UNITED NATIONS
Office on Drugs and Crime

Guidance Note

Cybercrime

Drafted by DTA, Organized Crime and Criminal Justice Section (G. Murray), with inputs from DO, DPA and DM/ITS

5 January 2010

Introduction

"*Cyber crime threatens all of us and thanks to the ever-greater use of computers in every area of our lives, this even includes people who do not go online. Cyber crime has witnessed an astonishing growth since the millennium and represents perhaps the greatest challenge for public law enforcement worldwide. Cyber police suffer from both poor funding and a lack of qualified personnel*[1]".

According to the FBI in 2008, revenues from cybercrime have exceeded drug trafficking as the most lucrative illegal global business, estimated at reaping in more than US$1 trillion annually in illegal profits. This estimate has been quoted widely, although there are questions as to it's accuracy[2]. Suffice to say revenues from cybercrime are certainly significant and increasing.

The development of new information and communication technologies (ICTs), including the use of computers and databases, have deeply changed the way our societies operate. Government agencies and companies rely on networks and store sensitive information electronically. Individuals use Internet for all sorts of activities from e-shopping to banking or maintaining contacts through social web-based networks.

At the same time, this worldwide proliferation of ICTs has given rise to increasing forms of cyber-crime, which pose threats not only to the confidentiality, integrity, or availability of computer systems, but also to the security of critical infrastructure. Computer systems, the Internet, databases etc. have become tools of crime, constituting both an opportunity to facilitate the commission of traditional crimes such as fraud or extortion, and a vehicle for new types of crimes, which emerge in parallel to the development of new technologies. These emerging crimes include illegal access to computers and databases, modifying or damaging data, identity theft, to quote but a few. Career criminals, including those involved in organized crime, are now using cyberspace to conduct many of their criminal activities and, since professional criminals are not out for "technological adventure", their better skills would normally ensure that they are less likely to get caught than for example the amateur hacker. Indeed, criminals and international criminal organisations have learnt, and continue to learn, to proficiently make use of sophisticated means to further their activities. In many ways, cybercrime has proved to be a very attractive niche; it allows criminals to easily operate trans-nationally, and make huge profits without taking too many risks.

Cybercrime is a relatively recent form of criminal activity. The investigations go along with a number of unique challenges such as the high speed of data exchange processes, the involvement of various providers even in a simple data exchange process or the international dimension of Cybercrime. To be able to react to the challenges, law enforcement agencies need the right legal instruments and specific training with regard to their being able to identify offender and collect the evidence required for criminal proceedings. In addition problems of jurisdiction arise at both the national and international levels. Jurisdiction is based on the concept of boundaries, and laws are based on "territorial sovereignty". However, cyberspace has no physical boundaries. It is not constrained by national

[1] "McMafia" by Misha Glenny, April 2008

[2] "'Cybercrime exceeds drug trade' myth exploded", by John Leyden, The Register, 27 March 2009

boundaries - criminals can change their locations from one country to another country within seconds in the cyber-world, irrespective of their physical location. Thus, to combat cyber-crime effectively, international cooperation must be further enhanced. It is also vital that technical assistance and training tools be provided to those developing countries where there is a lack of capacity and expertise to deal with cyber-crime. This will enable them not only to share knowledge and information to properly detect, investigate and prosecute cybercrime, but also to overcome the deepening digital divide between developing countries and developed countries in this field.

That said, the patterns change quickly, and with access to the Internet over the next 5 – 10 years increasingly being through mobile Internet systems, it is clear that even those countries where, today, the problems may be less will be increasingly affected. One example are social networks that have been set up only few years ago and are today one of the most popular services.

Owing to the worldwide impact of internet crime, countries are using various forms of legal, organizational, and technological approaches to fight it. The legal approach aims to restrict cyber crime activities through legislation. The organizational approach aims to enforce laws, to promote cooperation, and to educate the public through the establishment of dedicated organizations. The technological approach aims to increase the effectiveness and efficiency of cyber crime analysis and investigation with the help of new technologies[3]. Developing countries must be able to rely on an appropriate legal arsenal where definitions and offences can include new technologies development, and where laws criminalize the use of computers, access devices and the internet for criminal purposes.

Indeed, it is of concern that, given the current legal vacuum and lack of capacities in many countries, such countries are potential grey zones from which cyber criminals could operate and target the rest of the world with *de facto* impunity. In this context, it is of major importance to support the establishment of effective legal frameworks to deal with computer-related crimes. Broadhurst notes that, the effective control of cyber crime requires more than cooperation between public and private security agencies. He argues that the role of the communications and IT industries in designing products that are resistant to crime and that facilitate detection and investigation is also crucial[4].

1. Purpose of the guidance note

The purpose of this guidance note is to outline how UNODC can best formulate and deliver technical assistance and capacity-building activities which will assist countries address the problems posed by cybercrime at both regional and national levels.

Through its network of Field Offices, UNODC can play an important role in helping Member States to address some of the serious issues posed by cybercrime. The Office's solid expertise in countering various forms of transnational organised crime (for example with

[3] Chunga, W. et al. (2004), "Fighting cyber crime: a review and the Taiwan experience"
[4] Broadhurst, R. (2005), "Developments in the global law enforcement of cyber-crime",

respect to illegal trafficking in persons, illicit drugs, firearms, and money laundering), all of which can generate huge profits for the organised crime groups, and in addressing corruption and governance issues which often are at the origin of such criminal activity, and in assisting Member States with the ratification and implementation of the international legal conventions and protocols related to terrorism, can be successfully applied in this sector. Some of the services and tools mentioned in the UNODC Menu of Services could be relevant for the prevention and curbing of cybercrimes, and should be made available, as relevant, to Member States and other interested parties confronted with these issues.

2. Forms of Cybercrimes

For the purposes of this guidance note, Cybercrime can be defined across a range of offences which have been recognized by bodies such as Interpol, Europol, the Council of Europe, the European Union, the Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), the Organization of American States (OAS), the Commonwealth of Nations, the Group of Eight (G8), the Organization for Economic and Development Cooperation (OECD), to name but a few.

Computer crime, cybercrime, e-crime, hi-tech crime, electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. Such crimes may be divided broadly into 2 types of categories: (1) crimes that target computer networks or devices directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

The former is the basic form of computer related offences, which are against the confidentiality, integrity and availability of computer data and system, including illegal access; interference with computer data and computer system; theft of data; interception of data in the computer system. Some examples include hacking, cracking, virus/worm attack, time or logic bombs, spyware malware and other malicious code, Trojan horses, web jacking , denial of service attacks, salami attacks, data diddling, and email bombing.

The latter is the expanded form of computer related offences, which play a greater role in practice and where computer and telecommunication systems are used as a means to attack certain legal interests which mostly are protected by criminal law against attacks using traditional means. Examples include child sexual abuse and exploitation, economic fraud, forgery and identity theft, phishing scams, trafficking in human beings, illicit sales of controlled substances, terrorism, cyber-stalking or harassment, cyber bullying, information warfare and intellectual property crimes.

Although there is no definitive list of what constitutes cybercrime or computer related crime, according to Broadhurst[5] , a general consensus appears to have emerged about what falls within the scope of the offences that occur in cyberspace:

• Telecommunications Theft;

[5] Broadhurst R., Chantler Nic., (2006) Report of the "Expert Group Meeting on the Development of Virtual Forum on Cybercrime"; Also, (2009) "Cybercrime Update: Trends and Developments", pages 33 and 34.

• Hacking an other forms of illegal access to computer systems;
• Illegal Interception of Telecommunications;
• Piracy Copyright Theft;
• Cyber Stalking;
• Electronic money laundering and Tax evasion;
• Electronic Vandalism, Use of the Internet for Terrorist Purposes, Denial of Service, Extortion;
• Sales and Investment Fraud, Forgery (Classic Pyramid schemes);
• Electronic Funds Transfer Fraud and Counterfeiting (Carding);
• Identity Theft and Misrepresentation;
• Content Crime - Offensive Materials;
• Espionage;
• Resource Theft - illegal use of PC.

At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual. Also at this end of the spectrum is the growing crime of identity theft. Midway along the spectrum are transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting. These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the Internet. Another aspect of this type of crime involves individuals within corporations or government bureaucracies who deliberately alter data for either profit, personal or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These include spamming, hacking, and denial of service attacks against specific sites[6].

As indicated above, cybercrimes can include any of the following: Pirated software and CDs; Sales of illegal items; Online child abuse and exploitation; Hacking; Cyber-bullying; Fencing stolen goods; Slander/Stalking; Spread of virus/malware; Illegal gambling; Sales of personal information, Sales of pharmaceuticals, including counterfeit or fake drugs; fraud and identity-related crime; use of the internet for terrorist purposes; Denial-of-Service attack; Network attack; Phishing. To expand on some of these further, particularly those which relate more specifically to the work of UNODC:

a) Child Abuse and Sexual exploitation:

The diffusion of child sexual abuse images and the auctioning of trafficked women online are examples of how the Internet can lead to more victimization of vulnerable groups. Here, the Internet has made the commission of what might be termed 'traditional' crimes easier – or more widespread[7]. Distribution of child sexual abuse and exploitation material is a criminal offence which was relatively well-contained prior to the Internet: it is now a widespread

[6] Elements for this section have been taken from various sources

[7] GERCKE, "Obligations of Internet Service Provider in the Fight Against Child Pornography", *Computer Law Review International*, 2009, page 65

social harm[8]. As more individuals access the Internet, the cyber criminal has a broader range of potential victims within reach[9].

