OCTOPUS PROGRAMME

Threats, Trends and the Perspective of Europol

Strasbourg, 21st – 23rd November 2011

The Threat

- The threat from cyber crime is multi-dimensional, targeting citizens, businesses, and governments at a rapidly growing rate.
- Cyber attacks are getting more and more sophisticated and the new generation of malware aim not only at disrupting the computer networks but also at extracting financial and personal data which is the new e-commodity.
- Organised crime use internet technologies that play a key-role in facilitating most forms of criminalities such as e-frauds, production and dissemination of child abusive images, e-extortion, e-laundering = Old Crimes, New Tools.

The Trends

- There is now a sophisticated and self-sufficient digital *underground economy* in which data is the illicit commodity.
- Cyber crime rates continue to increase in line with Internet adoption: mobile Internet access and the continuing deployment of broadband internet infrastructure throughout the world therefore introduces *new levels of vulnerability*
- Cyber crime is a truly global criminal phenomenon does not respond to *single jurisdiction* approaches to policing, cloud computing is a clear example
- Criminals *get organised* on internet, offering their skills or are hired by criminal organisation to perpetrate crimes
- The regulations do not have *the same pace* as technologies
- Investigations gather large mass of data to manage and *digital forensic* plays an important role

European Cybercrime Centre

- At EU level a European Cyber Crime Centre (ECC) will be established by 2013, to cope with the increasing threat of Cybercrime.
- A feasibility study for the establishment of such a Centre is being conducted by RAND Europe, to be delivered in December 2011.
- The results of the feasibility study will include recommendations as to where an ECC would be best placed, what resources are required and an estimation of the costs for its realisation.
- Informed by this study, the Commission will issue a communication in March/April 2012 which will decide the centre's scope, key capabilities, budget and location.

Strategy of Europol toward ECC

- Operational and intelligence capabilities having dedicated Analysis Work Files that provide analytical support for cybercrime investigations in Member States
- Internal computer forensic capability and “On the spot” forensic support for investigations in Member States
- Internal operational capability in cybercrime
- Development of platforms for experts (IFOREX) and reporting (ICROS) for cybercrime
- Enlarging the business to join cybercrime/cybersecurity (ENISA)
- New strategic insight into cybercrime that informs national and EU policy measures (iOCTA)
- Hosting the European Union Cybercrime Task Force and chairing European Financial Coalition, and membership of the Virtual Global Taskforce
- Specialised R&D and training capability through an Outreach Programme toward no-law enforcement entities.

Challenges

- Cyber crime involves a large number of stakeholders, PPP is a keyword
- Protection of targets of attacks is a commitment of different entities, a broad collaboration is needed
- Due to the mobility of data and the virtualization of networks, new concepts of data retention and protection can be foreseen in the future
- Encryption methods challenge LE in the interpretation of data to be investigated
- Cyber security and cyber crime is a chain to be built
- Fill the gap between investigation and prosecution
- Need to reinforce international legal instruments to investigate cyber crime

EUROPOL

Back or to the Future?