Octopus Interface Conference
Cooperation against Cybercrime
1 - 2 April 2008
Council of Europe

Tackling the use of the Internet for criminal activities
The Role of UNODC
(Workshop 3)

Ladies and Gentlemen,

It is my pleasure to be here today to represent the United Nations Office on Drugs and Crime (UNODC).

First, for those of you who may be unfamiliar with the work of my Office, let me give you some background on the mission of the United Nations Office on Drugs and Crime (UNODC). To be very brief, we strive to contribute to the achievement of security and justice for all by making the world safer from crime, drugs and terrorism. As the only global intergovernmental body in this area, we facilitate policy-making on issues relating to crime and terrorism prevention and drug control. We are custodians of global crime conventions, such as United Nations Convention against Transnational Organized Crime and its three Protocols on human trafficking, illegal migration and firearms, as well as United Nations Convention against Corruption. Other important global instruments we have are a wide range of soft laws (standards and norms) in crime prevention and criminal justice, adopted by our governing bodies. The Office is also tasked to promote international cooperation in criminal matters, such as extradition and mutual legal assistance. These tasks are complemented by our extensive programme on technical assistance in crime, drug and terrorism.

These instruments are powerful tools to be used in fight against cybercrime and, referring to the UN level, the TOC Convention is the most relevant in that it does provide a legal basis for international cooperation to combat cybercrimes. Although the Convention applies only in cases where an organized criminal group is involved, and defines a group as such if one of its objectives is to generate a "financial or other material benefit" (article 2), most of the serious cybercrimes fall within the scope of the Convention. For example, taking identity-related crime, the cases where stolen or fabricated identification or identity information is treated as a form of illicit commodity and bought, sold or exchanged by organized criminal groups. This treatment of a "subject matter" as a form of illicit commodity being bought, sold or exchanged by organized criminal groups would also apply to the use of the Internet for child abuse/exploitation.

Over the past few years, both the Drug and Crime Commissions – our governing bodies, together with the UN Congress on Crime Prevention and Criminal Justice, through various Resolutions, have recognized the important contribution of the United Nations to regional and other international forums in the fight against cyber-crime. They have invited UNODC to explore the feasibility of providing assistance to address computer-related crime under the aegis of the United Nations and in partnership with other similarly focused organizations.

Being the only global body that deals with the crime-oriented aspects of the misuse of information technologies, my Office has undertaken action over the last years to assess the threats posed by such misuse, and develop strategies to confront them. Some specific areas where we have been engaged to date include the use of the Internet for: identity-related crime, the sale of internationally controlled drugs, and child abuse/sexual exploitation.

Let me now give you some more detail on UNODC's work in those areas:

<u>Identity-related Crime</u>

On the positive side, the technological advancements and the rapid developments in the use of Information and Communication Technology's (ICT's) have further increased security to ensure integrity of digital identity information, such as that recorded on credit cards, debit cards and passports. But, on the other hand, they have also created new opportunities to steal or copy and misuse such information. New emerging challenges

indicate the acute need to understand the nature of the complex problems encountered in this area and take efficient measures against abuses of identification information incited by the evolution of cybercrime.

UNODC conducted a study on "fraud and the criminal misuse and falsification of identity", which was released in early 2007. One of the novelties of that study was its approach to deal with an old problem from a new criminal justice perspective and consider abuses of identity or identification information as distinct criminal offences, as opposed to the traditional approach of criminalizing other activities committed using false identities. This study was also the first effort to tackle differences and deviations in definitional and conceptual approaches at the national level with regard to the criminal misuse and falsification of identity. The general term "identity-related crime" has been used to cover all forms of illicit conduct involving identity, including offences described as "identity fraud" and "identity theft".

The study is expected to be used as a resource by the law enforcement and policy-making authorities of Member States at the national level, and as the basis and springboard for further research or analysis. In addition, the information gained through the study could be utilized for the purpose of developing useful practices, guidelines or other materials in the prevention, investigation and prosecution of fraud and the criminal misuse and falsification of identity.