This rapid development in the use of information technologies, in particular the Internet, has given a new dimension to online child abuse and exploitation, creating an environment for its proliferation. Consumers (today most often in developed countries) purchase illegal materials via computer servers from sources sometimes based in other, less developed, States. This is of particular concern as online crime is an adjunct to offline violence and abuse suffered by children. Consumers unsatisfied by their online activities have also been known to travel to countries to abuse children.

Today, a large share of child sexual abuse and exploitation sites and images appear to be of a commercial nature, generating huge amounts of proceeds for organised crime syndicates. Such criminal activities highlight the significant importance of fostering the best possible cooperation between governments, the Internet industry, police, educators, hotlines, NGOs, children's charities, psychologists and financial investigators. This is needed due to the complexity of such investigations, which can be time consuming because they are often coordinated across jurisdictions and target networks of offenders using varying levels of security. It is also important to try to rein in the predators before, and not after, the act, by working with the major Internet, computer and mobile phone companies.

b) Trafficking human beings:

In the area of trafficking human beings 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 bureaus 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 can also be part of the solution. Technologies could be better used to detect, report and disrupt the recruitment and exploitation of victims via the Internet and support intelligence-led investigations on trafficking in persons. While the criminals already exploit the internet effectively 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, in particular those searching the internet for jobs and migration services.

---

[8] Understanding Cybercrime, 2009, page 32

[9] KRONE, "A Typology of Online Child Pornography Offending", *Trends & Issues in Crime and Criminal Justice*, No. 279; COX, "Litigating Child Pornography and Obscenity Cases", *Journal of Technology Law and Policy*, Vol. 4, Issue 2, 1999.

c) Economic fraud, and identity theft:

On the positive side, the technological advancements and the rapid developments in the use of Information and Communication Technologies (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.

Fraud is any dishonest misrepresentation of fact intended to induce another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by altering computer input in an unauthorized way; altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions; altering or deleting stored data; or altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes. (Source : http://en.wikipedia.org/wiki/Cybercrime).

Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data. The protected legal interest is the security of electronic data which may have consequences for legal relations. (Source: Council of Europe, Convention on Cybercrime –Explanatory Report, 81.)

Identity theft is a crime used to refer to fraud that involves someone pretending to be someone else in order to steal money or get other benefits. The person whose identity is used can suffer various consequences when he or she is held responsible for the perpetrator's actions. In many countries specific laws make it a crime to use another person's identity for personal gain. Identity theft is somewhat different from identity fraud, which is related to the usage of a 'false identity' to commit fraud. Identity theft means impersonating a real person. Identity theft may be used to facilitate crimes including illegal immigration, terrorism, and espionage. Identity theft may also be a means of blackmail. There are also cases of identity cloning to attack payment systems, including online credit card processing and medical insurance (Source : http://en.wikipedia.org/wiki/Identity_theft). Further detail on identity theft is contained in "Legal Approaches to Criminalise Identity Theft", prepared by Dr. Marco Gercke.

d) Illicit sales of controlled substances, particularly pharmaceutical preparations:

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. For several years, the Internet has been exploited for criminal activities, including drug trafficking. The problem extends beyond the sale of illicitly manufactured natural and synthetic drugs such as heroin or amphetamines; it also include pharmaceutical preparations containing narcotic drugs and psychotropic substances, such as

oxycodone and hydrocodone, methylphenidate and the group of benzodiazepines. Most of these preparations have properties similar to illicitly manufactured drugs and their abuse can be as dangerous as the abuse of heroin, cocaine or amphetamines; they should only be available on prescription and consumed under medical supervision.

However, so-called "Internet pharmacies" illegally sell such drugs without the required prescription. In 2008, a study in the United States identified 365 sites offering internationally controlled substances for sale. Only two of these sites had been certified by the National Association of Boards of Pharmacy as legitimate Internet pharmacy practice sites. Illegal Internet pharmacies exist in all regions and their products have been seized in many countries in the world. While these pharmacies provide an easy source of illicit drugs to drug abusers, they are also purchased by drug traffickers and eventually end up being peddled at the street level. "The online sale of such pharmaceuticals by unscrupulous racketeers is no different from the trafficking in illicit drugs, as it endangers lives just as much as street sales do."[10]

e) Use of the internet for terrorist purposes

The Internet has also become a tool for terrorists and radical groups. It allows for anonymous and cheap communication and international coordination. Propaganda can be delivered online through videos, images and texts. Internet and social networks are used for recruitment and mobilization of supporters and sympathizers, targeting in particular young people and increasingly women. There is also evidence (please quote source) that Internet has been used for fund raising, training (online instructions and manuals) and coordinating attacks. Computers, networks and databases can become the target of terrorists aiming at bringing down critical infrastructure, such as air traffic control systems, power stations, government databases or banking systems. According to the report of the CTITF Working Group on Countering the Use of the Internet for terrorist purposes - http://www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf - *para. 87. Perhaps the single most compelling conclusion to emerge from the Working Group's activities has been that there is no single, easily identified 'use of the Internet for terrorist purposes'. Terrorism could occur on, or by means of, the Internet, but it is disputable whether it has happened yet. Terrorists use the Internet in a variety of different ways, many of which are indistinguishable from ways in which everyone else uses it. Finally, and most confusingly, the Internet hosts a great deal of activity and material that may be related to terrorism. But establishing firm connections between online social actions and offline terrorist violence is not always straightforward*

Further examples of widespread and frequent types of cybercrimes are contained in Annex I (NB that this list with some explanations is not conclusive and that new such crimes continue to evolve rapidly).

Cybercrime cases are some of the most complex, with the result that they involve complicated ways of investigations. Though variation exists, many cybercrimes are exceedingly tricky from two standpoints: (1) technologically and (2) legal. Indeed criminals may turn to cybercrime for this very reason: they may assume that, due to the complex

[10] Professor Ghodse, President, INCB, March 2009

nature of the field, law enforcement officials will be mostly ineffectual. Prosecuting cybercrimes often entails as much complexity as understanding the underlying technologies themselves. Several challenges related to the investigation of Cybercrime have already been identified. They range from the need for an international coordination of investigations as a result of the international dimension of the network to technical aspects such as the use of encryption technology or means of anonymous communication by the offenders.

The most common forms of cybercrime – such as content-related offences, online child sexual abuse and exploitation, or computer-related fraud and forgery - will usually have effects in more than a single jurisdiction. For example, it could involve a host computer, a consumer, a distributor, and a producer, all four of which may reside in a different state subject to a wide variation in domestic laws. For this reason, cybercrime investigations are very complicated and international cooperation is crucial. They require the ability to effectively request and respond to requests for mutual legal assistance and joint investigations. The judicial profession and law enforcement officials, especially in developing countries, need to be trained to deal with these specific and novel types of crime.

The potential cybercrime perpetrators, regardless of whichever nationality they belong to, 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.

Another aspect is the fact, that by committing an offence the offenders in general make use of different services operated by Internet Service Providers (ISP). This raises questions related to the liability of ISPs and how they can support investigations. In addition, ways of communication and cooperation between these services and Internet service providers (ISPs) within criminal investigations need to be established.

As a result of the above, over the past few years, both the Drug and Crime Commissions, UNODC's 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 at the global level to regional and other international forums as a multilateral platform in the fight against cyber-crime.

3. UNODC existing mandates

The transnational nature of cyber crimes, the established involvement of organized criminal groups as well as the governance failures which often sustain these forms of criminality, make them highly relevant to UNODC mandates. Cybercrime often relies on governance failures in the criminal justice system (law enforcement, prosecution, judiciary etc.). The link between the activities of such criminal groups, the fostering of conflict and the resultant impact upon peace and security is of particular concern.

The UN is capable of being identified as the only global organization that forms a forum of its 192 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, and the actions of the UN have unique advantages in coordinating international positions.

The Council of Europe Convention on Cybercrime[11] provides a legal basis for cooperation in a much broader context than that of the Council of Europe Member States, as it is open for accession to other States as well.

However, the United Nations Convention against Transnational Organized Crime (UNTOC) can also be utilized, where applicable, with a view to fostering international cooperation in this field. UNTOC commits States parties to introduce a range of measures for the strengthening of mutual legal assistance, extradition and other forms of judicial and law enforcement cooperation to combat all serious crime[12], including cybercrime, among its 147 States Parties. As such UNODC assists states in the implementation of this Convention, also helping with technical assistance and training.

