people of

[*] Reference is made to the presentations of the three panelists, which are available at <http://www.odccp.org/palermo>.

the state in question. Many States have been concerned that their sovereignty is being threatened, but the focus has been on the perceived effects of so called humanitarian intervention, specifically the use of force against a State to prevent violation of humanitarian law and human rights.

- However, much more serious threats to the sovereignty of States are phenomena of a completely different nature. We have discussed one of them in this panel: cyber crime. As I see it, this is a threat that may pose a real challenge to all States, including the most powerful and well organized.

- If this is so, all States, irrespective of whether they are developed or developing countries have a common interest to protect themselves or – more correctly – their peoples.

- In other panels, we have heard the expression that the phenomena we are discussing are intertwined. Seen in the perspective of state sovereignty and state security, we can identify several related threats that fit into the picture in addition to cyber crime: terrorism, drug trafficking, certain financial crimes, corruption, money laundering, just to mention a few.

- To make the picture complete, one could also add other phenomena, such as: poverty, HIV-AIDS, global warming, desertification, and depletion of natural resources. All these phenomena constitute threats to peace and security in the world. Consequently, members of the Security Council are presently discussing how to define “threat to peace and security” in the contemporary society.

- Returning to cyber crime, we have heard many references to international cooperation. This is of particular importance in this case. The importance of maintaining the dialogue between developed and developing countries has also been stressed; it is essential that everybody be on board.

- With respect to universal jurisdiction, one must draw the conclusion that there has been great hesitation among States to accept this concept. However, because of the very nature of cyber crime – irrespective how we ultimately define it – the need for a truly universal jurisdiction may present itself with even greater emphasis than before; traditional crimes can almost always be addressed through some other method: territoriality, nationality, right of protection etc. But these concepts may not prove sufficient in the case of cyber crime.

- The point has also been made that legislation may not be the only method. Alternative solutions may have to be sought. The notion of guardianship has been stressed. It was said that much could be achieved through the market place, i.e. by those who use cyber space, through self-help. Empowerment of users to filter information was suggested. The responsibility of end-users was stressed. Elements of self-regulation of the business were indicated.

- Stakeholders were identified: Government; law enforcement agencies; the judiciary; business, and users. The need to involve non-governmental organizations was stressed. The role of the United Nations was emphasized in the discussion.

- Another problem is that cyber crime tends to defy quantification. This means that we have to be careful. We must not create a phantom and drive the problem out of proportion. At the same time we must be vigilant and make sure that things do not get out of our hands.

- Yet another problem is that too vigorous supervision risks violating personal integrity and privacy.

- There is no agreement on what constitutes cyber crime, but elements of their nature have been outlined, and several variations of what constitute such crime have been suggested in the panel.

- With respect to the need for legislation to provide for criminalization, five acts have been suggested in the panel. They are: (1) unauthorized access to a computer system; (2) interference with lawful use of a computer or computer system: (3) destruction or alteration of data within a computer system; (4) theft of intangible property, and (5) obtaining value by deception (including electronic systems).

- If legislation along these lines is deemed appropriate, it may be necessary to make the act crimes under international law, which would make it possible to apply the principle of universal jurisdiction. Would States be prepared to accept such a far-reaching solution, or would they hesitate with reference to their sovereignty? Will discomfort over extraterritorial regulation weaken? At the same time, one conclusion is that the territorial principle will still be an indispensable element in law enforcement.

- An additional point made is the danger of premature regulatory effects. There would be a need to find a balance between the need to legislate and a “tolerance degree” of illegality (which, I assume, by definition means that we already have some legislation in place).

How do we cope with all this? May I suggest: through cooperation and good will among us all. I am aware that this sounds like a platitude. But – do you have a better suggestion? Sooner or later, we will all be affected by the new phenomena in the cyber world!