United Nations
A Time for Renewal

ELEVENTH UN CONGRESS
ON CRIME PREVENTION AND CRIMINAL JUSTICE
Bangkok, Thailand 18-25 April 2005

Committee II
9th Meeting* (PM)

BKK/CP/19
22 April 2005

CRIMINALIZATION OF COMPUTER WRONGDOING PREREQUISITE

FOR COMBATING CYBERCRIME, WORKSHOP TOLD

Speakers in Crime Congress Workshop Address Evolving Nature
Of Cybercrime, Digital Divide, Harmonization of Laws, Cooperation with Private Sector

Crime had grown so fast in the "bottomless world of cyberspace" that legal and law enforcement bodies should "step up to the plate", the keynote speaker of a workshop on measures to combat computer-related crime told the Second Committee of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice this afternoon.

Kraisorn Pornsutee, Permanent Secretary, Ministry of Information and Communication Technology, Thailand, went on to say that a prerequisite for combating computer-related crimes was to criminalize acts of computer wrongdoing. Attitudes, however, varied greatly from country to country as to what constituted a nuisance and what was a crime. The next crucial element of any international effort against cybercrime was to facilitate technology transfer and engage in capacity-building. Legal and technology experts needed to cooperate closely without any barriers whatsoever. The digital divide between the legal and technical matters needed to be closed at the national, regional and global levels to effectively put up a fight against what was essentially a global crime wave.

Panellists this afternoon addressed matters of the evolving nature of computer-related crimes, the digital divide, technical assistance, cooperation with the private sector and the harmonization of law. A number of case studies in international cooperation were also presented.

One of the panellists, Professor Peter Grabosky of the Australian National University, said digital technologies now provided ordinary citizens with the capacity to inflict massive harm. He described three trends in computer crime: sophistication, commercialization and integration. Sophistication meant the greater skill and capacity that criminals brought today. Crime followed opportunity, and development would attract new crime. One such area was wireless networks. Regarding commercialization, he said hackers now offered their services on a fee-for-service basis, in other words, "hackers for hire". Integration meant the combination of different criminal acts in furtherance of the same criminal enterprise.

He said that, as of now, there had not been any catastrophic successes in the area of cyber terrorism -- attacks against computers and networks to intimidate or coerce a government or its

(more)

* 8th Meeting was not covered.

people in furtherance of political or social objectives. For the time being, terrorists preferred truck bombs to logic bombs. The Internet was an ideal medium for propaganda, however, and digital technology was ideal for psychological warfare. In order to control cybercrime, it was important to strive for harmonization in criminal law to develop a seamless mutual assistance framework. Technology would continue to grow and, as it did, new criminal opportunities would be created. Those who failed to anticipate the future were in for a huge shock when it arrived.

Gareth Sansom, Director, Technology and Analysis, Criminal Law Policy Section, Department of Justice, Canada, addressing the subject of the "digital divide", said there had been progress over the past decade, and the gap was gradually closing. All things being equal, however, it would take decades for countries at the bottom of the divide to reach the status of the countries in the middle. There were distinct patterns of vulnerability for cybercrime. Countries at the lower end of the digital divide were used as staging grounds to launch attacks.

Amanda Hubbard, Trial Attorney, Computer Crime and Intellectual Property Section, Department of Justice, United States, provided a case study in which speedy cooperation was required regarding a kidnapping case in South Africa in order to track down the perpetrator who was using an e-mail address. Thanks to innovative technical assistance at the Internet service provider, the kidnappers were apprehended and the victim was freed. Cyberspace moved much faster than human beings, she said. Speed was key when saving property or lives. Other important lessons included not neglecting traditional law enforcement techniques; building relationships between police forces, prosecutors and judges; and cooperating with the private sector.

Ioana Albani, Chief, Prosecutor's General Office Attached to the High Court of Cassation and Justice, Romania, described the evolution in Romanian law regarding cybercrime. She said there were difficulties in finding the right jurisdiction, for instance the place where the crime was committed (Romania) and the place where the crime produced its results (at that time almost always in the United States). She stressed that Romania, even without the necessary resources, had answered and was still answering international requests for legal assistance.