The most common forms of computer-related crimes would indeed fall within the definition of UNTOC as they are transnational and involve an organized criminal group. They are committed with the aim of achieving material or financial benefit. In this regard, an interpretative note to article 2 of the Convention indicates that the aim of obtaining, directly or indirectly, a financial or other material benefit (element of the definition of an organized criminal group) could be interpreted broadly to include crimes in which the predominant motivation may be sexual gratification, such as the receipt or trade of materials by members of child grooming rings, the trading of children by members of pedophile rings or cost-sharing among ring members. The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially women and children would also be relevant to the issue of the use of ITCs, including the Internet, to facilitate child abuse and exploitation.

Another example of where UNTOC can help is with 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 sexual abuse and exploitation. Article 29 of the UNTOC is also of particular interest, as it requires parties to develop specific training programs for law enforcement personnel including prosecutors and investigating magistrates. Cybercrime is specifically referred to in subparagraph (h), which states that such programs shall deal with "methods used in combating transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology". The UNTOC, therefore, constitutes a powerful basis to overcome challenges in international cooperation in cybercrime matters.

In as far as acts for which the internet is used for terrorist purposes fall within the substantive scope of the 16 international conventions and protocols related to terrorism, the mandates of UNODC in assisting Member States with the ratification and implementation of these international legal counter-terrorism instruments are also relevant.

[11] Council of Europe, *European Treaty Series*, No. 185.

[12] Serious crime is defined under UNTOC as a conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years.

In November 2009, the General Assembly, in its draft resolution A/Res/64/, "Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity", in paragraph 11 "Draws attention to the emerging policy issues identified in the report of the Secretary-General … (A/64/123) - piracy, cybercrime, sexual exploitation of children and urban crime - and invites the United Nations Office on Drugs and Crime to explore, within its mandate, ways and means of addressing these issues".

Similarly, December 2008 General Assembly resolution A/Res/63/195 on "Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity", also highlights cybercrime in paragraph 7 as follows: "Draws attention to the emerging policy issues identified in the report of the Secretary-General, inter alia, …, the sexual exploitation of children, economic fraud and identity theft, …, and, in the context of advisory services and technical assistance, the issue of cybercrime, and invites the United Nations Office on Drugs and Crime to explore, within its mandate, ways and means of addressing these issues."

The specific issue of child sexual abuse/exploitation is underlined in Resolution 16/2, in particular paragraphs 7 and 16, of the Commission on Crime Prevention and Criminal Justice of April 2007 "Effective crime prevention and criminal justice responses to combat sexual exploitation of children". The Resolution encourages Member States to take appropriate measures, consistent with their international obligations and national legislation, to prevent and make efforts to eliminate the use of mass media and information technologies, including the Internet, to facilitate or to commit child sexual exploitation offences. A report (E/CN.15/2009/14), based on information received from Member States on the issues raised in resolution 16/2, was discussed at the April 2009 Crime Commission. The replies received indicated as follows:

> Most of the reporting States have adopted national legislation in conformity with international instruments governing the rights of the child, as well as various measures to promote the investigation and prosecution of relevant offences, international judicial cooperation, awareness raising, protection of child victims and witnesses and collaboration with civil society.
>
> In relation to the use of information and communications technology in child sexual exploitation, attention is drawn to the fact that the use of such technology for child sexual abuse and exploitation is a relatively new phenomenon and few countries indicated that adequate or specific legislative and other measures were in place. It should be pointed out, moreover, that an increasingly large proportion of child sexual abuse websites are of a commercial nature, generating significant proceeds for organized criminal groups. States should therefore ensure the coverage of those offences under the Organized Crime Convention, with domestic legislation adequately criminalizing such offences and sanctions that reflect their gravity and meet the serious-crime threshold.
>
> Replies also emphasized the importance of fostering the best possible cooperation

among law enforcement authorities to investigate complex forms of cybercrime, including in particular online child sexual abuse, as well as between law enforcement authorities and Internet service providers.

It was further agreed during the 2009 Crime Commission that the Thematic Debate in 2011 would focus on this same topic. The use of ICTs, including the Internet, for child sexual abuse and exploitation is in addition included for discussion during the UN Crime Congress to be held in Salvador, Brazil, in April 2010.

In 2005, the Bangkok Declaration on Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, endorsed by General Assembly resolution 60/177 of December 2005, welcomed the efforts to enhance and supplement existing cooperation to prevent, investigate and prosecute high-technology and computer-related crime. The Declaration further invited the Commission on Crime Prevention and Criminal Justice to explore the feasibility of providing assistance to Member States in addressing computer-related crime under the aegis of the United Nations, and in partnership with other similarly focused organizations (paragraph 16).

In 2003, the Secretary-General appointed a High-level Panel on Threats, Challenges and Change. Its final report, "A More Secure World: Our Shared Responsibility" (A/59/565) noted that transnational organized crime is one of the six major threats with which the world is confronted. Further, a number of instruments adopted by the international community have recognized the growing threat of cybercrime.

The "Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century", endorsed by General Assembly resolution 55/59 of December 2000, called for the development of action-oriented policy recommendations on the prevention and control of computer-related crime and invited the Commission on Crime Prevention and Criminal Justice to undertake work in this regard (paragraph 18).

In addition, 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 sessions.

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.

Other resolutions relevant for UNODC include:

- ECOSOC resolution E/2007/20 (26 July 2007) on "International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime".

- ECOSOC resolution 2004/26 (21 July 2004) on "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes".

- ECOSOC resolution 2004/42 (21 July 2004) on "Sale of internationally controlled licit drugs to individuals via the Internet".

- Commission on Narcotic Drugs Resolution 52/5 (2009) on "Exploration of all aspects related to the use of cannabis seeds for illicit purposes" requests the INCB to "gather from Member States regulatory information on cannabis seeds, including on the sale of cannabis seeds through the internet".

- Commission on Narcotic Drugs Resolution 50/11 (2007) on "International cooperation in preventing the illegal distribution of internationally controlled licit substances via the Internet.

- Commission on Narcotic Drugs Resolution 48/5 (11 March 2005) on "Strengthening international cooperation in order to prevent the use of the Internet to commit drug-related crime".

- Commission on Narcotic Drugs Resolution 43/8 (15 March 2000) on curtailing the availability of controlled pharmaceuticals and precursor chemicals for illicit purposes through the misuse of the World Wide Web.

4. Areas of intervention for UNODC

As the only global intergovernmental body working in crime prevention and criminal justice, UNODC has the clear mandate to implement the United Nations Convention against Transnational Organized Crime. Specifically, article 29 (Training and technical assistance) of UNTOC requires Parties to develop specific training programs for law enforcement personnel, including prosecutors and investigating magistrates, dealing among others with methods used in combating transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology.

UNODC possesses significant comparative advantages for addressing the above-mentioned complex challenges and technical assistance needs, thanks to its specialized technical competence, operational capacity and long-term expertise in crime prevention, criminal justice and the rule of law. UNODC assistance, to date, has included institutional and operational capacity building of law enforcement and judicial bodies, in relation to investigation, prosecution and adjudication of serious crimes; assistance in legislative drafting; improving international cooperation and exchange between law enforcement authorities etc., and such activities can also be undertaken to counter cybercrimes. It is important to note that, in terms of cybercrime, such assistance has been developed and undertaken by many – national Governments, regional entities, NGOS etc., although much has also been on a fairly *ad hoc* basis, this not necessarily leading to long-term capacity building and sustainability within the targeted country.

UNODC's specific niche in countering cybercrimes relates to the above-referred to global mandates to fight trans-national and organized crime, its ability, as an honest broker with a multi-lateral platform, to promote international cooperation, and its specific focus on the developing world. Further, its network of Field Offices are well placed to identify areas where national governments could benefit from UNODC assistance to counter the use of ICTs for criminal activities.

In as far as acts for which the internet is used for terrorist purposes fall within the substantive scope of the 16 international conventions and protocols related to terrorism, the work of the Terrorism Prevention Branch in assisting Member States with the ratification and implementation of these international legal counter-terrorism instruments is also to be considered.

However, in dealing with cybercrime, UNODC must adopt a comprehensive, partnership, and multidisciplinary approach, pooling its already proven legal, law enforcement and technical expertise to counter criminal activities, with the specific and well-developed expertise of those key partners already involved in countering cybercrime. There are numerous international actors and stakeholders – including other UN entities – who are already engaged in cybercrime issues and, even if they have differing mandates and focus areas (see Annex 2), UNODC must seek to work in coordination and "complementarity" with them.

As mentioned, although many partners are already active in this area, UNODC offers a multilateral platform as a standard-setter in crime prevention and criminal justice matters, with a focus on developing countries. UNODC's role should be to partner with, and bring

together the experts/tools/ISPs etc to tackle the problem in a country/region. 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, and ensuring long-term sustainability in dealing with the problems of computer-related crime. Such needs should be/have been identified within the respective frameworks of the UNODC Regional Programs.

The importance of building partnerships with the private sector to formulate and implement effective measures to counter computer-related crime is paramount if we are to achieve any long-term and sustainable success. Relationships between commercial entities and law enforcement agencies definitely 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. Further, there needs to be increased understanding and knowledge between the first responder law enforcement officials and the prosecutors and judges who then deal with cybercrime cases.

