

CyberCrime@IPA
Global Project on Cybercrime
European Union Cybercrime Task Force

SPECIALISED CYBERCRIME UNITS
Good practice study

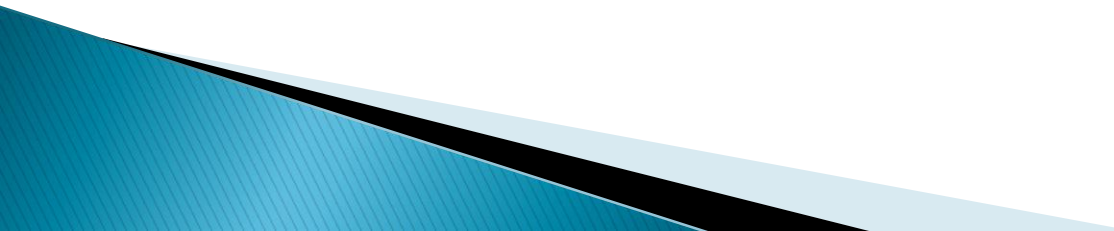
Strasbourg, November 21-23, 2011

Background

Study prepared jointly by:

- **CyberCrime@IPA joint CoE/EU project**
- **Global Project on Cybercrime CoE**
- **European Union Cybercrime Task Force**

Experts:

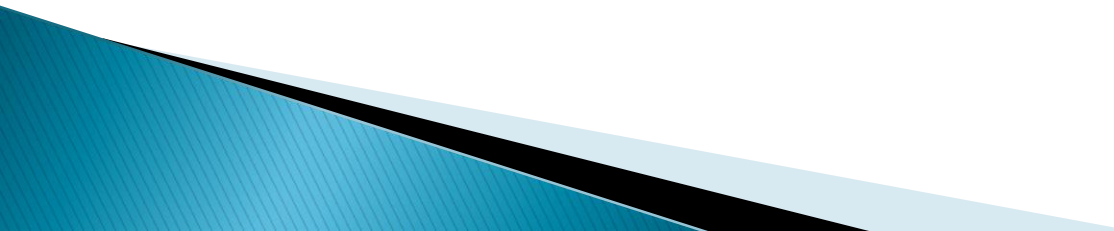
- **Virgil Spiridon**, Head of Cybercrime Unit, Romanian National Police, Romania
 - **Yasmine Ourari**, Legal Adviser, Federal Computer Crime Unit, Belgium
 - **Marjolein Delplace**, Strategic Analyst, Federal Computer Crime Unit, Belgium
- 

Contributions by:

Albania	Sector against cybercrime
Australia	Cybercrime Operations
Austria	Criminal Intelligence Service – Unit 5.2 Computer Crime
Belgium	Federal Computer Crime Unit
Bosnia and Herzegovina (Republika Srpska)	Department for High-tech Crime
Brazil	Computer Forensic Unit
Croatia	Organised Crime Dep. and Economic Crime and Corruption Dep.
Cyprus	Office for Combating Cybercrime
Czech Republic	Information Technology Crime Section
Finland	Cybercrime Intelligence Unit, Cybercrime Investigations Unit, Crime Laboratory
France	Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication - OCLCTIC
France	Cybercrime division (Gendarmerie)
Ireland	Garda Computer Crimes Investigation Unit
Kosovo*	Cybercrime Investigation Unit
Luxembourg	Section Nouvelles Technologies
Mauritius	Information Technology Unit
Montenegro	Division for Combating Organised Crime and Corruption
Romania	Cybercrime Unit-Romanian National Police
Romania	Service for Combating Cyber Criminality-Cybercrime Unit Prosecution
Serbia	Special Prosecution Office for High Tech Crime
Spain	Brigada de Investigación Tecnológica
"The Former Yugoslav Republic of Macedonia"	Cybercrime Unit

PURPOSE OF SPECIALISED UNITS

Primary role of specialised cybercrime units:

- ▶ Investigating and/or prosecuting offences against computer data and systems
 - ▶ Investigating and/or prosecuting offences committed by means of computer data and systems
 - ▶ Carrying out computer forensics with respect to electronic evidence in general
- 

Creation and allocation of resources for specialised units justified by:

- ▶ Increase of cybercrime in all regions of the world
- ▶ Large amount of crime proceeds and damage caused
- ▶ Need to protect citizens
- ▶ Cybercrime affects national interests and security
- ▶ Evolution of an 'underground economy
- ▶ Increasing demand for computer forensics



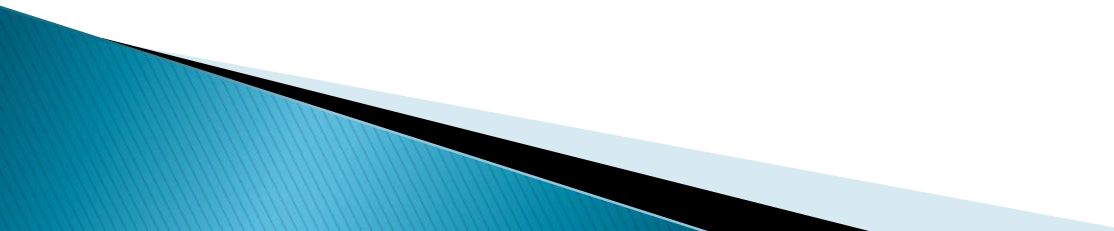
Need for specialist skills and specialised services

TYPES OF SPECIALISED UNITS

- ▶ **Cybercrime Units (offences against + by means of computers)** – e.g. France, Cyprus, Czech Republic, Mauritius, Romania, Spain
 - ▶ **High Tech Crime Units (against + technical support)** – e.g. Austria, Belgium, Ireland, Luxembourg
 - ▶ **Computer Forensic Units (forensics + technical support)** – e.g. Brazil
 - ▶ **Central Units (intelligence + support)** e.g. UK
 - ▶ **Crime-specific Units** – e.g. UK-CEOP
 - ▶ **Specialised Prosecution Units** – e.g. Romania, Belgium and Serbia
- 

FUNCTIONS AND RESPONSABILITIES

Strategic responsibilities

- **Drafting national legislation on cybercrime**
 - **Contributing to national strategy on cybercrime**
 - **Prevention**
 - **National systems for reporting criminal activities**
 - **Cooperation at national and international level**
 - **Intelligence analysis and dissemination**
 - **Defining guidelines for investigations**
 - **Delivering training programmes**
 - **Assessment and analyses of cybercrime phenomena**
- 

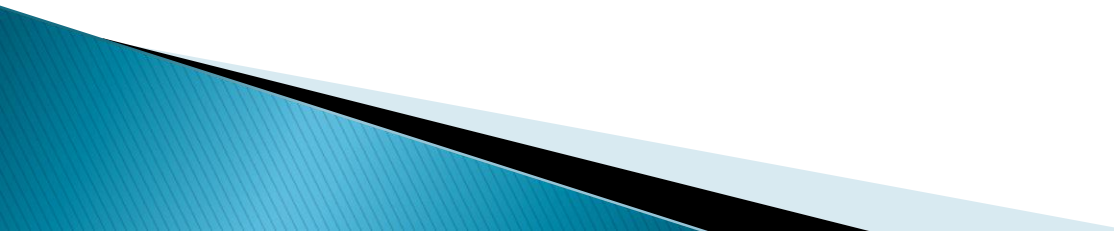
FUNCTIONS AND RESPONSABILITIES

Tactical responsibilities

- Coordinating and conducting investigations
- Collection, examination and analysis of digital evidence within the forensic science framework of the country
- Coordination of regional/territorial units
- Specialised support to other non cybercrime police units
- Practical interagency cooperation
- The private sector
- International cooperation

Sometimes major differences between countries

STEPS TOWARDS THE CREATION OF A SPECIALISED UNIT

- 1. Assessing needs and making a decision**
 - 2. Legal basis**
 - 3. Manager of the unit**
 - 4. Staffing the unit**
 - 5. Training programme**
 - 6. Equipment and other resources**
 - 7. Independence of and knowledge about unit**
 - 8. Action plan / evaluations mechanisms**
- 

ASSESSMENTS AND CONCLUSIONS

- ▶ Specialised units are necessary
 - ▶ One important element of a comprehensive response
 - ▶ Personnel, equipment, training remain challenges
 - ▶ Performance depends on staff, motivation, inter-agency, public/private and international cooperation
 - ▶ Assessment of performance to justify resources
 - ▶ Too much cybercrime/electronic evidence for one unit to handle → assist/support other units
- 