Hamish McCulloch, Assistant Director, Interpol General Secretariat, explained how the Interpol child abuse image database was used to identify the victims and perpetrators of child pornography. He provided examples of several cases in which the use of the database had resulted in the identification of children and conviction of the offender. While it was not an offence in many countries to possess images of child abuse, it was, however, an offence to abuse a child. Investigations focused on the prosecution of distributors of images. Law enforcement needed to shift its focus to the identification of victims.

In the ensuing interactive dialogue, representatives explained how their own countries dealt with computer-related crimes and the difficulties encountered therein. They stressed the importance not only of international cooperation but also of training of law enforcement personnel, judges, prosecutors and lawyers in the complex issue of cybercrime. They asked how training could be best provided, and how Interpol and the United Nations, in particular the United Nations Office on Drugs and Crime could be helpful in that regard.

Participating in the discussion were the representatives of Ukraine, Austria, Libya, France, Spain, United Kingdom, Argentina, Canada, Morocco and Chile.

Individual experts Christopher Ram and Ehab Elsonbaty also spoke, as did representatives of Microsoft and the World Federation of Scientists.

The workshop was organized by the Korean Institute of Criminology, whose President, Taehoon Lee also addressed the Second Committee.

Background

Committee II of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice held a workshop this afternoon on the theme "Measures to combat computer-related crimes".

A background paper (document A/CONF.203/14) highlights the challenges posed by computer-related crimes, or "cybercrime", and contains a number of recommendations. According to the paper, the worldwide proliferation of new information and communication technologies has given rise to more forms of computer-related crime, which pose threats not only to the confidentiality, integrity or availability of computer systems, but also to the security of critical infrastructure. Technological innovation gives rise to distinct patters of criminal innovation. Different threats from computer-related crimes mirror, therefore, differences across the spectrum of the so-called "digital divide".

When combating such crimes, a number of forensic problems challenge investigators, prosecutors and judges. Effective investigation and prosecution of computer-related crime often require tracing criminal activity through a variety of Internet service providers or companies, sometimes across national borders, which may result in difficult questions of jurisdiction and sovereignty. Computer-related crime, therefore, necessitates international cooperation, which requires countries to be equipped with the necessary legal, procedural and regulatory tools. A number of regional and interregional efforts have been undertaken in recent years, leading to several significant accomplishments. In order to bring those efforts to fruition, it is necessary to support a wide range of research on the various aspects involved in combating computer-related crime to foster an active partnership between government and the private sector.

The four regional preparatory meetings for the Congress proposed a number of recommendations, including: to examine current experience and existing national legal frameworks and arrangements for cooperation between States, as well as between States and Internet providers; to examine ways to promote cooperation between governments and the private sector; to explore ways of enhancing the capacity of governments to develop special investigative techniques; to deal with the use of computer technology in exploiting women and children, especially pornography and paedophilia; to examine the feasibility of establishing a global Internet task force; and to consider proposing the negotiation of a new convention against computer-related crime.

Computer-related crime includes theft of telecommunications services or computer services by using hacking techniques. Servers and websites could be targets of denial-of-service attacks, viruses and worms. Computers were also used as instruments to commit crime, such as modification of data, electronic vandalism, forgery and counterfeiting, information piracy, industrial espionage and copyright infringement. There were many types of computer-related crime

involving attacks on banks or financial systems, as well as fraud involving transfer of electronic funds. Other problems involve telemarketing and "phishing" or spoofing spam. Existing offences such as extortion and harassment are also carried out online. In recent years, increasing attention has been devoted to the relation between terrorism and the Internet, as the Internet was being used to facilitate terrorist financing and as a logistics tool for planning terrorist acts.

