The Council of Europe and Cybercrime

Cybercrime – the Facts

The Internet has a tremendous impact on societies all over the world. In 1999 there were 300 million Internet users. The number doubled to 600 million by 2002 (figures from INSEAD/World Economic Forum: The Network Readiness Index 2003 – 2004).

E-commerce is taking off. According to the Economist (15 May 2004), Americans are expected to be spending more than $200 billion dollars on line in 2004, and Europeans are beginning to match their enthusiasm.

Globalisation of markets is made possible by the Internet. Potential customers are now available, world-wide, at the push of a button. The same is true for the anti-globalisation campaigner: they can also rally support through the net.

The reliance on the Internet makes societies vulnerable. The main risk is cybercrime.

Daily threats range from spams to viruses, hacking, identify theft, fraud and child abuse.

Potential threats include cyber-terrorism, that is, shutting downs of entire essential infrastructure or the use of computers as weapons – disabling critical systems or threatening whole populations.

Information and communication technologies provide organised crime with new tools to carry out old-style organised crime, and new tools for new types of crime:

Organised crime groups use the Internet for major fraud and theft. They can exploit differences in the law in different countries to carry out their crimes.

Internet allows easier laundering of money gained from classical crime: techniques include over- or under-invoicing and cyber auctions. E-banking and the use of e-money makes it easier to move around dirty money.

The Internet makes it easy to work anonymously and network with other criminals.

Cybercrime threatens every member of society - not only Internet users:

- Individuals and businesses are exposed to fraud by using the Internet.
- Hackers can "steal" their bank details by hi-jacking legitimate systems – for instance inserting pages where the client is asked to give personal data which would allow access to their cash.
- Children become the victims of paedophiles.
- Hackers also threaten life and business if they disable systems with "denial of service attacks".

Spam is not just a nuisance but can be life threatening if it blocks essential systems in hospitals or emergency control centres, and can lead to the loss of millions of Euro for business.

Racists and fascists disseminate their bigoted materials through their hate websites or spams.

Even if 99.9% of the 600 million Internet surfers were to it use it for legitimate reasons, this would still leave 600,000 potential offenders.

A few individuals can create havoc on the Internet – viruses such as Sasser and I-love-you disabled key systems world-wide.

According to the Internet Fraud Complaints Centre (figures from Nov 2003), cybercriminals caused an estimated 150 – 200 billion Euro worth of damage in 2003.

Cybercrime poses many challenges to law enforcement and criminal justice systems.

The Internet makes it easy to operate from foreign jurisdictions, especially where regulations and enforcement capacities are weak.

Data moves at high speed and is difficult to track.

Even law enforcement authorities can be accused of cybercrime. FBI agents who used hacking techniques to track down two hackers in Russia have been counter-charged with cybercrime offences.

Cybercrime can be a diffuse concept with different meanings in different societies. This hampers international co-operation.

The Council of Europe Cybercrime Convention

Facts

The Council of Europe Convention on Cybercrime, which entered into force on 1 July 2004, is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international co-operation between State Parties to this treaty.

It is not limited to Europe, and other countries are expected to join. Canada, Japan, South Africa and the USA have signed the convention. The US have also ratified it.

So far (12 March 2007) it has been signed by 43 countries, including five non-member states of the Council of Europe, and ratified by 19.

The Convention is complemented by a Protocol on Xenophobia and Racism committed through computer systems (1 March 2006). The protocol has been signed by 31 countries and ratified by 10.

The Convention and its Protocol are followed by the Committee on Cybercrime (T-CY).

The Council of Europe helps countries to ratify, accede and implement these treaties through the Project on Cybercrime.

Why is it the right solution?

Societies need to be protected against cybercrime, but there must be freedom to use and develop information and communication technologies properly, and a guarantee that people can be free to express themselves.

If there is one crime that requires international co-operation, it is cybercrime. Cybercriminals rely on being able to operate across borders and exploit differences in national law.

Law enforcement and criminal justice authorities need to be given the means to prevent and control cybercrime.

Measures against cybercrime must be based on law; and laws need to be harmonised or at least compatible to permit co-operation.

The Convention meets these needs.

It provides a clear concept of cybercrime by requiring countries to criminalise four types of offences, thus promoting a harmonised approach:

- Offences against the confidentiality, integrity and availability of computer data and systems (CIA offences) – including illegal access to computer systems, illegal interception, data interference, systems interference, misuse of devices.
- Computer-related offences – including computer-related forgery and fraud.
- Content-related offences – that is, child pornography (the Protocol to the Convention adds racism and xenophobia).
- Offences related to infringements of copyright and related rights.

It sets up procedures to make investigations more efficient.

- By immediate preservation of computer data.
- By empowering authorities to request the hand-over of specific computer data.
- By allowing investigators to collect traffic data and intercept the content in real-time.

It puts procedures and systems in place that make international cooperation work more effectively. For example:

- It sets up a 24/7 network that works 24 hours a day, seven days a week to provide immediate help to investigators at any time.
- It facilitates extradition and the exchange of spontaneous information.
- It helps authorities from one country to collect data in another and facilitates mutual legal assistance between countries.

The Convention is based on the principles of the European Convention of Human Rights. It is subject to a range of conditions and safeguards. This means that people’s right of expression or right to privacy will not be sacrificed.

Cybercrime is one of the major challenges facing modern society. The Council of Europe believes the Convention is an ideal way for governments to anticipate problems and resolve them, working together to create security for the citizens of Europe and beyond.