CyberCrime@IPA

EU/COE Joint Project on Regional Cooperation against Cybercrime

www.coe.int/cybercrime

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Strasbourg, France

Version 26 October 2011

CyberCrime @ IPA

Law Enforcement Training Strategy

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

For further information please contact:

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe
Strasbourg, France

Tel: +33-3-8841-2103
Fax: +33-3-9021-5650
Email: cristina.schulman@coe.int
www.coe.int/cybercrime

Contents

EXECUTIVE SUMMARY

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. Police work involves the recognition and collection of evidence in an electronic form of any offence.

Adoption and implementation of a sustainable and standards based training strategy for law enforcement officers will mean that at all levels they receive the appropriate training to be able to recognise and deal with digital evidence; as well as investigate crimes involving technology and are sufficiently trained to investigate cybercrime and forensically investigate digital evidence.

This report recognises that cybercrime/computer enabled crime/digital evidence impact on each project area in the region in different ways and requires individual strategies to be developed as well as identifying areas where a regional approach 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 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 and also those that are common across the region. 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 recognized, along with the roles that academia and industry may play in the process.

The joint European Union and Council of Europe project (CyberCrime@IPA) provides an opportunity for the development of national and regional 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.

1 BACKGROUND

1.1 The CyberCrime@IPA project

The joint regional project of the European Union and the Council of Europe on cooperation against cybercrime under the Instrument of Pre-Accession (IPA) started on 1 November 2010. Countries and areas participating in CyberCrime@IPA are Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo[1]. The project has a duration of two years and a budget of Euro 2.78 million. The project is implemented by the Council of Europe. It comprises eight expected results.

Expected result 4 is related to law enforcement training strategies: Law enforcement training strategy agreed by Ministries of Interior and implementation initiated

The first activity under this result is to create a regional working group for law enforcement training to prepare a proposal for a law enforcement training strategy. Activity 4.4 refers to centres of excellence for cybercrime training following the 2Centre approach. Furthermore, activity 4.6 is to support the participation of one law enforcement expert from each project area in the distance learning Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by University College Dublin (UCD). These issues were addressed through a study visit to Dublin. The visit took place between 23rd and 27th May 2011, with delegates from each project area and consisted of cybercrime investigators and representatives of national training institutions.

The study visit proposed the following outcomes:

- To create a regional working group for law enforcement training
- To present the work of ECTEG
- To discuss the training materials developed with EU funding and managed by ECTEG and UCD
- To familiarise participants with the Cybercrime Centres of Excellence Network for Training Research and Education (2Centre) project and approach
- To discuss conditions for participating in the MSC programme at UCD
- To prepare a draft proposal for a law enforcement training strategy.

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 area.

1.2 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

[1] All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo.

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.

2 Elements of a law enforcement training strategy

During the study visit, participants discussed the elements that should be part of law enforcement training strategy on cybercrime investigations and computer forensics.

2.1 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

2.2 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

2.3 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.

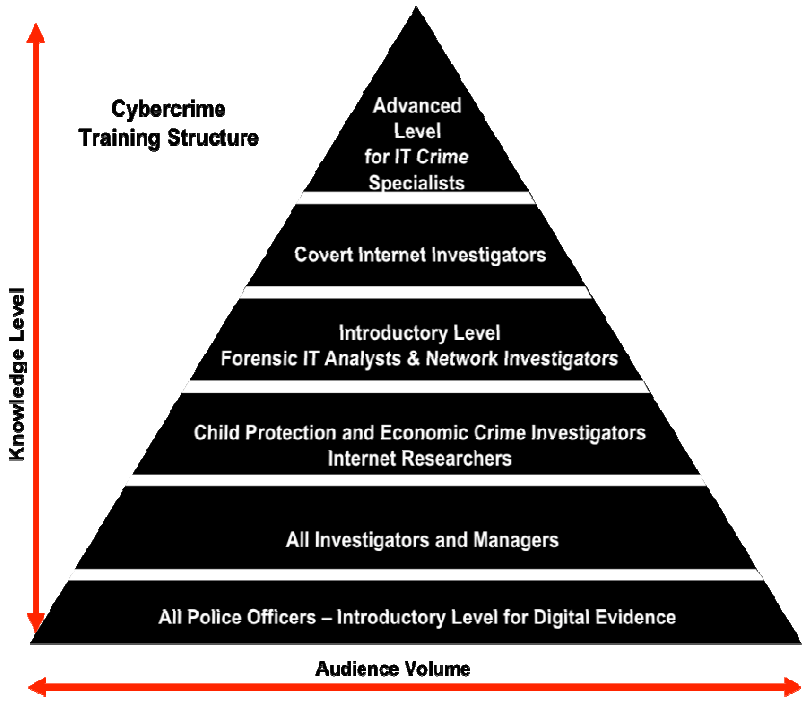
There are no generic names for roles within different organisations, however by describing the functions of the roles identified in this report, it is anticipated that it will be possible to translate the descriptors into local and regional roles.