The working paper contains some recommendations, including a broad, inclusive focus to address problems of cybercrime, going beyond criminal law, penal procedures and law enforcement. International cooperation at all levels should be developed further. All States should be encouraged to update their criminal laws as soon as possible in order to address the particular nature of computer-related crimes. Governments, the private sector and non-governmental organizations should work together to bridge the digital divide, raise public awareness about computer-related crime and to enhance the capacity of criminal justice professionals.

The working paper further recommends that attention should be devoted to establishing, improving and broadening the current practical tools for international information sharing, and early warning systems, using Interpol, alert mechanisms of the Group of Eight, the Convention on Cybercrime, Computer Emergency Response Teams (CERTs) and the Forum of Incident Response and Security Teams (FIRST). Computer-related crime policy should be evidence-based and subject to rigorous evaluation to ensure efficiency and effectiveness.

SLAWOMIR REDO of the United Nations Office on Drugs and Crime introduced the background paper.

Welcoming Remarks

TAEHOON LEE, President, Korean Institute of Criminology, said the rapid growth and globalization of information technologies had dramatically changed the way people communicated. Millions of people paid bills, consulted professionals, conducted research and made connections with family and friends in cyberspace. As cyberspace continued to become an integral part of life, cybercrime or computer crime posed new challenges to the criminal justice system. The global nature of cybercrime raised difficult legislative problems of jurisdiction as criminals used offshore servers and Internet sites to avoid domestic regulations. Crime in cyberspace, such as cyberterrorism, cyber-money-laundering, cybergambling, Internet fraud and cyberstalking, could occur instantaneously, and offenders targeted victims in other countries where the offence was not easily detected.

The seriousness of cybercrime was reflected in the fact that cyberspace had become the target of terrorists and organized crime groups, he said. Unfortunately, there were few bilateral or multilateral treaties or conventions addressing important cybercrime issues. The Council of Europe Convention on Cybercrime was the first international treaty on the subject. The Korean Institute of Criminology was a government-sponsored research institute tasked with analysing trends, causes and consequences of crime and providing control measures and preventive policies. The Institute's primary goal was to assist in the Government's criminal justice policy formulation through research. He hoped the workshop would serve as a valuable forum to promote international operation on crime prevention and crime control.

Keynote Address

KRAISORN PORNSUTEE, Permanent Secretary, Ministry of Information and Communication Technology, Thailand, said the workshop had been organized to find ways to combat computer-related crimes. For that, a prerequisite was to criminalize acts of computer wrongdoing. Attitudes varied greatly from country to country as to what constituted a nuisance and what was a crime. For example, in Thailand, lese-majesty was considered to be a crime of the most serious magnitude. In some jurisdictions, it was an act that fell under freedom of speech. That was but one example of the task in reconciling internationally what was to be considered a crime.

He said the next crucial element of any international effort against cybercrime was to facilitate technology transfer and engage in capacity-building. Information and communication technology had developed at a breakneck speed. Legal and technology experts needed to cooperate closely without any barriers whatsoever. The digital divide between the legal and technical matters needed to be closed at the national, regional and global levels to effectively put up a fight against what was essentially a global crime wave. In his country, his Ministry was the spearhead in the effort to bridge the digital divide. And its network reached into the smallest village. Crime had grown so fast in the "bottomless world of cyberspace" that legal and law enforcement bodies should step up to the plate.

Recent Trends in Cybercrime

PETER GRABOSKY, Professor, Australian National University, said digital technologies now provided ordinary citizens with the capacity to inflict massive harm. The uptake of digital technology was uneven around the world. What was happening in Country A on one side of the digital divide would happen next year in Country B on the other.

He described three trends in computer crime, namely sophistication, commercialization and integration. Sophistication meant the greater skill and capacity that criminals brought today. The speed with which viruses travelled the world was much more rapid today, and it was possible to produce perfect imitations of legitimate websites, using them to infect visitors and steal credit card information. The term "phishing" was used for the practice of sending messages that appeared to be from a legitimate source to a criminal site. Crime followed opportunity, and development would attract new crime. One such area was wireless networks. "War driving" meant driving around in a motor vehicle with an antenna to locate access points.

