GLACY
Global Action on Cybercrime
Action globale sur la cybercriminalité

Draft version 5 August 2014

Restricted

Law Enforcement Training Strategy

Project area specific strategies

Prepared under the GLACY project

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

1 EXECUTIVE SUMMARY

This report recognises that cybercrime/computer enabled crime/digital evidence impact on each project area in different ways and requires individual strategies to be developed as well as identifying areas where the potential to work with others, either within or without the current projects, may be more suitable.

Many current efforts to ensure that there are a sufficient number of trained staff to deal with these matters has been aimed at those with the greatest technical requirement. Training programmes and qualifications have been developed up to and including academic Masters Programmes. An encompassing strategy is necessary to ensure that law enforcement staff at all levels is suitably trained and educated. This involves identifying those that will come across technology in all its forms as either a source of evidence, a method of investigation or taking and dealing with complaints of such crimes.

Much of the required training may be incorporated within existing programmes that are delivered on a national level, in the same way that dealing with other types of evidence or crimes are already included.

The law enforcement roles that are affected are manifold and include: First responders, Managers, Specialist investigators – child protection, economic crime, financial investigations, accident investigation, drugs investigation, major investigations, digital forensic investigators, Internet internet crime investigators, network crime investigators, in fact almost all members of law enforcement organisations. The levels of knowledge required differ and it is important that this is recognised. Failure to spread knowledge across organisations and putting all the resource into the specialist cybercrime investigators, will create a very heavy top end approach that may lead to overqualified staff dealing with fairly basic work. This can be avoided by including training at all levels as suggested in this report.

Activities and aspirations in each project area are set out in the report. Each project area has its own requirements, own challenges, own opportunities and also those that are common with others. The recommendations set out some of the things that may be achieved by cooperative action and in particular the potential for the development of national or regional centres of excellence to carry this work into the future. The importance of involving training organisations as well as cybercrime units in the development and implementation of cybercrime strategies is recognised, along with the roles that academia and industry may play in the process.

The joint European Union and Council of Europe GLACY project provides an opportunity for the development of national strategies for law enforcement training that are crucial to the success of potential to create real and lasting differences to the capabilities of countries to combat all types of cybercrime, including those traditional crimes where technology is now an integral part. This requires training to be introduced across the entire law enforcement community in order to succeed.

Delegates from the priority countries of South Africa and the Kingdom of Tonga were not able to participate in the workshop. Their needs should be taken in to consideration in future GLACY project activities, as the situation report country visits identified an extensive need for training in these countries.

2 BACKGROUND

2.1 The GLACY project

GLACY is a joint project of the European Union and the Council of Europe aimed at supporting countries worldwide in the implementation of the Budapest Convention.

The specific objective of GLACY is to enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime.

Results are expected in the following areas:

- Engagement of decision-makers
- Harmonisation of legislation
- Judicial training
- Law enforcement capacities
- International cooperation
- Information sharing
- Assessment of progress.

The duration of the project is from 1st November 2013 to 31st October 2016.

As the use of technology increases on an exponential basis, crimes against the confidentially, integrity and availability of targeted computer systems are more common. Offences committed by means of computer systems, such as fraud, child pornography and intellectual property crimes are increasing rapidly. Moreover, police work involves the recognition and collection of evidence in an electronic form in relation to any offence.

Adoption and implementation of a sustainable and standards based training strategy for law enforcement officers will mean that at all law enforcement officers receive training at the appropriate level to be able to recognise and deal with electronic evidence, to investigate crimes involving technology, and some of them to investigate cybercrime and forensically examine electronic evidence.

In 2011, the Council of Europe, through the CyberCrime@IPA joint project with the EU encouraged countries of South-eastern Europe to develop comprehensive law enforcement training strategies.

Moreover, law enforcement authorities were encouraged to request access to the training materials developed by the European Cybercrime Training and Education Group (ECTEG), the Secretariat of which is hosted by the EC3 at EUROPOL.

The workshop held at Europol brought together delegates from the GLACY and Cybercrime@EAP projects for a series of activities, aimed at commencing the process of the development of national training strategies in cybercrime and electronic evidence in each project area.

Objective

The aim of the workshop is:

- To prepare elements of domestic law enforcement training strategies for each of the participating countries. This is to be achieved through workshop sessions with the assistance of international experts.

- To facilitate access to law enforcement training materials developed by ECTEG. Participants will join a meeting of ECTEG that will take place at the EC3 on 12 and 13 May, that is, at the same time.

- To create a working group among the participant countries for law enforcement training.

- To undertake study visits with EC3 and the Netherlands National High-Tech Crime Unit, in order to assist the process of the strategy development.

Participants

The workshop is primarily for representatives of law enforcement training institutions and cybercrime units in management positions and responsible for training. The CyberCrime@EAP and GLACY projects funded travel and per diem expenses for:

- 1 representative of law enforcement training institutions and 1 representative from specialised cybercrime units from each Eastern Partnership country: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine;
- 1 representative of law enforcement training institutions and 1 representative from specialised cybercrime units from each of the following GLACY priority countries: Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga.

The meeting met its objectives and each project area commenced work in identifying the requirements of an individual training strategy to meet their needs.

This document identifies what is happening in each project area, what is needed in the future and how that may be achieved, through recommendations to the project areas.

2.2 Aim of the report

The aim of this report is to enable the development of a training strategy for the region and for each project area to be able to incorporate relevant parts in their individual strategies. The report recognises that each area will need to consider its own needs in relation to its current and future experience of technology enabled crime and to create a response according to those needs. It further recognises that areas are at different stages of building their response to this type of criminality and that certain training activities may be better suited to a regional rather than a national approach. Those in the project area may benefit by the sharing of training and resources and this report will highlight how this may be successfully achieved and compatible with their national approaches.

The report will also address key issues at different levels of law enforcement activity and seek to break down knowledge and skill requirements for specific functions, to assist countries in their training programme development activities.

3 Elements of a law enforcement training strategy

During the study visit, participants considered the report that was prepared during the Cyber@IPA project and its findings, and discussed the elements that should be included as part of law enforcement training strategies on cybercrime investigations and computer forensics. Each project area prepared a presentation and a draft paper, in which the elements were expanded upon. The intention is that each country uses these documents to continue working towards the development of individual strategies, during and after the GLACY project. The following format was suggested as a template for each country to work to. It is not exclusive and participants were encouraged to consider their own requirements. The explanation of each of the elements is set out in the following sub-sections.

3.1 Justification

This part should explain why a training strategy is necessary and why resources should be allocated.

For example:

- Societies rely on ICT and are vulnerable to risks:
    - Economic, social, political, security, human rights
    - = Actual and potential risks and impact justify investment in training and institution building

- Types of offences:
    - Attacks against computer data and systems (cia offences)
    - Offences by means of computer systems (forgery, fraud, child pornography, IPR-offences etc)
    - Electronic evidence related to any offence
    - = All LEOs need to be trained at different levels

- Technological developments:
    - Mobile devices, cloud computing, social platforms, etc.
    - = LEOs need to keep up to date, update training programmes/materials and conduct relevant research to maintain their knowledge

3.2 Objective

The objective of a training strategy could typically be formulated as follows:

- To ensure that LEA agencies/officers have the skills/ competencies necessary for their respective functions to
    - Investigate cybercrime,
    - Secure electronic evidence,
    - And carry out computer forensics analyses for criminal proceedings
    - Assist other agencies
    - As well as contribute to network security.

Considerations: Sustainability, standardisation, certification, institutionalisation, efficiency, scalable, linked to other institution building measures, skills of prosecutors and judges, establish system

3.3 Training requirements (needs analysis)

This section should seek to break down the requirements for training as it relates to specific roles within law enforcement as part of an overall strategy.

It is almost impossible to imagine a crime that may not have the potential to involve technology in one of a number of forms, namely where the technology is either:

- a target of criminal activity;
- a facilitator of criminal activity;
- a witness to crime;
- a communications tool used by criminals or used for storage of potential evidence in electronic devices.

A training strategy should realise and cater for the different levels of knowledge and skills needed by individual law enforcement staff tasked with investigating crimes involving technology. For example the knowledge required by a first responder in being able to recognise and deal with digital evidence, or deal with the complaint of a technology related crime, is different to and less technical than that required by staff tasked with extracting and analysing evidence recovered from digital devices or those tasked with investigating electronic attacks on elements of critical national infrastructure.

There are no generic names for roles within different organisations, however by describing the functions of the roles identified in this report, it is anticipated that it will be possible to translate the descriptors into local and regional roles.

For the purpose of this report the functions are categorised as follows:

- **First Responder** – an individual who is tasked with attending emergency reports and reports of crime; collecting information from complainants and preserving evidence of all types at crime scenes, including digital evidence.

- **Generic Investigator** – an individual who is tasked with investigating no specific crime types that are normally less complicated than specific crime types. These generic crime types may involve the use of technology by criminals or the preservation of digital evidence.

- **Specialist Investigator** – an individual who is responsible for the investigation of a specific type of crime such as economic crime, narcotics, child abuse, major crime investigations, financial investigations. These have different features in particular in the use of technology.

- **Internet Crime Investigator** – an individual with the responsibility of investigating crimes on the Internet. These may range from online auction fraud, phishing or on line harassment. The key feature of the crime is that the Internet is the vehicle for its commission. Investigators will not engage in online interaction with suspects.

- **Covert Internet Crime Investigator** – an individual who engages in online covert activity in order to prevent and detect crime. This role requires the investigator to engage with suspect on line using approved identities and will normally require the individual to undertake extensive training to become approved for such activities

- **Network Crime Investigator** – an individual responsible for the investigation of crimes where the technology is the target of the crime, such as denial of service and attacks on the critical infrastructure of organisations or countries. These members of staff are at the top level of the investigative tree.
- **Digital Forensic Investigator** – an individual tasked with the capture, analysis and reporting of matters relating to digital evidence. It is normal for such individuals to be

independent from investigators and may be located in forensic science departments. Depending on the structure of the organisation, they may have a tiered structure of responsibility.

- **Managers** – individuals responsible for the management and supervision of others detailed above. They will have responsibility for ensuring the health, safety and welfare of staff as well as the acquisition and allocation of resources required by their staff to conduct their roles. They may be in a generic management role or have specific responsibility for "cybercrime" investigators or digital forensics operatives.

Each of these roles has different learning requirements. As a general rule, those with the more generic functions are greater in number and require less training than those with the specialised functions who by their very nature are less in number. A demonstration of this is given in the following schematic.

It is essential that each role attract the appropriate level of training and education to enable to be effective and to interact with other cybercrime investigation functions both nationally and internationally.

There are core skills that are required by all law enforcement officials, in other words, those at the base of the above illustration. All other trainings build on those core competencies. In order to provide a basis for the first level of training, it is suggested that any training programme incorporate the following:

After attending an initial training module the participants should be able to:

- Check that the necessary authorisations are in place
- Conduct preparatory research concerning the capabilities of the subject of the investigation
- Identify and select the appropriate tools and consider multiple options to meet the needs of capture or seizure of evidence
- Recognise devices capable of storing electronic evidence and determine whether they require capturing or seizing
- Identify any health and safety risks associated with the electronic devices
- Consider the volatility of data and its preservation

- Identify external connections to and from devices
- Isolate the scene and secure the electronic evidence sources to prevent contamination and external interference
- Determine whether to capture electronic data or to seize electronic devices
- Keep a record of the state of the device and potentially relevant information in the immediate vicinity
- Take appropriate action to safeguard the device and relevant information for the application of physical forensic examinations
- Preview the contents of the device in a forensically sound manner
- Choose and apply the appropriate power off method for the device
- Photograph and label the components of the device making specific reference to ancillary leads and connections to the device
- Appropriately package, seal and label the device in accordance with current procedures
- Conduct a preliminary risk assessment of the requirements for the evidentially sound and safe capture of electronic evidence
- Ensure the preservation of third party and volatile data sources
- Capture and preserve electronic evidence in accordance with legal and organisational requirements
- Document the electronic evidence capture throughout the process so that all actions can be reproduced by a competent third party
- Create an evidential product of the data sources to a suitable medium
- Keep accurate records of procedures using appropriate documentation.

It should be considered appropriate to incorporate these learning points within an existing training regime undertaken by all new recruits into a law enforcement organisation. As far as existing staff are concerned, the learning points should be included in any update programmes that exist or delivered by other means such as e-learning where such facilities exist. This update exercise should of course be unnecessary once existing staff are trained and the materials incorporated in new recruit training. All other training programmes for the other roles listed above, should build upon the objectives for the first level and assume that trainees have already undertaken training to provide the knowledge and skills listed.

The next level of training is for the generic, specialist and Internet crime investigator and they have very similar requirements built on the core skills outlined above. In particular, it is necessary for the investigator to have a level of knowledge that incorporates the Internet, activities that may be conducted by criminals using the Internet and how they may use the technology to assist in their investigations.

In order to assist those planning training programmes, the following list of outcomes for this group of students is provided:

- Summarise the history of the Internet and describe the functions of routers, hubs and switches.
- Understand and differentiate between types of IP addresses.
- Describe the function and operation of Internet utilities such as WWW, Email, Social Networking, Newsgroups, Chat and Instant Messaging.
- Resolve and describe how domain names are allocated.
- Interpret web server logs and HTML code of web pages.
- Locate and interpret e-mail headers and summarise anonymous services.
- Carry out online investigations in line with national legislation and Human Rights considerations.
- Identify online services available to assist investigations.
- Acquire different types of online information meeting evidential standards.
- Evaluate online information to establish reliability.
- Summarise elements of Internet crime & discuss case studies.

It should be recognised that these outcomes are indicative of course content but are not exhaustive. It is the responsibility of each area to incorporate the correct learning outcomes within their programmes, by conducting training needs analysis in respect of each role.

The role of the Covert Internet Investigator is one that will require the same knowledge as the above group but with much more level of detail in relation to the covert nature of their work and with an understanding of legal and procedural as well as technical considerations. In many countries, this activity requires special authorisation and approval. In order to assist the developers of the training strategies, the following list of tasks that should be capable of being undertaken by trained individuals is provided:

- Identify the function of the Internet and its applications.
- Describe the evidential requirements and admissibility of evidence during online activity.
- Describe the methodology for evidence capture and corroborations.
- Identify equipment and software required for effective online undercover investigations.
- Describe best practice in legend building and fieldcraft.
- Identify the legal issues pertinent to undercover online investigations.
- Describe the communications methodologies used.
- Prepare written statements for legal proceedings.
- Identify the challenges and risks faced by online undercover investigators

Training in this subject is normally broken down into the following categories:

Theory and Good Practice - covers the basic requirements for establishing a covert online capability including:

- Introduction to the Internet and its applications
- Covert Internet Operations
- Codes of Conduct
- Hardware acquisition and use
- Operating Systems acquisition and use
- Software acquisition and use
- Evidence capture and Corroboration Methodology
- Anti-forensics techniques
- Cover Story Building and Fieldwork
- Risk assessment and authorities
- Matching equipment to the cover story
- Online payment methods
- Agent Provocateur & Legal Issues
- Open Source Capabilities – opportunities and risks

Communications - Examines specific issues of interest to undercover roles in respect of the following:

- Web Browsing
- E-mail
- Newsgroups
- ICQ and Instant Messenger
- IRC and Web chat
- Social Networking Sites
- Encryption
- Crossover Communications

File Sharing - Includes application reviews, traceability, dangers and specific issues relating to:

- File Transfer Protocol
- Peer to Peer
- Internet Relay Chat
- Social Network Sites
- Bit Torrent Sites

- Online storage
- Cyber lockers
- Online auctions

Preparation of Statements and Evidence – Challenges to documents and statements

The role of Network Crime Investigator will require different skill sets depending on the type of crime being investigated and it is not possible in a document such as this to provide an exhaustive list; however there are some sets of knowledge and skills that will be required by all such investigators and these are as follows:

To know and understand:

- Current, relevant legislation, policies, procedures, codes of practice and guidelines for conducting network investigations
- Web site structures and protocols
- Web applications, coding and vulnerability
- Fixed and wireless network and communication protocols, topology and devices, network based attack and vulnerability methods, security methods and procedures and interception methods
- Voiceover internet protocol VOIP
- Digital encryption, public key infrastructure (PKI) and virtual private network (VPN)
- Identify and deal with systems running encryption
- The use of operating systems (e.g. UNIX, LINUX, Windows Server)
- The types of non-standard operating systems that you may come across and how to deal with these
- Obtain evidence, information and intelligence for a network investigation
- The sources of relevant evidence, information and intelligence
- Assess the available information and intelligence for a network investigation
- Assess the factors that may impact on the network investigation
- Identify additional support which is available and may be required for the network investigation
- Maximise useful evidence and minimise loss of potential evidence
- Prevent the cross-contamination of evidence
- Identify and develop initial lines of enquiry
- Identify and deal appropriately with suspects
- Volatility of data and how to preserve it
- Types of actions necessary to preserve third party and volatile data sources (e.g. ISP data sources, cached data)
- Initial preservation of evidence against loss
- Conduct investigations at an international level
- Electronic evidence capture and preservation techniques
- Determine the regulatory bodies involved
- Identify the relationship and links between e-crime and other types of criminal activity
- Types of documentation that must be completed
- Purpose of documenting information on investigations

The next levels of staff requiring training fall into a more specialised area of work. The digital forensics investigator will have a specific function to deal with the capture, analysis and reporting of evidence recovered from digital devices and requires a level of training that will allow them to give evidence in criminal proceedings that may go beyond that of simply providing evidence of fact. Their work may involve the interpretation of evidence and the provision of evidence of opinion. It is right that those fulfilling these roles are provided with opportunities to develop their skills and to undertake professional and academic programmes of learning as well as the capability of keeping their knowledge up to date and relevant through programmes of continual professional development (CPD).

It is acknowledged that not all digital forensic units will have similar structures. It is normal that new units have one or two people who are responsible for all aspects of the forensic process, from collection of evidence, imaging of devices, examination, analysis and interpretation of evidence as well as the preparation of reports and other associated activities. As units mature and increase staff numbers it is common for the functions to be separated to ensure that the most qualified staff carries out activities commensurate to their knowledge and experience. This allows better use of resources.

The role of a digital forensics investigator is one that is of vital importance to the criminal justice system. Such investigators should be able to demonstrate a level of knowledge and skills that enable them to produce evidence that may be used effectively in court proceedings. It is essential that they follow a distinct path of education and training that will lead to professional and/or academic qualifications. It is often then case that organisations approve the purchase of forensic software and send staff on training courses to use that software without ensuring that they have the background knowledge to understand how those tools work and use them effectively as part of a range of appropriate tools. While this may seem worthwhile, all these courses are aimed at teaching students how to use the tool and assume background knowledge. Many of the courses do not contain an assessment of the student knowledge but do provide a certificate. It is essential that these "tool" training course form part of the overall plan for the individual and are not simply used as a quick fix.

