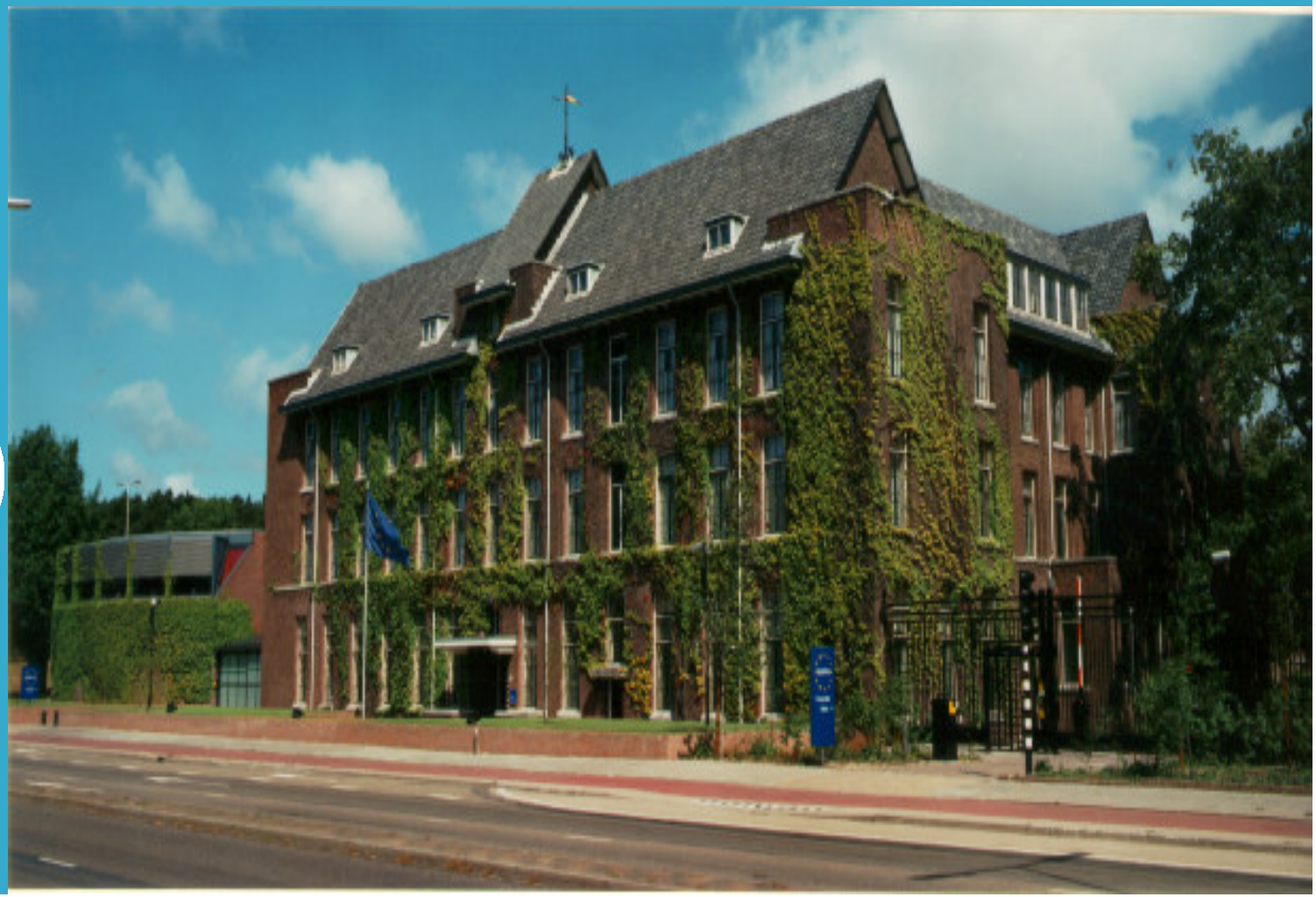
# Octopus Programme

# Strasbourg, 1-2 April 2008

EUROPOL



# High Tech Crimes

CYBER CRIME: **computer as <u>TARGET</u>**

- **Hacking (D-DOS, Botnets, Zombies…)**
- **Crimewares (Virus, Worms, Trojans…)**
- **Spamming (blackmail, cyber-stalking…)**

COMPUTER RELATED CRIME: **computer as <u>TOOL</u>**

**E-Frauds, E-Laundering, Child Pornography, E-Terrorism, Phishing, ID-Theft, Drugs, Extortions….**

# People Organized / Criminal Organizations?

- Are there people organised to commit crimes on the internet?
- Are there people hired and paid by criminal groups to help them to commit crimes on the internet?
- Are there people who offer their skills to illicitly gain money using internet?
- Are there scattered cells that illegally operate on the internet?