Regarding commercialization, he said that legitimate electronic commerce provided opportunities to exploit that commerce. Hackers now offered their services on a fee-for-service basis, in other words, hackers for hire. Integration meant the combination of different criminal acts in furtherance of the same criminal enterprise. Extortion included communicating a threat electronically, targeting information systems, demanding payment in digital form and using digital technology to collect intelligence about victims.

Cyberterrorism referred to unlawful attacks against computers and networks to intimidate or coerce a government or its people in furtherance of political or social objectives, he continued. There had been no catastrophic successes yet, however. For the time being, terrorists preferred truck bombs to logic bombs. Terrorists could send and receive message aided by encryption.

Digital technology was good for collecting information. The Internet was an ideal medium for propaganda. Digital technology was also ideal for psychological warfare, projecting images of hostage executions with profound impact.

The challenge for lawmakers was to differentiate between the legitimate uses of cyberspace from communications directly in furtherance of terrorism, he said. To control cybercrime it was important to strive for harmonization in criminal law to develop a seamless mutual assistance framework. Technology would continue to grow and, as it did, new criminal opportunities would be created. Those who failed to anticipate the future were in for a huge shock when it arrived.

Digital Divide and Cybercrime

GARETH SANSOM, Director, Technology and Analysis, Criminal Law Policy Section, Department of Justice, Canada, said the term "digital divide" invoked the idea of a gap between the haves and have-nots, in this case linked to information and communication technology. The digital divide brought to mind differences in the capability to use information and communication technology between different groups. "Infostate" was an indicator that comprised different elements that constituted how individuals and organizations communicated, as well as how information might be acquired, as well as the education level within a country that enabled people to use information and communication technology. There had been progress over the past decade, and the gap was gradually closing. All things equal, however, it would take decades for countries at the bottom to reach the status of the countries in the middle.

He said the widespread adoption of computer networks had realized dividends in the economic area. There were, however, also distinct patterns of vulnerability for cybercrime. Countries at the lower end of the digital divide were used as staging grounds to launch attacks. Emerging information and communication technology infrastructure was disproportionately vulnerable to attacks.

The type and scale of computers and networks were different for corporate and consumer groups. A monolithic response to cybercrime was, therefore, not viable. Consumers had become vulnerable to telemarketing fraud, phishing and online auction fraud.

The matter of computer viruses was another issue. One class of those viruses was called "worms". Worms were independently replicating and autonomous, seeking out their own targets. Some types of worms replicated too fast for human intervention. They would require an automated defence. Some worms showed high penetration in countries with a high infostate, more so than in countries with low infostate density, and vice versa.

He said worm infections occurred mostly in the most advanced countries. Developing countries saw an explosion of usage of mobile phones. There was now a new virus that specifically infected mobile telephones and that virus was spreading primarily in developing countries. Some virus infections might only be a staging ground for another type of attack. Fast worms became a new tool for committing cybercrime and opened a window of opportunity for other crime. Those new uses of worms might expose developing countries to new threats at the same time that they sought to adopt information and communication technology.

Case Studies in International Cooperation

AMANDA HUBBARD, Trial Attorney, Computer Crime and Intellectual Property Section, Department of Justice, United States, provided a case study, noting that, on 16 July, the United States Department of Justice received an emergency request for assistance from a Federal Bureau of Investigation (FBI) attaché in South America. The federal police reported that a woman had been kidnapped. They requested assistance from the Justice Department to track down the individual who was using an e-mail address. The user could have been anywhere in the world, but had chosen an Internet service provider that provided free mail access as it was easy and fast. By midday that day, the attaché had obtained the address for the Internet service provider e-mail account and set up a trap and trace order on the account. Later that day, the Department of Justice contacted a United States district court to let it know they needed a "pen trap" order. A judge had been asked to stay late so that, when the information arrived, he would be able to help find the victim.