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
- 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.

2.4 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.

2.5 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.
- 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
- All countries should register an interest in the 2CENTRE project by signing up at www.2centre.eu
- Each project area should consider how it will maximise the benefits derived from the opportunities offered by the inclusion of a place on the MSc programme at UCD as part of this project.

2.6 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 has begun 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 the region.

3 COUNTRY/AREA SPECIFIC STRATEGY OUTLINES

3.1 Albania

3.1.1 Justification for training strategy

Albania has seen a dramatic increase in use of computers, Internet and high technology, both in public and private sector. At the same time, people now have the possibility to access the Internet, through mobile phones, using 3G technology. That means positive developments for Albania, but great opportunity for criminals to undertake their criminal activity through computers and Internet. The new age generation of criminals, are knowledgeable in the use of technology and the possibilities it gives to them, to fulfil their criminal intention. They can easily use Internet communications as a more secure way for them to deal drugs, illegal trafficking etc.

From a variety of sources such as new police structures and latest statistics, it can be shown that cybercrime is a real issue in Albania and is increasing every day. When the forensic digital evidence laboratory began working, there were a maximum of 5 to 10 cases per month. Nowadays this laboratory handles a minimum of 20 to 30 cases per month. This shows that digital evidence is becoming a great tool for a successful investigation.

It can be seen that technology is having more impact on crime than it was before, and will be only increase in the future. Computers systems are also being targets of cyber-attacks, by criminals with the purpose of profit. Increases in the following crimes have been seen:

High tech targeting computers systems, Internet users for:

- Credit card fraud
- Internet fraud
- Computer fraud
- Data Counterfeiting
- Illegal intrusion
- Unauthorised access
- Misuse of electronic devices

High tech as a modus operandi for committing crime:

- Child pornography on Internet
- Money laundering on Internet
- Corruption
- Counterfeiting (money, identity documents etc.)
- Drug smuggling
- Illegal trafficking
- Other crimes

3.1.2 Objectives of the training strategy

The main objective of the Albanian law enforcement training strategy will be to ensure that police officers at all levels have the required knowledge and skills to undertake their roles in the fight against cybercrime and specifically should cover the following aspects:

- Increase of resources for cybercrime trainings

- Development of cybercrime training based on 3 levels (basic, specialised, advanced)
- On-going improvement and updating of training modules
- Provide knowledge and skills for police officers prosecutors and judges to:
- Investigate cybercrime
  - Secure electronic evidence,
  - Carry out computer forensics analyses for criminal proceedings.

3.1.3 Training requirements (needs analysis)

The following categories of learning have been identified for each role described as part of a needs analysis for Albania:

Cybercrime Investigator
- Awareness in Cyber Crimes
- Modus Operandi of Cyber Crimes
- Internet Architecture
- Information Gathering Techniques
- Basic Internet Investigation Techniques
- Command Line Interpreter
- Network Live Investigation Techniques
- IRC, P2P Investigations Techniques
- Server Respond Analyses
- Crime Analyses
- Report Writing
- Computer Forensics For Investigators
- Skimming Investigation Techniques
- Carding Investigation Techniques
- Phishing, Wishing, Smashing Investigation Techniques
- Covert Investigation Techniques
- Wireless Investigation Techniques

Forensic examiners:
- 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 Storages (CD/DVD, HDD, BluRay, Flash, MMC etc.)
- DataBase Basics
- Network Forensics (Silent Runner, Prodiscover network etc)
- Malware analysis
- Steganography
- Live Data Forensics
- EnCase
- FTK
- Xways
- Payment systems (MSR, skimmer, ATM)
- Password Recovery Tools (PRTK, Passware etc.)
- Data Recovery Tools - Software/Hardware (PC3000,DataCompass, HDDoctor, FlashDoctor etc.)
- Mobil Forensics Tools (CelleBrite, Paraben, XRY, Tarantula etc.)

