Key note address
Current threats and future challenges posed by cybercrime

Michel Quillé, Director of Europol

OCTOPUS INTERFACE CONFERENCE

ON COOPERATION AGAINST CYBERCRIME

Council of Europe, Strasbourg, 10 March 2009

1. Introduction
Characteristics of cybercrime

The rapid development of technology has improved the possibilities for criminals as well. For computer, cyber-, and high tech crime, the common denominator is the use of technology for criminal activities.

Computers can be used by criminals in two ways. They may be the target of an attack. They may be also a facilitating factor in committing crimes.

The violation of privacy and the theft of personal and financial data are the main high tech crimes. These are:

- Hacking
- Cracking of passwords
- Copyright infringement
- Phishing and pharming
- Spreading malicious codes and child abuse images.

The use of the internet is the main vehicle in facilitating these criminal activities.

In general terms, criminals engaged in these activities are individuals who:

- Are organised to commit crime on the internet
- Hired by criminal groups to commit crime via internet

- People who regularly offer their services to the best bidder to commit crime on the internet
- Scattered cells, spread all over the world, which illegally operate on the internet.

An important common characteristic is that for them the internet creates unique opportunities.

Criminal groups are very difficult to trace on the internet. This is because there are deficiencies in key areas, such as:

- Global information about the internet itself
- Common reporting system on internet crimes
- Reporting system for the victims
- Spread of information
- Data retained by the private sector
- Common strategy at an international level.

2. Europol response to the cybercrime challenge

Computer crime is an explicitly mandated area for Europol.

In addition, occurrences of high-tech crime become apparent in all other crime areas within the Europol mandate.

This renders computer crime increasingly ‘horizontal’. Furthermore, high-tech crime is virtual and thus it’s completely cross-border. You could say it is borderless.

The current law-enforcement capacity to deal with high-tech crime throughout the EU is far from homogeneous. There is clearly an asymmetrical development. Some MS are forging ahead with great advances in certain areas. Other MS are behind in terms of technology. This creates the need to have a centralised service to assist all MS. This assistance should be focused on:

- Coordinating joint activities
- Promoting the standardisation of approaches and quality
- Identifying and sharing best practice.

Only this way can we ensure a homogenous EU law enforcement response to high-tech crime.

How can Europol help in making this a success?

Europol’s core business is to provide support to the competent authorities in the EU member states in their fight against organised crime and terrorism. Europol does this by serving member states in the capacity of:

- Information facilitator
  - Info-Ex
  - LBx
- Crime analysis provider
  - Strategic (TE-SAT, OCTA)
  - Operational
- Operational support provider
  - On the spot, on demand
  - No coercive powers.

To specifically fight cybercrime, a dedicated platform to serve all the needs of MS has been created. Since 2002, the High Tech Crime Centre at Europol has been fulfilling this function.

Moreover to further pursue this goal, Europol is working on the creation of the so-called cybercrime platform. This platform is to comprise 3 constituent sub-platforms.

A. Platform for reporting offences noted on the Internet

Following a proposal made by the French Presidency, Europol has been invited to coordinate a European response to internet-related crime. This is to be done by creating a European platform for reporting offences noted on the Internet. The Presidency also invited Europol to develop common strategies to fight internet-related crimes. This initiative foresees achieving its objectives in several phases and concluding by mid 2010.

The idea is to establish a platform compliant with the legal framework as well as security and data protection requirements at Europol. It should also be compliant with the business needs of the member states.

More specifically this solution should:

- Improve coordination of investigations at European level
- Support Joint Investigation Teams
- Avoid duplication of work in investigations by building up an alert system enabling
    - Prompt reaction of concerned MS
    - Coordination of internet investigations
- Provide the basis for operational and strategic analysis
- Give insight into new crime trends or threats and allow swift action by MS
- Compile statistical data whenever necessary.

B. Dedicated Analysis Work File

As a follow up to the member states' initiative called "OC exploiting ICT", Europol proposed to open a dedicated AWF. The AWF will be called *Cyborg* which stands for cyber organised crime. The objective of the AWF is to support in the best way the needs of MS in fighting cybercrime.

Most of the member states say that they are affected by internet or ICT-driven organised crime. The aim of this crime is financial gain through computer attacks. Most of the countries mention cybercrime elements such as:

- Malicious software used for ID theft
- E-banking attacks
- Use of ‘money mules’ for laundering the illegal gains.

The new AWF will additionally strengthen the investigation support given by Europol to member states. The AWF is expected to be put in place presently.

C. Cybercrime knowledge platform

A third sub-platform is called ‘Cybercrime knowledge’. It consists of a portal-base facility where the exchange of best practice will take place. No personal data will be exchanged. This technical recipient will be a fundamental tool for Europol to support cybercrime investigations. It will aid the investigators to keep them abreast of technical skills.

Cybercrime investigations require expertise and specialisation in different areas. There is no so-called ‘expert in cybercrime’. This expertise comprises several areas ranging from internet to forensic investigations. The cybercrime learning process consists of two elements. It is formed not only by studying the theory. It also means learning through practice. Cybercrime expertise gets outdated in a very short time unless a regular update is guaranteed.

In 2007 an *ad-hoc* working group on harmonisation of cybercrime training was established at Europol. The working group is composed of:

- Various law enforcement organisations (such as member states’ high tech crime units and police academies)
- Academic bodies
- International organisations (such as EC, CEPOL, Interpol, Eurojust, OLAF, CoE, and UNDOC)
- Private sector, such as Microsoft and Ebay.

This ensures that there is a high standard in cooperation and coordination of training courses. The training courses are accredited by respective universities.

3. Conclusions

The increasing technological advances offer great opportunities to all individuals, including criminals.

Consequences from this for law enforcement are following:

- Lack of consistent OC data caused by the internet volatility
- Increasingly beneficial ‘horizontal’ use of hi-tech for OC
- Rapid growth of the underground economy through attacking computer systems
- Consistent growth of social engineering on the internet
- More flexible organised crime structures thanks to the internet:
    - Criminal organisations can easily change tactics after a police crackdown

- They have several links at international level with other members
- They exploit the internet as a networking tool.

What are then Europol recommendations on counter-action? In a nutshell, let me present 5 main points regarding the best response to these new challenges.

First, there is a need to share more intelligence and cooperate. The more information is shared, the easier it is to build an efficient common strategy to properly fight HTC.

Second, there is a need to improve common understanding with private industry. The private sector is one of the main sources and ways for law enforcement to tackle HTC.

Third, there is a need to educate users of internet on how to utilise technologies. Handling HTC is not only a law enforcements' issue. Therefore proper awareness programmes for the users should be organised. Information is an asset and it has to be protected. Education is the keyword.

Fourth, the ratification of the Cybercrime Convention should occur. We should aim for it to become the common international legal platform. Moreover, all countries should make an effort to update their legislation, keeping pace with technology.

Finally, there is a need to harmonise forensic investigations to have a common approach in presenting evidence in court.

Irrespective of different legal systems and languages, the same technical tools are used in hi-tech crime investigations. This makes cooperation in HTC easier than one could think.

Thank you very much for your attention.