Two hours later, the Justice Department had obtained the order, she said. The FBI agents in the field office where the service provider was located began monitoring traffic immediately for any information they could find. Innovative technical assistance at the Internet service provider found a way to link the address with a beaconing device so that he could be notified within seconds of a perpetrator logging into the account. The federal police in the participating country also used other methods to search for the kidnappers. The following morning, the targets of the investigation accessed the e-mail account. The police received the Internet protocol address and placed a trace that showed that the account was being accessed from a South American country. While it could have been anywhere in the world, because of online real-time investigative efforts they had been able to find out that the person was in the country. They worked with a local service provider to follow up on trace information provided by the FBI, closing in on where the kidnappers were checking the account. The police moved in and were able to free the victim, who was elderly and in bad health. Swift action on the part of all saved her life.

Cyberspace moved much faster than human beings, she said. Speed was key when saving property or lives. Other important lessons included not neglecting traditional law enforcement techniques; building relationships between police forces, prosecutors and judges; and cooperating with the private sector.

IOANA ALBANI, Chief, Prosecutor's General Office Attached to the High Court of Cassation and Justice, Romania, said a lack of resources had led to the failure of investigations into the first cases of Internet fraud reported in Romania. In 2000, the authorities had decided to establish an office for the investigation of computer-related crimes in the Prosecutor's General Office Attached to the High Court of Cassation and Justice. When investigating the first cases, a first criminal charge was established, that of fraud. Regardless of the environment, those criminal actions were considered deception, and the first cases were filed by using charges of fraud, forgery or identity theft, and several people were convicted.

There were difficulties in finding the right jurisdiction, she continued. Was it that place where the crime was committed (Romania) or the place where the crime produced its results (at that time almost always in the United States)? With the support of the legal attaché of the United States Department of Justice, a new modus operandi was established to meet standards required by the

Romanian courts. Romania had signed the Budapest Convention on Cyber Crimes in 2001, and legislative measures had been taken to counter cybercriminality. An inter-ministerial working group, joined by representatives of civil society and Internet providers, was established.

In 2002, there was a boom in information and communication technology, as well as a boom in complaints about fraud committed by Romanians on the Internet, she said. The Romanian Parliament had adopted special legislation on electronic commerce. It was now criminal to forge electronic payments. The new law offered law enforcement agencies an instrument sufficient for prosecution. In April 2003, a law on countering cybercriminality had been adopted that criminalized several acts against the integrity and confidentiality of information technology data. Child pornography was also addressed. Through the law, a special department within the Prosecutor's General Office Attached to the High Court of Cassation and Justice had been established, with the duty to answer international information requests regarding cybercrime. Also, the police had established a special service within their General Inspectorate.

The Romanian Public Ministry and Inspectorate of Police ran a website to communicate in an accessible language with the computer community. It disseminated information on legislation in the field, gave warnings, received complaints, and provided statistics, as well as a forum for discussion. Regarding international cooperation, she said that Romania, even without the necessary resources, had answered and was still answering international legal assistance requests. Her country had ratified the European convention on cybercriminality in 2004.

HAMISH McCULLOCH, Assistant Director, Interpol General Secretariat, explained how the Interpol child abuse image database was used to identify the victims and perpetrators of child pornography. The purpose of the database was to support law enforcement globally. An investigator would want to know several things, including whether the child was investigated; where the child was; whether the image was known; and whether the image had been distributed. Was there evidence in the picture to identify the child? Since the inception of the database, the number of images had increased. Individuals in 100 countries were involved in the distribution of the images. There were some 10,000 to 20,000 victims from more than 14 countries. Interpol received 20 to 30 new requests per month

He then provided examples of several cases in which the use of the database had resulted in the identification of children and conviction of the offender. While it was not an offence in many countries to possess images of child abuse, it was, however, an offence to abuse a child. Investigations focused on the prosecution of distributors of images. Law enforcement needed to shift its focus to the identification of victims.