Trainers
- Trainer Development Course
- Training Management

- Internet Investigator Course
- Analyst Course
- Basic Computer Forensics Course
- Awareness in Cyber Crimes
- Modus Operandi of Cyber Crimes
- Internet Architecture
- Basic Internet Investigation Techniques
- His/Her Training Field Topics

Crime investigators

- Modus Operandi of Cyber Crime Types
- Evidence: Integrity and Stability
- Data Storing Capacity Electronic Devices
- Computer Forensics For Investigators
- Information Gathering Techniques

3.1.4 Training capabilities and resources

Albania is in the fortunate position in that it has had a number of trainers already qualified as trainers through the support of the PAMECA III project, which has enabled the development of a "train the trainer course" which trained 23 investigators.

It is anticipated that for the cybercrime training strategy, some of these trainers can be used as trainers to deliver cybercrime trainings, after they have been familiarised with the curricula of the specific trainings. In addition to this, there are 6 police employees trained in Belgrade in the OSCE cybercrime train the trainer course. These trainers may be used as trainers in specific modules. For some specific training, it is expected that trainers from academy and industry may be used.

3.1.5 Other considerations

The Police Training Centre is the only police facility where all training programmes, courses etc. take place. In that Centre there are several buildings that are used for classrooms, dormitories, cafeteria etc. In the main building, there is a computer laboratory that has 20-25 workstations equipped with computers, Internet access and training support tools such as equipment for presentations, flip-charts, smart board etc. The Training Centre can accommodate and feed all participants.

For some specific training that cannot be developed and delivered by police resources, there exists the possibility to cooperate with industry and academy. This can be done, through joint meetings, with the purpose of raising their interest in the fight against cybercrime, and entering formal cooperation agreements.

3.1.6 Implementation of the strategy / next steps

The strategy in Albania should develop to support the necessary training at all levels and consider a regime of assessment for each course. Consideration should be given to engaging with academia to incorporate accreditation and qualifications into the programme for the specialist investigator. Engagement with industry partners may be able to help deliver the more technical levels of training and provide information about technology advances, which will inform the continued development of the strategy. Albania should examine existing resources such as the training material available through ECTEG with a view to incorporating them into a structured training programme. It is important to develop a training strategy that incorporates the requirements of staff at all levels of law enforcement and work towards

incorporating training into existing programmes, where appropriate. For higher-level training that doesn't already exist, this should be developed and delivered in the country and where it is more relevant staff should take advantage of training offered at regional or international level. Albania should seek membership of ECTEG and register as interested parties with 2CENTRE.

Progress should be reviewed during the CyberCrime@IPA project with a report on developments at the final project meeting.

3.2 Bosnia and Herzegovina

3.2.1 Justification for training strategy

Bosnia and Herzegovina has seen a rising trend of criminal activities related to computer systems and data in line with the increased use of the information infrastructure and new technologies in the country. These crimes have serious influence on the citizens of Bosnia and Herzegovina as well as the wider impact on citizens worldwide.

3.2.2 Objectives of the training strategy

According to the internal police organisation and legislation about police officers, and with practical experience in this field, the stakeholders in Bosnia and Herzegovina who require "cybercrime" and digital evidence training have been identified as first responders, cybercrime investigators and child protection investigators for basic training and Police inspectors from the Cybercrime Department (RS Police), Police Directorate (FBiH Police) and Crime Police Unit (Brcko District Police) for advance training.

First responders are identified as: Officers from different police agencies, who are responsible for first response to any type of crime committed in the area of their responsibility.

Cybercrime investigators are described as: officers from different police agencies, who are responsible for: Cybercrime investigations, dealing with crime scenes and securing evidence, search and seizure of digital evidence, interviewing suspects, collection of criminal intelligence from the internet, analytics, presenting cases to judges and prosecutors.

3.2.3 Training requirements (needs analysis)

The levels of knowledge and learning required for each level above, the following requirements have been identified:

First responders: The officers from different police agencies, who are responsible for first response on any type of crime that is committed in the area of their responsibility.

Their responsibility:

1. Responding to the incident,
2. Recognising the area of the crime scene,
3. Isolating the scene and securing electronic evidence sources to prevent contamination and external interference;
4. Securing the crime scene,
5. Not allowing anyone to enter or leave the crime scene,
6. Not interfering with evidence
7. Ensuring the safety of all persons at the scene while protecting the integrity of all evidence—traditional and electronic.

