European Union / Council of Europe
Project on Cybercrime in Georgia

Tbilisi-2 March 2010

- How to create a specialized cyber crime unit
- Recommendations
- Priorities

How to create a specialized cyber crime unit

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.

This unit must include at least two sections:

- investigative section and
- digital forensics section.

Recommendations

Completion of the national legal framework and harmonization with the European standards

- 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. In fact it is the only international legal instrument to fight 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.)

Development of a national strategy for the security of computer systems

- The computer attack against Georgia that took place last year proves the fragility of computer systems at governmental level as well as at civil institutions or business level.
- It is considered necessary to draft a national strategy to define the security of computer systems, the critical infrastructure, the institution with responsibilities in this field and a joint working method for these institutions for preventing and taking the first measures in case that computer attacks occur.
- The creation of a response centre for incidents – CERT will be helpful for a better evaluation of the threats against computer systems, for reporting these events, for collaboration of institutions and for reacting in case that computer attack occur.
- A part of this national strategy should refer to the modernization and specialization of police structures for preventing and combating this phenomenon.

Development of a national strategy for the security of computer systems

- Even if computer threats are not too diverse in Georgia and the impact of new IT&C technology in committing cybercrimes is not too high, it is just a matter of time for them to affect Georgia, too.
- The occurrence of certain types of computer frauds or Internet child pornography in other geographical areas more remote or close to Georgia, does not mean that they cannot occur soon in Georgia. It is useful to know and prevent this events, learning from others' mistakes and experience in order to fight the crimes more efficiently whenever they occur.
- The unit should be created at central level and developed step by step in accordance to the financial resources and the operational environment in Georgia.
- The unit should be initially formed by 4 or 5 police officers to deal with the investigation of cybercrime activities and with issues related to the research and investigation of computer systems for the purpose of identification and collection of digital evidence.

Priorities for the new cyber crime unit

- 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

Development of instruments and procedures needed for investigating and researching these crimes

- The novelty and the technical nature of the investigation of cybercrimes require internal working procedures to be developed and implemented in such situations. These procedures must be based on the legislation in force for the criminal offences facts and the associated technical procedures (computer search, etc.). They should also take into account the internal regulations for performing investigations at the level of police structures in Georgia.
- The procedures must regulate the steps to be followed by different types of investigations, the necessary stages for a safe collection of digital evidence, the steps to be followed for investigating certain types of digital evidence, etc. The procedures must also deal with the admissibility of evidence in criminal proceedings and the measures to be taken to ensure that all data collected is retained and presented in a form acceptable to the judicial system of Georgia.

Creation of a specialized unit for cybercrime investigation

Among the investigation competences of this unit, we recommend to include the following:

- computer frauds,
- frauds with electronic means of payment,
- computer attacks and
- child abuse through computer systems.

- The personnel to be hired in this unit should be formed of experienced police officers for performing police investigations, who have computer skills and speak a foreign language spoken on international level.

- The selection might be done according to the human and financial resources from the existing policemen in the Ministry or even from the graduates of universities specialized in computers and communications.

Development of instruments and procedures needed for investigating and researching these crimes

- These procedures should be drafted by experts of the new cybercrime structure, after establishing the unit, based on training courses they will attend and on their experience as policemen. The procedures should be also approved by prosecutors.
- Cybercrime prevention is also important, and the new unit should develop a crime prevention strategy that will incorporate public awareness activities as well as education programmes for schools and other organisations dealing with safe use of the Internet.
- It is important that the public is aware of the existence of a cybercrime unit that can help in cases and this can be achieved by advertising its investigative capacity and a place to which cybercrime may be reported. A procedure for accepting reports of cybercrime should be established by for example the creation of a website, telephone line and email address dedicated to reporting such crimes.

Development of instruments and procedures needed for investigating and researching these crimes

- The creation of contacts and collaboration protocols with other informative competent structures from other departments of the Ministry of Internal Affairs is very important for ensuring an efficient information exchange is essential.
- There must be created a database in the context of creation of the unit and the reporting and investigation of cybercrimes.
- In order to provide some support in this context the following documents are identified as being of particular use.
- The European Commission published a document outlining good practice for the seizure and handling of digital evidence entitled “Seizure of e-evidence”. It remains the only international guide covering this area and should be seen as a good base for developing procedures to deal with digital evidence.
- Interpol has been developing an IT Crime Manual which is available to all Interpol Member Countries.

Provision of a training programme and equipping the new unit

- Any specialised unit that is created will only be as successful as the knowledge, skills and education of the people who will staff the unit. In the area of cybercrime, the level of training required to become an effective operative is lengthy, continuing and sometimes expensive.
- Staff of the unit will have varying requirements for training depending on their roles within the organisation, for example a digital forensics technician will require different training than an investigator responsible for cyber attacks on the Georgian CNI.
- There are however some similarities in the training and it is appropriate for each to have an understanding of the others work. At the introductory stage, it is appropriate for all unit staff to receive basic training on digital forensics and network investigations.

Provision of a training programme and equipping the new unit

The equipping of the new unit is essential and must be done with minimum costs and gradually, depending on the needs. This will include:

- adequate space for the new created structure;
- secure storage for exhibits
- sufficiently powerful computers for workers;
- overt and covert Internet connections;
- necessary software and devices for forensically processing computer systems and other devices;
- applications needed for performing computer investigations, etc.

Development of cooperation relations with private sector and creation of proper mechanisms for international cooperation

- The development of a partnership with the private sector is important from several points of view, such as knowing and building trusted relationships with the ITC companies, the Internet providers, the banking environment, etc.
- Such partnerships are helpful for better prevention and for educating citizens and clients of such companies in order for them to know and to be aware of the danger of the cybercrime as well as putting into place preventive measures to protect their assets.
- Greater communication with private sector entities generates a mutual trust which leads to encouraging the notification and reports of these cybercrimes by citizens or above-mentioned institutions.
- The knowledge and experience of these companies may help and contribute to the training and equipping of the personnel.

Development of cooperation relations with private sector and creation of proper mechanisms for international cooperation

- For better international relations and awareness of the importance of international cooperation issues we recommend the establishment of the **24/7 contact point**, in order to provide exchange of information in emergency situations in the area of cybercrime.
- This contact point should operate within the new created police structure and provide the exchange of data and information based on the national legislation in force, in emergency situations.
- It represents an important tool to receive requests from abroad and send requests to other countries and it should not be looked as a cooperation institution of its own, but as a functional unit, available 24 hours a day.

Questions?