It is important to recognise the possibility for there to be varying training paths relating to different functions as well as between staff of the same grade who may specialise in particular aspects of digital forensics; such as different operating systems or device types that require specialised knowledge. It is therefore essential to identify training and education paths for each individual. A learning portfolio that identifies not only formal training but also gives the opportunity for a record of achievement against objectives to be maintained may support this. This is useful not only for the career of the individual but also to ensure that the status of the individual may be tested within the criminal justice system.

Digital forensic investigators require a broad set of skills and knowledge and then will specialise as they become more proficient. It is expected that such investigators will have a sound technological background. For those that are able to demonstrate technical proficiency the following are a list of tasks that should be achievable after completing an introductory training course:

- Check that the necessary authorisations are in place
- Establish the scope of the investigation in consultation with the client
- Identify and select the correct equipment
- Conduct the investigation in accordance with legal and organisational requirements
- Conduct the investigation using evidentially sound forensic tools and techniques
- Conduct cross tool validation of results
- Perform necessary and proportionate research activities to obtain additional information
- Consult with relevant third parties to obtain information relevant to the investigation
- Create a working product for further investigation
- Review the scope of the investigation throughout the process, based on findings
- Document the investigation so all actions can be reproduced by a competent third party
- Provide a clear and accurate oral presentation of the findings
- Establish the content and purpose of the report, and identify the audience
- Conduct an impartial evaluation of the significance of the forensic examinations
- Produce an accurate, impartial and complete written report based on the findings
- Provide a clear and accurate oral presentation of the findings
- Keep accurate records of the process using appropriate documentation

The final group are the managers of cybercrime and digital forensic units who will be making strategic and tactical decisions. It is imperative that this group have sufficient knowledge and skills to be able to make effective decisions. They are also responsible for staff welfare and need to appreciate the different health and safety issues that arise from staff dealing with evidence in

digital form, whether these are at the basic level or the impact of dealing with specific crime types such as child abuse or terrorism. The level of training needed by this group will very much depend on the way that strategies develop in each project area and therefore no breakdown is provided at this stage. This is work that may be continued at national or regional level by the working group assembled under this project.

The information provided above is only to give a guide to those that will be developing training programmes in the future and are of course subject to local needs.

3.4 Training capabilities and resources

Training capabilities and resources required will differ between countries and even between courses within programmes. There are generic requirements; however each course training pack that is developed should contain a detailed list of all the resources required for each event. This will include details of classrooms, technology, trainers as well as specifics for each course delivery. These requirements should be identified during the course development phase. The availability of trainers is another key consideration. It is often the case with countries developing their capacity to deal with cybercrime and electronic evidence, that they do not have an adequate number of trainers with suitable knowledge. It is essential that all potential resources be considered, such as academia and industry trainers, as well as international organisations and training resources.

3.5 Other considerations

There are a number of actions that may be included within the plans of all countries in the region. These include:

- Those that are not already members of ECTEG should consider joining the organisation as associate members.

- All countries should apply for access to existing ECTEG training materials and establish if they are useful for inclusion within the training programmed at a national level.

- All countries should consider the viability of establishing a national or collaboration in a regional 2Centre of Excellence.

3.6 Implementation of the strategy

It is important that each project area begins to adopt national cybercrime training strategies at an early stage. Each project area has begun to identify how this may be achieved and this is dealt with in some detail in the sections below. The regional working group that is created under this project should begin to work together and should continue to do so during and after the project, to provide support, share information and assist in the development of compatible training in and between countries. In order to support the continued collaboration, a group has been created in the Octopus Community.

4 COUNTRY/AREA SPECIFIC STRATEGY OUTLINES

4.1 Armenia

4.1.1 Justification for training strategy

Nowadays, crimes committed by means of computer are more common and they are going to increase day by day. Therefore, Armenia is not protected from those kinds of crimes. According to the brief statistics, from 2009 to 2011 there were registered 36 cybercrime cases, whereas in 2013 the number of registered cases are 82 and in the first quarter of 2014 there are already registered 22 cases related to cybercrime. For instance, theft committed by means of computers (5 cases), computer sabotage (4 cases), illegal appropriation of computer data (11 cases), and illegal dissemination of pornographic materials items (2 cases). As we see the increase will be continued and we are sure that it may include much more spheres of life. The most efficient way to prevent and to react to cybercrime cases is to have officers who are specially and technically trained in that unique sphere.

4.1.2 Objectives of the training strategy

All the police officers should be aware of cybercrime and the level of trainings should be different for each stakeholder group. The stakeholders are:

- High tech crime division officers,
- Cybercrime investigators,
- Prosecutors,
- Judges,
- Experts of National Bureau of Expertise and
- First of all first responders, (According to Armenian law regulation, a person used to report about crime to Regional Police Departments. And this is very important that first responders should be able to identify cybercrime cases).

For the officers who are responsible for investigating cases where high technologies may have been used (terrorism, illegal migration, human trafficking, intellectual properties and money laundering etc), the level of basic knowledge on computers and electronic evidences for all police officers should be mandatory.

4.1.3 Training requirements (needs analysis)

Training requirements for stakeholders groups are:

All police officers

- To be aware of what is a crime committed by means of computer

The first responders

- Basic technical knowledge on computer systems
- Crime scene examining
- Obtaining first necessary electronic evidence
- Immediate data preservation

Cybercrime investigators

- All important fields related to cybercrime cases (types of cybercrime, new forms of cybercrime, how to investigate the case efficiently etc.)
- To be aware of obtaining electronic evidences

- How to make appropriate international requests via High tech crime unit (the main goals of request)

Computer Forensics

- Basic computer forensics
- Forensic tools
- Operating systems
- File Systems
- Working principles of data storage
- Network forensics
- Malware analysis
- Live data forensics

High tech crime unit officers

High tech crime unit officers should be trained in all the above mentioned fields and not only in advanced level and should be able to react very quick to any kind of request from other stakeholders:

- Computer systems
- Data preservation
- Forensic
- International cooperation
- Information gathering techniques from network
- Internet investigation techniques

4.1.4 Training capabilities and resources

In order to teach students, Armenia needs to have qualified staff as trainers through the support of donors. After they are familiarised with the curricula of the cybercrime training process, those people can be used as a cybercrime trainers. Yet, they would be able to prepare a strong strategy for the police officers, investigators, prosecutors, judges and examiners. Here we should mention the importance of cooperation with local industry for establishing frameworks to support the law enforcement by delivery of training, harmonising important and effective programs via available resources. Therefore, for the obtaining above mentioned results, Armenia needs to gain support from international institutions and organizations by getting training materials and keeping continuing collaboration as well.

The Educational Complex of Police deals with all the training programs, courses etc. for Police officers and law enforcement agencies. There are two computer laboratories with about 30 computers, Internet access and training support tools such as flip- charts, smart board, equipment for doing presentations etc in each. Besides, the Educational Complex of Police is in the process of creating an electronic library where all training materials would be introduced to its registered users. For some specific training that cannot be delivered by Police resources, exists the possibility to collaborate with industry and academia. This can be done through joint meetings, round table discussions, seminars etc. Therefore, this kind of cooperation will lead to develop law enforcement strategies against cybercrimes. Armenia should examine the materials provided by ECTEG with a view to incorporating them into national training programs. Via using and implementing these, the requirements of all staff at all levels would benefit. For getting high-level training, programs should be delivered in that country where can be taken advantage of training offered at regional or international levels. Armenia should register as interested parties with 2CENTRE in order to pursue collaboration in terms of delivering partnership. Progress should be reviewed during the GLACY project with a report on developments at the final project meeting.

The most efficient way to train all police officers and students of Police Academy is to have technically equipped auditorium with all possible tools concerning computer systems, computer forensic and other related to identify and investigate crimes committed by means of computer,

modern computer system, forensic tools, diagnostic tools, projection systems and practical tools to show the cybercrime case process

4.1.5 Other considerations

At the moment all probable subjects related to crimes committed by means of computers are depending on high tech crime unit officers to deliver the training. As types of cybercrime cases are increasing daily it is very important for the unit to stay up to date and be trained in all the possible fields concerning cybercrime; the unit should have qualified specialists in all types of cybercrime who will be responsible for each type of case and its investigation. These means that they also should be involved in trainings such as train trainers to be aware of all requirements related to cybercrime cases and be ready to give any advice to stakeholders. In order to obtain the most efficient way of organizing such kind of trainings should be organized round table discussion involving all stakeholders to this subject.

4.2 Azerbaijan

4.2.1 Justification for training strategy

On February 8, 2013 Azerbaijan launched its first telecommunications satellite, Azerspace-1, into orbit. This was one of the greatest achievements that Azerbaijan has accomplished since its independence. Azerspace-1 enables us to render telecommunications, Internet, television, and radio broadcasting services to Europe, the Middle East, Central Asia, and Africa. Now, all of the state TV channels of Azerbaijan and some private channels are broadcast via Azerspace-1. The transition to digital broadcasting has almost been completed in the country and, currently, 96% of the population can access digital TV broadcasting. Enormous actions have been taken to enable citizens to benefit from the opportunities created by the application of state-of-the-art technologies. Consequently, 70% of the population uses the Internet, half of which are broadband internet users. There are 110 mobile subscriptions for every 100 people. The application of 3G and 4G technologies is also being extended. Preparatory works for the implementation of a project to install a fiber-optic network, making providing high-speed broadband internet services through the "Fiber to the Home" project possible, have been already completed and the project will be implemented this year. The year of 2013 will also be remembered for the foundation of the Azerbaijan Information Technologies University. Approximately 60 students with high admission grades already study at this university. The competence and experience gained at this university will enable young people to meet the demands of an information society as well-qualified specialists. There have been some great achievements as a result of the development of e-government. The usage of e-signature and e-payments has been largely extended and the quality and coverage area of e-services provided to citizens by state bodies on a one-stop shop principle has been increased. With the view of the further continuation of legal and expedient measures in this field, state programs on the extension of e-services in state bodies in 2014-2016 and the development of e-government have been drafted and are planned to be adopted this year. Considerable steps have also been taken regarding the provision of information security in the country. The State Agency for Special Communications and Information Security, and the Electronic Security Center, have started their activity with the purpose of improving works being carried out in this field, protecting the information resources and systems of state bodies from possible threats, and raising nationwide preparedness and awareness on cyber security.

Rapid development of information technologies around the world, including Azerbaijan, leads to emergence of new types of problems and threats. Issue of Internet security becomes immediate with the growth of internet usage, as mankind's achievements in the field of information technology are not always used in good faith.

Usage of high technologies by transnational organized criminal groups in large scales is known fact. International terrorist groups make every effort to benefit from scientific achievements, to involve experts in the field of information technologies, communication tools, computers etc. Terrorist organizations actively use Internet network for recruitment of new members, justification of terrorist acts, training potential terrorists, to keep close relationship among their members etc.

As cybercrimes, particularly cyber terrorism is getting more dangerous character; need of improvement of activity of the Ministry of National Security of Azerbaijan Republic in this field has increased. Existence of necessary technical opportunities, as well as knowledge and skills are important for effective struggle against illegal activities in the relevant sphere.
As a respond to mentioned threats and continuity of development Azerbaijan law enforcement needs to be ready for these challenges. Because of it law enforcement trainings need to define in proper structure and met with defined criteria and updated with new technologies and risks.

4.2.2 Objectives of the training strategy

First Responders
(selected personnel in all departments):

- How to respond to the incident;
- Recognizing the area of the crime scene;
- Securing the crime scene;
- Concept an Kinds of Cybercrimes;
- Objects and Subjects of Cybercrime;
- Organization and Law Principles;
- Operating Systems Basics;
- Basics of mobile forensics;
- Search and Seizure;
- Information Gathering with Computer Technologies;

Cybercrime investigators
They have responsibility of gathering relevant information and opening and processing the case.

- Concept an Kinds of Cybercrimes;
- Objects and Subjects of Cybercrime Fighting;
- Organization and Law Principles of Cybercrime Fighting;
- Cybercrime Detection and Prevention;
- Operating Systems Basics;
- Computer Technologies Using in Investigation Methods;
- Methods of Criminal Intelligence;
- Information Gathering with Computer Technologies Using;
- Payment Systems.
- VoIP and Wireless Investigations;
- Money Laundering Investigations;
- Investigation of Sexual Abuse of Children on the Internet;
- Linux Investigations;
- Special Information Gathering Techniques.
- International Experience of Cybercrime Fighting;

Digital Forensic Experts

- Mobile Forensic;
- Data Storage Recover and Search;
- Computer search and seizure;
- Cloud computing investigations;
- Live Data Forensics;
- Malware Analysis and Investigations;
- Macintosh, FreeBSD, Solaris Forensic;
- Cryptography and Steganography;
- Data mining and databases.

4.2.3 Training requirements (needs analysis)

All cybercrime investigators and especially first responders should be able to:

- Identify and select the appropriate tools and consider multiple options to meet the needs of capture or seizure of evidence

- Identify any health and safety risks associated with the electronic devices

- Take appropriate action to safeguard the device and relevant information for the application of physical forensic examinations

- Choose and apply the appropriate power off method for the device

- Photograph and label the components of the device making specific reference to ancillary leads and connections to the device

- Appropriately package, seal and label the device in accordance with current procedures

- Capture and preserve electronic evidence in accordance with legal and organisational requirements

- Document the electronic evidence capture throughout the process so that all actions can be reproduced by a competent third party

4.2.4 Training capabilities and resources

1. Academy of the Ministry of National Security of Azerbaijan Republic
- Department of Programming and Information Technology (5-year training program)

2. Educational Centre of the Institute of Information Technologies of ANAS (Azerbaijan)
According to the certificate of the Educational Centre ECDL (European Computer Driving Licence) the Centre got the status of the certified test center realizing the reception of test examinations in on-line mode and training of computer courses according to the European standards in 2004.

From 2004 according to the certificate of Local Academy CISCO the Educational Centre acquired the right for organization, reception of examinations and delivery of the international certificates of IT Essentials-1, IT Essentials-2 courses.

The main directions of the Education Centre are:

- Studding the subject of "Informatics" to all candidates for doctoral degree and authors of dissertation of our Republic and entrance exams fore minimum of Ph.D. (Decision was accept on 25 October, 2002 and on 16 December, 2002 by the board of Commission of the Supreme Certification under the presidency of Azerbaijan Republic;

- Distance education;

- Organization of courses and education in the field of Informational Technologies;

- Organizing of courses and certification for those who wants to get popular international programmers in the world ECDL (European Computer Driving License), CISCO Local Academy, Microsoft;

- Certification of knowledge in IT;

- Consulting service in IT;

- Improvement of trade level of IT scholars and preparing IT scientists;

- Organizing special courses on computer technology and usage of program guarantees for listeners with different levels.

3. Cyber Security Center of the Republic of Azerbaijan
Engages in reporting on existing and potential threats in the field of cyber security at country level, as well as educating the public, private and other institutions and providing methodological assistance to them.

Consideration should be given to engaging with academia to incorporate accreditation and qualifications into the programme for the cyber investigators and the international partners countries or organizations, which may be able help deliver the more technical levels of training and provide information about technology advances.

4.2.5 Other considerations

Azerbaijan has sufficient resources to create and develop a national centre of excellence in cybercrime training and should work towards the creation of such centre.

4.3 Belarus

4.3.1 Justification for training strategy

Belarus follows the global trend of moving from an industrial society towards the information one with a rapid growth of telecommunications and interactive technologies in the recent years. Today even remote villages may have access to the Internet.

According to the data of the International Telecommunication Union, in 2012 Belarus occupies 41st place by the ICT Development Index out of 157 countries of the world (Korea leads in the ranking) and surpasses most of the CIS countries.

Belarus has National Programme accelerated development of services in information and communication technologies on the 2011 - 2015 years. The purpose of the National Programme is to create conditions for accelerated development of services in information technology, promoting the development of information society on the basis of innovation and to improve the quality and efficiency information for the population, business and government, including the formation of the state system of providing electronic services to ensure effective application of modern ICT.

The national program includes 9 sub-programs:
"National Information and Communication Infrastructure", "E-Government", "E-Health", "E-employment and social protection", "E-learning and human capital development", "Formation of national content," "Electronic Customs", "Security of ICT and digital trust", "The development of export-oriented IT industry".

The implementation of this programme advanced the use of ICTs both by citizens in their everyday life and in the activities of government and business entities. Nowadays, the Internet is widely used by people and organizations for paying taxes, various utility bills, obtaining information, etc.

At the beginning of 2014 the total number of subscribers and Internet users in Belarus amounted to 9.4 million, of them 8.4 million are private persons. Number of subscribers to wireless Internet access increased to 6.6 million.

At present there are 102,000 registered domain names in Belarus. According to the non-commercial organization CENTR, which studies ways of development of national domain zones (primarily European ones), in November 2013 – February 2014 the BY zone grew by 5.7%, showing the fastest growth among European domain zones. The Belarusian domain zone went ahead of the Portuguese domain zone, the Icelandic one and the Czech one.

The domain zone BY is at the peak of its growth in anticipation of the 20th anniversary of the zone's establishment. Over 55% of all the domain names in the Belarusian domain zone were registered in the last two years.

The National Security Concept of Belarus of 2010 mentioned several threats facing the ICT field:

- Rise of crime using ICT technology within Belarus;
- Unauthorised access from outside to the information resources of Belarus that harm its national interests;
- Insufficient safety arrangements protecting the vital information facilities.

Since 1999 when information security crimes (cybercrimes) were first described by the Criminal Code of Belarus the advance of information technologies has changed old crimes and has brought about new forms of crimes involving computer data and various computer systems. The statistics indicates that the number of such crimes is on the rise. In 2012 over 2,000 high-tech crimes were recorded. In 2013 the number exceeded 2,500.

Cybercrimes represent an international problem because, as a rule, such crimes are committed by transnational organized criminal groups, which members use the Internet, easily cross virtual borders between nations, and exploit the imperfect legislation of various countries. In Belarus the legislation allows fighting such crimes effectively. We understand that domestic and interstate cooperation adequate to these challenges can help law enforcement agencies counteract cybercrimes.