Type of education needed for first responders:

1. Introduction to Computer Forensic
2. Basic Mobile Forensics
3. Search and Seizure
4. Training for understanding the behaviour of high-tech criminals.
5. Social engineering training

Cybercrime investigators and managers: Officers from different police agencies, who are responsible for:

1. Cybercrime investigations,
2. Collecting crime intelligence information on the Internet,
3. Analytics,
4. Presenting the case to prosecutors and judges,
5. Responding to the incident,
6. Recognising the area of the crime scene,
7. Securing the crime scene,
8. Profiles of the types of electronic devices commonly encountered in crime scenes; providing a general description of each type of device, and describing the potential evidence that may be found in each type of device.
9. Search and Seizure of digital evidence
10. Interrogation of suspects.

Type of education needed for cybercrime investigators and managers:

1. Introductory IT Forensic & Network investigations,
2. Core skills in Mobile Phone Forensics,
3. Applied NTFS Forensics,
4. Internet investigations
5. Network investigations,
6. Linux as an Investigative Tool, all parts,
7. Wireless LAN & VoIP
8. Live Data Forensics
9. Forensic Scripting using BASH,
10. Windows7/Vista Forensic,
11. Intermediate Mobile Phone Forensics,
12. Databases & Data Mining,
13. Training for understanding the behaviour of high-tech criminals,
14. Social engineering training
15. Offensive Security training

3.2.4 Training capabilities and resources

Bosnia and Herzegovina has two Police Academies, neither of which has the current capacity to deliver cybercrime training, nor trainers able to deliver such training. The only persons with sufficient knowledge to deliver cybercrime training are the inspectors from the cybercrime department, who have their own responsibilities and can only participate in a limited number of training activities. Bosnia and Herzegovina does not have specialised academia that can deliver such kind of training.

3.2.5 Other considerations

Currently the Ministry of Internal Affairs of the Federation has no certified digital forensic examiners and a limitation in available equipment, and use the private sector for examinations of digital evidence.

3.2.6 Implementation of the strategy / next steps

The strategy in Bosnia and Herzegovina should develop to support the necessary training at all levels and consider a regime of assessment for each course that is incorporated into its training programme. Consideration should be given to engaging with academia to

incorporate accreditation and qualifications into the programme for the specialist investigator. Engagement with industry partners may be able to help deliver the more technical levels of training and provide information about technology advances, which will inform the continued development of the strategy.

Bosnia and Herzegovina should examine existing resources such as the training material available through ECTEG with a view to incorporating them into a structured training programme. It is important to develop a training strategy that incorporates the requirements of staff at all levels of law enforcement and work towards incorporating training into existing programmes, where appropriate.

It is recognised that for higher-level training that doesn't already exist, it may be necessary to rely on a mixture of training that is developed in the country and match this with training offered at regional or international level. Bosnia and Herzegovina should seek membership of ECTEG and register as interested parties with 2CENTRE.

The Federation Ministry of Interior should consider whether it is in its long term interests to bring the digital forensics function in house and to provide the necessary training to staff to allow this to take place. Significant savings an improvement in the capability of staff will be achieved.

Progress should be reviewed during the CyberCrime@IPA project with a report on developments at the final project meeting.

3.3 Croatia

3.3.1 Justification for training strategy

Croatia has some statistical information to demonstrate the increase in cybercrime offences with computer fraud being the highest ranked. Other types of crimes such as credit card fraud, attacks on computer systems, data deletion and other related crimes are also on the increase, along with a strong increase in phishing and identity theft and crimes related to social networks. Another security threat is the growing use of IT as a way of communication that has almost replaced the use of mobile phones in everyday communication between the perpetrators of criminal acts/members of organized groups. Interception of such traffic should also be of relevance for law enforcement and therefore, the proper education in this field should be considered.

The obvious growth of criminal acts related to cybercrime and the growing use of information technology on daily basis, has led the Croatian police and justice system to be more aware of the lack of expertise in the field of cybercrime and the need for basic and specific training in this area.

3.3.2 Objectives of the training strategy

The levels of training identified as appropriate for Croatia are to establish a satisfactory education system, which would give police officers/crime investigators functional knowledge at the following levels:

- Education/training on all levels (basic/specialised) with proper equipment/training materials/resources/trainers
- Investigation of cybercrime
- Collecting/Securing digital evidence,
- Search/Forensic analysis of evidence
- Presentation of the evidence (consistent with the needs of the judicial system)
- Protection of the network infrastructure

It is recognised that the law enforcement training strategy should be compatible and aligned with education programs concerning cybercrime at other institutions such as judges & prosecutor training centres.