DTA/OCS is currently finalising a comprehensive thematic program to assist primarily developing countries, where cyber technologies are rapidly increasing and where already many of the internet users are located, to develop the necessary legal and technical foundations to effectively fight cybercrime. The proposed framework will draw on the expertise and experience of those partners already active in the field. It aims at fighting computer-related crimes as follows:

1. Assisting Member States in the adoption of adequate legislation that would constitute a solid basis for effective investigation and prosecution of computer-related crimes.
2. Building the operational and technical knowledge of judges, prosecutors and law enforcement officials on issues pertaining to cybercrime, through training, the adaptation/development of training materials on investigation and prosecution of computer-related crime etc.
3. Training the law enforcement authorities to effectively use international cooperation mechanisms to combat cybercrime.
4. Raising awareness of civil society and create momentum among decision-makers to coalesce efforts to prevent and address cybercrime.
5. Identifying and disseminating good practices and promoting public-private partnerships in preventing and combating cybercrime.

Also, in light of Resolution 16/2 (*Effective crime prevention and criminal justice responses to combat sexual exploitation of children),* the project, as required, will aim to target the misuse of ICTs, in particular the Internet, for child sexual abuse and exploitation in developing countries. Specifically, it will aim to: (a) 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 investigations; (b) develop and/or adapt, together with key involved experts and institutions, education and training materials for children, teachers and parents on the safe use and dangers of the Internet, promote the establishment of cyber tip lines, and carry out other awareness-raising activities; and (c) 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/take-down websites, identify and remove illegal content, identify offenders, assist in the installation of investigation tools, collect data etc. As with the law enforcement component, UNODC will fully involve those key players already engaged in this field, for example to develop and adapt existing training/and education materials for use in developing countries where the need is identified.

In terms of what needs to be done to further promote international cooperation in combating cybercrime, aside from possibly creating of working groups with operational skills at regional levels and ensuring x-fertilisation, there would certainly be room for the development of a platform, possibly along the lines of Automated Donor Assistance Mechanism (ADAM), to ensure the coordination of cybercrime activities. Such an Internet-based tool for the coordination of technical assistance and capacity building in the field of countering cybercrimes would be useful for all involved organisations and agencies. UNODC has already been asked on various occasions as to whether this would be possible and has discussed the idea with some of the key partners, including IT companies. Such a tool would automatically provide partners with essential information in order to avoid the duplication of activities and projects, as well as perhaps even coordinating donor assistance.

As true experts in the cybercrime field are relatively few, and as UNODC is a relative newcomer in addressing cybercrime, UNODC will fully involve those persons and institutions which have already developed and delivered such tools and/or training, to review and adapt materials, as necessary, for such use. Experts specialized in providing training will be identified to assist UNODC in running and delivering the tools and training courses to support Member States in the strengthening of their legislation to prosecute HTC offences, and build the capacity of their law enforcement and legal authorities to act effectively in their investigation. The whole idea is not to duplicate or re-invent but rather to use/build on/adapt what's already out there for use in the developing world. All of the above-foreseen activities will therefore be carried out jointly with relevant partner agencies.

DTA/OCS, taking the lead, will work with interested UNODC Field Offices to design appropriate activities and, in collaboration with the relevant experts (depending on the specific needs identified), technically assess them to ensure that the planned activities project are compatible with the relevant mandates and that they are complementing, rather than duplicating, other such activities. DTA/OCS, in addition, will also continue to build and act as a liaison with the relevant and involved partners.

It should be noted that this is a general guideline and that specific interventions in the area of cybercrime and related matters will be framed, as mentioned earlier, in the context of the UNODC Regional Programs to be conceived jointly between the respective regional office and the inter-divisional task forces at HQ. It should further be noted that cybercrime may not necessarily be a priority for every region, and that requirements should be selective in terms of themes when it comes to technical assistance and capacity building activities, depending on the needs of the respective government(s). UNODC's experience to date in dealing with cybercrime at the global level suggests that care needs to be taken in developing programmatic activities. Therefore, all programmatic activities in the area of cybercrime should be in consultation with HQ.

Some of the above were also recommendations of an informal expert group meeting (EGM) of key institutions and experts held at UNODC in October 2009[13]. The EGM was arranged specifically to discuss and assess UNODC's role in the fight against Cybercrime. It considered the initiatives and programs that are already in place by other organizations, institutions and national authorities, and assessed as to how best UNODC can collaborate with these existing activities and programs to promote a more coordinated and sustainable approach to combating Cybercrime in developing countries. A SWOT (strengths, weaknesses, opportunities and threats) analysis of UNODC, which was carried out by the participants at the meeting, is contained to this guidance note as Annex 5. The experts further recommended the following concrete actions for UNODC over the next 12 months:

UNODC should be in the position to report on the following areas of activity undertaken, with partners as appropriate;
• Regional, in-depth technical needs assessments carried out, including up-to-date capability (new initiatives);
• Concrete UNODC "umbrella" program plan;
• Funding opportunities identified.

Virtual Forum in Korea

DTA/OCS has 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 also has 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 (online) by early 2010, and, assuming success, it will be further developed to make the technical assistance and training available, first to additional developing countries in the Asian region and, at a later date, to other regions of the world where law enforcement authorities need to be better equipped to deal with cyber-crimes. The materials will be adapted as appropriate.

Identity-related Crime

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

[13] The final report will be shared with all field offices when finalised

conduct involving identity, including offences described as “identity fraud” and “identity theft”.

As a step further, in December 2007, UNODC created a consultative platform for the purpose of developing strategic proposals to address identity-related crime, and established a 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 was to facilitate exchange views on the best course of action and the most appropriate initiatives that need to be pursued under the platform. The group has, to date, met three times and has provided a series of guidelines and directions for future activities which include, among others: the undertaking of further research; more enhanced consultations with the private sector; the elaboration of research papers; the compilation of examples of relevant legislation; the development of materials on best ways and means to promote international cooperation to combat identity-related crime; and the compilation of best practices for the protection of victims.

The first results of the work of the group, including two research papers on legal approaches to identity-related crime and protection of victims of identity-related crime, were brought to the attention of the Commission on Crime Prevention and Criminal Justice at its 18th session on 16-24 April 2009. At that session, related issues were also the subject of a thematic debate.

Internet pharmacies

UNODC is encouraging Member States to take measures to prevent this misuse of the Internet. 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 also 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. The Board has developed a set of guidelines that will assist Governments in addressing this important problem. These guidelines were presented by the INCB President at the March 2009 CND. The guidelines contain information that will assist Governments in their efforts to prevent the use of the Internet for drug trafficking. The INCB will continue work in this area. Recently, as per CND resolution 52/5, UNODC is mandated to conduct a global survey on Cannabis Seeds and present this survey to the fifty-third session of the CND in 2010. This would include gathering regulatory information on cannabis seeds such as the sale of cannabis seeds through the Internet.

As per Resolution 50/11 of the Commission on Narcotic Drugs, UNODC can act to prevent the illegal distribution of internationally controlled licit substance via the internet. This is done when, upon the request of any Member State, UNODC works in conjunction with other Member States, who have experience in investigating drug-related Internet-based crime, to provide necessary equipment, training and assistance in this area.

Use of the internet for terrorist purposes

The use of the Internet for terrorist purposes represents a serious threat and more efforts are needed to gain a better understanding of the issue. In this regard, it is noted that the Counter-Terrorism Implementation Task Force, which brings together 23 entities of the United Nations System and Interpol with a view to ensure overall coordination and coherence in the counter-terrorism efforts of the United Nations system, including collaborative work to support the efforts of countries for implementing the United Nations Global Counter-Terrorism Strategy, has established a Working Group on Countering the Use of the Internet for Terrorist Purposes, in which UNODC participates. The objectives of the Working Group are to identify and bring together stakeholders and partners with a view to sharing information, as well as to identify possible ways to counter the threat at the national, regional and global levels and to examine what role the United Nations might play in coordinating action by Member States.

The Working Group published a report in February 2009 (http://www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf -) which concludes by suggesting some ideas for future UN work in this area. These include:

- Facilitating Member States sharing best practices;
- Building a database of research into use of the Internet for terrorist purposes;
- Conducting more work on countering extremist ideologies that are spread through the Internet;
- Explore the added value, viability, and desirability of creating international legal measures aimed at limiting the dissemination of terrorist content on the Internet;
- Fostering partnerships with the private sector and industry. These non-traditional stakeholders play an important role in protecting data and developing safeguards, and in establishing standards of acceptable content;

Based on the recommendations made in the report, the CTITF Working Group is planning to undertake, among others and subject to the availability of extra-budgetary funding, further work on legal issues related to countering the use of the internet for terrorist purposes, in particular through research on Member States' and international organizations' experience in developing a legal framework and the implementation thereof.

Trafficking in persons

The DO/AHTMSU/UN.GIFT is conducting a study and expert discussion on: i) the use of new technologies by traffickers for the recruitment of victims via the internet, ii) the use of technologies to detect, report and disrupt the recruitment and exploitation of victims via the Internet, and iii) the use of new technologies to support intelligence-led investigations on trafficking in persons.