# Is Organized Crime behind E-Crimes?

- Organised Crime:
  - **Issues in mapping – Internet is volatile and has no boundaries**
  - **OC uses horizontally Internet to easily pursue illicit goals**
  - **Internet eases the links amongst the members**
  - **Internet makes the organisational structure very flexible**
  - **Relies in uncoordinated action from investigative bodies**
  - **Relies on the slowness of the procedures**
  - **Uses internet technologies to launder the money**

# BOTNETS and Crimewares

- Main issues:
  - **Drones armies manipulated from remote**
  - **Crimewares, not only destroy the system but now also extract data**
  - **Criminal split their activities between compromised machines:**
    - **The coder, who writes the code**
    - **The launcher, who launches the executable file**
    - **The miner, who extracts the data**
    - **The washer, who launders the money using e.g. e-mules**

*The splitting techniques makes more difficult*

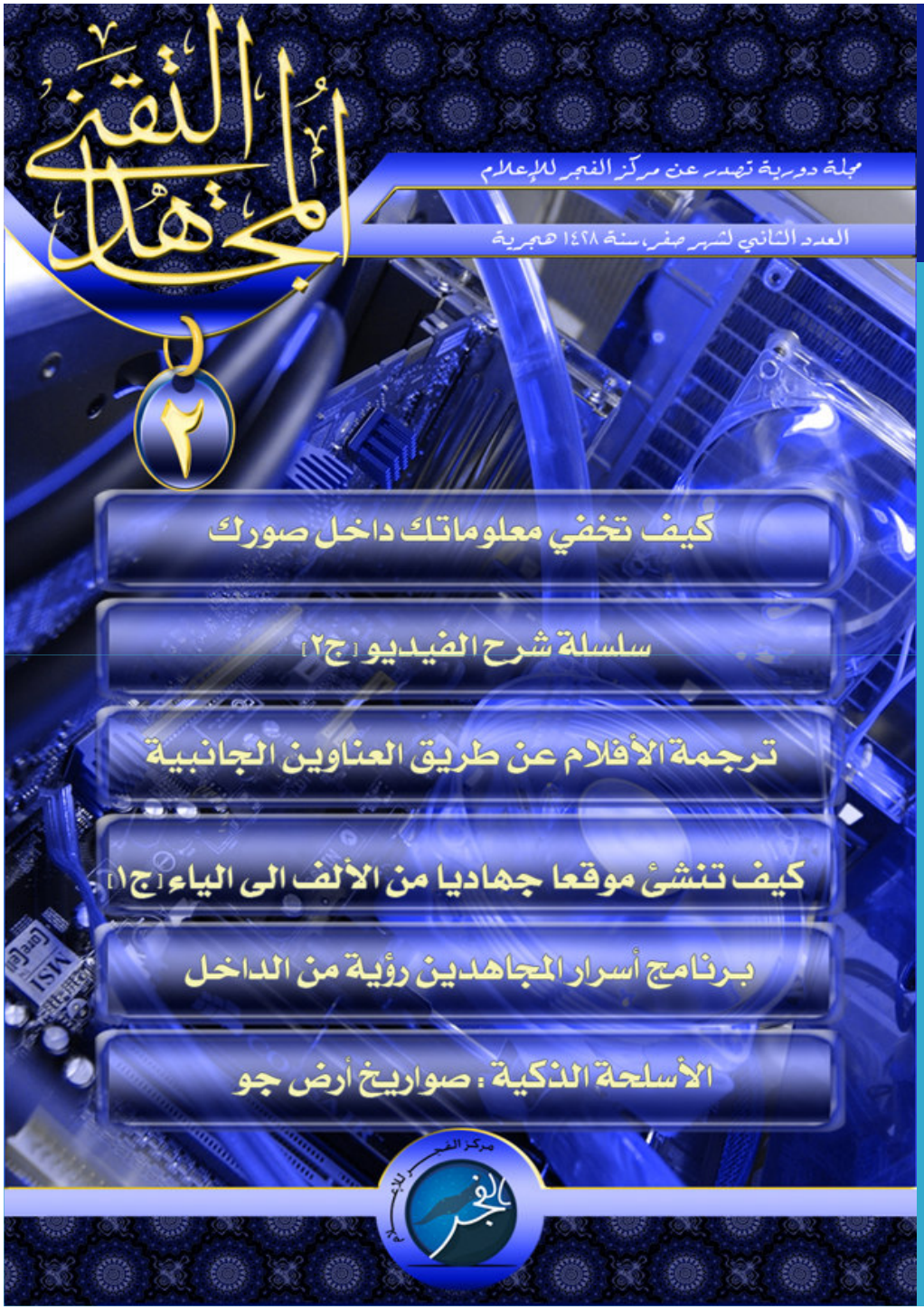
*to map the criminal process in its entirety*

