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

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

- Since the attacks on government systems that took place immediately before the invasion by Russia in 2008, Georgia has identified the combating of cybercrime and cyber attacks as a priority.
- These attacks involved denial of service attacks on government networks that in turn impacted on the ability of the Georgian authorities to communicate with its population and its ability to protect itself and conduct its everyday business.
- Since these incidents Georgia started to pay more attention to the cybercrime phenomenon, security of computer systems and protection of critical national infrastructure.
- An inter-ministry working group was created to define a general policy for preventing and combating cybercrime. This working group does not have specific tasks or fixed deadlines. The working group is an important first step for the awareness level and understanding of the phenomenon of cybercrime, but no significant progress will be achieved without setting clear and specific objectives to be reached within this framework.

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

- The identified risks and computer threats should be considered on the global level that may impact on Georgia. The fact that currently the status of the cybercrime in Georgia can be only reflected by the computer attack of 2008, doesn't necessarily mean that other criminal activities are absent or cannot start in the future.
- The surrounding countries from the former Soviet Union are mainly affected by on line criminal activities which can and undoubtedly will extend to Georgia as the availability of technology in business and the general population increases.
- As regard to the private sector, ITC companies, banks, ISP's and others responsible for the CNI of Georgia, there are no known partnership associations created to engage in debate that can result in projects for prevention and education.
- Public/private partnerships have proved very successful in other jurisdictions and entities working in isolation and without discussion are less likely to succeed.

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

- Currently, in Georgia there is no specialised structure within the Ministry of Internal Affairs for investigating the types of cybercrime identified in this report. In addition there are no specialised police officers in this field.
- Moreover, there are no prosecutors assigned to work with this kind of investigations and no training courses are offered on this subject.
- Until now, with the exception of the computer attack of 2008, according to the known and reported situation there are only a small number of complaints related to threats sent through the Internet.
- The national legislation criminalises certain activities but it doesn't entirely cover the area of illegal activities in the field of cybercrime, nor does it comprise the necessary procedures for research and investigation of digital evidence.

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

- There are no specialized police units to perform specific activities of computer forensics and there are no working procedures to follow when dealing with digital evidence.
- The training and awareness level for judges is rather limited, not only with regard to cybercrime but to the impact of new technologies and their use for crimes.
- Georgia does not have any specific procedural laws or regulations dealing with the collection, handling, examination, analysis or presentation of digital evidence in criminal proceedings, nor does it have any safeguards to protect the rights of individuals in respect of this very specific type of evidence.

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

The necessity for creation of the cyber crime unit

- The computer attack suffered in 2008 shows that certain societies, are not adequately prepared to fight these threats
- Critical National Infrastructure protection is essential for countries to be able to function
- As numbers of users of communication systems increases with the development of the infrastructure, the threats will also increase.
- The increasing importance of cybercrime in the world
- To provide citizens with the confidence that there is a capability to deal with cybercrime issues and digital forensics at national level
- Financial institutions use computer systems on large scale
- Technical and operational methods and the availability of advanced technical devices are in continually changing and improving.
- The activities in the field of cybercrime have a strong cross-border nature
- The traces left by cyber-criminals remain for only relatively short periods
- Knowledge of international standards for data retention and preservation are essential

The necessity for creation of the cyber crime unit

Prevention and combating cybercrime is and must be a priority, taking into account the following features:

- creation and assurance of a safe business environment both for ITC activity and for others who use computer systems for their businesses;
- ensuring the trust of the population and the legal entities in the Internet as a safe means of communication and method of conducting business activities and using electronic means of payment;
- ensuring safety for children's use of the Internet;
- protection of critical infrastructure;
- establishing a public-private partnership and efficient international cooperation structures aimed primarily at supporting the operational segment activities

The investigation and interpretation of digital evidence requires the specialisation of law enforcement agents and staff and the use of specialised tools and software

How to create a specialized cyber crime unit

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.

