UNITED NATIONS
Office on Drugs and Crime

www.unodc.org
www.11uncongress.org

The Eleventh United Nations
Congress on Crime Prevention and Criminal Justice,
18-25 April 2005, Bangkok, Thailand

Fact sheet 6

COMPUTER-RELATED CRIME

Information and communication technologies (ICTs) are changing societies around the world: improving productivity in traditional industries, revolutionizing labour processes and remodelling the speed and flow of capital. However, this rapid growth has also made new forms of computer-related crime possible.

Computer-related crime is difficult to fully grasp or conceptualize. Often, it is regarded as conduct proscribed by legislation and/or jurisprudence that entails the use of digital technologies in the commission of the offence; is directed at computing and communications technologies themselves; or involves the incidental use of computers with respect to the commission of other crimes.

Types of computer–related crime

- Several computer-related crimes target ICTs themselves, such as servers and websites, with global computer viruses causing considerable damage to both business and consumer networks.
- Electronic vandalism and professional forgery or counterfeiting.
- Theft or fraud, for instance, hacking attacks on banks or financial systems, and fraud involving transfers of electronic funds.
- Computers are used to facilitate a wide range of telemarketing and investment fraud involving deceptive practices.
- "Phishing" or "spoofing spam" is the construction of e-mail messages with corresponding web pages designed to appear as existing consumer sites. Millions of these fraudulent e-mails are distributed, claiming to come from banks, on-line auctions or other legitimate sites in order to fool users into answering by submitting financial, personal or password data.
- Dissemination of illegal and harmful material. During the past years, the Internet has been used for commercial purposes by the legitimate "adult entertainment industry". However, the Internet is now increasingly used for the distribution of material deemed to be legally obscene in several countries. Another area of concern is child pornography. Since the late 1980s, it has been distributed increasingly through a range of computer networks, using a variety of Internet services, including websites. A certain proportion of the distribution of child pornography has been linked to transnational organized crime.
- In addition to the Internet being used for dissemination of hate propaganda and xenophobic materials, evidence suggests that the Internet has been used to facilitate terrorist financing and distributing terrorist propaganda.

The digital divide and computer-related crime

The distribution of ICTs around the world is not uniform. There are vast differences in the type and number of technological advances in different parts of the world. The so-called digital divide was recognized by the United Nations Millennium Declaration in 2000, which articulated eight Millennium Development Goals aimed at achieving measurable improvements in the lives of the largest portion of the world population. One of the goals, calling for development of global partnerships for development, also calls for cooperation with the private sector, for making available the benefits of new technologies—especially ICTs. At the same time, as the benefits begin to spread, it is necessary to increase awareness of the threats and vulnerabilities associated with computer-related crime.

The Declaration of Principles adopted by the World Summit on the Information Society states that today the benefits of the information technology revolution are unevenly distributed between the developed and developing countries and within societies. The Declaration also includes the commitment to turning this digital divide into a digital opportunity for all, in particular for those who risk being left behind and being further marginalized.

Crossing borders: transborder crime and computer forensics

Investigating computer-related crime is not an easy task, as most of the evidence is intangible and transient. Cyber crime investigators seek out digital traces, which are often volatile and short-lived. Legal challenges also arise owing to problems of borders and jurisdictions. The investigation and prosecution of computer-related crime highlights the importance of international cooperation.

Solutions through international cooperation

The increasing density of ICTs also increases the frequency of domestic computer-related crime, which requires States to establish domestic legislation. National laws adapted to address cyber crime may be required to effectively respond to foreign requests for assistance or to obtain assistance from another country. Compatibility with the laws of other nations is an essential goal when developing legislation; international cooperation is needed owing to the international, transborder nature of computer-related crime. Formal international mechanisms are needed in order to respect States' sovereign rights and to facilitate international cooperation. For mutual legal assistance to function successfully, substantive offences and procedural powers in one jurisdiction ought to be compatible with those in another.

Various initiatives have been taken to raise awareness and promote international cooperation in combating computer-related crime, including actions by the Council of Europe, the European Union, the Group of Eight, the Organisation for Economic Co-operation and Development and the United Nations. In a workshop dedicated to this topic, the Crime Congress is expected to offer a unique opportunity to discuss in depth the challenges posed by cyber crime and measures to foster international cooperation against it.

For further information:

www.unodc.org and www.unis.unvienna.org

V.05-82111