As a step further, in December 2007, UNODC created a consultative platform for the purpose of developing strategic proposals to address identity-related crime. We are establishing a core group of experts from Governments, private sector entities, international organizations, as well as research and academic institutions. The main intention behind the creation of such a multi-stakeholder think tank is to brainstorm on the best way forward and provide advice and guidance on possible long-term strategies against this emerging form of crime.

Internet pharmacies

Turning now to the use of the Internet for the sale of pharmaceuticals, it is clear that the unauthorized trade in internationally controlled licit drugs ordered via the Internet has reached epidemic proportions and UNODC is encouraging Member States to take measures to prevent the misuse of the Internet for the illegal offer, sale and distribution of internationally controlled licit drugs. Member States can develop policies to terminate such sales through greater coordination between the judicial, police, postal, customs and other competent agencies. The International Narcotics Control Board (INCB) has been working actively in this area with national experts from Governments and international organizations as well as from concerned industries, including the pharmaceutical industry, Internet service providers and financial institutions.

During regional Meetings of Heads of National Drug Law Enforcement over the past couple of years, UNODC also considered measures to counteract new trends in the use of technology by groups engaged in drug trafficking and organized crime, and, not surprisingly, the common denominator of the overall discussions and conclusions reached, highlighted the fact that the majority of front-line law enforcement agencies are not well prepared to meet the challenge either through lack of understanding or lack of technical resources.

Virtual Forum in Korea

We have also been developing a *virtual forum against cybercrime* together with the Korean Institute of Criminology (KIC). This is initially a pilot initiative which aims to create a virtual cyber-crime forum located on a digital platform for law enforcement and judicial officials, and academics, from developing countries. It will provide training courses and technical advice on the prevention and investigation of cyber-crime, with a special focus on effective law enforcement and judicial cooperation. It will also have a research site. Although a regional initiative, at this stage, experts include representatives from G8 countries, law enforcement and training experts, and academics. The pilot is expected to be up and running by early Summer, and, if successful, we would hope to develop such an initiative in other regions of the world.

Child abuse/exploitation

Finally, another area which UNODC is starting to tackle is that of the use of the Internet for child abuse/child exploitation. As you all know, the rapid development in the use of information technologies, in particular the internet, has given a new dimension to online child abuse/exploitation. Today, a large share of child pornography sites and child abuse images appear to be of a commercial nature, generating huge amounts of proceeds for organised crime syndicates, and this requires that governments, the Internet industry, police, educators, psychologists and financial investigators all work together to fight child abuse online. It is also

important to rein in the predators before, and not after, the act, by working with the major Internet, computer and mobile phone companies. Some issues which could be considered include:

- The need for a united law enforcement approach to take ownership of commercial child sexual abuse websites with significant longevity (up to 10 years), hopping between server and police jurisdiction;
- The possibility that relatively few crime syndicates operate large 'families' of abuse websites;
- Combating these operations should be part of the work of agencies already set up to combat organised crime and corruption;
- Legislation – no harmonisation of laws regarding viewing/possessing/downloading child sexual abuse online images - Without this, there can be little incentive for preventative blocking initiatives;
- Also, without legislation criminalising the consumption of images of children being sexually assaulted, the demand remains high, thus increasing the supply and more children to be abused;
- In some countries, host companies and ISPs have no obligation to register with the established Hotline (if there is one), plus the Hotline, in some cases, only notifies member hosts if they have illegal content; Thus, minimal notice and take-down occurs, and such countries remain hosts of this content;
- Blocking – little worldwide or even EU-wide endorsement;
- The need for a lot more thinking outside of national systems to deal with child exploitation and the possibilities for partnering with a view to targeting the less developed countries.