Assumptions or Risks

The adoption of effective laws to address cybercrime depends on the political context in which it is set. In this regard, the willingness of governments and parliamentarians to

support such laws through the approval process is critical. This will include, as necessary, meetings and other relevant lobbying and awareness-raising activities.

Assumption also applies when conducting trainings. It is critical that judges, prosecutors and law enforcement officials who will be trained have enough visibility and influence within their own institution/department. This would greatly contribute to create a momentum to strengthen responses to cybercrime. It would also ensure the dissemination of know-how and lessons learned from the trainings and workshops organized. In this respect, UNODC will make sure that working contacts with national officials and other relevant partners will be used to organize workshops in the most efficient way possible. The effective investigation and prosecution of computer-related criminal offences will also depend in fine on the availability and quality of IT equipment that can be used by relevant officials.

In order for activities to be successfully implemented, it is expected that governments show commitment and follow-up to make productive and effective assessment missions, meetings and trainings. Changes in governments or in counterparts should not impede, substantially change or cancel programs, plans and activities.

5. Partnerships with relevant actors

As indicated under the previous section, DTA/OCS will continue to develop strategic synergies with the many international and regional organisations, governments, NGOs and ISPs involved in the different areas of tackling cybercrime. Working contacts and partnerships have been established by DTA/OCS since 2007 with almost all relevant partner agencies in the field of cybercrime, and, as UNODC's work on cybercrime becomes more developed, new synergies with other thematic, geographic and substantive entities will also be sought.

In UNODC, in particular, the new thematic cluster on transnational organized crime will be closely involved in the development/adaption of resource materials and training for the use of law enforcement officials. The work of the Terrorism Prevention Branch is relevant for activities falling within the scope of its mandate in assisting Member States with the ratification and implementation of the international conventions and protocols related to terrorism. TBP will also continue to represent UNODC in the Counter-Terrorism Implementation Task Force and in its Working Group on Countering the Use of the Internet for Terrorist Purposes. ITS may also contribute in terms of expertise, awareness and security of systems, and with the development of training centres in developing countries as required and appropriate. Finally, the UNODC Field Offices will play a pivotal role in channeling specialized expertise and sustained assistance from the substantive offices at headquarters directly to countries through a cooperative and complementary approach.

Annex I

Examples of widespread and frequent types of cybercrimes

(1) Crimes that target the computer directly

a) Illegal access – hacking, cracking, computer trespassing

Illegal access covers the basic offence of dangerous threats to and attacks against the security of computer systems and data. The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion, i.e. hacking, cracking or computer trespassing should in principal be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data and secrets, to the use of a system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer related fraud or forgery, cyber terror. (Source: Council of Europe, Convention on Cybercrime –Explanatory Report, 44.)

b) Interference with computer data and computer systems

Cyber criminals can undertake activities to damage, delete, deteriorate or alter computer data, and hinder computer systems by inputting, transmitting, deleting, deteriorating or altering computer data, using various kinds of tools as mentioned above.

Computer viruses are self-replicating programs which attach themselves to a computer or a file and then circulate themselves to other files and computers on a network.

Worms, unlike viruses, do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory, thus creating a hole of missing information. (Source: Wikipedia; http://en.wikipedia.org/wiki/Computer_virus)

Time bombs or Logic bombs are event dependent programs which involve the insertion of routines that can be triggered later by the computer's clock or a combination of events. When the bomb goes off, the entire system, perhaps worth millions, will crash. Even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date. (Source: http://www.scit.wlv.ac.uk/~cm1988/CP3349%20SLAPA/computer_crime.htm)

Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent. While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habits, sites that have been visited, but can also interfere with user control of the computer

in other ways, such as installing additional software, and redirecting Web browser activity. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs. (Source: Wikipedia; http://en.wikipedia.org/wiki/Spyware)

Trojan Horse describes a class of computer threats that appear to perform a desirable function but in fact perform undisclosed malicious functions that allow unauthorized access to the host machine, giving them the ability to save their files on the user's computer or even watch the user's screen and control the computer. Trojan Horses can be easily and unwittingly downloaded. For example, if a computer game is designed such that, when executed by the user, it opens a back door that allows a hacker to control the computer of the user, then the computer game is said to be a Trojan horse.

Web jacking is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. (Source: http://www.naavi.org/pati/pati_cybercrimes_dec03.htm)

Denial-of-service attack (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a computer resource unavailable to its intended users. It generally consists of the concerted efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name-servers. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. (Source: Wikipedia; http://en.wikipedia.org/wiki/Denial-of-service)

Salami attacks are normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. For example, a logic bomb was introduced in a bank's system, which deducted 10 cents from every account and deposited it in another specific account. (Source: Wikipedia; http://en.wikipedia.org/wiki/Denial-of-service)

Data diddling involves altering raw data just before a computer processes it and then changing it back after the processing is completed. **Email bombing** refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.
(Source: Wikipedia; http://en.wikipedia.org/wiki/Denial-of-service)

c) Interception of data

It is necessary to protect the right of piracy of data communication just like protecting private conversations from illegal tapping and recording of oral conversations. The offence is applied to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer. (Source: Council of Europe, Convention on Cybercrime –Explanatory Report, 51.)

(2) Crimes facilitated by computer

Such serious cybercrimes, though continuously expanding in variation, include some of the following activities:

a) Phishing is a popular form of fraud. It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online banks, online payment processors, or IT Administrators are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. (Source: http://en.wikipedia.org/wiki/Phishing)

b) Obscene or offensive contents: The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be illegal. Many jurisdictions place limits on certain speech and ban racist, blasphemous, politically subversive, libellous or slanderous, seditious, or inflammatory material that tends to incite hate crimes. The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with entrenched beliefs. (Source: http://en.wikipedia.org/wiki/Cybercrime)

c) Illicit sales of controlled substances, particularly pharmaceutical preparations: Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away. Furthermore, traditional drug recipes were carefully kept secrets. But with modern computer technology, this information is now being made available to anyone with computer access. (Source: http://en.wikipedia.org/wiki/Cybercrime)

d) Cyber-Stalking, harassment: Cyber-stalking is the use of the Internet or other electronic means to stalk someone. It has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals, to harass another individual, group of individuals, or organization. The behaviour includes false accusations, monitoring, the transmission of threats, identity theft, damage to data or equipment, the solicitation of minors for sexual purposes, and gathering information for harassment purposes. (Source: http://en.wikipedia.org/wiki/Cyberstalking)

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. Any comment that may be found derogatory or offensive is considered harassment. (Source: http://en.wikipedia.org/wiki/Cybercrime)

e) Gambling : Online gambling is a general term for gambling using the Internet. This can include online casinos, online poker, online sports betting, online bingo etc. The rapidly mushrooming number of illegal gambling and betting websites is heightening concerns among authorities about global corruption, money laundering and gambling addiction. In the past, people who wanted to gamble had to get together in a certain place. But the development of information technology enables them to gamble online, at any time, at any place, whenever they want. These gambling sites are very often hosted by organized crime groups and the profits generated by running gambling sites are used to maintain and expand the organization. They may also provide an easy means for money laundering, as it provides criminal anonymity, remote access, and access to encrypted data

f) Intellectual property crime: Intellectual property is legal property rights over creations of the mind, both artistic and commercial, and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; ideas, discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property include copyrights, trademarks, patents, industrial design rights and trade secrets. The majority of intellectual property rights provide creators of original works economic incentive to develop and share ideas through a form of temporary monopoly. (source: http://en.wikipedia.org/wiki/Intellectual_property)

Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the internet, which cause concern both to copyright holders and those who work professionally with computer network. The reproduction and dissemination on the internet of protected works, without the approval of the copyright holder, are extremely frequent. Such protected works include literary, photographic, musical, auto-visual, computer program and other works. The ease with unauthorised copies may be made due to digital technology and the scale of reproduction and dissemination in the context of electronic networks made it necessary to take steps against intellectual crimes and enhance international co-operation in this field. (Source: Council of Europe, Convention on Cybercrime –Explanatory Report, 107.)

Annex 2

Some global and regional governmental and non-governmental organisations involved in countering cybercrime[14]

A. Global

1. ITU – International Telecommunication Union

Mandate/Scope;

As a specialised agency within the United Nations the ITU deals with standardisation and development of telecommunications and additionally plays a role in cybersecurity issues. The ITU was the lead agency at the World Summit on the Information Society (WSIS) which took place in Geneva (2003) and Tunis (2005). The output of the first round of the summit was a 'Geneva Plan of Action' which underlined the need for governments to work in cooperation with the private sector to "prevent, detect, and respond to cyber-crime and misuse of ICTs". The output of the second round of the summit was the nomination of the ITU as the sole facilitator of Action Line C5 dedicated to building confidence and security in the use of information and technology. In 2007 the ITU Secretary-General launched the ITU Global Cybersecurity Agenda. Among its goals are the elaboration of strategies, for the development of model cybercrime legislation, and for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.