# BOTNETS and Crimewares

- BOTNETS are very flexible, used for multi-purposes such as:
  - **To make money (rent, extortions, industrial espionage etc.)**
  - **To steal personal and financial data**
  - **To boost up the social engineering (phishing and its varieties)**
  - **To perpetrate huge spamming**
  - **To threat the victim extorting money**
  - **To attack critical information infrastructures networks**
- The peril is coming from everywhere: prevention is difficult

# Cyber Terrorism

- 2 realities in place:
  - **Terrorist organisations**
    - **Propaganda**
    - **Attack critical networks**
    - **Improve communication amongst inners, gather funds (charity)**
    - **Distance learning (internet creates vicinity)**
  - **Black Hats**
    - **Attack networks**
    - **Hired and paid by criminal organisations**
    - **Likely train other criminals**




***The Technical Mujahid***

***Periodical issued by al-Fajr media centre, issue # 2, February / March 2007***

***How to hide information in pictures***

***The series: presentation on videos***

***Translating films through subtitles***

***How to create jihadist websites from A to Z***

***"Secrets of the Mujahideen, an inside view"***

***Smart weapons: surface-to-air missiles***

# Production and dissemination of child abusive images on the internet

- 2 new realities about child offenders:
  - **Child abusers**
  - **Child pornographers**
- CP generates huge revenues
- Continuous growth of the phenomenon, redundancies of images over internet
- Ever new technology used to groom children such social networking, blogs sites
- Peer to Peer still most used to exchange pictures
- Need of more efforts toward the victim identification
- Improve the control toward the issue
  - **families, social entities, governments**

# Conclusions

- The use of hi-tech is more and more beneficial for criminals: as 'facility-weapon' and as untraceable communication platform
- Rapid growth of underground economy, money is driving factor: Criminal Organisations have understood how to exploit internet
- Regulatory issues – many domestic laws still apply (CCC to be ratified and implemented)
- Difficulties to map out internet crimes: lack of common reporting system and reluctance in reporting by the victims
- Lack of international common strategy: countries still focus on domestic issues
- Lack of effective common understanding with private industry

# Points of discussion (1)

- **Internet investigation methods:**
  - In matters of how and where to collect intelligence/evidences
  - In matters of new invasive computer wiretapping (online search/surveillance)
- **Forensic investigation methods:**
  - Is the target the suspect's machine only?
  - Is there a need to create a common forensic tool?
  - Is there a need to find a common understanding on what e-evidences mean?
  - Is there a need to discuss and agree on how to commonly present the evidences at court?

# Points of discussion (2)

- **Creation of a common reporting system:**
  - To have a reliable picture of internet crimes
  - To steer an international and effective strategy to fight cyber crimes
- **Improvement the cooperation/understanding with private sector:**
  - Data retention/preservation, Intelligence support to LEA
  - Service Level Agreement, Confidentiality Agreement
- **Education on how to use internet technologies**

# Thank You
# for Your Attention


Nicola DILEONE

**High Tech Crime Centre**

**Raamweg 47**

**PO-Box 90850**

**2596HN The Hague**

**The Netherlands**

**Tel:** +31 (0)70 302 51 32

**Mob:** +31 (0)6 24 82 31 76

**Fax:** +31 (0)70 318 08 39

Nicola.Dileone@europol.europa.eu

HTCC@europol.europa.eu