Discussion

CHRISTOPHER RAM, individual expert observer from Canada, asked if, considering the ever changing nature of cybercrime, technical assistance materials could be considered, such as the United Nations Manual of Cybercrime which was last published in 1994. What was the extent to which crime prevention could be built into new technology? To what extent should fighting cybercrime be born by the State? In what other way could technologies be used by authorities to counter cybercrime?

Mr. GRABOSKY said the manual referred to had been produced a long time ago, and a revision was long overdue.

SCOTT CHARNEY, of Microsoft, said that the private sector had an enormous role to play. On the proactive side, the information and communication technology industry had to produce usable technology to ensure that crimes did not occur. It also had a responsibility to work with law enforcement. The information technology industry must also provide training for law enforcement and help in capacity-building.

Mr. McCULLOCH, of Interpol, said his organization used technology in a number of ways. With the increasing number of videos being circulated with kidnapping victims, there was a highly secure communication network through which, for instance, dialects could be tracked down. The analysis of images was also important in identifying victims. The clue to a country was often found in a remote corner of the picture, and the moment that was the case, modern technology could be used to get a response back from a country. Interpol hoped to develop resource centres of excellence with experts in various fields.

Mr. SANSOM noted that cases of technical ability to collect digital evidence required forensics training at the officer level. Computer worms were sometimes written by programmers in a number of different countries. When the worm was released, it had spread to dozens of other countries, launching subsequent attacks. Worms were active, communicating with a central control point to update them and provide them with new modules.

Ms. HUBBARD (United States), addressing the issue of assistance, noted that the International Legal Law Enforcement Assistance Centre in Bangkok held training sessions.

Mr. REDO said there were a number of projects concerning training. The United Nations had produced a manual on the control of computer crime in the 1994. That would need to be more actively followed up. Following the Congress, the Secretariat would be looking into the issue of technical assistance.

VALERIY PIDPALY (Ukraine) noted that computer crime was an offence under his country's criminal code. The criminal code had been amended on numerous occasions. In 2004, new provisions were added to the code, establishing that computer crimes would be investigated by the country's Interior Services. During the recent election, an investigation had been carried out into the case of a virus causing disruption of the country's computer system. On 1 January 2005, a new law had entered into force, establishing liability for cybercrimes. He hoped that the sharing of experience in the field would promote the introduction of proposals to improve methods to target cybercrime.

WOLFGANG SPADINGER (Austria) said he had been both impressed and frightened by the presentations. It was imperative that the international community concentrate on the area of technical cybercrime. What were the major impediments for their investigations and for the prevention of cybercrime and what could the international community do to overcome those impediments?

MUSTAPHA M. OMAR DEBARA (Libya) raised the issue of crime resulting from the increased use of electronic payments. Many banks were now using such systems, and there were great weaknesses in the systems. Crime had existed since the dawn of civilization, and it would be difficult to imagine the complete suppression of crime. Yet, the fight against crime had been ongoing. In fighting crime, however, the rights of individuals ultimately needed to be respected.

Responding to the various questions, Mr. SANSOM said a series of basic building blocks needed to be in place in order to address the major impediments, including laws at the domestic level to gather evidence. Mechanisms were also needed at the international level. He also suggested greater recourse to mutual legal assistance measures.

Also addressing the issue of impediments, Mr. McCULLOCH explained that the legislation of a number of countries did not permit them to send a picture for the Interpol database.

Ms. HUBBARD (United States) stressed the need to develop greater outreach and partnerships with the private sector since it controlled the vast majority of critical infrastructure. Without that sector's knowledge and input, progress would never be made. Sharing resources and training opportunities was also critical. The International Telecommunication Union (ITU) had been looking at the issue of harmonization to allow investigations to proceed faster. The technical aspect of cooperation was often harder than police cooperation.

Regarding development projects, she said the United States had two outreach programmes through the World Bank and the United States Agency for International Development (USAID) that looked at the information security standards when new telecommunications were going into a country. It was better to look at security on the front end so that people running the system would understand the default settings for the software and how to keep security running.