3.3.3 Training requirements (needs analysis)

There is no documented training strategy for law enforcement officials in Croatia in the area of cybercrime investigation and digital forensics. However, there are significant aspects of the Police High School education programme, which deals with the subject matters. Croatia has an agreement on cooperation in preventing and resolving computer incidents and other forms of computer crime that the Ministry of Interior has signed with CARNet - Croatian Academic Research Network, since 2010

The Police Academy also has award-granting status, which will allow any cybercrime training programme to be integrated into the existing education system and to ensure that qualifications are available to investigators. The component parts of the Police Academy, namely the High Police School, the Department for Professional Training and Specialisation and the Department for Law Enforcement Training are able to incorporate cybercrime elements into their existing programmes and create new programmes that are required. At this point the Police Academy plays the leading role in ensuring all types of resources are available.

There is currently a project to introduce e-learning into the classes at the Police Academy:

3.3.4 Training capabilities and resources

The aims of the project are to implement new ways of teaching that rely on the ICT technologies, like e-learning to greatly enhance the educational structures in Croatia, so that all forms of specialization and training would be more available and less expensive. A strategic approach to introducing e-learning represents a milestone on the path towards modern, competitive and customer oriented educational institution. This type of transformation will ensure comprehensive monitoring of the needs of certain age and interest groups, with partial retention of the traditional ways of teaching to cater for students who do not have access to new technologies.

The objective of introducing e-learning is to put some teaching modules on line and for this purpose it would be necessary to introduce an electronic library to enable the use of large quantities of material from the teaching unit. This will allow students to actively participate in using it in everyday learning.

3.3.5 Other considerations

Croatia can currently provide enough experts for specialised training in cybercrime on an intermediate level, but for advanced training, will need regional cooperation and help from international experts.

3.3.6 Implementation of the strategy / next steps

Croatia has already implemented aspects of cybercrime training within its existing programmes and has plans to utilise e-learning as a platform for delivering training. It is necessary to develop a training strategy to underpin the current and future activities. The strategy in Croatia should develop to support the necessary training at all levels and consider a regime of assessment for each course. Consideration should be given to engaging with academia to incorporate accreditation and qualifications into the programme for the specialist investigator. Engagement with industry partners may be able to help deliver the more technical levels of training and provide information about technology advances, which will inform the continued development of the strategy. Croatia should examine existing resources such as the training material available through ECTEG with a view to incorporating them into a structured training programme. Within the strategy, it is likely to be that where higher-level training doesn't already exist, this should be developed and delivered in the country and where it is more relevant staff should take advantage of training offered at regional or international level. Croatia should seek membership of ECTEG and register as interested parties with 2CENTRE. The fact that Croatia has already begun the proves of incorporating cybercrime training together with the fact that the police academy has academic status should lead to considering the development of a centre of excellence to support the requirement in Croatia and potentially within the region.

Progress should be reviewed during the CyberCrime@IPA project with a report on developments at the final project meeting.

3.4 Montenegro

3.4.1 Justification for training strategy

Montenegro has seen a significant increase in criminal offences involving technology in the period from 2007 to 2011, based on an analysis of criminal charges and modus operandi. In this period the National police of Montenegro submitted more than 130 criminal charges; these criminal charges include offences of computer crime such as; misuse of credit cards and credit card fraud, abuse of author's rights, unauthorised use of computers and computer networks and etc. In the period from 2004, Internet usage has increased by some 444% from 50,000 to 296,000 users. Criminals are using IT for preparation and execution of most complicated criminal acts related to all forms of crime especially in the area of organised crime and corruption.

3.4.2 Objectives of the training strategy

The objectives of the national strategy for Montenegro are considered to be:

- To ensure that Police officers at all levels have necessary skills to investigate cybercrime, secure and investigate digital evidence.
- Raise awareness of computer crime in Montenegro,
- To provide adequate education for every level of police officers, prosecutors and judges
- To provide security for all users of computer network and similar
- To use preventive measures in computer crime (legislation, standardisation, certifications, institutionalisations and etc.)
- To provide effective prosecution for offenders in computer crime

3.4.3 Training requirements (needs analysis)

The proposed training strategy for Montenegro will:

- Analyse the current situation in order to identify adequate training for police officers,
- Determine number of trainees, level of training (beginners, advance) and the duration of training programmes.
- Determine the equipment for the training such as computers, internet connections, adequate software, whiteboard, smart board etc.
- Determine the facilities in which training will be delivered
- Provide the trainers for each level of courses/seminars
- The courses/seminars up to advance level can be held nationally in mother tongue in above-mentioned institutions. Advanced levels of training will be delivered in English language and on international basis.
- University, industry and non-government trainers will be identified for delivering training which the Law enforcement officers cannot deliver.