2. Group of Eight (G8) Initiatives

Mandate/Scope;

Set up a "Subcommittee on High-tech Crime" to deal with the fight against Cybercrime. G8 Justice and Interior Ministers adopted Ten Principles and a Ten-point Action Plan to fight High-tech crimes. This plan includes the principles of: 1) not providing safe havens for abusers of information technologies, 2) coordination among concerned states in the investigation and prosecution of international high-tech crimes, regardless of where harm has occurred, and, 3) training for law enforcement personnel to tackle high-tech crimes. The Communique of the 1999 G8 Ministerial Conference on Combating Transnational Organised Crimes in Moscow includes a number of principles that formed the basis of a number of contemporary international strategies such as Council of Europe Convention on Cyber Crime. This includes the development of a 24/7 network of contacts requiring participating countries to establish points of contact for transnational investigations which are accessible at any point in time. Various meetings of G8 Justice and Interior ministers have repeatedly made reference to the Convention on Cyber Crime and repeatedly stated the need to create global capacities to combat cyber-crime.

[14] Please note that this list is not conclusive and that, through error, some important institutions may have been omitted.

3. INTERPOL - International Criminal Police Organisation

Mandate/Scope;

INTERPOL is the world's largest international police organization, with 187 member countries. Created in 1923, it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime. INTERPOL collects, stores, analyses and shares information on cybercrime with all its member countries through a global police communications system known as I-24/7. Other aspects of INTERPOL's cybercrime programme include the facilitation of operational cooperation amongst member countries through a list of contact officers. called NCRPs (National Central Reference Points), available at all times for cybercrime investigation. It also seeks to increase exchange of information among member countries on cybercrime methods through regional working parties and training workshops. The working parties are located in each continent to provide more localised services to member states. INTERPOL is capable of assisting member countries in cybercrime investigations through investigative and database services. Finally, it also organises an International Conference on Cybercrime every two years to bring together experts from law enforcement, private industry and academia to present and discuss the latest technologies used to combat cybercrime.

4. International Organisation on Computer Evidence

Mandate/Scope;

The International Organization on Computer Evidence (IOCE) was established in 1995 to provide international law enforcement agencies a forum for the exchange of information concerning computer crime investigation and other computer-related forensic issues. Comprised of accredited government agencies involved in computer forensic investigations, IOCE identifies and discusses issues of interest to its constituents, facilitates the international dissemination of information, and develops recommendations for consideration by its member agencies. In addition to formulating computer evidence standards, IOCE develops communications services between member agencies and holds conferences geared toward the establishment of working relationships. In response to the G-8 Communique and Action plans of 1997, IOCE was tasked with the development of international standards for the exchange and recovery of electronic evidence. Working groups in Canada, Europe, the United Kingdom, and the United States have been formed to address this standardization of computer evidence.

B. Regional

1. Council of Europe

Mandate/Scope;

The Council of Europe has highlighted the international nature of computer-related crimes since its conference on economic crimes in 1976. Its work culminated in Convention on Cybercrime which opened for signatures, including at the global level beyond EU borders, in 2001 in Budapest. So far 45 countries have signed the convention (as well as non-members of the council, such as; the USA, Canada, Japan, and South Africa), and 23 have ratified it. A number of countries such as Argentina, Pakistan, Philippines, Egypt, Botswana, and Nigeria have drafted parts of their legislation in accordance with the convention, even though they have not signed it. The Convention has proved to be a good starting point for model

legislation and was followed by an additional protocol on the criminalisation of racism and the distribution of xenophobic material. Most recently, in 2007, the Council introduced a Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse which has a provisions dealing with child pornography and the solicitation of children for sexual purposes.

2. European Union

Mandate/Scope;

The EU has primarily worked on the harmonisation of substantive criminal law with EU law amongst its member states. It has also worked to ensure co-ordination EU between members states represented in other international fora such as Council of Europe and the G-8. European Commission produced a "Framework Decision on Attacks against Information Systems" which takes note of the Council of Europe Convention on Cybercrime but concentrates mainly on harmonisation of substantive criminal law provisions in order to protect infrastructure elements. However, the European Court of Justice held that the Commission had overstepped its mandate in issuing a communication with this "Framework Decision". In 2007 an EU Directive was passed that placed Internet Service Providers under duty to store certain traffic data necessary for the identification of offenders in Cyberspace. This has led to controversy as any communication on the Internet will be covered by this Directive. The European Commission also published a communication in 2007 emphasising the Council of Europe's Convention on Cybercrime as the predominant international instrument on combating cybercrime.

3. OECD - Organisation for Economic Cooperation and Development

Mandate/Scope;

The OECD provides a setting for to compare policy experiences, seek answers to common problems, identify good practice and coordinate domestic and international policies. It has conducted a number of studies on the possibility of international harmonization of criminal law vis-à-vis computer crime. Within these studies it has given a minimum list of offences that countries should consider criminalizing. Its Information, Computer and Communications Policy (ICCP) Committee created a set of guidelines for information security in 1990 which were reviewed and amended in 2002. The OECD has also published reports on the impact of Spam on developing countries, and a report on the legislative treatment of "Cyberterror" in the domestic law of individual states.

4. Europol

Mandate/Scope;

Europol is the European Union Law Enforcement Organisation that handles criminal intelligence. Its mission is to assist the law enforcement authorities of Member States in their fight against serious forms of organised crime. Europol also coordinates the European Commission Prevention of and Fight against Crime (ISEC) programme to develop and deliver harmonised cybercrime training for all 30 European Union and candidate countries. Experts from Europol and INTERPOL, representatives of Internet service providers and academics are also involved in the programme, as is UNODC.

5. Asia-Pacific Economic Co-operation (APEC) Leaders

Mandate/Scope;

The Asia-Pacific Economic Cooperation (APEC) group is a forum for twenty one Pacific Rim countries (styled 'member economies') to cooperate on regional trade and investment, liberalisation and facilitation. APEC's objective is to enhance economic growth and prosperity in the region and to strengthen the Asia-Pacific community. In 2002 APEC leaders released a statement on fighting terrorism and promoting growth to enact laws relating to cybercrime and develop national investigating agencies capabilities. After this APEC adopted a Cybersecurity strategy which refers to existing international approaches by the UN and the Council of Europe. APEC also organized a conference on Cybercrime legislation in 2005 to help promote cooperation on cybercrime issues across the region.

6. The Commonwealth

Mandate/Scope;

The Commonwealth is a voluntary association of fifty three countries which support each other and work towards shared goals in democracy and development. The Law Ministers of the Commonwealth countries decided in 2002 to order an expert group to develop a legal framework for combating Cybercrime on the basis of the Council of Europe Convention on Cybercrime. The expert group presented their report and recommendations in 2002 which were converted into the Draft Model Law on Computer and Computer Related Crime later that year. This model law is in line with the standards defined by the Council of Europe Convention on Cybercrime.

7. Arab League and Gulf Cooperation Council

Mandate/Scope;

Although no regional agreement exists among member states a number of states have taken action individually to start drafting legislation or take measures against Cybercrime. Pakistan has a Draft Electronic Crime Act (2006) and both Egypt and the UAE also have draft laws that are yet to be formally passed. The Gulf Cooperation Council also recommended in 2007 that its member states seek a joint approach that takes into consideration international standards.

8. Organisation of American States (OAS)

Mandate/Scope;

Amongst a number of initiatives the OAS has tackled the issue of Cybercrime under the ambit of REMJA (the Ministers of Justice or Ministers or Attorneys General of the Americas). This section of the OAS held a number of meetings and produced recommendations such as the establishment of an intergovernmental experts group on cybercrime. This group is mandated to complete a diagnosis of criminal activity which targets computers and information/uses computers as the means of committing an offence and complete a diagnosis of national legislation, policies, and practices regarding such activity. At the most recent REMJA meeting in 2008 it recommended that member states give consideration to applying the principles of the Council of Europe Convention on Cybercrime and to adopt legal and other measures required for its implementation. It also recommended strengthening cooperation with other international organisations and agencies in the area of cyber crime such as the UN, EU, APEC, OECD, and G-8. Further, it recommended that member states establish specialised units to investigate Cybercrime and identify authorities

which will serve as points of contact in this matter and expedite the exchange of information and obtaining of evidence.

9. ASEAN - Association of South-East Asian Nations

Mandate/Scope;

The Association of South-East Asian Nations (ASEAN) and has nine member states. The aims and purposes of the Association are: (1) to accelerate economic growth, social progress and cultural development in the region and (2) to promote regional peace and stability through abiding respect for justice and the rule of law in the relationship among countries in the region and adherence to the principles of the United Nations Charter. A number of ASEAN countries have started to improve their domestic legislation using the Council of Europe Convention on Cybercrime as a basis. In order to facilitate this ASEAN has organized a number of regional workshops in order to brief its member states on the aims and content of the Cybercrime Convention. In addition the workshops have been used to help map and share information on Cybercrime legislation at the ASEAN Member State level and assess the relevant provisions of their national legislation with those of the Convention on Cybercrime with a view to its subsequent strengthening and/or the promotion of further AMS accessions to the Convention.

