Council of Europe
Project on Cybercrime in Georgia
Report by Virgil Spiridon and Nigel Jones

Tbilisi – 28-29, September 2009

Presentation Contents

- An assessment of the Georgian view of cybercrime and current capability to investigate
- The necessity for creation of the cyber crime unit
- How to create a specialized cyber crime unit
- Recommendations

An assessment of the Georgian view of cybercrime and current capability to investigate

The necessity for creation of the cyber crime unit

How to create a specialized cyber crime unit

Recommendations

- **Completion of the national legal framework and harmonization with the European standards**
- **Development of a national strategy for the security of computer systems**
- **Creation of a specialized unit for cybercrime investigation**
- **Development of instruments and procedures needed for investigating and researching these crimes**
- **Provision of a training programme and equipping the new unit**
- **Development of cooperation relations with private sector and creation of proper mechanisms for international cooperation**

Completion of the national legal framework and harmonization with European legislation

The existence of adequate legislation is essential for fighting cybercrime.

The **Council of Europe Cybercrime Convention** is a positive example of international legal instrument helping many countries in designing their national legislation in the area of cybercrime.

The legislation must be looked from several angles:
-the acts that should be criminalised (in this area of crimes new ways of committing crimes or new types of crimes appear all the time;
-the procedures for investigating and researching these crimes (computer search, access to computer systems, etc.),
-the definition of the international cooperation framework (the point of contact 24/7, spontaneous exchange of data and information, sending and responding to the mutual assistance requests, extradition, etc.)

	Internal Procedures
1.	Procedure for efrauda.ro
2.	Procedure for investigating child pornography on the Internet
3.	Procedure for investigating internet fraud
4.	Procedure for investigating phishing attacks
5	Procedure for investigating credit card frauds (skimming activities)
6.	Procedure for examination the counterfeit credit cards and technical equipments
7	Procedure for seizing the computers and electronic storage devices
8	Procedure for computers searches
9.	Procedure for investigating computer intrusions
10	Procedure for analyzing computer data

Questions?