3.4.4 Training capabilities and resources

There are trainers within the criminal police department, forensics centre, IT department of the police and the police academy Danilovgrad. The trainers who can provide training up to a certain level have received international education through various projects and have relevant education in the field of information technology and digital forensics.

These trainers will be supported at the higher level by specialist trainers from entities within academia and industry, with whom the national police have excellent cooperation. It is expected that advantage will also be taken of places offered on other international courses.

3.4.5 Other considerations

Through international projects such as CyberCrime@IPA and other similar projects, it is envisaged that law enforcement staff from Montenegro will be provided top-level specialised training for police officers who are in charge of combating digital crime and also for digital forensics investigators.

3.4.6 Implementation of the strategy / next steps

The initial plan for delivering training will be:

- To analyse the current situation and provide appropriate training
- Determine number of trainees, level of training (beginners, advance) and the period of time that is needed for training be delivered.
- Determine the equipment required for the training such as computers, internet connection, adequate software, whiteboard, smart board etc.
- Determine the facilities in which training will be delivered (meeting rooms and classrooms of National Police and Police Academy Danilovgrad)
- Identify and provide the trainers for each level of courses/seminars
- The courses/seminars up to advance level can be held nationally in the mother tongue in the above-mentioned institutions. For upper and advanced level of courses/seminars; these should be delivered in English language and on an international basis.
- Involve universities; industry and non-government agencies for delivering training which the Law enforcement officers cannot deliver.

In order for the above road map to be successful it is necessary that the strategy in Montenegro should develop to support the necessary training at all levels and consider a regime of assessment for each course. Consideration should be given, as suggested in the road map, to engaging with academia to incorporate accreditation and qualifications into the programme for the specialist investigator and with industry partners, who may be able to help deliver the more technical levels of training and provide information about technology advances, which will inform the continued development of the strategy.

Montenegro should examine existing resources such as the training material available through ECTEG with a view to incorporating them into a structured training programme. It is important to develop a training strategy that incorporates the requirements of staff at all levels of law enforcement and work towards incorporating training into existing programmes, where appropriate. For higher-level training that doesn't already exist, this should be developed and delivered in the country and where it is more relevant staff, as identified in the road map, should take advantage of training offered at regional or international level.

Montenegro should seek membership of ECTEG and register as interested parties with 2CENTRE.

Progress should be reviewed during the CyberCrime@IPA project with a report on developments at the final project meeting.

3.5 Serbia

3.5.1 Justification for training strategy

The Republic of Serbia has seen a rising trend of criminal activities in cyber space. At the moment more than 50% of Serbia's population is using computers and Internet on a daily basis and this number is increasing by the day. The authorities have seen a wide range of criminal activity, which have information technologies (IT) either as a target or as a mean to commit other criminal activities. One of the aspects of using IT as a secure method of communications among the members of organised crime groups and terrorists is posing a major threat to national security. Increasing use of various electronic devices is also leading to the seizure of a large number of electronic evidence that could be used as evidence in all types of crimes and subject to a valid forensics process.

In the area of cybercrime Serbia has encountered offences against the security of computer data, crimes against intellectual property rights, crimes against property, electronic business and legal transactions, cybercrime money laundering, illegal gambling, criminal acts against freedom and human and civil rights, xenophobia, sexual freedom, child pornography, public peace and constitutional order and security of the Republic of Serbia.

3.5.2 Objectives of the training strategy

The goal of the training strategy for Serbia should be to establish a functional and sustainable education system, which as goal would produce LEA officers with appropriate knowledge at different levels. The key objectives are identified as:

- Building a training infrastructure
- Providing enough human and material resources for constant education
- Developing basic training material for all LEA officers
- Developing advanced training modules
- Securing electronic evidence,
- Carrying out computer forensics analyses
- Investigating cybercrime
- Giving support and advice to other Government Agencies
- Presenting evidence to the court
- Adopting necessary skills to Intercept Internet communications, contribute to network security and protect critical infrastructure

Considerations in adopting the strategy are: sustainability, standardisation, certification, institutionalisation, permanent budgeting, efficiency, scalability, connecting and synchronising with other government agencies, support from the private sector, improving technical level of knowledge for the prosecutors and judges.