How to create a specialized cyber crime unit

The unit should have the following main tasks:

- perform investigations for combating cybercrime;
- collect and analyse data and information;
- carry out technical activities for researching computer systems;
- draft internal rules and procedures for cybercrime investigation;
- assist other police departments in performing investigations;
- perform activities for international judicial assistance for criminal issues, within national and international mutual assistance request;
- conduct public awareness cybercrime prevention activities
- research
- intelligence gathering
- training
- equipments and software
- digital Forensics function

Recommendations

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

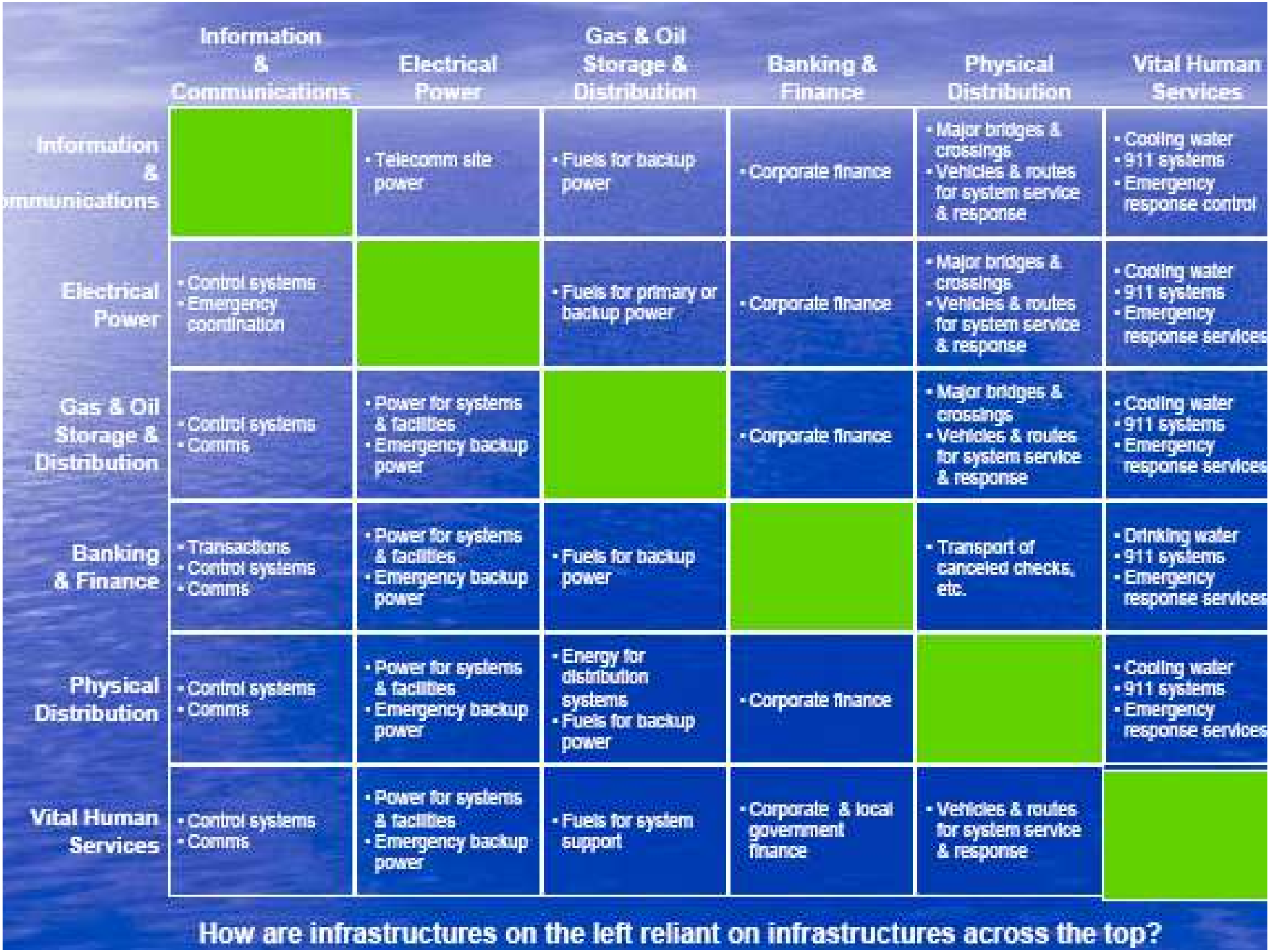
- Although the legal issues are being dealt with in another report, it is important to highlight those legal issues that directly impact on the ability to provide practical countermeasures against cybercrime in all its forms.
- The existence of adequate legislation is essential for fighting cybercrime. 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.

