CYBERCRIME PRESENTS A MAJOR CHALLENGE FOR LAW ENFORCEMENT

03 Jan 2011

Press Release

The Hague, the Netherlands

The world is evermore dependent on high–tech communications and banking systems. At the same time, the underground economy where cybercriminals trade their illegally obtained information, skills and tools, is flourishing.

Whilst the value of the cybercriminal economy as a whole is not yet known, the most recent estimate of global corporate losses alone stands at around €750 billion per year. The scale of the problem is itself a threat to law enforcement response capability – with more than 150 000 viruses and other types of malicious code in circulation, and 148 000 computers compromised per day (source: McAfee).

“Cybercrime is borderless by nature – this also makes criminal investigations more complicated for law enforcement authorities. To effectively tackle cybercrime, adequate cross–border provisions are needed, and international cooperation and mutual assistance within EU law enforcement, and between the EU and third countries, needs to be enhanced.” says Rob Wainwright, Director of Europol. He continues: “As the EU’s criminal intelligence and information hub, Europol has advanced IT tools and a large team of professional analysts and experts ready to support the work of European law enforcement authorities in their fight against cybercrime.”

As part of the Stockholm Programme, whose aim is to create a single area of justice and security for the European Union’s 500 million citizens, Europol has been invited to step up strategic analysis on cybercrime. Several conclusions and initiatives have been agreed upon to define a concerted strategy to fight cybercrime effectively. This will be carried out in a way appropriate to the multiple crimes committed by these means: sexual violence and child sex abuse imagery, terrorist activities, attacks on electronic networks, fraud, identify theft, etc.

To contribute to the strategic planning for a European Cyber Crime Centre, Europol has produced the iOCTA* - a Threat Assessment on Internet Facilitated Organised Crime. The iOCTA's findings address current and future challenges and are based on EU law enforcement intelligence and open source material.

This week, Europol will deliver a series of press releases related to the challenges caused by

cybercrime.

Europol's iOCTA: Selected findings and recommended actions

- EU Member States already rank amongst the most highly infected countries in the world when it comes to computer viruses and malware. As internet connectivity continues to spread, EU citizens and organisations will be subjected to more cyber attacks, and to attacks from previously underconnected areas of the world. Combating cybercrime will therefore require new international strategic and operational partnerships.
- **Active partnership with the private sector** is essential, not only to share intelligence and evidence, but also in the development of technical tools and measures for law enforcement to prevent online criminality. The academic community also has an important part to play in the research and development of such measures.
- Because of the global reach and scale of internet facilitated organised crime, its disparate nature, and the unprecedented volumes of data involved, **centralised coordination of intelligence** gathering, analysis, training, and partnership management is required at an EU level, to ensure that Member States and EU agencies make the most effective use of resources. The establishment of a **European Cybercrime Centre**, as outlined in the recent Council conclusions on cybercrime and in the EU's Internal Security Strategy, will be an important and timely step forward.
- Awareness raising on individual and corporate user responsibility are key to combating cybercrime. **EU–wide awareness raising and points of contact** are required for a range of issues, including illegal downloading, social engineering, payment card security, securing wireless internet connections, and the risks to children. The use of crowdsourcing to gather intelligence on cybercrime from internet users should also be considered.

Europol's role in the fight against cybercrime

- Europol is the European Union law enforcement agency. It plays a key role in the **European Cybercrime Task Force** – an expert group made up of representatives from Europol, Eurojust and the European Commission, working together with the Heads of EU Cybercrime Units to facilitate the crossborder fight against cybercrime.
- By means of its **cybercrime database**, Europol provides EU Member States with investigative and analytical support on cybercrime, and facilitates crossborder cooperation and information exchange.
- **Strategic analysis of Internet Facilitated Organised Crime** (iOCTA) assesses current and future trends in cybercrime, and informs both operational activity and EU policy.
- The **Internet Crime Reporting Online System (ICROS)** and **Internet & Forensic Expert Forum (IFOREX)** are currently in development. These will provide centralised coordination of reports

of cybercrime from EU Member State authorities, and host technical data and training for law enforcement.

CRIME AREAS Cybercrime • High-Tech crime
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES European Cybercrime Center (EC3)

Source URL: https://www.europol.europa.eu/newsroom/news/cybercrime-presents-major-challenge-for-law-enforcement