Growing of cybercrime such as:

- illegal access to computer systems
- unauthorized actions with data stored in a computer system
- online use of stolen credit card
- skimming
- illegal online payments
- production of false cards
- creation and distribution of viruses, botnets
- spyware
- creation and distribution of pornographic content
- DDoS attacks against websites of public authorities
- GSM fraud; breaches of telecom regulations, including illegal broadcasting

Growing of computer-related crime such as:

- advertising and selling drugs (chemical) in Internet
- money laundering and transferring money throw electronic payment system (e.g. Webmoney)
- sharing of society dangerous information in Internet (about explosive materials, weapons, way of creation of drugs)
- abuse of personality in Internet
- people trafficking

Specific crime areas:

- Child pornography on Internet
- Money laundering on Internet
- Using electronic payment systems in criminal purpose
- Other crimes (electronic evidence related to any offence)

4.3.2 Objectives of the training strategy

On one side:

- Operatives from Ministry of Interior
- Investigators from Investigative Committee
- Examiners (Experts) from Forensic Committee
- Prosecutors
- Judges

On the another side:

- Trainers and teaching Stuff from Academy of MIA (Ministry of Interior)

The Academy of the Ministry of Interior provides for university degrees in law (4-year course) with specialisations in various fields related to law enforcement; it provides for most staff of the Ministry's agencies, of the Investigative Committee.

The Training Centre (Academy of MIA) provides training on cybercrime issues for new recruits and international students. The courses, approved by international specialists, include training on child abuse on the Internet and other cybercrime issues.

Within the high-tech crime units (Ministry of Interior and Investigative Committee) the new staff already have certain skills in the handling of electronic evidence. Training is organised on a regular basis to upgrade the knowledge and improve professional skills. These units frequently prepare guidelines for other units of the Ministry and Committee on the handling of electronic devices, interacting with ISPs.

Belarus considers that all forms of international cooperation, including joint training, are useful. Arrangements with academic institutes or industry bodies – provided they are not yet in place – would also be an asset to develop and deliver training courses on cybercrime and digital forensics.

The following groups and subjects have been identified as the target for training: First Responder (Operatives from Ministry of Interior)

- Securing the crime scene
- Digital data storing media and devices
- Operating Systems basics
- Search & Seizure (all digital media, computers and cell phones, network devices that could contain vital information, labeling, packing and transport)
- Types and Modus Operandi of cybercrime and cyber related offences

Cyber Crime Investigator from Investigative Committee

- Introductory IT forensics & Network Investigations
- Internet Investigations
- Advanced computer technical training
- Computer Forensic (Encase, XWays, FTK);
- Linux & MAC OS
- Wireless LAN & VoIP
- Databases & Data mining

Experts from Forensic Committee

- Basic computer forensics (Partition - Format, File Signatures, Deleted Files, System Shutdown)
- Operating systems (Linux, Mac, Windows)
- File Systems - Fat, Ntfs, Mac, Linux
- Working principles of data storage (CD/DVD, HDD, BluRay, Flash, MMC etc.)
- Database basics
- Network forensics
- Malware analysis
- Steganography
- Live data forensics
- EnCase
- FTK
- Xways

4.3.3 Training requirements (needs analysis)

Specific key points:

1. Collecting of electronic evidence (EE) – type of EE, the way of seizure, discloser of different type of EE
2. Storing of EE (proper methods for this, different type of situation – system on or off mode, packing and labelling EE, creation of proper service document of its actions
3. Transferring EE to examiners (experts) and definite the questions in different situations (it depends from type of EE, mobile phone, harddisk, DVD disks, live-analyse and purpose of analyse
4. Analysing of result of examination with together another evidence
5. Using result in criminal procedure (who, how, goals)

Level of training:

1. First responders (operatives, investigators from local police station)
2. Specialized units of MIA and Investigative committee
3. Experts (examiners)
4. Trainers (teaching stuff)

4.3.4 Training capabilities and resources

For this purpose we can use at first period teaching stuff from Academy of MIA also invited in special cases, questions – investigators, forensic experts and technical specialist
In second period (later) – if we will create Nation Cyber Centre (NCC) - teaching stuff will composed by practical specialists, scientists and trainers which are will be working there (for example- investigator – 2/3 time -real case, 1/3 working time - teaching trainers - 1/3 time -real case, 2/3 working time - teaching and science

Now we have:

- Academy of MIA
- International training centre
- Practical units of MIA, Investigative Committee which are sharing of practical knowledge

A course on high-tech crime was introduced at the Academy in 2011 and at the international training centre. It deals with international cooperation, national and international legal framework, investigation measures, interview of suspects and specific cybercrime offences.

The Department on Investigation of Crimes against Information Security and Intellectual Property of Main Investigative Department of Investigative Committee of the Republic of Belarus currently organises another training on electronic evidence, use of special investigative measures and other, as well as on methodology and practice of investigations. The Investigative Committee approved this course and provided for the trainers.

In March 2013, 94 persons attended in Investigative Committee a seminar on cybercrime. Many governmental bodies, including the Academy, the Ministry of Justice, the Prosecutor General and the Ministry of Interior took part in event.

An international conferences on cybercrime was in June 2012 at Academy of MIA, July 2013 at the Institute for National Security and in this year at 19 of June will be at Academy of MIA;

What we want:
To create National Cyber Centre (NCC), which are include specialist from each state agency.

The Investigative Committee of Belarus in April 2014 has put forward an initiative to set up a center to counteract cybercrimes in Belarus. The official said that plans have been made to set up a cutting-edge center at a Belarusian education institution for the sake of discussing the theory and practice of counteracting cybercrimes. The center will enroll both university professors and law enforcement officers, who specialize in cybercrime investigations.

The center is supposed to enable research in the area of criminal law, criminal proceedings, and forensics. It will host regular meetings of scientists, representatives of law enforcement agencies and the private sector for the sake of sharing experience and finding solutions to existing problems, for working out strategic approaches to cybercrime control, for working out educational problems for this field.

On 15 April 2014 the Investigative Committee hosted a working meeting to discuss the creation of the cybercrime center in Belarus. The meeting gathered representatives of the Investigative

Committee, including those involved in information security crime investigations, representatives of the Supreme Court, the Prosecutor General's Office, the Interior Ministry, the State Security Committee, the Operations and Analysis Center under the President of the Republic of Belarus, the State Border Committee, the State Forensics Committee, and the State Customs Committee. The experts also discussed matters concerning investigations into information security crimes, the application of criminal law norms that envisage responsibility for information security crimes, and procedural peculiarities involved in such investigations.

What we need:

- A decision for creating of NCC from decision makers
- Modern equipment, soft and methods of forensics, detecting and teaching
- Preparing of teaching stuff in modern methods in this sphere

By using two languages: Russian, English.

The questions of certifications will be resolved in according of Belarussian Education Code with Ministry of Education and International Partners – may be CoE – ECTEG, Interpol, another international cybercrime centre by recognised of each other.

4.3.5 Other considerations

1. Creation of NCC
2. Participation in EU educational and practical projects (ECTEG, common operations in combating cybercrimes and sharing of information and knowledge about it (2-3 times in year)
3. Practical assistant from EU bodies in teaching methods, equipment and special soft.

In 2012 has been established a group of experts (from Ministry of Interior, Investigative Committee, banks) under the auspices of the National Bank. It has already developed recommendations on the use of online payments systems – for instance, making test transactions for online purchases.

4.4 Georgia

4.4.1 Justification for training strategy

In Georgia, annual statistics of technological crimes is rising rapidly and the main reasons for that is the country's progressing dependence information technologies (IT). In Georgia, IT infrastructure is not only the target or means of commission of the crimes, but it can also provide very useful evidentiary information on other offences such as murder, robbery and other cases. In that regard, it should be mentioned that evidence that is provided by use of technological means in practice is much more valuable in comparison with other traditional evidences (such witness testimonies) since they are so called "static evidences" (reflects objective reality and is not dependent on personal subjective assessment of the events connected to the case at hand). Since cybercrime statistics are growing rapidly in Georgia and there is a lack of enough human and material resources, the country should choose qualitative approach according which Georgia will constantly continue capacity building of its small but effective cybercrime law enforcement staff in order to strengthen the fighting against cyber offences.

The crime areas that can be impacted by technology are identified as follows: economic crimes, terrorism related offences, crimes against human beings and etc.

4.4.2 Objectives of the training strategy

The main stakeholders that require training in Georgian law enforcement agencies are identified as follows:

MIA Cybercrime Division is the main responsible body for combatting cybercrimes in Georgia. The Division requires trainings mainly on cyber investigation techniques, search and seizure of digital evidences, malware analysis and related staff. The division is also responsible for 24/7 international cooperation in line with Budapest Convention on Cybercrime. Taking into account that Cybercrime Division is newly established in Georgia, it would be of utmost importance for relevant staff to be trained on the specificity of international cooperation as required by the Budapest Convention.

MIA Forensic Division carries out forensic service on all types of cases including cybercrimes. For these purposes, Forensic Division has Computer Forensic Unit that carries out handling of digital evidences and further processing. Division issues decisions on the validity of digital evidences that are attached to the criminal case file and have evidentiary proof in the national courts. Cybercrime forensic specialist are necessitated training on the following issues: seizure and further processing of digital evidences, trainings on the tools necessary for processing digital evidences, international best practices on the processing of digital forensics and etc.

MIA Operative-Technical Department assists Cybercrime and Forensics Division in most complex cybercrime cases. Therefore, training level for the employees of the Operative-technical Department should be much more advanced rather that in the case of Cybercrime or Forensic Divisions. In that line, it would be most convenient if the course for Operative-Technical Department would be more focused on reverse engineering, advanced malware analysis, advance network and cyber investigation techniques.

Financial Investigation Service combats economic and financial crimes that are committed through cyber means as well. In that regard, they necessitate trainings for illegal online money transfers.

Taking into account that MoJ Forensic Bureau rechecks the results provided by police forensic experts, the training level for their employees should as advanced as possible. Therefore, it would be of utmost importance the employees of the Bureau would undergo trainings related to advanced digital forensics, cryptoware and etc.

4.4.3 Training requirements (needs analysis)

Training for Georgian cyber law enforcement agencies should be more oriented on technical issues along with the legal framework. As already mentioned above, trainings should be conducted on the following issues: cyber investigation techniques, search and seizure of digital evidences, intermediate and advanced level of malware analysis, seizure and further processing of digital evidences, trainings on the tools necessary for processing digital evidences, international best practices on the processing of digital evidences, reverse engineering, advanced network investigation techniques, handling digital evidences that are encrypted, methods necessary for combatting cryptoware and other related staff.

Besides the requested trainings indicated in this section, Georgian relevant law enforcement agencies require trainings also on the following issues: conducting preparatory research concerning the subject of the investigation; identify the appropriate tools to meet the needs of capture or seizure; recognizing devices capable of storing electronic evidence; considering the volatility of data and its preservation; choosing and applying the appropriate power off method for the device; photographing and labeling the components of the device making specific reference to ancillary leads and connections to the device; appropriately package, seal and label the device in accordance with current procedures.

4.4.4 Training capabilities and resources

In Georgia there is availability to teach students legal frameworks necessary for combatting cybercrimes including material and procedural part of national legislation. At the same time, Georgia possesses qualified specialists eligible to deliver trainings on international police cooperation in line with Budapest Convention and internal regulations.

Georgia needs international experience mainly on technical subjects such as advanced malware analysis, reverse engineering, cryptoware and etc. Possible donors in that line can be European Cybercrime Centre, Council of Europe and the relevant national agencies of the EU countries.

Specialists residing in Georgia can teach the students organizational and legal framework that regulates cybercrime issues nationally. In that regard, Georgia will be able to launch the courses on standard operational procedures related to first handling and further processing of digital evidences.

Ministry of Internal Affairs and Data Exchange Agency will mainly provide specialists at the national level. At the same time, it will be possible to acquire specialist on different subjects from educational institutional. However, the knowledge that they can provide to Georgian law enforcement officers is relatively limited.

Taking into account fruitful cooperation experience with EU technical assistance program (TAIEX), there is the possibility to address this organization for cybercrime training issues. For these purposes, relevant Georgian agency should draft project proposal for TAIEX through which it will be possible to invite foreign trainers into Georgia or send our law enforcement staff to other countries. Besides TAIEX, the Council of Europe under the GLACY project can provide significant assistance.

Training will be delivered in the premises of MIA Academy since it possesses part of necessary technical and material resources for cybercrime trainings. It is possible to organize cybercrime training in various language (English, French, Russian) since the MIA Academy has its own qualified staff that translates cybercrime training in a simultaneous manner. Technical trainings can be launched in English since major part of IT Terminology is in this language and it will not be a problem for Georgian law enforcement staff. However, MIA Academy needs the relevant educational base, material resources (books, other online materials) for forming effective

cybercrime training centre. It should be mentioned also that MIA Academy elaborated Independent System of Student Assessment that regulates certification issues in police. Furthermore, Academy actively works in order to obtain the status of Higher Education Institution through which diplomas of MIA Academy will have the same legal power as those of civilian institutions.

4.4.5 Other considerations

It would be better if the Strategy would include Action Plan that will provide all details necessary for fulfilment of Strategic Goals and Tasks. Action Plan should also be oriented on certain period: 1year, 2 years and etc.

4.5 Mauritius

4.5.1 Justification for training strategy

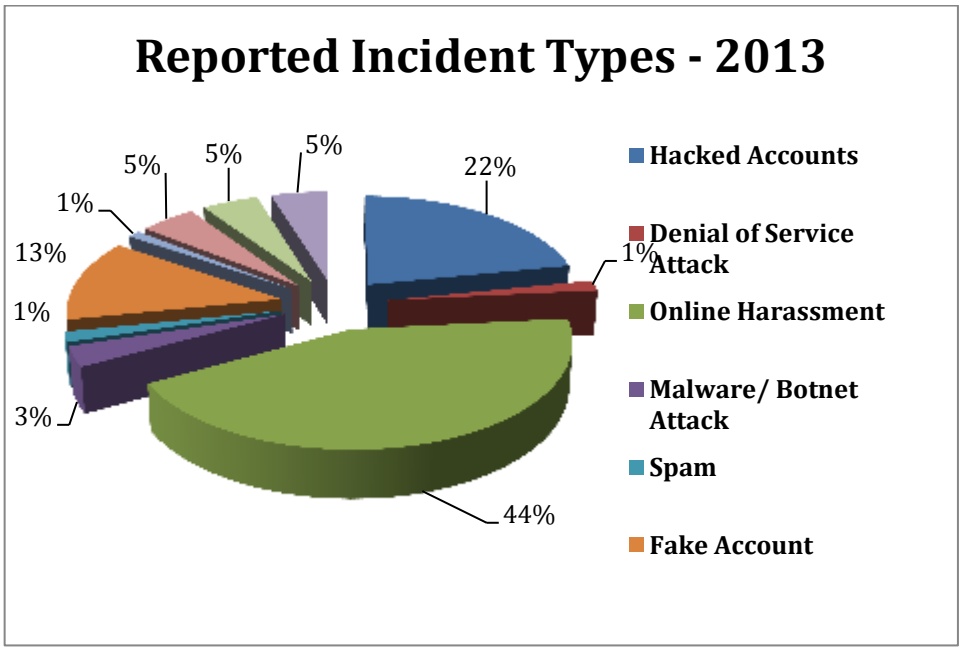
The fast economic and social development of Mauritius during the past decade has alongside brought a rapid development in the IT sector. The commitment of the government of Mauritius to make our island a knowledge hub has led to a massive investment in IT sector. The idea behind such investment is to make Mauritius a Cyber Island as well as to diversify the economy and benefit from globalization. There have been huge impacts in the Mauritian society where most families have now acquired their personal computer with easy Internet access. Furthermore, a large number of the population possess at least one mobile phone.

Current Trends and Challenges

The development of the Internet and digital technologies represent a major opportunity for Mauritius in transforming businesses and providing new tools for every day communication. Likewise other countries, the ICT sector in Mauritius is influencing the lives of people through direct or indirect contribution to the various socio-economic parameters such as employment and standard of living. It is indeed playing a significant role in transforming Mauritius into a cyber-hub in the African region. The Government has also been a key driver for increased adoption and promotion of IT based products and IT enabled services in the public services (e-Government services to citizens), education (e-learning, virtual classrooms) and financial services (mobile banking, Internet banking).

However, with the increased IT adoption, Mauritius is becoming more vulnerable to cyber threats. Security-related threats have not only become numerous and diverse but also more damaging and disruptive. For the past few years, new types of security related incidents have emerged in Mauritius, which is affecting individuals as well as businesses. For instance from year 2009 to 2013, 787 cases in breach of the Computer misuse and Cyber Crime Act 2003 and 5,869 cases in breach of the Information Communication and Technology Act have been reported to the Police. The above mention Acts are largely in line with the Budapest Convention.

The chart below shows the types of incidents reported at CERT-MU for the year 2013. The statistics indicate that the most frequent type of incident reported is Online Harassment, followed by hacked accounts and fake accounts.



Individual or companies who are victims of e-crime report such cases to law enforcement authorities. However, these IT offences are becoming a major challenge to the police as these culprits are operating under the shadow in a constantly changing environment and are using advance technologies. It becomes even more difficult when cases happen from outside the Mauritian jurisdiction.

4.5.2 Objectives of the training strategy

The Mauritius Police Force (MPF) is the national law enforcement agency for the Republic of Mauritius. It is governed by the Police Act 1974 and responsible for policing on mainland Mauritius, Rodrigues and other outer islands. It is headed by the Commissioner of Police and operates under the aegis of the Home Affairs Division of the Prime Minister's Office. The MPF is presently composed of about 13,000 Police officers posted in Divisions or Branches.

MPF has different levels of responsibility for investigating cybercrime:

1. Regular and CIDs Officers

The regular Police at Police Station/ local CID officers deal with minor Cases. These Police Officers have the following responsibilities:

- Recording cases
- Preliminary actions
- Preliminary enquiries
- Handling and Securing exhibits

2. Officers at Cyber Crime Unit in the Central CID

The Cybercrime Unit under the Central CID investigates serious offences/high profile cases. These Police Officers have the following responsibilities:

- Recording cases
- Preliminary actions
- Preliminary enquiries
- Handling and Securing exhibits

3. Police Officers at the IT Unit (Forensic Investigators)

The IT Unit is part of the Central Criminal Investigative Department (CCID) and in addition to providing technical support for the MPF technical infrastructure; they provide all digital forensic services to the MPF. The IT Unit has existed for about 10 years. The IT Unit is composed of 40 staff in total and 20 among them are involved in digital forensic. Investigators and forensic examiners are working separately, with separate responsibilities to ensure independence of the forensic process. All staffs in the IT unit are police officers. There are no civilians employed. Only qualified police officers with diploma, certification or extensive knowledge in IT are selected.

The unit has the following responsibilities:

- Forensic examinations
- Support in high-tech cases
- Training for the academy
- Support (consulting & forensic examination) for own police units and bodies (e.g. ICAC) as well as for other countries, e.g. Seychelles, Rodrigues.