3.5.3 Training requirements (needs analysis)

The following groups and subjects to be taught have been identified as the target audience for training:

- First Responder (this is a basic level of education which should be delivered to every law enforcement officer in Serbia)
  - Securing the crime scene
  - Demystifying Computer Hardware
  - 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, labelling, packing and transport)
- Types and MO of cybercrime and cyber related offences

– Cyber Crime Investigator
  - Introductory IT forensics & Network Investigations
  - Internet Investigations
  - Network Investigations
  - Linux & MAC OS (basic and intermediate course) (at the time this is not developed by E.C.T.E.G)
  - Linux as an Investigative tool – part one
  - Wireless LAN & VoIP
  - Databases & Data mining

– Computer Forensic Examiner
  - Introductory IT forensics & Network Investigations
  - Core skills in Mobile phone forensics
  - Applied NTFS Forensics
  - Network forensics (at the time this is not developed by E.C.T.E.G)
  - Linux as an Investigative tool – part one
  - Linux as an Investigative tool – part two

– Internet interception and network security specialists
  - Introductory IT forensics & Network Investigations
  - Internet Investigations
  - Network Investigations
  - Linux & MAC OS (basic and intermediate course) (at the time this is not developed by E.C.T.E.G)
  - Linux as an Investigative tool – part one
  - Wireless LAN & VoIP
  - Databases & Data mining
  - Linux as an Investigative tool – part two
  - Advanced Networks (at the time this is not developed by E.C.T.E.G)
  - Advanced Malware Analysis
  - Advanced Hacking & Network Intrusions (at the time this is not developed by E.C.T.E.G)
  - Linux for Specialists (at the time this is not developed by E.C.T.E.G)
  - Forensic Scripting using BASH
  - The legal framework needed to perform actions at all levels is already included in a regular curriculum for every law enforcement officer in Serbia.

– Economic Crime Investigators
– Child Pornography Investigators
  - Child pornography and Economic Crime Investigators should have the same training as the cybercrime investigators; however a set of specialised training activities should be identified for both categories. A number of training activities are available on these topics through international organisations and private sector.

– Senior Police Managers
  - A short training activity on cybercrime trends should be delivered at least once a year

3.5.4 Training capabilities and resources

The Republic of Serbia has enough trainers to deliver all training up to an intermediate level. This training can be performed by the trainers from the Ministry of the interior, and with a

help of Serbian private sector experts. When it comes to the advanced level of trainings, help of international experts will be needed. In relation to this, establishing a regional Centre of Excellence could be one solution to overcome the problem with developing and delivering advanced material. Regional cooperation in general will be a necessity when it comes to more advanced training. Serbia does not have enough training candidates to organized advanced training, therefore joining forces in the development and delivery of advanced training should be a requirement.

3.5.5 Other considerations

Serbia has a strong history of organising regional cybercrime training events and a clear plan for developing and implementing a training strategy. It is one of the countries that could provide an appropriate venue for a regional centre of excellence.

3.5.6 Implementation of the strategy / next steps

The implementation phase of the cybercrime training strategy has been identified as having a number of component activities as follows:

Activity 1: Developing effective training programs oriented to specific target groups (basic police training, investigators, specialist and top management);
Owners: Directorate for Police Education, Department for High-tech Crime and Academy of Criminalistic and Police Studies

Activity 2: Innovation of curricula of Academy of Criminalistic Police Studies on undergraduate and postgraduate studies and the creation and accreditation of new degree programs at the undergraduate and postgraduate level (Information technology in criminalistics) and specialist studies (Forensics of digital data);
Owners: Academy of Criminalistic and Police Studies and Department for High-tech Crime.

Activity 3: Developing the capacity to deliver regional and international training in the field of countering high-tech crime.
Owners: Department for High-tech Crime and Academy of Criminalistic and Police Studies and other institution (specialized colleges, private sector).

Activity 4: Establishing a Centre of Excellence
Owners: Ministry of Internal Affairs, Academy of Criminalistic and Police Studies, Department for High-tech Crime, Ministry of Education and Science and foreign partners (ECTEG, 2CENTRE etc.).