C. NGOs / Think Tanks / Academia

1. Anti-Phishing Working Group (APWG)

Mandate/Scope;

The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that results from phishing, pharming and email spoofing of all types.

2. European Financial Coalition (EFC)

Mandate/Scope;

The EFC is made up of payments companies and the police across Europe, and aims to stop sites that make a profit from selling or hosting these images by tracking the payments made to these sites. The EFC seeks to bring together all stakeholders involved in the fight against the commercial sale and distribution of child abuse images. These stakeholders shall help to identify, locate and safeguard victims while identifying, locating and arresting members, amongst other activities such as facilitating properly coordinated law enforcements investigations. Some of the members of the EFC's steering group include; the Child Exploitation Online Protection Centre (U.K), Europol, VISA Europe/MasterCard/PayPal and Microsoft.

3. International Association of Internet Hotlines (INHOPE)

Mandate/Scope;

INHOPE was founded in 1999 under the European Commissions Safer Internet Action Plan in order to combat growing concerns related to illegal content. It is an umbrella organization of national hotlines providing a possibility for internet users to report illegal content on the internet. INHOPE represents and coordinates a global network of Internet Hotlines and supports them in their fight against illegal content, this global network currently consists of

33 Hotlines in 29 different countries all over the world. Its stated mission is to support and enhance the performance of Internet Hotlines around the world in order to ensure that swift action is taken in responding to reports of illegal content. Effectively, INHOPE provides a single point of contact for global reports of illegal content to initiate global activities.

4. The International Centre for Missing & Exploited Children (ICMEC)

Mandate/Scope;

ICMEC was founded in 1998 and launched by the U.S.-based National Center for Missing & Exploited Children, it works to identify and coordinate a global network of organizations fighting child-sexual exploitation and abduction.

ICMEC's work brings promise to children and families by:

• Establishing a global resource to find missing children and prevent child-sexual exploitation;

• Creating national centers and affiliates worldwide;

• Building an international network to disseminate images of and information about missing and exploited children;

• Providing training to law enforcement, prosecutors, judges, legal professionals, nongovernmental organizations, and government officials;

• Advocating and proposing legislative changes in laws, treaties, and systems to protect children worldwide;

• Conducting International expert conferences to build awareness, encourage and increase cooperation and collaboration between and among countries; and

• Working along side financial industry and law enforcement to combat commercial child-sexual exploitation.

5. University College Dublin

Mandate/Scope;

The Centre for Cybercrime Investigation at the University College Dublin offers an MSc in Forensic Computing and Cybercrime Investigation. The programme is an international part-time MSc level programme, which is restricted to police officers. The purpose of the course is to produce graduates with skills that enhance their ability to investigate cybercrime. It introduces the concepts, principles, and professional practice in forensic computing and cybercrime investigation. The training is delivered mostly online with annual examination sessions taking place in Dublin and in associated training centres. Now an accreditation scheme also exists with the ongoing EC-funded ISEC programme. This allows students who have done ISEC intermediate courses to carry those credits towards the award of an MSc degree.

6. Canterbury Christchurch University

Mandate/Scope;

The University offers an MSc in Cybercrime Forensics which is currently only a part-time course for Law enforcement officers only. The programme is to be delivered with the UK's National Centre for Policing Excellence High-Tech Training Centre at Wyboston. The aim of the course is to equip students with the skills to assist in the investigation of a crime which involves the use of IT equipment and acquaint them with the legal, ethical and professional consideration which must be taken into account. Additional objectives are to enable crime scene examiners to recover and interrogate evidence more effectively, as well as to enable

the assembly of evidence for a court that is clear and supportive of evidential needs. The University also has an accreditation scheme with the UK NPIA High Tech Crime Training Centre, academic credit from which can be carried towards a number of post-graduate awards that can culminate in an MSc.

7. Asian School of Cyber Laws, Pune (ASCL)

Mandate/Scope;

Asian School of Cyber Laws is a registered society and public charitable trust headquartered in Pune, India. They offer a number of Diploma courses in Cyber Law and Cyber Crime Prosecution and Defence. They also offer postgraduate Programmes in Cyber Security and Incident Response, and Cyber Crime Investigation. ASCL has previously assisted the Indian government in framing rules associated to its Cyber legislation (Information Technology Act, 2000). In addition ASCL has conducted training programmes for government and police officials from Mauritius and Malaysia on Cybercrime investigation. Their training programmes on cybercrime investigation have also been conducted at a number of Indian government institutions such as the National Police Academy and the National Insurance Academy. Further, The ECommerce & Development Report 2003 recently published by the United Nations Conference on Trade and Development has quoted the findings of the Computer Crime and Abuse Report (2001-02) published by Asian School of Cyber Laws.

8. Cybercrime Research Laboratory - Macquarie University (CRL@mq)

Mandate/Scope;

CRL@mq was established in February 2007 by Macquarie University and National Australia Bank to conduct research into cybercrime and methods for the prevention and mitigation of cybercrime. The group will also create a refereed cybercrime journal to publish research of the group and other researchers in this area. CRL@mq's research will focus on: phishing and other financially motivated cybercrime attacks upon financial institutions, cybercrime where the system or network is a tool of criminal activity (e.g., spamming) or where a system is the target of criminal activity (e.g., unauthorized access), and traditional crimes facilitated using computers and networks (e.g., child porn, fraud). It's specific areas of research include; the disposition and nature of cybercrime groups, Botnet behaviour and prevention, the emergence of "Crimeware", customer behaviour with phishing emails, spamming tools and countermeasures, mapping the phishing networks and support structure, economics of phishing and the phishing marketplace, preventative measures against phishing for ISPs and regulatory agencies, as well as automated phishing email detection and classification.

9. National Government Authorities

Mandate/Scope;

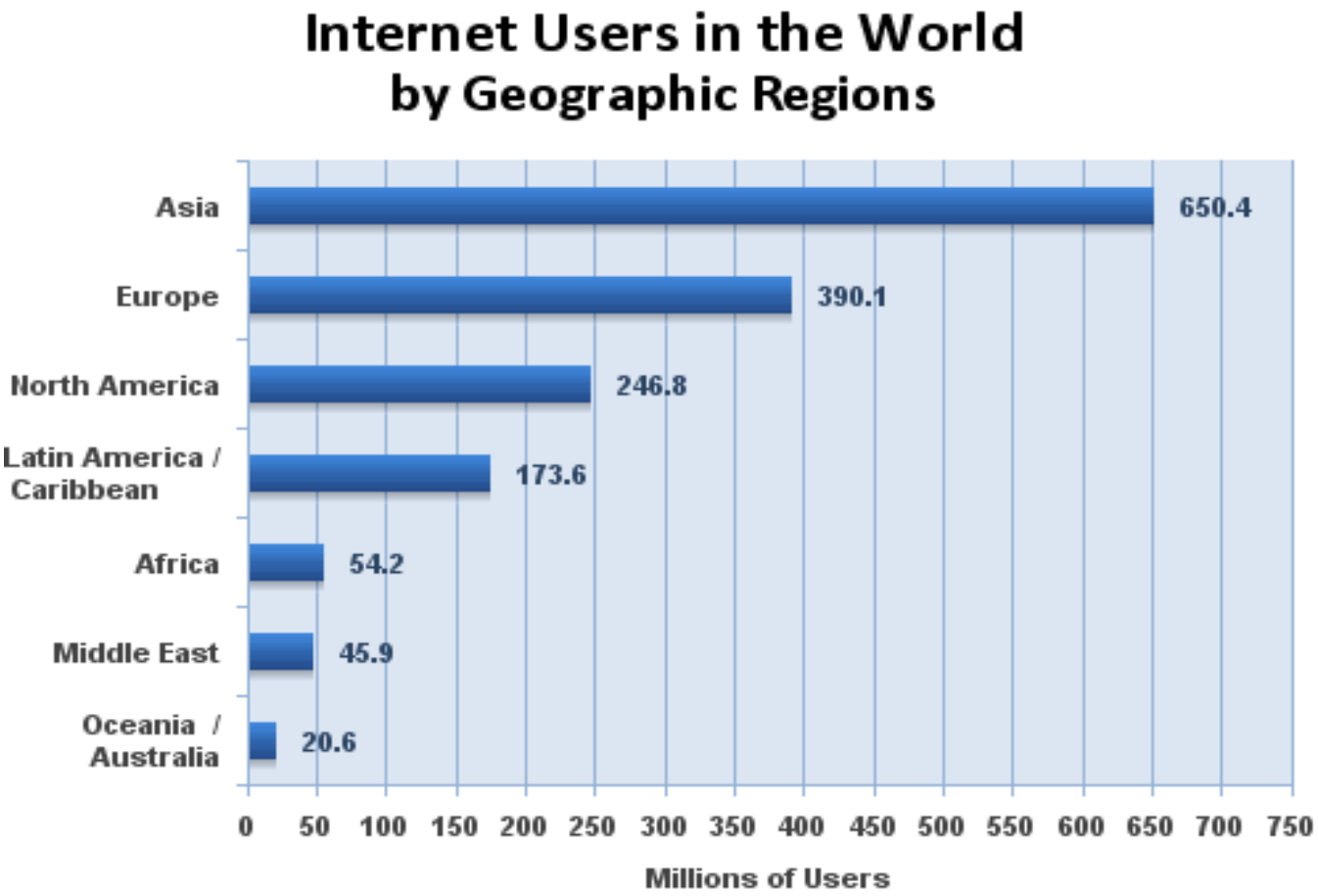
A number of countries have set up national authorities or adapted existing law enforcement agencies to address cybercrime related issues. Examples include the creation of the Cybercrime and Intellectual Property Section in the United States Department of Justice, and Cyber Action Teams within the FBI.