4. Police Prosecutors

In Mauritius cases (including cyber cases) are prosecuted by the Police Prosecutors. These Police Officers have the following responsibilities:

- Preparation of case file

- Relevant laws applicable
- Presentation of digital evidence in court

5. Police Training School

The Police Training School (PTS) of the MPF is the institution responsible for the trainings of both, new recruits as well as experienced officers. Each year the school trains 800-900 new recruits. After joining the MPF they get a 2-year initial training. There are just a few, very basic elements of cybercrime and electronic evidence training in this programme. Within the 2-year period the recruits participate in a continuing training programme, which offers some more contents in this area. These Police Training School have the following responsibilities:

- Training of new recruits
- Ensure continuous development of all police officers and other law enforcement agencies (e.g. Mauritius Revenue Authority, Prison department)
- Preparation of Training Needs Analysis for the MPF
- Liaise with external institution (e.g. Universities) to conduct relevant courses to police officers.

4.5.3 Training requirements (needs analysis)

Electronic evidence may be encountered in any type of crime and it is essential that police officers have the knowledge to recognise and handle such evidence, to ensure the effectiveness and fairness of investigations. To this end Police Officers should be provided with the appropriate knowledge and skills both within their foundation/initial training and during developmental training. This will enable them to identify potential cybercrimes and deal with them appropriately, including being able to recognise when it is necessary to call upon specialist investigators or resources.

1. Regular Police and CIDs Officers

All Police Officers (about 13,000 including Rodrigues Island) need to be trained on basic First Responding for electronic evidence and First Responders need to be trained on

- Cyber Crime Offences
- Introduction to Electronic Evidence Principles and Procedures
- Evidence Sources
- Electronic Evidence
- Search and Seizure on site and on Suspect
- Handling of Exhibits- including packaging, Transport & Storage

2. Officers at Cyber Crime Unit in the Central CID

Cyber Crime Investigators need to be trained on the following:

- Cyber Crime Offences
- Introduction to Electronic Evidence Principles and Procedures
- Evidence Sources
- Electronic Evidence
- Search and Seizure on site and on Suspect
- Handling of Exhibits- including packaging, Transport & Storage
- Ethical Hacking
- Basic Digital Investigation including:
    - Search & Seizure –Dead Box Scenarios
    - Search & Seizure –Live Data Scenarios
    - *Practical Session on Search and Seizure*

3. Police Officers at the IT Unit (Forensic Investigators)

Police Officer from the IT Unit need to be trained on the following:

- Digital Forensics (for Beginners)
- Advanced Digital forensic training

- Live data collection
- Linux, Mac forensics
- Server forensics
- Network forensics
- Advanced forensics on Mobile phone and tablets
- Video Forensics (Leva certified)
- Advanced Email forensics
- Intrusion testing
- Ethical hacking
- Training on setting up a internet/network watch patrol re child pornography, Paedophile abuse on social networking (re racial/antisocial comments)

4. Police Prosecutors

The Police Prosecutors needs the following training:

- Electronic Evidence
- Analyzing Evidence
- Preparation and Presentation of Evidence
- Admissibility of Digital Evidence in Court
- Jurisdictions – including Cross Border Cases

5. Police Training School

Instructors of Police Training School need to be trained on the following:

- Cyber Crime Offences
- Introduction to Electronic Evidence Principles and Procedures
- Evidence Sources
- Electronic Evidence
- Search and Seizure on site and on Suspect
- Handling of Exhibits- including packaging, Transport & Storage
- Basic Digital Investigation including:
    - Search & Seizure –Dead Box Scenarios
    - Search & Seizure –Live Data Scenarios
    - *Practical Session on Search and Seizure*

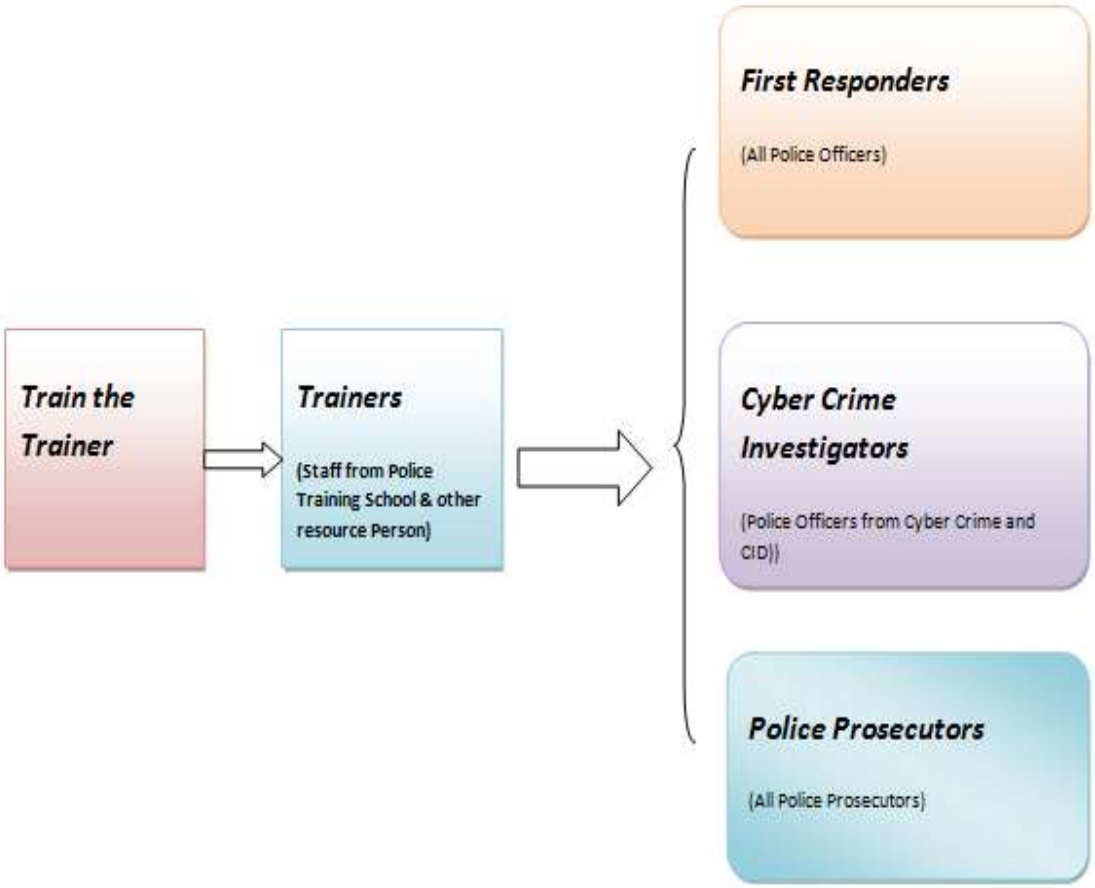
4.5.4 Training capabilities and resources

The Police Training School is the institution responsible for the trainings all Police Officers. Actually the PTS is only providing training on the relevant laws pertaining to Cyber Crime. However, no training on how to respond to cyber offences was given to Police Officers.

Training Strategies
First Responder – Cyber Crime Investigators – Police Prosecutors

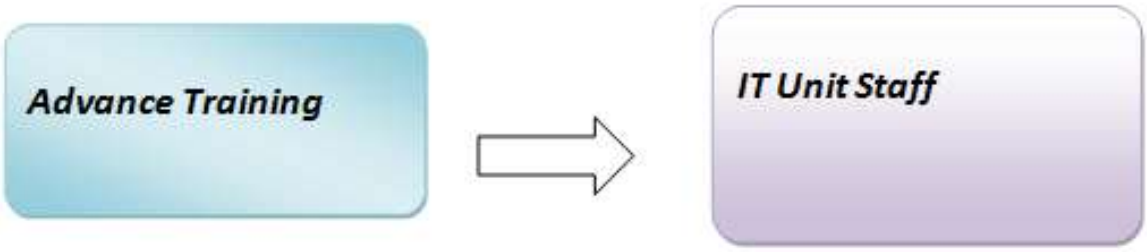
To cope with the new challenge that the IT sector represent, the Mauritius Police Force has to developed new strategies to deal with e-crime. Thus, our Police Officers need to be trained to acquire the sufficient knowledge and skill to deal efficiently with such offences.

Actually no Police Officers have been trained on how to conduct training on cyber cases. A Train the Trainers course is also being envisaged to develop the competencies of trainers to deliver training at Force and Divisional level to compensate the deficiencies. The training strategies for first responders, Cyber Crime investigators and Police Prosecutor is as per below diagram:



Digital Forensic Examiners – IT Unit

The staffs of IT Unit (Digital Forensic Examiners) have been given training by donors (From UK, USA, India...). It is being contemplated that in the near future advance training has to be envisaged to deal with upcoming technical aspect of cyber crime and digital evidence. It will also help to track down offenders and assist in a successful prosecution.



The Mauritius Police Force has the following Training centres:

- Police Training School Beau-Bassin
- Police Training School Les Casernes
- 7 – Divisional IT Training Centres (Including Rodrigues Island

Training for First responders, Cybercrime Investigators and Police Prosecutors can be conducted at above training Centres. The centres can be equipped with required logistic equipment by the Police IT Unit.

The Mauritius Police Force in collaboration with the universities in Mauritius can work out a training program to enhance knowledge and skills of Police Officers on electronic crime. The universities can issue certificate to successful candidates.

English is the official language and French is commonly used in Mauritius. Therefore training can be conducted in English or French or both.

4.5.5 Other considerations

- Sensitization campaign on Cyber Crime by all stakeholders including Law Enforcement agencies, Ministries, Press, School.
- Partnership with both public & Private Sectors.
- International Corporation with law enforcement and other agencies.

4.6 Moldova

4.6.1 Justification for training strategy

According to the official statistics, nowadays the population of the Republic of Moldova is 3,938,679 citizens and the number of the registered Internet users is over 620.300.

Due to the development of the IT services, Moldova has one of the best wired Internet connections in the world, as well as one of the cheapest Internet services in terms of price per Mbit. Moreover, 3G /4G technologies are becoming more and more popular.

Approximately 50% of the territory of the capital city Chisinau is covered by free access Wi-Fi networks. Also, in January 2014, the national ISP "Moldtelecom" started 1GB/s Internet.

The impact

Cyber security.

The implementation of information technologies in all areas of state activity in the Republic of Moldova, such as: economic, social and administrative services, has determined the evolution of criminality and its extension over cyberspace. Thus, in the last years the computer networks and electronic information are increasingly used for criminal purposes, and obviously the data that could become the evidence of these crimes are also stored and transmitted through these networks by the perpetrators.

In the last period of time, botnet attacks, hacking and malware attacks, attacks on governmental and private websites are becoming more frequent. The criminals are using 3G and 4G technology, special technical means and sophisticated software. Personal data leakage usually takes place through social networks and even as a result of illegal data interception. Criminals obtain illegal income after cheating the users by sending spam letters with tempting offers, publishing announces about inexistent facts, using the on-line shops. In order to stay unanimous, the criminals often use the proxy servers, VPNs, open public Wi-Fi networks. In such cases, it usually takes a long to identify the offenders. The impact of technological progress on the methods of committing crimes has determined the appearance of new "modus operandi" of the criminals. Thus, the traditional crimes started to move to the virtual space.

Online sexual exploitation of children.

As a result of the significant growth of the opportunities offered by electronic communications, children also became victims of cybercrime. Child sexual abuse and sexual exploitation are particularly serious forms of crime. Sexual abuse in childhood is an extremely traumatic event that can change a person for life, causing interruption of emotional, spiritual, intellectual, sexual and social interest and also other kind of negative influences, and the persistence of the phenomenon undermines the core values of modern society.

The study "Violence against children in Moldova", implemented by UNICEF shows that 10% of children are exposed to sexual abuse. Very often, for grooming children, criminals use social networks and other chat networks such as "Skype". Also the offenders use file sharing networks that allow fast exchange of pictures and videos of child pornography content without using central data servers or the Web.

Frauds related to bank cards and other electronic payment systems.

The modernization of the technical information managed by the national banks, for the safeguard and protecting the confidential data (PSI DSS, 3D Secure, etc.) also has determined the evolution of the criminality in this field, which implements new methods of realizing illegal transactions.

Thus in the last years several changes of the criminal behavior in this field took place:

- The physical criminal activity is changing progressively to the virtual offences;

- The criminals are well aware of the ATM's components (especially the location of the video cameras) and more often are using different methods of disguise (masks, hats, hoods, artificial beards, etc.);
- Due to the fact that the banks in Republic of Moldova are currently implementing smart cards with chip instead of simple bank cards with magnetic stripe, the criminals are starting to adjust their illegal activity to the vulnerabilities of the new card payment system.

Beside the above-mentioned, since 2011 the Government of Moldova started a mass support of the IT sector. In this context, the private business sector has benefits, as well as the students of the IT faculties have a range of facilities.

Eventually that motivates a lot of young men to pursue a career in IT and it is obvious that a major percentage of the cyber criminality springs namely from the mentioned activity.

4.6.2 Objectives of the training strategy

The specific key points that should be learned are:

- Information technology security investigators – investigation of production and illegal use of special technical means, intellectual property crimes, informational attacks: hacking, refail, spam, malware, unauthorized access of the computer and telecommunications systems, e-commerce, financial pyramids, on-line hazardous games etc.
- Child protection investigators – investigation of child pornography, online sexual abuse and exploitation of children, grooming etc.
- Electronic payment means investigators – investigation of frauds related to bank cards and other electronic payment systems, such as embezzlement of funds, cloning, phishing etc.
- Operational assistance officers – first response, technical assistance activities using modern technology and software, data carving, file systems examination, data recovery, mobile forensics, etc.
- Strategic investigators – threat analysis, vulnerability assessment etc.
- Forensics – data carving, file systems examination, data recovery, mobile forensics etc.
- Other policemen, prosecutors and judges – basic training course on technical aspects of computer related crimes.

4.6.3 Training requirements (needs analysis)

The main academic institution in this area is the "Stefan cel Mare" Academy of the Ministry of Internal Affairs. At the moment the academy has 3 computer classes, where the teachers provide basic theoretical course on the following topics:

- General concepts regarding informational security
- Vulnerabilities of informational systems
- Malware and Anti-Malware
- Controlling access to informational systems
- Protection of information through classification
- Cryptography
- Cryptography Systems
- Ecommerce and the digital signature
- Protection and security of networks
- Computer network security techniques
- Management of informational security
- Informational security policies (models)
- Legal aspects regarding informational security in Republic of Moldova
- International Law aspects regarding informational security
- Preventive and Investigative methodologies regarding informational crimes

Total of 30 lessons (16 theory and 14 practice)

4.6.4 Training capabilities and resources

At the moment there are 3 teachers that are able to train the beneficiaries, out of which one is fluent in English (from the technical point of view). Considering their experience and background, they are able to conduct the new trainings with the proper training of trainers. In case if this amount of trainers will be insufficient, there is an option of involving in the trainings the colleagues from the Technical University from Moldova, who are teaching students at a new speciality since 2014 – "Informational security". Eventually the team of trainers needs to undergo an international training of trainers.

Taking in consideration that in the Republic of Moldova there are 29 officers who work in the cybercrime unit and 5 computer forensics, we can assume that at the moment it will be more efficient to build their capacities by training in the field of their activity made by practical cybercrime investigators and forensics.

The basic cybercrime training will be delivered at the "Stefan cel Mare" Academy, in form of theoretical courses and practical exercises. At the moment the academy has sufficient computers, but no law enforcement dedicated software for investigating cybercrimes, as well as no computer or mobile forensic software. Also, if specific hardware configuration for network or other investigations will be required, it must be identified.

The training can be delivered in Moldavian language, but taking in consideration that most of the citizens of the country possess Russian language, training at international level could be delivered.

4.6.5 Other considerations

In order to organize the trainings within the "Stefan cel Mare" Academy, an analysis of the owned equipment must be done.

Due to the fact that the EnCase, FTK, XRY and Celebrate software have been identified as to be learned obligatory by the operational assistance officers and forensics, as in order to organize the training on file systems and databases, the minimum requirements of the equipment should be determined. If they do not suit to the technical needs, new it will be necessary to purchase additional equipment.

4.7 Morocco

4.7.1 Justification for training strategy

LES TIC sont devenues un instrument stratégique de développement du royaume du Maroc, depui s la gestion des affaires personnelles, jusqu'à la sécurité de l'état.

Durant ces dernières années le Maroc a connu une évolution significative de l'utilisation des TIC d ue entre autres à l' informatisation de l'administration publique et de la dématérialisation des servi ces publiques ainsi que le renforcement de l'arsenal juridique, la mise en place des institutions org anisationnelles notamment le CNDP (conseil nationale de la protection des données publiques), l'or ganisme de tiers de confiance qui concerne la signature électronique, le CERT national, etc.

Cette évolution a engendré l'apparition de nouveaux types d'infractions, des nouvelles menaces m ais aussi de nouveaux modes opératoires.

En effet les TIC sont très utilisées pour commettre des infractions portant atteinte aux systèmes d e traitement automatisé des données mais aussi pour faciliter la commission des crimes classiques tels que le terrorisme, les infractions a caractère économique et financier, la pédophilie, les escro queries, etc.

En effet, le nombre des affaires() liées a la cybercriminalité connait une recrudescence très consid érable qui est due également à l'usage de plus en plus important des réseaux sociaux (plus de 6 m illions de profils Facebook) afin de perpétrer des infractions liées au chantage et à la sextorsion.

C'est ainsi que l lutte contre la cybercriminalité est devenue l'une des priorités de notre gouverne ment.

ICT has become a strategic tool for development of the Kingdom of Morocco, since the management of personal affairs, until the safety of the state.

In recent years Morocco has experienced a significant change in the use of ICT among others due to the computerization of the public administration and the dematerialisation of public services and strengthening the legal arsenal, the establishment organizational institutions including the CNDP (national council for the protection of public data), the organization escrow regarding the electronic signature, the national CERT, etc.

This development has led to the emergence of new types of offenses, new threats but also new procedures.

Indeed, ICTs are used to commit offenses against the automated systems of data processing but also to facilitate the commission of traditional crimes such as terrorism, offenses economic and financial, paedophilia, fraud, etc.

Indeed, the number of cases related to cybercrime knows a very considerable increase is also due to the use of increasingly important social networks (more than 6 million Facebook profiles) to commit offenses blackmail and sextorsion.

Thus the fight against cybercrime has become a priority for our government.

4.7.2 Objectives of the training strategy

Les services de répression qui travaillent dans le domaine de la lutte contre la cybercriminalité

dans notre pays sont la Direction Générale de la Sûreté Nationale et la Gendarmerie Royale. Il est à noter que la Direction Générale de la Surveillance du Territoire sera dotée du bureau central des investigations judiciaires (BCIJ) qui sera également concerné par la lutte de ce fléau.
Les unités spécialisés dans la lutte contre la cybercriminalité des services de répression précités sont généralement composés de deux catégories:

Les investigateurs: généralement des officiers de police judiciaire, ayant bénéficié d'un module de formation sur les notions de base en matière de cybercriminalité et de preuves numériques, qui travaillent sur le terrain pour le recueil de la preuve numérique (perquisitions, auditions, constats, etc.)

