

ROMANIA

ROMANIAN NATIONAL POLICE

Directorate for Combating Organized Crime



Cyber Crime Unit

Strasbourg, 23-25 March, 2010

GENERAL INSPECTORATE OF ROMANIAN POLICE

Directorate for Countering Organized Crime

Trafficking of
Human
Beings

Money
Laundering and
financing the
terrorism

**Cyber
Crime Unit**
29 police officers

Trafficking
of Drugs

**Internet and credit
card
fraud section**

**Computer crimes and
forensic section**

15 BCCO –Cyber Crime Unit
7 police officers

26 County Offices 1-4 police officers

How we started...

- Define the competences
- Select the personnel
- Training and equipment
- Develop the private-public cooperation
- Develop the International cooperation
- Create the instruments and procedures for investigations
- Develop the reporting system

How we defined ...

A specialised police unit for cybercrime investigation must fulfil the following requirements:

- to support the operational situation and requirements;
 - to be connected to the realities of information society;
 - to be flexible with regard to organisational changes and criminal phenomenon;
 - to take into account the financial and human resources of the organisations they are part of.
- The unit must include at least two sections:
 - investigative section and
 - digital forensics section.

The role of Cyber Crime Unit

- Establishing the strategies, policies, evolutions, evaluations, etc
- Drafting the national legislation on cybercrime
- Coordination of the field offices
- Develop the internal standard procedures (10 cyber crime procedures)
- Investigations/technical activities/undercover activities
- Establish the national training program/ implementation of the new methods
- Developing the internal cooperation
- Coordination of the international cooperation

The private-public partnership

- To set the contact points
- To define the way of communications
- To have regularly meetings
- To attend at common events
- To participate in common projects
 - Safernet.ro
 - Advisory Panel

Area of common interests

- Legislation (cyber crime legislation -criminal activities and procedures, regulations on the ISP, data retentions, data preservation, etc)
- Education
- Training
- Contact points
- Prevention/combating of cyber crime activities
- Inform each other about cybercrime trends
- To encourage the report of the cyber crime activities

International cooperation

- Private-public cooperation
- Law enforcement
- Mutual Assistance Request
- 24/7 contact point
- European Arrest Warrant
- Joint Investigation Team

Types of the most common illegal activities

Credit card frauds

- skimming
- phishing
- buying/selling cc on the internet

Internet frauds

- auction frauds
- WU frauds
- compromising users' credentials

Unauthorized computer access

Child pornography on the Internet

Trends

- Reorientation of the criminal groups for the cyber-crimes activities (internet fraud, card related fraud, etc)
 - less risks
 - use of the new technology
 - financial income
 - limitations on investigation/prosecution
- The criminal groups are well organized and structured
- The high level of Internet and computer education in Romania
- 80% of IT fraud and phishing attacks originated in Romania are aimed US citizens
- 80% of credit card fraud (skimming) committed by Romanians targets West European citizens
- **Statistics - 2009**
 - 102 cases(indictments)/766 offences/482 people charged/289 people arrested

Virgil SPIRIDON

*Head of the Romanian National Cyber Crime
Unit*

Tel/fax: 004 021 3111579

Cell phone: 004 0740309441

Email: cybercrime@politiaromana.ro

virgil.spiridon@root.ro