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

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.)


Government Operations
Gas & Oil Storage and Delivery
Emergency Services
Water Supply Systems
Critical Infrastructures
Telecommunications
Banking & Finance
Electrical Energy
Transportation


Information & Communications
Electrical Power
Gas & Oil Storage & Distribution
Banking & Finance
Physical Distribution
Vital Human Services
Information & Communications
• Telecomm site power
• Fuels for backup power
• Corporate finance
• Major bridges & crossings
• Vehicles & routes for system service & response
• Cooling water
• 911 systems
• Emergency response control
Electrical Power
• Control systems
• Emergency coordination
• Fuels for primary or backup power
• Corporate finance
• Major bridges & crossings
• Vehicles & routes for system service & response
• Cooling water
• 911 systems
• Emergency response services
Gas & Oil Storage & Distribution
• Control systems
• Comms
• Power for systems & facilities
• Emergency backup power
• Corporate finance
• Major bridges & crossings
• Vehicles & routes for system service & response
• Cooling water
• 911 systems
• Emergency response services
Banking & Finance
• Transactions
• Control systems
• Comms
• Power for systems & facilities
• Emergency backup power
• Fuels for backup power
• Transport of canceled checks, etc.
• Drinking water
• 911 systems
• Emergency response services
Physical Distribution
• Control systems
• Comms
• Power for systems & facilities
• Emergency backup power
• Energy for distribution systems
• Fuels for backup power
• Corporate finance
• Cooling water
• 911 systems
• Emergency response services
Vital Human Services
• Control systems
• Comms
• Power for systems & facilities
• Emergency backup power
• Fuels for system support
• Corporate & local government finance
• Vehicles & routes for system service & response
How are infrastructures on the left reliant on infrastructures across the top?

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 already existing working group for analysing and assessing the risks in the field of computer systems security and for drafting the general policy should present such report, together with an action plan comprising the responsible institutions and each institution's tasks.

Creation of a specialized unit for cybercrime investigation

- According to the organization and functioning of the Ministry of Internal Affairs of Georgia, a specialized unit for computer crimes could be created within the Criminal Police Department having as main tasks the investigation of the actions in the field of cybercrime and the assistance provided to other police structures for performing investigations.
- 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.

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

- 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.

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.