At this stage, UNODC, in this area, is currently looking to:

- Support Member States in the strengthening of their legislation to prosecute offences of this nature, and build the capacity of their law enforcement authorities to act effectively in their investigation;

- On the awareness side, develop education and training materials for children, teachers, parents on the safe use, and dangers, of the internet. The focus of our work would be geared of course towards the less developed countries.

- Work closely with internet service providers (especial local ISPs) to provide appropriate information to law enforcement authorities concerning suspected child exploitation offences, consistent with national legislation, in order to ensure that those suspected offences are investigated. ISPs can especially assist police and law enforcement agencies to eg block websites, identify and remove illegal content, identify offenders, assist in the installation of investigation tools, collect data etc.

Clearly, although many partners are already doing a lot in this area, the UN offers the multilateral platform as a standard-setter with a focus on developing countries. Our role could be to partner with, and bring together the experts/tools/ISPs etc to tackle the problem in a country/region.

Another very important area which UNODC is engaged in is trafficking in human beings. Earlier last year we launched a Global Initiative to Fight Human Trafficking intended to raise awareness and build strategic partnerships involving Governments, NGOs, industry, media etc. In this area also, the internet provides a fast, convenient and inexpensive way of connecting people between cities and across borders, but it is also increasingly being misused by criminals. Traffickers now have, literally at their fingertips, an effective, unrestricted and often anonymous means for recruiting their victims. Online employment agencies, in particular model or artist agencies and marriage bureaux are all ploys to lure potential victims. Internet chat websites are often used to befriend potential victims. The risks for young people to fall into the traffickers' net have substantially increased.

More information about the different methods used by traffickers to recruit their victims via the internet will lead to a better understanding of the problem which will, in turn, assist in the proposing of appropriate legal, administrative and technical measures. The internet is not only part of the problem; it is also part of the solution. Yet, while the criminals already exploit effectively the internet for their purposes, we are still lagging behind leaving untapped the large potential the internet offers in investigating human trafficking and raising awareness among the general public and in particular those searching the internet for jobs and migration services.

I'm not stating anything new when I emphasise the importance of building partnerships with the private sector to formulate and implement effective measures to counter computer-related crime. But relationships between commercial entities and law enforcement agencies really do need to be developed further, not only to reduce the level of computer-related crime, but also to speed up the response once a crime has occurred. One possible partnership strategy could include assistance from business in identifying areas where existing law

was inadequate; building capacity, for example, by providing training for law enforcement authorities and by raising awareness of new trends and technologies; working with law enforcement authorities in investigations and sharing general information; educating consumers about issues of online safety; preventive elements such as building effective security mechanisms into products; and providing incentives to the public to obtain information on the activities of perpetrators of computer-related crime. But whatever we do we have to do it together, and partnerships amongst international and regional entities such as Council of Europe, INTERPOL, UNODC, ITU, G8, EUROPOL (to name but a few) need to be further enhanced for collective efforts of tackling cyber crime.

Priority should be accorded to the provision of technical assistance to Member States in need with a view to addressing the lack of capacity and expertise in dealing with the problems of computer-related crime. Such assistance can take on a variety of forms, including: the provision of experienced personnel and advice from Member States and the private sector; the development of training courses and material; strengthening the prosecution services to deal with cyber-crime; and measures to ensure that law enforcement officials are continuously well informed about developments in technology. Development of tools and manuals at the international level is also essential.

Cybercrime is a recent form of criminal activity and it requires efficient and effective criminal justice systems, sound preventive policies and transparent financial regulations. Solutions to the problem are not to be found in either developing or developed countries acting alone. Cybercrime is a truly global challenge, and it requires the cooperation of all of us. The work before us is tremendous. We must first identify gaps in various existing domestic laws and regulations and find out the best combination of laws for countries with different legal traditions. It is not a simple task.

Cybercrimes do not respect borders, the patterns change quickly, and with access to the internet over the next 5 – 10 years being through mobile internet systems, we can be sure that, even those countries where, today, the problems may be less, will be increasingly affected.

Thank you.