www.coe.int/cybercrime

CyberCrime@IPA

Conference on strategic priorities in the cooperation against cybercrime

Dubrovnik, Croatia, 13 – 15 February 2013

Tools: Specialised cybercrime units – good practice study

alexander.seger@coe.int

1

CyberCrime@IPA/EU CTF: good practice study

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

Strategic task:

- Cybercrime strategies
- Legislation
- Analysis, intelligence
- Reporting systems, etc.

Tactical tasks:

- Conducting investigations
- Coordination operations
- Collection and analysis of electronic evidence, etc.

2

CyberCrime@IPA/EU CTF: good practice study

Types of specialised units:

- Cybercrime units (crimes against and by means of computers)
- High-tech crime units (crimes against computers)
- Computer forensic units
- Central units (policy, analysis, coordination, support)
- Crime-specific units (e.g. carding, CAM)
- Prosecution-type units

Creating a specialised unit – Steps:

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 / evaluation mechanism

3