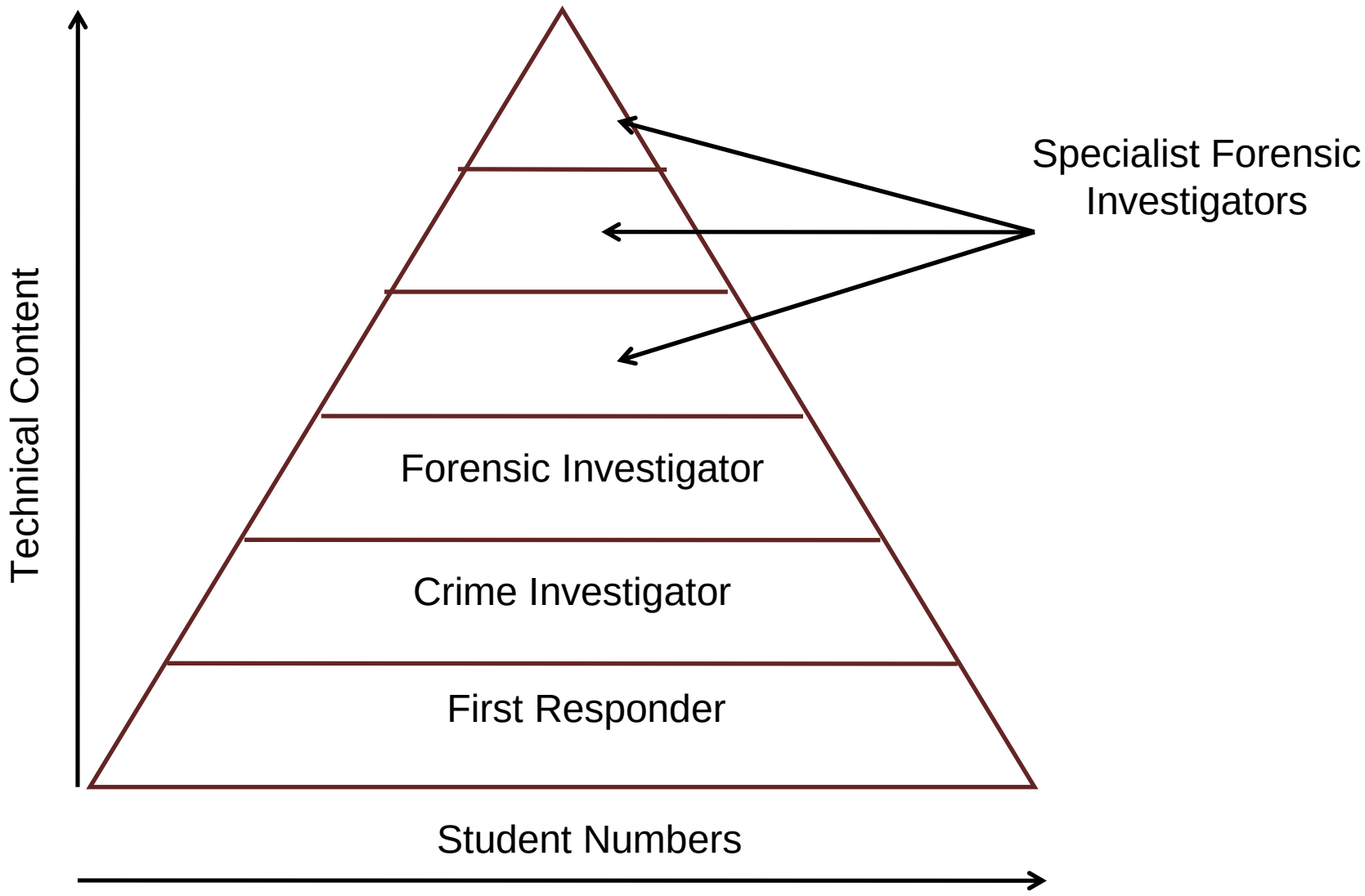
Provision of a training programme and equipping the new unit