Les examinateurs: généralement des ingénieurs et des techniciens lauréats des grandes écoles spécialisées dans le domaine des nouvelles technologies, ayant bénéficié de quelques formations spécialisées en la matière, qui travaillent dans les laboratoires d'analyse de preuves numériques (investigations numériques, récupération des données, les constats techniques, les investigations cybernétiques, etc.)

Il convient de signaler que nous avons des services spécialisés dans les affaires économiques et financières, la pédophilie, le terrorisme, ... Qui travaillent en collaboration avec les unités de la cybercriminalité lorsque les TIC sont utilisés pour commettre ces crimes.

Law enforcement agencies working in the field of fight against cybercrime in our country are the General Directorate of National Security and the Royal Canadian Mounted Police. It should be noted that the General Directorate of Territorial Surveillance beyond will have the central office of judicial investigations (BCIJ) which will also be involved in the fight this scourge.

Specialized in the fight against cybercrime repression services are generally composed of two categories:

Investigators: usually police officers, who received a training on the basics of cybercrime and digital evidence, working on the ground to the corpus of digital evidence (searches, interviews, observations, etc.)

Examiners: generally engineers and technicians winners from major schools in the field of new technologies, having received some specialized training in this area, working in the laboratories of digital evidence (digital investigations, data recovery, technical findings, cyber investigations, etc.).

It should be noted that we have specialized in economic and financial affairs services, paedophilia, terrorism ... Who work with units of cybercrime when ICTs are used to commit these crimes.

4.7.3 Training requirements (needs analysis)

Afin de répondre a chaque profil exerçant au sein des unités spécialisées dans la lutte contre la cybercriminalité, il s'avère nécessaire de mettre a la disposition des investigateurs et examinateurs des modules de formation adéquats couvrant principalement les infractions cybernétiques les plus répandues au sein de la société marocaine qui pourraient être énumérés comme suit:

Pour les investigateurs:

- Les nouveaux modes opératoires des attaques aux systèmes d'information (ransomware, ddos,...)
- Reconnaissance de la scène de crime
- Techniques de recueil des preuves numériques

- Récupération des données volatiles (interprétation des lignes de commande, techniques d'investigations en ligne,...)
- Techniques d'enquêtes liées aux fraudes a la carte bancaire (phishing, skimming, carding,...)
- Techniques d'investigations des réseaux sans fil
- Techniques d'analyses des traces des serveurs d'hébergement.

Pour les examinateurs:
- Analyse forensics sur les différents systèmes d'exploitation (Windows, Linux, mac) utilisant différents systèmes de fichiers (fat, ntfs,...)
- Analyses des techniques d'anonymat (Tor, proxy, vpn, web invisible,...).
- Osint: analyse et recueil d'information depuis les sources ouvertes.
- Analyses forensics des réseaux informatiques.
- Analyse des Malware.
- Sténographie.
- Analyse des fichiers cryptés et protégés par mot de passe.
- Récupération des fichiers supprimes et endommagés.
- Analyses des supports de stockage endommagés
- Formation avancée sur les outils forensics (Encase, FTK, Xways).
- Analyse forensics des terminaux mobiles (smart phone, tablette, carte sim,....)
- Analyse des différents systèmes de payement.
- Investigations sur du contenu multimédia (image, vidéo,....).

To meet each profile exercising in specialized units in the fight against cybercrime, it is necessary to make available to investigators and examiners appropriate training modules mainly covering cybercrime most widespread in the Moroccan society that could be listed as follows:

For investigators:
- New procedures attacks on information systems (ransom ware, ddos)
- Recognition of the crime scene
- Techniques collecting digital evidence
- Recovery of volatile data (interpretation of command lines, investigation techniques online)
- Techniques relating to fraud investigations credit card (phishing, skimming, carding)
- Investigations of wireless networks technologies
- Technical analysis of traces of hosting servers.

For Examiners:
- Forensics analysis on different operating systems (Windows, Linux, Mac) using different files systems (fat, ntfs)
- Analysis of anonymity techniques (tor, proxy, vpn , invisible web) .
- OSINT: analysis and information from open source code.
- Forensics analyses of computer networks.
- Analysis of Malware.
- Steganography.
- Analysis of encrypted and password protected files.
- Recovery of deleted and damaged files.
- Analysis of damaged storage media
- Advanced on forensics tools (Encase, FTK, Xways) training.
- Forensics analysis of mobile devices (smart phone, tablet sim card)
- Analysis of the different payment systems.
- Investigations on multimedia content (image, video).

4.7.4 Training capabilities and resources

Etats des lieux:
Depuis la création des unités spécialisées dans la lutte contre la cybercriminalité, certains

examinateurs ont bénéficié de formations en la matière, dans le cadre de coopération internationale, qui leurs ont permis de former de leur part les investigateurs en activité ainsi que des nouvelles recrues.
Cette approche qui a donné ses fruits, a permis aux bénéficiaires d'être édifiés sur les nouvelles techniques d'enquête en matière de cybercriminalité.

Cependant, il a été permis de constater que cette stratégie de formation des formateurs ne peut être appliquée que pour les modules de formation de base.

Ainsi, l'aide du secteur privé et les universités peut contribuer efficacement pour assurer des modules de formation avancée, d'autant plus que ces organismes ont exprimé leur volonté pour collaborer dans ce domaine.

Il est a signaler que la proposition de créer au Maroc un centre d'excellence en matière de cybercriminalité , déjà mentionné sur le rapport de situation de notre pays établi dans le cadre du projet "glacy", demeure une alternative opportune d'autant plus qu'il va réunir un nombre important d'intervenants représentant le secteur privé et publique.

L'institut royal de police dispose d'un laboratoire d'analyses forensics, dédié a la formation en matière de cybercriminalité et d'une maison témoin qui pourrait être utilisée comme une éventuelle scène de crime cybernétique.

Cet institut dispose également d'un amphithéâtre et de plusieurs salles de formations équipées de matériel logistique.

De même, au niveau régional, les sièges des préfectures de police, disposent de salle de réunions équipées qui peuvent être utilisées pour animer des sessions de formation.

Étant un pays francophone, il est souhaitable d'organiser des formations en langue française afin de cibler un grand nombre de participants. Cependant, la langue anglaise ne constitue pas vraiment un handicape pour la formation au Maroc.
A la fin de chaque formation, les stagiaires bénéficient des certificats de participations qui peuvent être délivrées par les autorités compétentes.

State of play:
Since the creation of specialized units in the fight against cybercrime, some reviewers have received training in this area within the framework of international cooperation, which led to their form from them investigators in activity as well as new recruits.
This approach has borne fruit , allowed beneficiaries to be built on the new techniques of investigation of cybercrime .

However, It was found that this strategy of training of trainers can not be applied for modules of basic training.

Thus, using the private sector and universities can contribute effectively to provide advanced training modules , especially as these organizations have expressed their willingness to cooperate in this field.

It was noted that the proposal to create a centre of excellence Morocco cybercrime , already mentioned in the status report of our established under the project " Glacy " countries remains a timely alternative especially that it will reunite important stakeholders representing the private and public sector numbers.

The Royal Institute of Police has a forensics laboratory analyses, dedicated to training on cybercrime and witness a home that could be used as a stage for eventual cybernetic crime.

The institute also has an amphitheatre and several training rooms equipped logistics materiel.

Similarly, at the regional level , the seats of prefectures police have private meetings rooms that can be used to animate training sessions.

As a francophone country, it is desirable to organize training in French language to target a large number of participants. However, English is not really a handicap for training in Morocco.
At the end of each course, students receive certificates of investments that may be issued by the competent authorities.

4.7.5 Other considerations

Stage pratiques au sein des services de répression des pays avant gardistes en la matière et signa taires de la convention de Budapest.

Practical internship in services repression countries trendsetters in the matter and signed the Buda pest Convention.

4.8 Philippines

4.8.1 Justification for training strategy

From 2003 to 2012, the Anti-Transnational Crime Division (ATCD) of the Criminal Investigation and Detection Group (CIDG) of the Philippine National Police (PNP) looked into 2,778 referred cases of computer crimes from government agencies and private individuals nationwide.

Records from the PNP show that there are 141 cybercrime cases under investigation; 24 operations conducted resulting to the arrest of 304 persons and filing of 47 cases in court. There are 521 number of requests received for examination; 2,054 electronic evidence examined and 2,575 reliable digital forensic examination and technical investigative support were provided to various law enforcement agencies.

Although there appears to be a larger workforce in the DOJ Cybercrime Office, NBI and PNP ACG constituting the cybercrime investigators, forensic examiners and designated prosecutors when compared with the reported cases under investigation and prosecution take into consideration other countries there is still a serious need for our workforce to receive regular trainings to be adept and equip themselves from the growing and advancing cyber related cases happening around the globe.

It is the policy of the Philippine government to address cybercrime issues and free the country from being a hub of cyber abuses and in fighting cybercrime it is necessary that cybercrime investigators, forensic examiners, prosecutors, judges and other stakeholders must be keeping pace with technology.

Besides even in the absence of an objective increase in the scope of crime, this demand is not expected to decrease. The state's responsibility to provide security to its citizens cannot stop at the threshold of cyberspace, and in this realm to the practical expressions of such responsibility must be defined as part of a democratic political process on a firm factual basis.
Crime has always been a widespread social phenomenon. Criminological explanations combine motivation, opportunity, and the existence of a guarding factor.[1]

The following action steps may be desirable to establish a cyber security framework where there is a need for capacity building:

1. Understand cybercrime from a global perspective;
2. Define a national cyber security strategy;
3. Develop public awareness of cybercrime and cyber security challenges (economic and management issues, political issues, social issues, technical issues, legal and law enforcement issues);
4. Promote a cybersecurity culture;
5. Train and inform on information and communication technologies and on security issues, and relevant legal provisions;
6. Develop cyber security education;
7. Propose a unified cyber security framework;
8. Put in place organizational structures to support a national cyber security strategy;
9. Create regional alert points for the provision of technical information and assistance regarding security risks and cybercrime;
10. Redefine law enforcement and legal framework in order to bring cybercrime perpetrators to justice;
11. Manage jurisdictional issues;
12. Develop acceptable practices for ICT protection and reaction;

[1] http://cdn.www.inss.org.il.reblazecdn.net/upload/(FILE)1362314977.pdf

13. Establish effective cooperation and promote cooperation and coordination at national and international levels;
14. Force information technology and content providers to improve the security of their products and services.[2]

4.8.2 Objectives of the training strategy

DOJ Cybercrime Office:

- Technical assistant – performing administrative function such as preparation of documents and receiving data
- Prosecutors- conduct preliminary investigation and file information in court
- State Counsel – handles cases requiring international cooperation
- Attorney position – handles formal complaints and request on cyber related issues
- Special investigator – to conduct investigation of cases lodged with the DOJ

NBI:

- Special investigator – investigate reported cybercrime cases; assist in the investigation and detection of cyber related crimes
- Forensic examiner - conduct investigation and assist in the case build-up

PNP:

Cyber Cop:

- Prepares the Incident Report;
- Interviews the complainant and secures the sworn statement and gathers digital evidence
- Prepares entrapment operation if, necessary;
- Applies search warrant, if needed
- Examines digital evidence, process data and analyzes froensics examination results;
- Prepares complaint for filing with the DOJ or concerned Prosecutor's Office
- Testify in Court or DOJ proceedings;
- Monitor the status of the cases filed for any possibility to submit other documents and pleadings.

Computer Forensic Examiner:

- To receive and document all incoming request for digital forensic examination of digital storage media (Hard Disk Drive, External Storage Media) from the computer system;
- Conduct Digital Forensic Examination on seized evidence;
- Recommend measures and collaboration of laws to enhance the digital forensic evidence admission in courts;
- Coordinate with other entities to address digital forensic examination matters;
- Maintain the evidence database on examination conducted;
- Attend court hearings on examined digital evidence;
- Monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection;
- Ensures submission of periodic reports; and
- Performs other task as directed.

Audio/Video Forensic Examiner

- To receive and document all incoming request for Digital Multimedia Evidence examination (Analog or digital media, including, but not limited to, film, tape, magnetic and optical media, and/or the information contained therein);
- Conduct forensic video examination on all incoming request particularly those pertaining to CCTV footage enhancement ;

[2] Ibid.

- Prepare official forensic examination report pertaining to Digital Multimedia Evidence examination conducted for investigative purposes;
- Create and maintain evidence database of Digital Multimedia Evidence examination conducted;
- Formulate guidelines, policies and best practices in Digital Multimedia Evidence acquisition, recovery, recovery, analysis and report making;
- Coordinate with other entities to address digital forensic matters which includes proper Closed Circuit Television (CCTV) installation, acquisition and preservation;
- Provide technical assistance to other PNP Units/Offices in the proper acquisition, extraction, preservation and documentation of CCTV footages in order to protect and maintain the integrity of Digital Multimedia Evidence which may later be used as evidence in court;
- Prepare and submit periodic reports and other related documents pertaining to Digital Multimedia Forensic examination needed by higher authorities;
- Attend court hearing to testify as expert witness and give testimony in court pertaining to the result of Digital Multimedia Forensic examination report submitted to the investigating body; and
- To perform any other task as may be directed by the Director, ACG.

Cellphone/Mobile Forensic Examiner:

- To receive and document all incoming request for cellphone/ mobile phones and other cellphone storage media for forensic examination;
- Conduct data extraction and data recovery and other digital storage mediaon cellphone/mobile evidence;
- Prepare official Forensic Examination Result pertaining to Cellphone/Mobile Forensic Examination for investigative purposes;
- Provide operational support to investigative units within the PNP, including the search, seizure, and evidence preservation from the crime scene;
- Formulate guidelines in cellphone/mobile forensic evidence on extraction and data recovery;
- Recommend measures and collaboration of laws to enhance the digital forensic evidence admission in courts;
- Coordinate with other entities to address digital forensic examination matters;
- Maintain the evidence database on cellphone/mobile forensic and other cellphone storage media examination conducted;
- Attend court hearings to testify as expert witness concerning cellphone/mobile forensics data extraction and data recovery examination report submitted in court;
- Prepare and submit periodic reports and other related documents pertaining to computer system and network forensic examination needed by higher authorities; and
- Performs other task as directed by the Director, ACG

4.8.3 Training requirements (needs analysis)

It is imperative that basic and advance introduction to computers must be learned by key personnel involved in fighting cybercrimes to be able for them to identify whether a related activity constitutes a violation of cybercrime, and if so in the course of investigation how an evidence may be gathered and preserved to be able establish a strong case against the perpetrators with an end-in-goal to stop cyber abuses

Listed are the activities that had been conducted by each agency with plans and actions:

DOJ Cybercrime Office

- Hosted the Regional Workshop on Protection of Children against Online Sexual Violence in South-East Asia: Law Enforcement Cooperation and the Criminal Law Benchmarks of the Budapest and Lanzarote Conventions in coordination with the Council of Europe;
- Participated in the 2013 9th and 10th T-CY Meeting and Annual Octopus Conference in Strasbourg, France.

- Conducted Basic Cybercrime Ethical Hacking Trainings with participants from NBI-CCD, PNP-ACG and OOC personnel.
- Conducted a two-day conference in Protecting Children in the Cyberage in partnership with IACACP and CWC of DSWD and IACAT and JJWC of DOJ.

Proposed Plan:

- Issuance of Implementing Rules and Regulations of Republic Act No. 10175;
- Validation of the Investigation and Prosecution Procedure Manuals for Law Enforcement and Prosecutors;
- Continuous effort to facilitate mutual legal assistance and extradition treaties and update the Philippine Extradition Law on dual criminality provision of computer-related offenses;
- Enhanced capability building trainings, seminars and workshop with primarily with three track of instructions: track for the prosecutors, track for the investigators, and track for digital forensic examiners;
-

NBI:

In 2014 the NBI-CCD will continue with its two major trust CAPACITY BUILDING and CAPABILITY ENHANCEMENT in order to cope with the fast changing technology and cyber environment.

- Team building and planning session – CCD group
- Local Trainings for Agents/Investigators:
- Basic Cybercrime Investigation Course - To be conducted every quarter
- Online investigation / familiarization on Online investigative tools – To be conducted every quarter
- Advance online Investigation course – Follow up course on the first two courses.
- Undercover investigation course – Twice a year
- Ethical Hacking course (basic) – Twice a year
- Ethical Hacking Course (advance) – Twice a year
- Seminar on proper handling of Electronic Evidence (Twice a year)
- Encase Training Module 1. Three times a year
- Encase Training Module II- Three times a year
- Encase Prometric Examination – Three times a year
- Cellebrite Training – Three times a year
- Foreign Training and Conferences:

PNP

- Train the Trainers in Computer Forensics Course (sponsored by INTERPOL)
- Digital Forensic Mentoring and Consultation (in cooperation with the U.S. Department of State Anti-Terrorism Assistance
- Asia Pacific Network Information Center (APNIC) Workshop (in partnership with APNIC)
- Four (4) Special Cybercrime Courses ("Cyber Cop" Basic Course):
    - Introduction to Cybercrime Investigation Course
    - Identification and Seizure of Digital Evidence (ISDE)
    - Introduction to Digital Forensics and Investigation (IDFI); and
    - Proactive Internet Investigation Course (PIIC).

There are four (4) Mandatory Courses for all personnel of PNP ACG, such as:

- Program of Instruction for Introduction to Cybercrime Investigation
- Program on Intsruction for Identifictaion and Seizure of Digitial Evidence (ISDE)
- Program of Instruction for Introduction of Instruction for Introduction to Digital Forensics and Investigations (IDFI)
- Program of Instruction for proactive Internet Investigation

The PNP Anti Cybercrime Group has the following existing training programs for its personnel:

- Introduction to Cybercrime Investigation
- Identification and Seizure of Digital Evidence
- Introduction to digital Forensics and Investigation

- Proactive Internet Investigation

To effectively combat cybercrimes, these personnel must be provided with the following to further enhance their competence in the investigation of cybercrimes and cyber related offenses as well as the conduct of digital forensic examination and cyber incident response:

- Advance Anti-Cybercrime Course (For those who have undergone the 4 Special Cybercrime Courses or the "Cyber Cop" Basic Course
- (10 days duration= 80 training hours)
- Executive Seminar on Cybercrime (For PSUPTs and up)
- (3 days duration= 24 training hours)
- Cyber Security (10 days duration= 80 training hours)
- Cyber Financial Investigation (10 days duration= 80 training hours)
- Mobile Forensic (10 days duration= 80 training hours)
- Advance Computer Forensic (10 days duration= 80 training hours)
- Practical Advance Investigation (10 days duration= 80 training hours)
- Practical International Cyber Investigation (10 days duration= 80 hours)
- Data Base Forensic (10 days duration= 80 training hours)
- Network Forensic (10 days duration= 80 training hours)
- Live Data Forensic (10 days duration= 80 training hours)
- Ethical Hacking/Penetration Testing (10 days duration= 80 hours)
- Malware Analysis (10 days duration= 80 training hours)
- Audio/Video Evidence Extraction (10 days duration= 80 training hours)

4.8.4 Training capabilities and resources

The PNP Training Service occupies a building structure inside the National Headquarters in Camp Crame with less than hundred classrooms accommodating more or less thirty (30) students per room. Specialized training is conducted annually and cybercrime is part of the training program.