JEAN-PIERRE VIDON (France) said cybercrime undermined the security of individuals, corporations, institutions, and also values. It required a comprehensive response which required technology and investigation. France was focusing on awareness-raising. There was also a need to intensify law enforcement efforts, not only by specialists but by all personnel to strengthen investigative capacities. It was necessary to monitor the Internet in order to identify illicit material of a terrorist, paedophile or racist nature. Technology research centres had to be established in order to stay a step ahead of offenders.

He said international cooperation must be developed as computer-related crimes did not take national borders into account. The Convention of the Council of Europe on Cybercrime had entered into force last year and was open to third-party States. Four non-European States had signed it. The Gendarmerie had created a department for the fight against cybercrime with the task of policing the networks. It also had the task of following up on any information received from individuals. Also a centre for analysis of paedophile images had been set up. That centre cooperated closely with counterparts abroad, especially with Interpol.

GARCIA MODILLO (Spain) said his country was creating a mechanism to monitor the use of new technologies by criminals. It also wanted to create indicators on Internet use. Spain wanted to examine innovative programmes to stay ahead of the game. He asked whether Interpol had a

specific programme in that regard. He also suggested that UNODC establish a contact network of experts.

Mr. MCCULLOCH said Interpol had held a major seminar on cybercrime in Lyon, which had attracted a large number of delegates. Interpol was also represented within the G-8 group, and it was important to avoid duplication of effort. The 24/7 call-out system was an example.

KEVIN McNULTY (United Kingdom) asked about the possibility of a computer crime manual. He also wanted to plug the 24/7 contact network; 39 countries had joined the network, and the more that did, the better. He wondered whether a database had already been established.

Mr. REDO said that, in the past, there had been training activities on the United Nations criminal justice information network. Ten years ago, the Government of the Republic of Korea had proposed a training course on the United Nations Criminal Justice Network.

Mr. McCULLOCH said there was a training manual specifically for officers investigating crimes against children. Interpol also partnered with the United States Centre of Missing and Exploited Children. Around 800 police officers had been trained in the last year. The subject of a database had been mentioned before. It was difficult to keep up to date.

GRACIELA SCARNATI ALMADA (Argentina) said it seemed that disparate efforts needed to be coalesced into one United Nations programme in order to better monitor the situation. It was like having a number of pearls but no string. Many countries did not even have legislation on cybercrime. Did the panel think that one of the United Nations programmes could act as coordinator for the various efforts?

DANIEL A. MacRURY (Canada) said that, as a front line prosecutor, he had experienced that cooperation worked in specific cases, as well as in the area of training. The 24/7 contact list of the G-8 was crucial, but equally crucial was to have better contacts with prosecutors worldwide on an ongoing basis. He suggested establishment of a contact list of all prosecutors worldwide, as well as a training manual for prosecutors.

Mr. SANSOM reacted by saying that the 24/7 contact network was restricted to computer crime and law enforcement agencies that already had a capacity and resources to deal with computer-related crimes. There was, indeed, room for other contact networks, such as for prosecutors.

Ms. HUBBARD (United States) said that, regarding a training manual for prosecutors, some resources were available within the Computer Crime and Intellectual Property Section of the United States Department of Justice. She did not now know of any centralized database on available training, but there was an informal network of prosecutors that was involved in training.

Mr. GRABOSKY drew attention to the fact that, at the regional level, organizations of prosecutors existed. Those bodies could provide a platform for training.

Mr. McCULLOCH said that Interpol had introduced a communication system called I-24/7, a virtual private network that was totally secure. Interpol bureaus in each country could pass out the tools to law enforcement agencies to get instant access to information in Interpol databases.

BRAHIM BOUABID (Morocco) said his country had been formulating legislation on computer-related crimes for two years. It had implemented a law on data-processing and against terrorism related to computer use. There were, however, problems of implementation and of the presentation of evidence. He asked how evidence should be handled and how to get technical assistance to judges and lawyers. Could the United Nations come up with a manual for judges, lawyers and prosecutors, maybe geared to specific types of judicial systems?

