Europol Cybercrime Centre

The perspective of Europol on Cybercrime

Courmayeur Mont Blanc, Italy, 2-4 December 2011
The threat from cybercrime is multi-dimensional, targeting citizens, businesses, and governments at a rapidly growing rate.

Cybercriminal tools pose a direct threat to security and play an increasingly important role in facilitating most forms of offline criminality.
The Challenges

- There is now a sophisticated and self-sufficient digital *underground economy* in which data is the illicit commodity.
- Cybercrime 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*.
- Cybercrime is a truly global criminal phenomenon which does not respond to *single jurisdiction* approaches to policing.
- Criminals *organise* themselves on the Internet, offer their skills or are hired by criminal organisations to perpetrate crimes.
- Regulation *does not keep pace* with technology.
• Disrupt the infrastructure of malicious code writers and specialist web hosts through the active identification of developer groups
• Active targeting of the proceeds of cybercrime in collaboration with private sector
• Improve knowledge on cybercrime
• Continue to develop insight into the behaviour of the contemporary cybercriminal by means of intelligence analysis, criminological research and profiling techniques
• Harness the intelligence of network and information security stakeholders
The ECC simultaneously pursues three lines of activity:

- **Operations** – provide investigative support by coordinating and contributing to Member States’ investigations. Includes operational analysis, specialist forensic support and technical forensic R&D tasks.

- **Oversight** – improves insight into criminal behaviour through strategic analysis, highlights future risks, and supervises knowledge management for the centre.

- **Outreach** – informs and influences through training and liaison.
The Instruments of Europol against Cybercrime, 
The Europol Cybercrime Centre
Creation of a recipient at Europol to host all the offences noted on the internet and reported at domestic level

To deliver reliable and up-to-date products to EU MS concerning the overview of internet crime types;

To deliver an early warning mechanism to MS as a tool for pre-emptive action against new cybercrime threats;

Advise the EU MS where to steer their future strategies in fighting Internet crimes
Focus of AWF on Cybercrime

- Focus on Internet/ICT driven organized crime aimed at financial gain
- Crimes defined in the cybercrime convention (art. 2-8) including but not limited to ID theft, e-banking scams, and e-commerce fraud and e-laundering
- Initially directed to malware driven e-banking attacks

Objective AWF CYBORG

- Building a cross-border information position on active groups
- Group structures, roles, Modus operandi, Routes for or money, Sequence of events; etc

Primary goal

- To support ongoing investigations or to initiate new cross-border cases
Cybercrime Business Model

Cybercrime group

“hackers”

“Command”

“e-launderers”

- Performing hacking
- Developing malware
- Building botnets
- Perform ID-theft
- Collect Personal Info
- Collect financial info
- Execute e-crimes
- e-banking
- e-commerce

- trade stolen goods, stolen information, malware, tools, expertise, skills

Underground Economy
Perceived Investigative Opportunities

- Criminal Groups
  - Analyse the malware
  - Follow the money

Underground Economy
- trade stolen goods, stolen information, malware, tools, expertise, skills
The new concept is to have **TWO** AWFs

- One AWF will focus on Serious and Organised Crime (Units O3, O5, O6, O7 and O8)
- One AWF will focus on Counter Terrorism (Units O4 and O9)
**AWF SOC**

SERIOUS & ORGANISED CRIME

<table>
<thead>
<tr>
<th>COPY</th>
<th>SMOKE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOYA</td>
<td>COLA</td>
</tr>
<tr>
<td>SYNERGY</td>
<td>CHECK POINT</td>
</tr>
<tr>
<td>CANNABIS</td>
<td>HEROIN</td>
</tr>
<tr>
<td>PHOENIX</td>
<td>FURTUM</td>
</tr>
<tr>
<td>COPPER</td>
<td>EEOC</td>
</tr>
<tr>
<td>MONITOR</td>
<td>TWINS</td>
</tr>
<tr>
<td><strong>CYBORG</strong></td>
<td>SUSTRANS</td>
</tr>
<tr>
<td>MMTC</td>
<td>TERMINAL</td>
</tr>
</tbody>
</table>

**AWF CT**

COUNTER TERRORISM

| HYDRA | 04 |
| DOLPHIN | 04 |
| PIRACY  | 05 |
| TFTP    | 06 |
| CHECK THE WEB | 09 |
• Act as AWF manager
• Task the Focal Point/Target Groups
• Process and cross check contributions not falling in an existing FP/TG
How will it work?

- MS/3rd parties
- AWF serious and organised crime
- Operational Centre
- AWF counter terrorism
- Regional support officers

INTELLIGENCE
INFORMATION
INFORMATION
INFORMATION
INFORMATION
The transition

- Current AWFs should become Focal Points within AWF SOC and AWF CT.
- FP and TG provide analysis and operational support
- As a second step the Focal Points will be reviewed together with the MS to assess the priority areas.
• Gather the European Cybercrime LE community under one umbrella to harmonise best practices and training
• Build a knowledge base (guidelines, white papers etc.) on technologically related matters
• Build a repository of commonly used scripts/software
• Encourage users to extensively share information and best practices
• Offer MS services to aid their investigations
• Established at Europol in July 2007
• Between 40-60 members as permanent participants
• LEA, international organisations, private industries, universities
• Mainly financed by COM under ISEC
• Harmonisation of training for LEA with accredited programme to universities (Bologna convention - ETCS)
• Master of Science on cybercrime
• Continuous follow-up in training modules development and delivery
• Introductory IT Forensics and Network Investigations
• Linux as an Investigative Tool Part 1
• Linux as an Investigative Tool Part 2
• Applied NTFS Forensics
• Mobile Phone Forensics
• Internet Investigations
• Network Investigations
• WiFi and VOIP investigations
• Malware Analysis
• Live Data Forensics
• Forensic Scripting using BASH
• Train the trainers
• Vista and Windows 7 Forensics
• Databases and Data mining
• Intermediate Mobile Phone Forensics
Strategic Group formed by the Heads of National Cybercrime Units in EU Member States, European Commission and Eurojust

Several issues discussed and action plan:

- Prompt response to serious cybercrime incidents
- Operational priorities to fight new cybercrime threats
- Relationships with non-Law Enforcement partners
- Relationship with non-EU Law Enforcement
- Technical and Legal issues on new trends and threats
Main concept – Three components:

1. A network of computers dedicated to the pre-processing and analysis of data obtained from digital sources in the framework of AWF activity

2. Specific laptops and tools to provide on-the-spot computer forensics support

3. A research and development laboratory for computer forensics including a decryption platform
Mobile Office
Added value: live checks and communication with Europol systems (Siena, Index System, EIS, AWF database), can be combined with any of the forensic tools below.

Forensic laptops
Added value: analyse computer files, extract data, compare hash values, search keywords, recover email traffic, decrypt protected files, provide expertise, filter for relevance, enables live checks.

Universal Forensic Extraction Device (UFED)
Added value: recover data from mobile phones, sat phones, PDA and navigation systems, recover deleted SMS, enables live checks with Europol information systems.
Thank you

Questions?

Roberto Fernández Alonso
Europol Cybercrime Centre
☎️ +31 (0)70 3531427
✉️ roberto.fernandez@europol.europa.eu