The PNP Training Service has pool of trainers mandated only to conduct trainings and educate the PNP officers and personnel. Lecturers/experts from the academe and international law enforcement institution and organization are invited to conduct specialized lectures, such as cybercrime.

The PNP Anti-Cybercrime Group is also in collaboration with the private industry and academe, such as the Philippine Computer Emergency Response Team or PhCERT and Philippine Institute of Cyber Security Professionals (PICSPro), particularly on cyber security.
Noteworthy to mention is the pending collaboration between the PNP ACG and National University (NU) to have a partnership in their curriculum for BS Information Technology Major in Digital Forensic.

The NBI is still in the process of crafting its training manual and training courses. The module is also in working progress

4.8.5 Other considerations

The PNP ACG has training programmes, which aim to enhance its capacity on cybercrime investigations and digital forensic examination of electronic evidence.

The funding requirement is shouldered by the PNP or through the national government. Donor/sponsor organizations usually funded the international trainings.

Some of the requirements for cybercrime training programs include, but not limited to establishment of training centre, pool of experts, technological equipment for hand-on instruction, and instructional materials.

As of now, the government is yet to utilize industrial resources for the training programs. It is recommended that some government projects be also undertaken with private industries, like the IBM, Samsung, etc., as well as telecommunication industry like Globe, Smart etc. due to their financial resources as well as advanced industrial perspective that could help in the enhancement of the government training capacity. Note that all trainings in the Philippines are conducted in English language.

The PNP Technical Service is conducting training without certification and academic accreditation as yet.

Microsoft through its Government Security Program gave the Microsoft Certification such as Microsoft Certified Professional (MCP), Microsoft Certified System Administrator (MCSA), and Microsoft Certified system Engineer (MCSE) after completion of the series of trainings and passing the online certification examinations. It is a free program for government Information Technology (IT) personnel.

While the other digital forensic certifications such as EnCase Certified Examiner, CelleBrite UFED physical and logical certified examiner are propriety certifications given by private institution after completion of a series of trainings, online certification examinations, and practical scenario certification examinations. The United States Department of State Anti-Terrorism Assistance Program (ATAP) sponsored the training and certification examinations. These training were taken locally but the trainers are foreign experts.

On the other hand, the NBI agents/investigators have attended various cybercrime investigation courses conducted by the bureau and other foreign law enforcement counterparts mostly from Homeland Security and FBI.

4.9 Senegal

4.9.1 Justification for training strategy

Au Sénégal, les TICS ont engendrées la recrudescence d'actes répréhensibles commis dans le cyberespace. On note de nouvelles infractions spécifiques sont commises liées à la cybercriminalité par exemple les atteintes aux systèmes informatiques et aux données informatisées, actes de piratages informatiques et intrusions frauduleuses, vol d'infraction….

Il y a également les infractions se rapportant au contenu telles que les infractions se rapportant au contenu, la diffamation, les injures, les menaces, les propagandes de nature à troubler l'ordre public via internet (mails, réseaux etc…).

Enfin comme infractions traditionnelles facilitées par les technologies, la police nationale constate des cas d'escroqueries, blanchiment, de séquestration parfois, des extorsions de fonds, fraude(fraude dans le e-commerce) ,d'usurpation d'identité et de trafic de drogues (échange de mails, plans de trafic via internet).

A côte de ces infractions se développe de plus en plus le phénomène de la prostitution en ligne au niveau d certains centres d'appels.

Même si le Sénégal ne connait pas d'attaques informatiques pour le moment, le cybercriminalité a connu des évolutions à deux niveaux.

D'abord, au regard des infractions commises, nous avons passé à une cybercriminalité liée aux atteintes aux biens à des atteintes aux données informatiques, au hacking, aux atteintes physiques (cas d'arnaques via net suivi de séquestration et de demande de rançon).

En second lieu, le Sénégal a passé d'une cybercriminalité qui était dans le passé l'œuvre d'étranger à l'implication des nationaux (victime de l'ingénierie sociale et acteurs principaux). On voit que la preuve numérique est capital et elle partout dans tous les cas connus par les services de police sénégalais d'où la nécessité d'une formation de base et continue d'un nombre important.

In Senegal, TICS have caused the resurgence of wrongdoing in cyberspace. Specific new offenses committed there related to cybercrime e.g. attacks against computer systems and computer data, computer hacking and acts of fraudulent intrusion, theft offences

There are also offenses related to content such as content -related offences, defamation, insults, threats, propaganda likely to disturb public order via internet (email, networks etc.).

Finally, as traditional crimes facilitated by technologies, the National Police found cases of fraud, money laundering, kidnapping sometimes, extortion, fraud (fraud in e -commerce), identity theft and trafficking drugs (mail exchange , traffic plans via internet).

A side of these offenses grows increasingly the phenomenon of prostitution in line at some call centres.

Although Senegal does not know of computer attacks for the time being, cybercrime has been changes at two levels.

First, with regard to offenses, we spent a cyber-related crimes against property damage to computer data, hacking, physical attacks (if scams monitoring via net capture and ransom) .

Secondly, Senegal spent a cybercrime in the past was the work of a stranger to the involvement of national (victim of social engineering and key actors) . We see that digital evidence is critical and throughout all known by Senegalese police cases where the need for basic training and continues to a significant number.

4.9.2 Objectives of the training strategy

Les services qui travaillent dans lutte contre le cyber crime qui ont besoins de formation en matière de cybercriminalité au Sénégal sont :

Les services centraux de la Police Nationale et de la Gendarmerie Nationale (Division des Investigations Criminelles de la Direction de la Police Judiciaire, Section de Recherches) et des commissariats de police et des brigades de gendarmerie. Les éléments des Brigade de Recherches de la Police Nationale qui sont le plus souvent les premiers sur la scène de crime informatique. Il y a également les enquêteurs de tous les services de police judiciaire qui traitent des cas de cybercriminalité et des crimes traditionnels qui sont facilités par les technologies et dont les moyens de commission est la technologie de l'information et de la communication. De même, les chefs de services de police ont besoin de cette formation pour pouvoir conduire et diriger bien les investigations et donner des indications sur la collecte des preuves contenues dans supports électroniques et numériques pour la manifestation de la vérité et surtout sur les procédures de collecte des preuves pour qu'elles soient recevables. Cette formation pourra les permettre de définir des stratégies locales au niveau de leurs services respectifs qui va aboutir une parfaite stratégies de cyber sécurité au niveau national.

Cette formation peut être étendue aux agents des services de police et gendarmerie qui lutte contre le terrorisme dans le domaine de la répression et de la prévention. Il peut s'agir des élément de la Direction de la Surveillance du territoire notamment la Division du Contre Espionnage de la Police Nationale. Les services spéciaux comme l'Office Central de Répression du trafic illicite et des stupéfiants, la Brigade des mineurs, la Brigade des mœurs ont besoin de cette formation. Les infractions relevant de leur domaine sont commises a moyen ou facilitées par les technologies.

Identification des rôles.

- Les enquêteurs en criminalistique auront pour rôle l'assistance technique dans le cadre des enquêtes. Ils aident les services à produire les preuves numériques selon les procédures requises(collecte, authentification, préservation et présentation des rapports d'expertise).
- Les enquêteurs les réseaux auront pour mission de la traque sur les réseaux (réseaux sociaux, réseaux de cyber pédophile..), l'analyse de tous les éléments issus des systèmes numériques qu'il s'agisse de PC, de serveurs, de Smartphones ou de tout objet.
- Les premiers intervenants seront chargés de préservation la scène de crime informatique de toute altération ou modification, collecté les données volatiles et de chercher toute autre preuve susceptible d'éclairer l'enquête, d'identifier les supports susceptible de regorger des preuves numériques, de les saisir, d'établir la chaine de possession et des les transporter au laboratoire pour expertise.
- Les enquêteurs sur la protection de l'enfance (Brigade des mineurs et Brigade des mœurs) se chargeront non seulement de prévenir, de protéger les enfants en ligne mais détecter tous les sites de cyber pédopornographie et en cas d'enquêtes d'identifier les sources de preuves
- Les enquêteurs sur la criminalité économique pourront identifier les réseaux de blanchiment de fonds en ligne, d'escroquerie en ligne.
- Pour ce qui est des crimes qui sont facilités ou commis au moyen de technologies au Sénégal, il faut dire c'est presque toutes les infractions. Il peut s'agir d'une manière générale du trafic des stupéfiants, de la traite des êtres , de l'immigration

irrégulière, les crimes économiques et financiers tels que les détournements de fonds, la blanchiment, les atteintes physique aux personnes telles que les séquestrations, les enlèvements, les viols(les réseaux sociaux facilitent les contacts et les interactions), les extorsions de fonds, les escroqueries, les atteintes aux données par le vol , l'altération et la modification.

Services working in the fight against cybercrime who need training on cybercrime in Senegal:

The headquarters of the National Police and the Gendarmerie Nationale (Division of Criminal Investigations Directorate of the Judicial Police, Research Section) and police and gendarmerie. Elements of Research Brigade of the National Police who are most often the first on the scene of computer crime. There are also investigators all criminal police handling cases of cybercrime and traditional crimes that are facilitated by technology and whose means of commission is the information technology and communication. Similarly, heads of police departments need this training to lead and lead well investigations and provide guidance on the collection of evidence in electronic and digital media for the truth and especially on the collection procedures evidence for them to be admissible. This training will enable them to define local strategies at their respective services, which will lead to perfect cyber security strategies at national level.

This training can be extended to officers of police and gendarmerie fight against terrorism in the field of law enforcement and prevention. It may be the element of the Directorate of Monitoring territory including the Counter Espionage Division of the National Police . Special services such as the Central Office for the Repression of Illicit Traffic in Narcotic Drugs and the Minors Brigade, Brigade manners need this training. Offenses in their area are committed by or facilitated by technology.

Identifying roles.

- Forensic investigators have role for technical assistance in the investigation. They help services to produce digital evidence according to the required procedures (collection, authentication, preservation and presentation of expert reports) .
- Investigators networks will have the task of tracking networks (social networks, cyber networks paedophile), the analysis of all elements from digital systems whether PC, servers, Smartphones or anything .
- The first responders will be responsible for the preservation of computer crime scene tampering or modification, collected volatile data and seek any other evidence to inform the investigation, identify carriers may abound digital evidence to seize , to establish the chain of custody and transported to the laboratory for expertise.
- investigators on the Protection of Children (Juvenile Police Brigade and morals) will be responsible not only to prevent, protect children online but detect all sites cyber pornography and cases investigated to identify lines of evidence
- The economic crime investigators will identify networks of money laundering online scam online.

Regarding crimes that are facilitated or committed through technologies in Senegal, this is almost all offences. It can be a general traffic narcotics, human trafficking, illegal immigration, economic and financial crimes such as embezzlement, the money, the physical attacks on persons such as kidnapping, abduction, rape (social networks facilitate contacts and interactions), extortion, fraud, violations of data theft, alteration and modification.

4.9.3 Training requirements (needs analysis)

Les besoins de formations pour les autres services de police et de gendarmerie.

Niveau 1: sensibilisation aux outils de l'internet

Niveau 2: initiation aux procédures d'enquête, préservation des preuves. Identification des preuves numériques, préservation, collecte, transport.

Niveau 3 : criminalistique: de la documentation jusqu'au rapport technico-légal.

Pour la Brigade Spéciale de lutte contre la Cybercriminalité et d'autres ingénieurs supérieurs en informatique sélectionnés.

- Renforcement les capacités des spécialistes et les permettre avec la possibilité de participer à des forums d'enseignements en ligne et discussion entre professionnels.
- Des modules de formations sur les domaines suivants :
- Les outils d'investigations en linux mac et formation,
- La programmation,
- L'audit des serveurs et des réseaux,
- L'initiation en matière d'enquête en ligne sur pédopornographie,
- Les technologies de partage de fichiers (applications P2P),
- Les technologies sur l'identification de vidéos et photos,
- Les investigations sur les réseaux sociaux,
- L'Interprétation des journaux du serveur Web et du code HTML des pages web
- Identification du matériel et des logiciels nécessaires pour infiltration en ligne efficace enquêtes,
- Les applications Web, le codage et la vulnérabilité
- connaissances sur le chiffrement numérique, l'infrastructure à clé publique (PKI) et le réseau privé virtuel (VPN)
- Les techniques d'anonymisation des adresses IP et la manière de les lever dans le cadre des enquêtes.
- Techniques d'investigations sur la car ding et skimming
- Formation sur le Cloud computing
- La formation d'experts en criminalistique se basant sur les profils.

Training needs for other police and gendarmerie.

Level 1: Awareness Internet tools

Level 2: introduction to investigative procedures, preservation of evidence. Identification of digital evidence, preservation, collection, transportation.

Level 3: Crime: documentation to technical -legal report.

For Special Brigade to fight against cybercrime and other senior engineers selected computer.

- Strengthening the capacity of specialists and provide with the opportunity to participate in forums of online courses and discussion among professionals.
- Training modules on the following areas:
- The tools mac linux investigations and training,
- Programming,
- The audit servers and networks,
- Initiation in investigating online child pornography
- The technology file sharing (P2P) ,
- Technologies on identifying videos and photos,
- Investigations on social networks ,
- The Interpretation of web server logs and HTML web pages
- Identifying the hardware and software required for infiltration effective online surveys,
- Web applications , coding and vulnerability
- knowledge of digital encryption, public key infrastructure (PKI) and virtual private network (VPN)
- The anonymization of IP addresses and how to get up in the investigation techniques.
- Techniques for investigations on the ding and skimming
- Training on cloud computing
- The training of forensic experts based on profiles.

4.9.4 Training capabilities and resources

- Pour ce qui est de la formation, le Sénégal ne dispose pas de formateurs suffisants. Par contre, pour les Niveau I, Niveau II et Niveau III, la Brigade Spéciale de lutte contre la Cybercrimalité pourrait participer à la formation des les autres services avec l'appui du secteur privé national, de la coopération et des autres partenaires comme le Conseil de l'Europe, Interpol, Europol, Francopol, ECTG, EC3 et d'autres spécialiste des autres polices.

- Pour la formation continue des éléments de la Brigade Spéciale et autres experts en informatique sélectionnés, la formation devait être assurer par des experts en matière de cyber crime pour les permettre d'atteindre un niveau supérieur. L'appui de la coopération du secteur privé national , du monde universitaire, du Conseil de l'Europe, Interpol, Europol, Francopol, ECTG et EC3 est nécessaire.

- Pour les moyens nécessaire à ces formations, en dehors des efforts nationaux c'est à dire la coopération entre le public et le privé, il faut non seulement la coopération internationale mais l'implication de structures cités ci-dessus.

Pour assurer la formation de la Police dans l'avenir, la Police sénégalaise peut miser sur la formation de base des nouveaux recrus de l'Ecole Nationale de Police en fonction de leur expertise en matière de TICS, procéder à une partage des connaissances déjà acquis entre les autres services, assurer la formation continue par une mise à jour perpétuel. Cela pourrait être facilité par des formations interne et de l'assistance de la coopération. Sur cette base, on peut envisager la formation d'un maximum de formateurs.

A l'Ecole Nationale de Police, il existe des salles disponible pour accueillir des formations. Les salles sont équipées et disposent de l'Internet. Il y a également une salle informatique qui peut abriter une formation pour un nombre limité. Une salle peut être dédiée à la formation en cybercriminalité (Directeur des Etudes de l'Ecole). Il serait souhaitable que cette salle soit équipée de matériel didactique, de logiciels d'apprentissage avec la possibilité d'accéder à des enseignements à distance.

Les ressources de l'industrie et du monde universitaire peuvent être impliquées par invitation après avoir identifié les bonnes ressources ou bien par contrat.

Au niveau national, la formation peut avoir lieu en Français et au niveau régional en Français et en Anglais et peut porter les techniques d'investigations numériques surtout les enquêtes sur les réseaux, le mode opératoire des cyber délinquants.

Pour la question des certification et des accréditions universitaires, il est nécessaire que les cyber investigateurs, les analystes et les experts soient certifiés. Pour ce faire, les centres de formation et les universités en la matière surtout français soient mis en contribution. Une formation en ce domaine n'existe pas au Sénégal.

1. As regards training, Senegal does not have sufficient trainers. By cons, for Level I, Level II and Level III , the Special Brigade fight against Cybercrimalité could participate in the training of other services with the support of the national private sector , cooperation and other partners such as the Council Europe , Interpol , Europol, Francopol, CTAS , EC3 and other specialist other fonts.

2. For the training elements of the Special and other experts selected computer Brigade, training should be secure by experts on cyber crime to achieve a higher level. Supporting the cooperation of the national private sector, academia, the Council of Europe, Interpol , Europol, Francopol , CTAS and EC3 is required.

3. For the means necessary for such training outside national efforts ie cooperation between the public and private sectors, it is not only international cooperation but the involvement of structures mentioned above.

To ensure the formation of the Police in the future, the Senegalese Police can build on the basic training of new recruits of the National Police Academy based on their expertise in ICTs, make a sharing of knowledge already acquired among other services, provide continuing education by putting perpetual day. This could be facilitated by internal training and assistance cooperation. On this basis, we can consider the formation of a maximum of trainers.

At the National Police Academy, there are rooms available to accommodate training. The rooms are equipped and the Internet. There is also a computer room, which can accommodate training for a limited number. A room can be dedicated to training cybercrime (Director of Studies of the School). It is hoped that this room is equipped with teaching aids, learning software with the ability to access distance learning.

Resources industry and academia may be involved by invitation after identifying the right resources or by contract.

At the national level, training can take place in French and at regional level in French and English and can carry digital investigation techniques especially network investigations , the modus operandi of cyber criminals.

For the issue of certification and academic accreditations, it is necessary that cyber investigators, analysts and experts are certified. To do this, training centres and universities in the above matter are in French contribution. Training in this field does not exist in Senegal.

4.9.5 Other considerations

No further information

4.10 Sri Lanka

4.10.1 Justification for training strategy

Cyber Crimes are a major component of Computer Crimes and is committed through the internet media where computers together with internet resources are used to distribute illegal data. It is stated that cyberspace is the fifth common domain after the sea, land, air and outer space. Cyber Crimes include pornography, phishing, sexual harassments, social networking issues economic crime and email attacks.