Ms. HUBBARD (United States) said there were several organizations providing technical assistance to prosecutors and judges. Her own organization had provided technical assistance to Nigeria on a bilateral basis. The Council of Europe had also been involved in some outreach programmes.

Mr. SANSOM said that a number of model laws had been developed, among them one for the Commonwealth. The G-8 had also undertaken model law initiatives, one regarding the collection of evidence.

Mr. VIDON (France) said his country had reviewed its own body of law regarding protection of computer systems and techniques necessary to combat crime. He invited the delegate of Morocco to get in touch with the French Ministry of Justice for information.

EHAB ELSONBATY, an individual expert, said pornography was a sensitive issue. How far could one cooperate with countries that criminalized pornographic websites? he asked. He suggested that not only saving child pornography images should be a crime, but also navigating to find child pornography should be a crime.

Mr. McCULLOCH said that, regarding adult pornography, Interpol did nothing unless asked for action. Resources were focused on children who were sexually abused. Different countries had gone to different degrees when writing their legislation. There were countries that had gone as far to say that viewing child pornography was legal, but that storing it was a criminal offence.

Mr. SANSOM noted that, regarding legal challenges, in cases where individuals sought not to store images on hard drives but evaded prosecution by viewing images, Canada had changed the child pornography law to address both supply and demand by adding two phrases into existing provisions. "Accessing" would address the question of user demand and "making available" would deal with streaming video sites.

Mr. GRABOSKY asked about images created digitally -- morphed images and not actual living beings?

Mr. McCULLOCH said legislation in that regard was not uniform. Some had addressed the issue, others had not. In some countries, one had to prove the age of the child and prove that the child was real. Figures were looking more and more real everyday.

Mr. DEBARA (Libya) asked if the Latin principle could be used concerning evidence in the field of cybercrime. Would criminal evidence need to be re-examined in a more specific fashion? Regarding how one gathered evidence, he said evidence was not always legitimate. Were there model cases which would improve understanding about how to counter the problems?

HECTOR SOTO CANDIA (Chile) said high-tech crime must be fought with advanced technology.

HENNING WEGENER of the World Federation of Scientists said the focus today had been primarily on individual victims. Were they missing the larger threat of cybercrime to society? Cybercrime could be highly destabilizing. He was speaking of critical infrastructure countries. In almost all countries, those critical entities were in private hands, including air traffic control, banking and energy. Today, the stabilizing features of interwoven societies were managed and controlled by digital means. Cyberwar was yet another issue.

Mr. GRABOSKY noted that private institutions with assets to protect were well advised to protect them. Most invested in the protection of their own assets quite substantially. In some cases it was a matter of good sense. In other cases, market forces would move institutions to protect their assets.

Ms. HUBBARD (United States) said that, from a State perspective, the United Nations was doing significant work in the area of critical infrastructure protection.

Mr. McCULLOCH explained that the responsibility of companies protecting their assets was similar to individuals being responsible for protecting their own property.

Summarizing the discussion, Mr. REDO, of UNODC, said seven key themes had emerged. The first theme was the evolving nature and speed of computer-related crimes and the array of offences that were encapsulated in cybercrime. That had raised questions about monitoring and data collecting. The second theme was that of the digital divide. Building of capacity had been mentioned in that regard. A third area of concern was the issue of technical assistance. What could be done? What was being done? What could the United Nations and UNODC do? The critical issue of training was also mentioned.

He said a fourth theme was international cooperation. As it had become clear, speed was required in many cases. Although the 24/7 network was mentioned, it had also been mentioned that it incorporated only States that had the resources to use it. It had been asked how that mechanism could be strengthened. A fifth theme was that of cooperation with the private sectors. As a sixth theme, the harmonization of law was mentioned. Much of that related to admissibility of evidence and gathering evidence in cybercrime matters. The final theme was the question of victims, both individual victims and collective victims such as societies, companies and States that could be targeted by cybercrime, including terrorism.

*** *** ***