10. Universities dealing with Cybercrime

Mandate/Scope;

Other than those mentioned above, a number of universities offer undergraduate courses in information security systems, and certain elements of cybercrime. Often universities that offer Information Technology degrees have modules in cyber-security and the maintenance of the infrastructural integrity of computer systems.

Annex 3



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Estimated Internet users are 1,581,571,589 for year 2008

Annex 4

Some arguments for placing cybercrime within the context of development aid

UN peace-building missions, international financial institutions, development agencies etc, see "Rule of Law Reforms" within a comprehensive development framework, ranging from poverty eradication to peace and security.

Well-functioning law and justice institutions and a government bound by the rule of law are important to economic, political and social development, and over the past years, practitioners in the development field have turned increasing attention to reforms intended to improve law and justice institutions, thus laying down the foundations for long-term stability, development, empowerment and good governance.

Human rights, the rule of law and democracy are interlinked and mutually reinforcing. Rule of law promotion at the national and international levels is seen by UNODC as being crucial to the achievement of the Organization's goals, but also a serious and long-term challenge in many of the environments we work. Overall, however, the work of the Office in the areas of rule of law and governance is interlinked with the broader development context. Efforts to target the strengthening of international norms and standards and their implementation, as well as developing the legal, institutional, societal and cultural environments needed to ensure stability and sustain peace, promote justice and reduce poverty, and protect human rights are all emphasized when providing assistance to developing countries, in particular post-conflict and transition states.

The central role that the rule of law plays in development was recognized and emphasized in the report of the United Nations Millennium Project, which stated that "[t]he successful scale-up of investment strategies to achieve the Millennium Development Goals requires a commitment to good governance. This includes upholding the rule of law through administrative and civil services and through legal and judicial institutions." The report also states that "[t]he rule of law, a prerequisite to sound governance, can affect the way policies are formulated and implemented." Reforming the rule of law and re-establishing justice systems becomes even more essential for post-conflict societies. Strengthening the rule of law in the wake of conflict is not only an investment for the recovery of the country but, by addressing the grave injustices of war and the root causes of conflict, can help in preventing a return to hostilities.

One cannot attain long-term and sustainable development in a country unless all elements (access to health, education, employment, human rights, a functioning criminal justice system, good governance etc) which constitute a democracy are included. Many of the aid budgets today now take this fully into account.

Taking this a step further, and turning to the specifics of cybercrime within the context of development aid.

In 2003, the Secretary-General appointed a High-level Panel on Threats, Challenges and Change. Its final report, "A More Secure World: Our Shared Responsibility" (A/59/565) noted that transnational organized crime is one of the six major threats with which the world is confronted. Further, a number of instruments adopted by the international community have recognized the growing threat of cybercrime.

Look at almost any conflict/unstable zone in the world (and most fall within the developing world), and you'll find spoilers with links to criminal groups. Conflict creates cover for illicit enrichment - whether it be drugs, natural resources, the trafficking of weapons and people etc. It also creates profitable new markets for smuggled goods. In the absence of the rule of law and licit competition, criminal groups fill a lucrative vacuum. Since they profit from instability they have few incentives for peace (if applicable) and/or sustainable development. Organized crime is therefore a major threat to keeping and building peace and stability, and - because of its transnational nature - has an impact on regional security. All of this can also be applied to cybercrimes, the bulk of which are increasingly likely to involve organized criminal groups and/or be x-border.

According to the FBI in 2008, revenues from cybercrime have exceeded drug trafficking as the most lucrative illegal global business, estimated at reaping in more than US$1 trillion annually in illegal profits. This estimate has been quoted widely, although there are questions as to its accuracy[15]. Suffice to say revenues from cybercrime are certainly significant and increasing.

The impact of illegal activities broadly covered by term "cybercrimes" is multiple, and such crimes have serious social, development and economic consequences, particularly in least developed countries, and are a threat to basic human rights.

Cybercrime activities conducted in such countries can deter foreign investment, and the lax (or non-existent) laws, simply attract criminals seeking safe haven for their activities. It is imperative, therefore, that developing countries take steps to fight cybercrime not least so that they can also benefit from the boom in e-business. Further, cybercrime and poor information security can deter the application of information technologies, especially business use of the Internet, which would normally assist those countries to increase commerce, investment, innovation, productivity and efficiency.

Therefore, the world's poorer nations have to do more than upgrade technology to protect against cybercrime and to meet international standards for the security of computerized information. They also have to establish laws that criminalize cyber attacks and enable police to adequately investigate and prosecute such activities.

See in the below link, one example from Burkina Faso.

Fraud, data piracy, seeking partners on the internet: women in Burkina Faso are as much victims as perpetrators. From Ouagadougou to Banfora via Bobo-Dioulasso, and from Ouahigouya to Dori, all towns with an internet connection are affected by this phenomenon. However, the fight against this crime is in the tentative stages, if not altogether non-existent.

[15] "'Cybercrime exceeds drug trade' myth exploded", by John Leyden, The Register, 27 March 2009

Legislation is still under development. See rest of article under http://www.genderit.org/en/index.shtml?apc=a--e96160-1&x=96160

Finally, F-Secure recently indicated that Mexico, India and Africa are predicted as the Next Hotbeds of Internet Crime. NB The new 17,000 km long network of fiber optic undersea cables connecting much of east and southern Africa with India and Europe. South Africa, Tanzania, Kenya, Uganda and Mozambique are already connected and plans are underway to add Ethiopia and Rwanda. The lower costs and higher bandwidth and lower latency of this will improve services at cyber cafes, personal use as well as mobile access. This is of course excellent on the one side in terms of narrowing the digital divide and bringing Africa up-to-speed, but the ICT criminals can also have a field day.

Taking the above into account, it is clear that this form of crime is becoming an increasing threat globally and in particular in those developing countries where adequate legislation, law enforcement capacities etc are not equipped to deal with it. Also, with access to the internet over the next 5 – 10 years being through mobile internet systems, we can predict that, even those countries where, today, the problems may be less, will be increasingly affected.

Democracy & governance, economic growth, education, global partnerships, and humanitarian assistance are all issues being addressed by development aid packages, and deterring the de-stabilizing effects of cybercrimes, which are not going to go away and can only increase, in developing countries, should also fall in this context.

Annex 5

SWOT analysis: UNODC and cybercrime

The following is the list, under each of the four headings, that experts in UNODC's October 2009 meeting felt were relevant. It is recognised within the analysis that an item may fall under more than one heading.

STRENGTHS

- Experience in organized crime
- International organization (CJS, LE + Legal + Gov)
- Strong regional presence (Field offices)
- Brings people together
- Consensus building
- Fund raising ability
- Presence in developing countries
- Other UN organizations
- Network of contacts
- Stakeholder relationships
- Brand
- Working tools
- Language diversity
- Network of training centers
- Political influence
- Complimentary programs (organized crime + corruption)
- Reach to civil society
- Enables early member involvements
- Sustainability of solution

WEAKNESSES

- No in-house cybercrime expertise?
- Late mover
- Slow mover
- Bureaucratic
- No clear definition of the issue
- Short term funding
- Credibility in cybercrime space
- Costly grandiose project base
- Flavor of month mentality
- Unclear mission on cybercrime
- Members can change priorities (regional)
- Goals to ambitious-cybercrime
- Comfort zone meetings/workshops
- Limited delivery capability in cybercrime

• Clashes/duplications
• Other UN organizations
• Increased confusion

OPPORTUNITIES

• Define the problem
• Crime Congress (Awareness opportunity)
• Design UNODC mission on cybercrime
• UNODC has opportunity to take leadership and work with international entities on cybercrime
• Opportunity to promote best practice on counter-cybercrime measures in developing countries
• Global focal point capability (for leveraging existing initiatives)
• Political awareness (linked to funding) and capacity building
• Stakeholder development
• Using existing material
• Leverage existing networks (database)
• Technological solutions
• Further analysis of phenomenon
• Public awareness opportunity
• Global cybercrime report
• Take training seriously

THREATS

• Clashes with organizations, which are already in the cybercrime space
• Lack of understanding of issue (UNODC + members)
• Budapest Convention is politically controversial
• Technological advances
• Over demand
• Over expectations
• Other UN organization views
• Field office independent actions
• Lack of resource in UNODC
• Scarcity of suitable resources
• Lack of prioritization in UN