Traditional crimes also impacted by the technology, criminals do uses digital equipment's and the cyberspace for do their activities to carry out in efficient manner. Most of the scammers are outsiders who visited Sri Lanka as a tourist. Due to that that main economics centres as well as banks, Stock exchange and e-business in a risk today; human smuggling, trafficking and drug dealers also benefitted by the technology. The officers who involved in investigations were not able to track down the technology savvy offenders due to their lack of knowledge and experiences. The growth in the telecommunications sector has resulted in high mobile penetration, rapidly growing internet penetration and increased potential in mobile related and e-commerce activities. Due to that cyber related offences were increased.

The first responders (law enforcement officers) who were handled cybercrime case were unable to grab ping point from victims and collecting digital evidence from the scene of crime.
This was directly affected to case solving rate of the country.
Therefore it is very much essential to have a proper strategy to training people who involved in combating cybercrime.

4.10.2 Objectives of the training strategy

1. First Responders (Who are collecting digital evidence)
    a. Scene of crime officers (SOCO)
    b. Local Police officers
    c. Police Narcotic Officers
    d. Women and Child bureau
    e. Officers from Criminal Investigation Department
    f. Tourist Police officers
    g. Fraud investigation bureau

2. Cyber Crime Investigators
    a. Data Analysing officers
    b. Network Investigating officers
    c. Cyber Surveillance officers
    d. Financial Data Investigators

3. Digital forensic Examiners
    a. Computer Forensics examiners
    b. Mobile Forensics examiners
    c. Networks Forensics examiners
    d. Audio & Video Forensics examiners

4.10.3 Training requirements (needs analysis)

First Responders (Who are collecting digital evidence)

- Identification (of fencers related to case , victim and witnesses, Media that contains potential evidence) and Preservation (So that data is not lost)
- Sri Lankan Laws related to computer crime investigation

    - No.36 of 2003 Inter-lectual Property Act
    - No: 19 of 2006 Electronic Transaction Act
    - No: 30 of 2006 Payment Device Act
    - No: 24 of 2007 Computer Crime Act

- Check the necessary authorizations, conduct preparatory research concerning the subject of the investigation
- Identify the appropriate tools to meet the needs of capture or seizure
- Recognize devices capable of storing electronic evidence; consider the volatility of data and its preservation
- Isolate the scene and secure the electronic evidence sources to prevent contamination and external interference
- Determine whether to capture electronic data or to seize electronic devices
- Keep a record of the state of the device and potentially relevant information in the immediate vicinity
- Choose and apply the appropriate power off method for the device
- Photograph and label the components of the device making specific reference to ancillary leads and connections to the device
- Appropriately package, seal and label the device in accordance with current procedures
- Capture and preserve electronic evidence in accordance with legal and organizational requirements
- Document the electronic evidence capture so that all actions can be reproduced by a competent third party
- Create a product of the data sources to a suitable medium
- Introduction of Analysis & Discovery (Scope of Investigation & Forensic software tools)
- Introduction of Documentation (Comprehensive notes & journals)
- Introduction of Verification (Hashing)
- Introduction of Presentation (Investigators & Court)

Cyber Crime Investigators

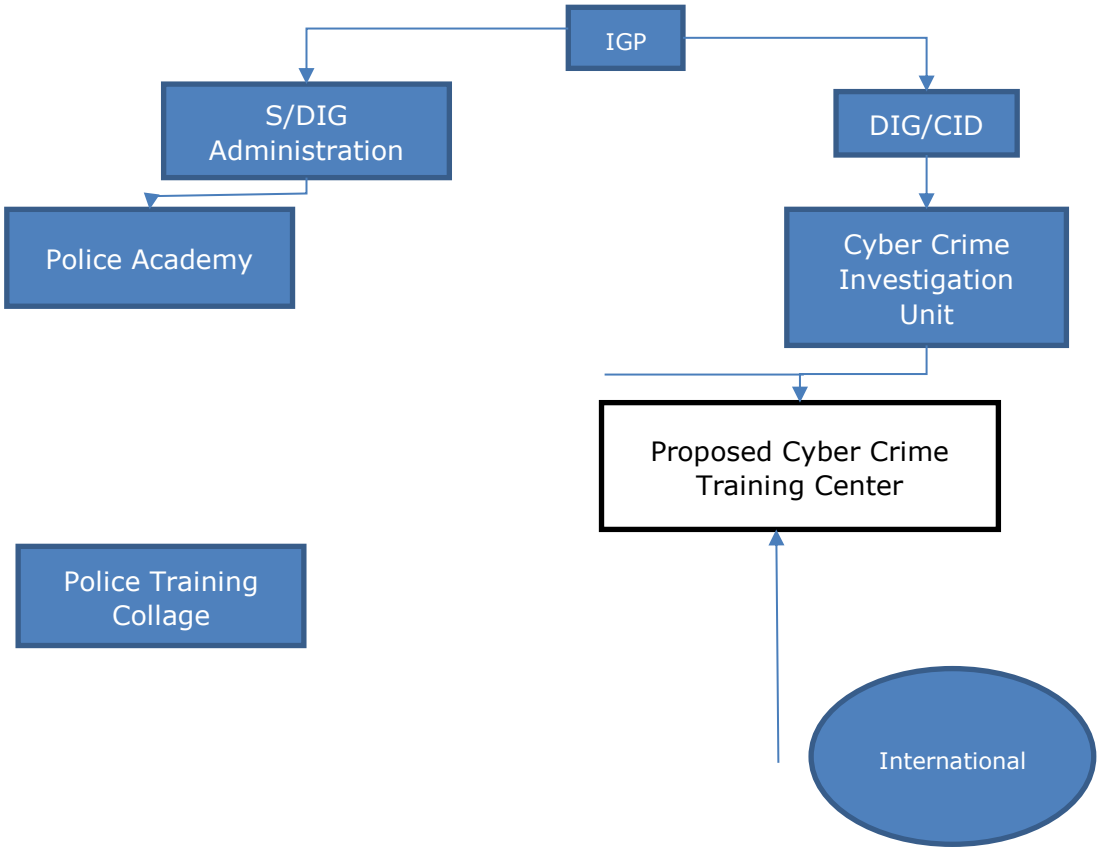
- Presentation (Investigators & Court)
- Sri Lankan Laws related to computer crime investigation
    - No.36 of 2003 Inter-lectual Property Act
    - No: 19 of 2006 Electronic Transaction Act
    - No: 30 of 2006 Payment Device Act
    - No: 24 of 2007 Computer Crime Act
- Tools for Investigation
- Modus operandi of cyber crimes
- Internet architecture Internet Investigations
    - DDoS,
    - Phishing,
    - Bot Nets
    - Malware Analysis
    - Social Networks issues
    - Etc…
- Cyber Surveillance & Techniques
- Network Investigations
- Payment Device fraud Investigation

Digital forensic Examiners
Analysis & Discovery, Documentation, Verification

- Sri Lankan Laws related to computer crime investigation
    - No.36 of 2003 Inter-lectual Property Act
    - No: 19 of 2006 Electronic Transaction Act
    - No: 30 of 2006 Payment Device Act
    - No: 24 of 2007 Computer Crime Act

- Tools for Forensics Examination
    - Imaging
    - Operating systems
    - File systems
    - Database systems and Data mining
    - Malware Analysis
- Reverse engineering
- Log Analysis
- Mobile forensics

4.10.4 Training capabilities and resources



Academia

1. University of Moratuwa
2. University of Colombo
3. University of Kelaniya
4. University of Peradeniya

Cert institutions:

1. SLCert
2. TechCert

Private Sector :

1. Microsoft Sri Lanka
2. IBM
3. NIBM
4. SLIIT

Other:

1. CCSL

1. Trainers- training for proposed cybercrime training center

- Experts from Local Universities (part time)
- Experts from Industry
- Experts from International
- Experts from Investigators
- Experts from Examiners
- Experts from Government entities (AG's Department, Government Analysts)

2. Police Academy and Higher training (Police officers who are working presently)

- cybercrime training center staff
- Experts from Local Universities (part time)
- Experts from Industry
- Experts from International
- Experts from Government entities (AG's Department, Government Analysts)

3. Police Training College (Recruit Police officers)

- cybercrime training center staff
- Experts from Local Universities (part time)
- Experts from Industry
- Experts from International

What resources are available to implement the strategy?

1. Available resource personnel's

- trainees from Cyber-crime unit and IT Division
- Experts from Local Universities
- Experts from Industry
- Experts from International
- Experts from Investigators
- Experts from Examiners
- Experts from Government entities (AG's Department, Government Analysts)

2. Available equipment's

- Computers
- Open source Software tools
- Interior items
- Location (IT Training center premises at Colombo 05)

Identify the requirements for a cybercrime training center;

- Forensic investigation server
- Write blockers
- Working bench
- Digital camera and the cam code
- Portable forensics toolbox
- Portable storage devices
- SATA HDD, IDE HDD, ……..etc
- Learning management systems
- Audio, video, mobile forensic tools
- Forensic Workstation (eg: FRED)

Logistical requirements.

- Local Area Network & furniture for the requirement
- Door access with a locking mechanism
- Evidence container, such as a safe or heavy-duty file cabinet with a quality padlock

- The lab server
- A number of digital forensics workstations.
- A number of workbenches.
- Conference table with chairs.
- Shelves for the lab internal library
- Communications options: LAN with access to the Internet

Also consider how industry and academia resources may be utilized in support of the strategy.

Also consider which training may be delivered at regional as well as national level and in which languages.
English – Notes and materials
Tamil and Sinhala - Explanations

Please also consider issues of certification and academic accreditation.

Stage 01: this will be benefitted police officers
- Certificate Couse fulltime 01 week
- Diploma
- Higher Diploma

Stage 02: those who successfully perform stage 01.3 would be able to follow stage 02.1 / Direct enrollment from University Grant Commission list/
- Degree
- Postgraduate Diploma
- Master's Degree

4.10.5 Other considerations

Support to the e-Sri Lanka national strategy plan. Please refer http://www.icta.lk/e-sri-lanka.html Training sessions to be organized especially to update the knowledge on technology, getting International Assistance like council of Europe, Also Sharing of experience is mandatory. Having an equipped cybercrime training centre is essential requirement to fulfil the training strategy.

4.11 Ukraine

4.11.1 Justification for training strategy

Cybercrime is ranked as one of the top five types of economic crime in Ukraine. Ukraine has seen a rising trend of cybercrimes and crimes committed by means of using high technologies. As of December 2014 more than 50% of Ukraine's population older that 16 years is using computers and Internet on a daily basis and number of internet users increased rapidly. Ukraine facing Increasing amount of retailing done using online websites, electronic payment, and then delivered via a courier or via other services. As result number of discovered and reported cyber crimes would is double every 4 months.

One of the aspects of using as a secure method of communications among the members of organized crime groups and terrorists is posing a major threat to national security. In addition, practice shows that at this point there are only but few organized criminal groups or individuals who do not heavily rely on using various types of IT in order to provide communication undetectable by security forces, or use modern technologies to conceal or change valuable evidence.

By looking at the overall situation in this field and especially at the permanently increasing trends in the activities of cyber criminals, it is clear that creating National Law Enforcement Training Strategy is of extreme importance for the future work of Ukrainian MoI. The IT is globally and extensively abused by the criminal community to commit certain forms of traditional crime such as fraud, extortion, blackmail, forgery and money laundering.

The nature of modern crime in general is that it becomes more IT-related, and educated experts who understand how criminals use technology for their own benefit will most certainly be a valuable contribution to any police unit in Ukraine and not just the ones involved in combating cybercrime directly.

Taking into account the above-mentioned reasons, creating this National strategy was a logical and necessary decision for the Ukrainian MoI which for a long time now has been faced up with a boom of cybercrime and cyber related offences (as it is the case with almost every other country in the world).

The final goal of the training strategy for Ukraine should be to establish a functional and sustainable education system, which at the end would produce LEA officers with appropriate knowledge at different levels.

4.11.2 Objectives of the training strategy

By analyzing the existing practices of the universities in the USA and EU member countries and comparing them with the respective situation in Ukraine, the following training groups and topics can be identified:

Cybercrime investigations

- Introductory IT forensics & network investigations
- Internet investigations
- Undercover on-line operations
- Network investigations
- Linux & MAC OS
- Linux as an investigative tool - basic
- Wireless LAN & VoIP
- Databases & data mining
- Basics of scripting

Computer forensic specialists

- Introductory IT forensics & network investigations
- Basic mobile devices forensics
- Intermediate and advanced mobile devices forensics

- Live data forensics
- Cloud forensics
- Malware forensics
- Applied NTFS forensics
- Network forensics
- TOR forensics
- Linux as a forensic tool – basic
- Linux as a forensic tool – advanced
- Commercial forensic solutions (EnCase, FTK)
- EnCase scripting
- Pearl and bash scripting
- Open source forensic solutions
- Encryption and decryption

Network security specialist and incident investigations

- Introductory IT forensics & network investigations
- Internet investigations
- Network investigations
- Linux & MAC OS (basic and intermediate course)
- Linux as an investigative tool (basic and advanced)
- Wireless LAN & VoIP
- TOR as an investigators tool
- Databases & data mining
- Advanced networks
- Advanced malware analysis
- Advanced hacking & network intrusions
- Linux for specialists
- Forensic scripting using BASH
- Chip-off and Jtag
- Live network investigations

Economic crimes investigator

- Credit card frauds, phishing, Nigerian scams, bank account hijacking
- Financial investigations (cyber laundering, digital wallets – BTC, LTC as alternative currencies),

Child pornography investigator

- Peer-to-peer data exchange
- DarkNet and TOR parallel Internet
- Underground pedophile forums and infiltration
- Nordic Mule

4.11.3 Training requirements (needs analysis)

All policemen and especially first responders should be able to:

- Check that the necessary authorizations are in place
- Identify legal framework necessary for all their activities in this field
- Conduct preparatory research concerning the capabilities of the subject of the investigation
- Identify and select the appropriate tools and consider multiple options to meet the needs of capture or seizure of evidence
- Recognize devices capable of storing electronic evidence and determine whether they require capturing or seizing
- Identify any health and safety risks associated with the electronic devices
- Consider the volatility of data and its preservation
- Identify external connections to and from devices

- Isolate the scene and secure the electronic evidence sources to prevent contamination and external interference
- Determine whether to capture electronic data or to seize electronic devices
- Keep a record of the state of the device and potentially relevant information in the immediate vicinity
- Take appropriate action to safeguard the device and relevant information for the application of physical forensic examinations
- Preview the contents of the device in a forensically sound manner
- Choose and apply the appropriate power off method for the device
- Photograph and label the components of the device making specific reference to ancillary leads and connections to the device
- Appropriately package, seal and label the device in accordance with current procedures
- Conduct a preliminary risk assessment of the requirements for the evidentially sound and safe capture of electronic evidence
- Ensure the preservation of third party and volatile data sources
- Capture and preserve electronic evidence in accordance with legal and organizational requirements
- Document the electronic evidence capture throughout the process so that all actions can be reproduced by a competent third party
- Create an evidential product of the data sources to a suitable medium
- Keep accurate records of procedures using appropriate documentation.

These are the most important aspects that every modern police officer should know, and they basically cover most of the first responder training needs. It should be emphasized that whether the trainees will become officers in cybercrime units or investigate traffic violations, there will always be a certain aspect of cyber education that they will require in order to be able to make a fully valid report. It is crucial to stress the fact that all students in every MoI educational institution should receive this or similar education.

The detectives, inspector dealing with cybercrimes and Internet crime investigators and has very similar requirements built on the core skills outlined above. In particular, it is necessary for the investigators to have a certain level of knowledge about the Internet, activities that may be conducted by criminals using the Internet and how the investigators may use the technology to assist in their investigations.

- Summarize the history of the Internet and describe the functions of routers, hubs and switches
- Understand and differentiate between types of IP addresses
- Describe the function and operation of Internet utilities such as WWW, Email, Social Networking, Newsgroups, Chat and Instant Messaging
- Resolve and describe how domain names are allocated
- Interpret web server logs and HTML code of web pages
- Locate and interpret e-mail headers and summarize anonymous services
- Carry out online investigations in line with national legislation and human rights considerations
- Identify online services available to assist investigations
- Acquire different types of online information meeting evidential standards
- Evaluate online information to establish reliability
- Summarize elements of Internet crime and discuss case studies.

Detectives and inspectors of the Operative-Technical department and Computer Intelligence units is the one requiring the same knowledge as the above-mentioned group but with a much greater level of detail in relation to the covert nature of such work. These investigators will require a high level of understanding of legal and procedural aspects of the investigation as well as technical considerations. The trained individuals should be competent to perform the following list of tasks:

- Identify the function of the Internet and its applications
- Describe the evidential requirements and admissibility of evidence during online activity
- Describe the methodology for evidence capture and corroborations

- Identify equipment and software required for effective online undercover investigations
- Describe best practice in legend building and field craft
- Identify the legal issues pertinent to undercover online investigations
- Describe the communications methodologies used
- Prepare written statements for legal proceedings
- Identify the challenges and risks faced by online undercover investigators.

Training in this subject is normally broken down into the following categories:

Theory and Good Practice - covers the basic requirements for establishing a covert online capability, including:

- Introduction to the Internet and its applications
- Covert Internet operations
- Codes of conduct
- Hardware acquisition and use
- Operating systems acquisition and use
- Software acquisition and use
- Evidence capture and corroboration methodology
- Cover story building and fieldwork
- Risk assessment and authorities
- Matching equipment to the cover story
- Online payment methods
- Agent provocateur and legal issues – Ukrainian legislation analysis
- Open source capabilities – opportunities and risks.

Communications - examines specific issues of interest to undercover roles in respect of the following:

- Web browsing
- E-mail
- Newsgroups
- ICQ and instant messenger
- IRC and Web chat
- Social networking sites
- Encryption
- Crossover communications.

File Sharing - includes application reviews, traceability, dangers and specific issues relating to:

- File transfer protocol
- Peer to peer
- Internet relay chat
- Social network sites
- Bit torrent sites
- Online storage
- Cyber lockers
- Online auctions

Internet interception and network security specialists require different skill sets depending on the type of crime being investigated. In general they should know and understand:

- Current relevant legislation, policies, procedures, codes of practice and guidelines for conducting network investigations
- Web site structures and protocols
- Web applications, coding and vulnerability
- Fixed and wireless network and communication protocols, topology and devices, network based attack and vulnerability methods, security methods and procedures and interception methods

- Voice over Internet protocol (VOIP)
- Digital encryption, public key infrastructure (PKI) and virtual private network (VPN)
- Malware and hacking investigative skills
- Systems running encryption
- Use of operating systems (e.g. UNIX, LINUX, Windows Server)
- Non-standard operating systems
- Obtaining evidence, information and intelligence for a network investigation
- Sources of relevant evidence, information and intelligence
- Assessing available information and intelligence for a network investigation
- Assessing the factors that may impact a network investigation
- Identifying additional support available and required for a network investigation
- Maximizing useful evidence and minimizing loss of potential evidence
- Prevention of cross-contamination of evidence
- Identification and development of initial lines of enquiry
- Identifying and dealing appropriately with suspects
- Volatility of data and how to preserve it
- Types of actions necessary to preserve third party and volatile data sources (e.g. ISP data sources, cached data)
- Initial preservation of evidence against loss
- Conducting investigations at international level
- Electronic evidence capture and preservation techniques
- Determination of the regulatory bodies involved
- Identification of relationship and links between e-crime and other types of criminal activity
- Types of documentation that must be completed
- Purpose of documenting information on investigations.