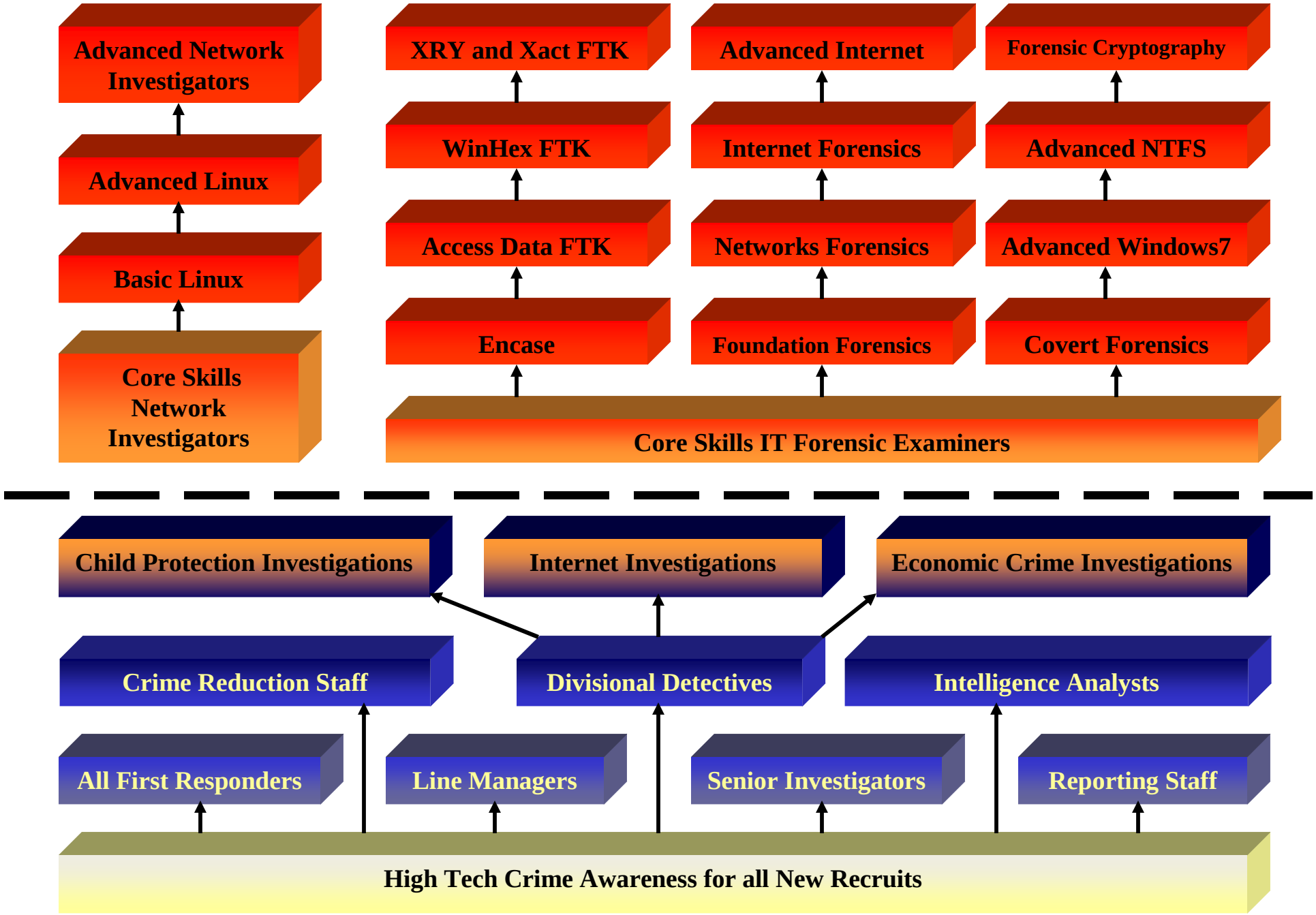
- Any specialised unit that is created will only be as successful as the knowledge, skills and education of the people who will staff the unit. In the area of cybercrime, the level of training required to become an effective operative is lengthy, continuing and sometimes expensive.
- Staff of the unit 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. Once the unit is established it will be necessary to identify a training path for each member of staff that will support the needs of the unit.

Provision of a training programme and equipping the new unit

- It is recommended that a learning portfolio be created for each member of staff that will enable a full record of an individual's learning and training to be maintained. One of the main reasons for this is to provide evidence to the judicial system of an individual's capability in this area of work.
- It is vital that each member of staff follows a programme of continuing professional development (CPD) once their core training has been completed. The changes in technological advance are so great that it is not possible to assume that someone trained in year one is still competent in year 3, if they have not followed a CPD programme. This may take the form of additional training, attendance at relevant conferences and workshops and exchange visits with other similar units in other jurisdictions.
- These initial training courses should be organised for the personnel right after the selection and even in a partnership with private companies, financial institutions and law enforcement agencies from abroad. There are training courses developed by various police structures and it is better to use them at this training stage rather than try to develop new courses.

Training Schematic




Advanced Network Investigators
Advanced Linux
Basic Linux
Core Skills Network Investigators
XRY and Xact FTK
WinHex FTK
Access Data FTK
Encase
Advanced Internet
Internet Forensics
Networks Forensics
Foundation Forensics
Forensic Cryptography
Advanced NTFS
Advanced Windows7
Covert Forensics
Core Skills IT Forensic Examiners
Child Protection Investigations
Internet Investigations
Economic Crime Investigations
Crime Reduction Staff
Divisional Detectives
Intelligence Analysts
All First Responders
Line Managers
Senior Investigators
Reporting Staff
High Tech Crime Awareness for all New Recruits

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.

The above list is only indicative and a specific outline of the requirements can be provided once the structure of the unit is identified.

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.
- These recommendations are the initial response to the challenges faced and will need refining once a decision is made to create a specialised unit. The final recommendations will very much depend on the structure of a unit, the staffing levels and importantly the funding available for implementation.

Questions?