Digital forensic specialists require a broad set of skills and knowledge and further specialization as they become more proficient. It is expected that such investigators should have a sound technological background. For those able to demonstrate technical proficiency, the following list of tasks should be achievable after completing an introductory training course:

- Check that the necessary authorisations are in place
- Establish the scope of the investigation in consultation with the investigation officer who is requesting the forensics
- Identify and select the correct equipment
- Conduct the investigation in accordance with legal and organisational requirements
- Conduct the investigation using evidentially sound forensic tools and techniques
- Conduct cross tool validation of results
- Conduct the investigation on various software platforms (the trainees should be able to do forensics on all OS's available on the market)
- Perform necessary and proportionate research activities to obtain additional information
- Consult with relevant third parties to obtain information relevant to the investigation
- Create a working product for further investigation
- Review the scope of the investigation throughout the process, based on findings
- Document the investigation so that all actions can be reproduced by a competent third party
- Establish the content and purpose of the report, and identify the audience
- Conduct an impartial evaluation of the significance of the forensic examinations
- Produce an accurate, impartial and complete written report based on the findings
- Provide a clear and accurate oral presentation of the findings
- Keep accurate records of the process using appropriate documentation

4.11.4 Training capabilities and resources

Ukraine has enough trainers to deliver only basic training. Basic training can be performed by the trainers from ministry of internal affair, and with help of Ukrainian Academia experts. When it comes to the intermediate and advanced training human resources in Ukrainian MoI are very

limited. In addition, currently Ukrainian MoI lacks resources to develop such trainings or to deliver them. Trainers, especially good ones, are also a scarce resource in this area. Thus, at the current stage, it might be easier and cheaper to use foreign experts to deliver short trainings with perspective to develop national training programs and train local trainers, including those from MoI educational system. The only persons with sufficient knowledge to deliver cybercrime training are the inspectors from the Division for combating cybercrime, who have their own responsibilities and can only participate in a limited number of activities.

Central body, Division for Combating Cybercrime, could be used as hub for facilitating training. With assistance provided by the OSCE PCU to the Interior Ministry to increase its anti-cybercrime capacities and donation of equipment a Cybercrime training center was established in the Division for combating Cybercrime of the Ministry of Internal Affairs. Cybercrime training center can host training session of almost any level on investigation of cybercrime for up to 20 participants.
Ukraine is covered by network of 17 Police academies and institutes, neither of which has current capacity to deliver cybercrime training on sufficient level, nor trainers able to deliver such training.
Kiev Police Academy can introduce a specialized cybercrime course with all policemen. However, the Academy lacks experts to conduct the trainings as well as methodological materials for the lecturers and handouts for the students. The only expert lecturer currently may be available is the representative of one of the Units from the Division for Combating Cybercrime. The Police Academy is in regular contact with the Division, expressing its wish to develop this direction, particularly via use of any training material available.

To conduct training for future police officers The Faculty for Combating Trafficking in Human Beings and Cybercrime of Kharkiv National University MoI, was formed (in the current legal framework and the existing format[3]) in 2012 as a response to an increasing need for skilled digital investigators.[4] When it comes to the legal framework for the operation of this institution, it is worth mentioning that Kharkiv National University of Ministry of Internal Affairs have received a 10-year license (expiring in 2023) by the Ministry of Education and Science of Ukraine and that their program is valid, accredited and that graduate students are entitled to a widely acknowledged diploma. Besides, all education programs are licensed within the Bologna framework, which means that they can accept international students enrolled in similar programs or send their students to continue their education at compatible universities worldwide.

The mission of the Faculty is to educate future law enforcement officers who will be assigned as investigators in the area of combating human trafficking and the criminal acts in the field of information technologies. In addition, their further role in the system of the Ukrainian MoI would be to assist in in-service training of the current staff employed in the Division for Combating Cybercrime and its regional departments. It should be noted that in spite of the fact that Ukraine is one of the major countries affected by the activities of the cybercrime criminals at the global level, this is the first and only institution in the country that has a program aimed at educating students of the above-mentioned profile.

4.11.5 Other considerations

Ukraine is one of the largest countries in the region, with huge territory and numerous population. Therefore, the effect of a crime originating from such a territory is by default transnational. Although the Ukrainian MoI makes outstanding efforts in fighting against all types of crime, its financial and human resources are very limited. A danger of crime to be exported not only beyond the country but beyond the region is a good reason for assisting local LEA in performing their tasks

[3] Some forms of IT education aimed towards investigating cybercrime offences were also available previously but not with a direct and clear commitment towards investigations in this field.

[4] MoI of Ukraine - Order 1062, November 20, 2012 “On Organization of Personnel Training at Kharkov National University of Internal Affairs”.

in more effective and timely manner. A good step in a right direction would be enabling LEA to have access to the modern technical solutions such as network interceptions, analytical software, trainings and high-end technical equipment. These improvements would also be an enormous asset to all LEA fighting against organized crime and corruption, thus helping local institutions in further professionalization. It is necessary to stress the positive role that international organizations such as the Council of Europe, OSCE, Europol and Interpol can have in this process. The international organizations can help not only by providing funds but also by providing guidelines, advice and expert assistance in numerous fields of policing. Large number of international experts that are available for the Council of Europe, OSCE, Europol and Interpol can also be an asset to the Ukrainian police providing prompt access to the world most experienced trainers. Finally, with the contribution of international organizations identifying local experts with above average potential to be included in train the trainer programs, thus enhancing the capabilities of the Ukrainian MoI to conduct similar trainings independently.

5 CONCLUSIONS AND RECOMMENDATIONS TO THE PROJECT AREAS

5.1 Conclusions

As identified in the situation reports for the GLACY countries and the assessment reports for the Cyber@EAP countries, none of the countries in the project region has developed a documented training strategy for law enforcement officers in the subjects of cybercrime investigation or digital forensics.

Several countries have introduced some elements of cybercrime training within their wider education and training programmes delivered; however these do not appear to be introduced as a result of any specific subject related needs analysis being conducted.

Notable activities among the countries are:

- The Philippines has provided information regarding what is a substantial input on the related subjects within training programmes for the Philippines National Police. This level of input is not provided for staff of the DOJ or NBI.

- Ukraine has developed 2 specific training courses with support from OSCE and international trainers and is creating a dedicated training centre for the subject matters.

- Sri Lanka has engaged with academia in country and is working with the University of Colombo in delivering training to law enforcement.

Most of the training delivered in cybercrime investigation and digital forensics is on an ad hoc basis by international organizations such as OSCE in the EAP region and from US and Australian organisations in some of the GLACY countries. Training on digital forensics is almost exclusively restricted to product vendor training, which deals with how to use the tools provided and is not a foundation to the subject.

There is limited evidence of the involvement of academia and industry in the development or delivery of cybercrime training courses, nor any specific academic or professional qualifications in cybercrime investigation or digital forensics present in the countries of either project; however the draft strategies of several of them, identify the need to engage with in such relationships.

The ad hoc nature of existing training in the region is not sustainable as it provides limited, although welcome benefits. The creation of a structured standards based programme that is not limited to single courses and which may lead to professional or academic qualifications is essential.

The participants in the workshop attended a substantial part of the ECTEG meeting and were introduced to the concept of that organisation as well as the materials it has developed. They had the opportunity take part in ECTEC work groups that sought to establish requirements for future training. All countries have been invited to join the EC3 SPACE, an online forum for discussion that has s specific areas set aside for ECTEG. Countries were also invited to make use of ECTEG materials to develop their programmes, taking advantage of the existing training courses that have been developed in Europe and elsewhere.

It is vital that the organisations responsible for training in each project area are involved in the development of national strategies. It was noticeable at the meeting in Europol, where there were a mix of delegations including those from training schools and investigators; the work they conducted was beneficial, with collaboration between the parties. The work that was conducted in Europol should be taken back to each project area and developed into national strategies that will

be implemented and not just left once created. It is also advised to units responsible for cyber training to share their national strategy document with current and future counterparts for their contribution to strategy document and implementation of strategy.

The final objective of the workshop was met, with the creation of the working group, consisting of the participants in the workshop. The Octopus Community is being used as the platform for continuing contact between the participants and the COE. It is also important to include South Africa and Tonga in this process. The regional working group may be able to assist the national development with exchange of ideas and training materials. Continuation of the working group beyond the current project is essential for success.

5.2 Recommendations

The recommendations that follow are at the national level and should be read in conjunction with the individual project area information that appears above.

- The development at national level of cybercrime training strategies incorporating the requirements of cybercrime investigators, digital forensics examiners and mainstream law enforcement staff relating to their role specific functions. This should include the development of individual training, education and continuous professional development programmes for the specialist cybercrime investigators.

- The creation and adoption of professional and academic qualifications should be considered collaboration with industry and academic partners. There are other organisations that have developed such programmes.

- It is recommended that those training courses, such as existing with the European Cybercrime Training and Education Group (ECTEG) should be investigated for suitability at project area level.

- It should be recognised that at this stage of development, some activities may be more suitable at the regional level while others are essential to be introduced at project area level. As a general guide, those activities with a higher technical component that may lead to the high level academic qualifications needed by a limited number of people in each project area; will be more suited to regional development and delivery at this stage. Those activities aimed at a wider audience, such as first responders, with a lower level of technical content may benefit from initial needs analysis being conducted a the regional level with delivery at project area level, taking into account legal and cultural differences.

- Countries should take up the offer to join both EC SPACE and the Octopus Community in order to continue to collaborate in the subject matters for the duration of both Cyber@EAP and GLACY projects.

- Concerted efforts should be made in each project area to ensure that those responsible for strategic law enforcement matters are acquainted with the threat of cybercrime and the exponential increase in that threat once technology continues to infiltrate the social and business communities. There is an opportunity to work together in the region and avoid the duplication of effort that has been so prevalent in other parts of the world. The regional working group that was created under this project should cooperate during the project phase and remain in existence after the project to work together and avoid duplication of effort.

- Project areas should follow their strategy document with an action plan to reach their goals in efficient manner.

6 ANNEXES

6.1 Annex 1 Agenda of the LEA Training workshop

CyberCrime@EAP
Joint project on cybercrime in the Eastern Partnership region

GLACY
Joint project on Global Action on Cybercrime

Draft version 17 April 2014

Law enforcement training strategies
and
access to training materials

International workshop under the CyberCrime@EAP and GLACY projects
Hosted by the European Cybercrime Centre (EC3) at EUROPOL
The Hague, Netherlands, 12 – 16 May 2014

Outline (draft)

Background

As the use of technology increases on an exponential basis, crimes against the confidentially, integrity and availability of targeted computer systems are more common. Offences committed by means of computer systems, such as fraud, child pornography and intellectual property crimes are increasing rapidly. Moreover, police work involves the recognition and collection of evidence in an electronic form in relation to any offence.

Adoption and implementation of a sustainable and standards based training strategy for law enforcement officers will mean that at all law enforcement officers receive training at the appropriate level to be able to recognise and deal with electronic evidence, to investigate crimes involving technology, and to investigate cybercrime and forensically examine electronic evidence.

In 2011, the Council of Europe, through the CyberCrime@IPA joint project with the EU encouraged countries of South-eastern Europe to develop comprehensive law enforcement training strategies.

Moreover, law enforcement authorities were encouraged to request access to the training materials developed by the European Cybercrime Training and Education Group (ECTEG), the Secretariat of which is hosted by the EC3 at EUROPOL.

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Objective

The aim of the workshop is:

- To prepare elements of domestic law enforcement training strategies for each of the participating countries (see the example of countries in South-eastern Europe). This is to be achieved through workshop sessions with the assistance of international experts.

- To facilitate access to law enforcement training materials developed by ECTEG. Participants will join a meeting of ECTEG that will take place at the EC3 on 12 and 13 May, that is, at the same time.

Participants

The workshop is primarily for representatives of law enforcement training institutions and cybercrime units in management positions and responsible for training. The CyberCrime@EAP and GLACY projects will fund travel and per diem expenses for:

- 1 representative of law enforcement training institutions and 1 representative from specialised cybercrime units from each Eastern Partnership country: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine;
- 1 representative of law enforcement training institutions and 1 representative from specialised cybercrime units from each of the following GLACY priority countries: Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga.

The working languages will be English and parts of the workshop will be assisted by French-speaking experts.

Programme (draft)

Monday, 12 May 2014	
0900hrs	Travel, logistics and orientation
1330hrs	Registration at EUROPOL
1400hrs	Introduction to EUROPOL/EC3
1600hrs	Visit to EC3 facilities
Tuesday, 13 May 2014	
0930hrs	Arrival for ECTEG meeting and registration
1000hrs	Opening and participation in ECTEG meeting - Presentation of GLACY project and country interventions
1145hrs	Presentation by European External Action Service
1300hrs	Lunch break
1400hrs	Training Competency Framework presentation by EC3/Europol
1430hrs	Introduction to law enforcement training strategies
1500hrs	Country presentations on current law enforcement training capacities
Wednesday, 14 May 2014	
0900hrs	Group work on domestic training strategies
1200hrs	Visit to Dutch National High-tech Crime Unit
Thursday, 15 May 2014	
0900hrs	Group work on domestic training strategies
1300hrs	Lunch break

1400hrs	Group work on domestic training strategies
Friday, 16 May 2014	
0900hrs	Presentations on draft strategies
1100hrs	Wrap up: steps to be taken and further support by GLACY and CyberCrime@EAP projects
1130hrs	Closing: Troels Oerting, Head of the European Cybercrime Centre
1200hrs	End of workshop

Location

The workshop will take place at EUROPOL:

Europol
Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

For details on how to reach EUROPOL see https://www.europol.europa.eu/content/contact-us

Contact

At the Council of Europe:

Polixenia Calagi
Project Officer
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania
Tel +40 21 201 78 87
Email Polixenia.CALAGI@coe.int

Lead Council of Europe consultant:

Nigel Jones
Email: nigeljones007@icloud.com

At the EC3 (EUROPOL)

Benoit Godart
Head of Outreach & Support
European Cybercrime Centre (EC3)
EUROPOL
Eisenhowerlaan 73, 2517 KK
The Hague, The Netherlands
Phone: +31 (0) 70 353 1919
benoit.godart@europol.europa.eu

6.2 Annex 2 List of participants

CyberCrime@EAP

Joint project on cybercrime in the
Eastern Partnership region

www.coe.int/cybercrime

Version 08 May 2014

International workshop under the CyberCrime@EAP
The Hague, Netherlands
12-16 May 2014

LIST OF PARTICIPANTS

Country		Surname	First name(s)	Position and institution
ARMENIA	Mrs.	BADALYAN	Anna	Senior Legal Adviser to the Legal Educational Institutions of Armenian Police
ARMENIA	Mrs.	BADALYAN	Ruzanna	Main Department for fight against organized crimes, Department for fight against hi-tech crimes, trafficking, illegal migration and terrorism, Operative (1 division)
AZERBAIJAN	Mr.	HAJIYEV	Hajiaga Azar	Ministry of National Security of Azerbaijan Republic
BELARUS	Mr.	LIAPIOKHIN	Aliaksandr	Academy of the Interior Ministry of the Republic of Belarus
BELARUS	Mr.	SUSHKO	Aleksandr	Investigative Committee of the Republic of Belarus
GEORGIA	Mr.	GADABADZE	Otar	Ministry of Internal Affairs Georgia
GEORGIA	Mr.	TIELIDZE	Giorgi	State Security and Crisis Management Council, Department of Internal Security and Public Order
MOLDOVA	Mr.	CARP	Terentie	Centre for development of projects and cooperation of the Academy "Stefan cel Mare" of Ministry of Internal Affairs, Moldova
MOLDOVA	Mr.	DEGTEARIOV	Artur	Centre for combating cybercrimes, General Police Inspectorate, Republic of Moldova
UKRAINE	Mr.	NOSOV	Vitalii	Cybercrime and Human Trafficking Combating Specialists Training Faculty, Kharkiv National University of Internal Affairs
UKRAINE	Mr.	RYBACHUK	Maksym	Division For Combating Cybercrime, Ministry of Internal Affairs of Ukraine
TURKEY	Mr.	SEN	Bilal	Expert
UNITED KINGDOM	Mr.	JONES	Nigel	Expert

International workshop at EUROPOL under GLACY project
The Hague, Netherlands
12-16 May 2014

LIST OF PARTICIPANTS

Country		Surname	First name(s)	Position and institution
MAURITIUS	Mr.	BALGOBIN	Harshanand Kumar	Police Inspector in charge of the IT Unit
MAURITIUS	Mr.	UMMUR	Bhimsen	Instructor at Police Training School
MORROCCO	Mr.	HEJJOUJI	Marouane	Ingénieur d'état, chef du service de lutte contre la cybercriminalité. Direction de la police judiciaire
MORROCCO	Mr.	TAKI	Abdeljalil	Commissaire Divisionnaire, Direction Général de la Surveillance du Territoire
MORROCCO	Mr.	ALAMI	Salim	General Directorate of National Safety - Judicial Police Direction
PHILIPPINES	Mr.	PONTANAL	Manuel	National Police Commission
PHILIPPINES	Mrs.	ANGELES	Herminia	Department of Justice
SENEGAL	Mr.	GUEYE	Papa	Police Nationale du Senegal
SENEGAL	Mr.	DIOUF	Papa	Gendarmerie Nationale
SRI LANKA	Mr.	SENEVIRATNE	Tharaka	Assistant Superintendent of police, ASP Computer Engineer - IT Division
SRI LANKA	Mr.	SENARATHNA	Sampath	Inspector of Police, OIC Cyber Crime Unit
TONGA	Mr.	VAIPUNA	Siosaia Fatai	Deputy CEO , Public Service Commission
TONGA	Mr.	FAAOA	Unga Afuhaamango	Deputy Commissioner of Police, Ministry of Police, Prisons & Fire Services
	Mrs.	OUASSILA	Belaloui	TRANSLATOR
	Mrs.	OOMS	Ana	TRANSLATOR
	Mrs.	MCKINNON	Geneviève	TRANSLATOR