It is important to remember that for the above activity list to be successfully achieved, it is necessary that the strategy in Serbia should be developed to support the necessary training at all levels and consider a regime of assessment for each course. Consideration should be given, to engaging with academia to incorporate accreditation and qualifications into the programme for the specialist investigator and with industry partners, who may be able to help deliver the more technical levels of training and provide information about technology advances, which will inform the continued development of the strategy.

Serbia should examine existing resources such as the training material available through ECTEG with a view to incorporating them into a structured training programme. It is important to develop a training strategy that incorporates the requirements of staff at all levels of law enforcement and work towards incorporating training into existing programmes, where appropriate.

Serbia has identified that the development of a centre of excellence is a key aspect of their activities. They have a strong history of delivering regional training, so are well placed to create a regional centre of excellence that may provide more advanced training in the region.

Serbia should seek membership of ECTEG and register as interested parties with 2CENTRE in order to pursue the discussions and potential collaboration with others in terms of developing a centre of excellence.

Progress should be reviewed during the CyberCrime@IPA project with a report on developments at the final project meeting.

3.6 "The Former Yugoslav Republic of Macedonia"

4.6.1 Justification for training strategy

The development and use of technology has serious impact on the crime in Republic of Macedonia. It has caused many complications, not only in the crime committed by using technical equipment but also in the manner of obtaining digital evidence and information for all types of conventional crime and organized crime. The impact of technology has been identified almost in all types of crime. Digital evidence is becoming more and more useful in the investigation process of all types of crime. The most impacted crime areas by technology beside computer crime are child protection, economic crime and in a small dimension the other conventional types of crime.

3.6.2 Objectives of the training strategy

The training strategy objectives have been identified as:

- Improving the awareness of Cybercrime.
- Improving the awareness has the purpose to of giving basic knowledge to all police officers for recognising cybercrime and digital evidence. This is planned to be achieved by incorporating the topics into the training of all police officers.
- Delivering basic cybercrime training in the framework of basic police education
- Integrating basic cybercrime training into basic police training will contribute to building more capacity for recognizing cybercrime. It will also help identify police officers that have more technical knowledge and have competencies to be a cybercrime investigator.
- Developing and deploying the resources for investigate cybercrime
- Planning and performing cybercrime training on the basic, intermediate and advance level.
- Developing the capacity for securing and dealing with digital evidence
- Developing the training capability in Republic of Macedonia for cybercrime investigation.
- Improving the national capacity for training that means trainers that are able to deliver a high level of training and are able to prepare the new training materials together with the representatives from private sector and academia.
- Preparing the high-level trainers and training in cooperation with international organisations, national industry and the National Technical University.
- Developing the capacity to create a national centre of excellence for cybercrime.
- Improve the relations and cooperation with the private sector and academia with law enforcement.

3.6.3 Training requirements (needs analysis)

The levels of individual that require training have been identified as the following:

- Police officer – for whom there is no need for special training, only the very basic introductory presentation (periodically).
- Inspectors of the local level - First responders, They have the responsibility of receiving the initial information of the criminal acts, recognising the type of criminal act, gathering relevant information and opening the case and processing the case to the competent department.
  - Basic knowledge of types, terms and criminal methods of Computer Crime
  - Knowledge of type of criminal offences related with cybercrime covered in the National Criminal Code;
  - To understand Modus Operandi: according to criminal activity to recognise type of criminal offences;
  - To know basic technical characteristic of computers and computer parts;
  - To have basic knowledge of operating system and use of the computer;
  - To recognize devices capable of storing electronic evidence;
  - Practical training relating to securing and seizing of computer equipment
- Investigators from the Regional sectors who deal with less complex investigations and give assistance to first responders. These Inspectors deal with the cases that are more in the national competences.
  - Same skills with first responders plus the following additional skills:
  - Practical training for usage of basic tools for computer crimes investigations
  - To know how to use basic commands in the command line, to be able to discover IP and MAC address on local computer;
  - To know to use tools for internet investigation, to be able to find the user of a specific IP address, country of origin and internet provider;
  - To know the function of email services and to be able to read email headers and find the IP address of sender with exact time and time zone.
- Specialist investigators, Investigators from the cybercrime department and computer forensics department.
  - Same skills as the above two categories and:
  - Advanced computer technical training
  - Functionality of hardware and software (Windows and Linux), the methods of storing data, processes of computers, locating and reading of computer logs;
  - Functionality of computer systems (network, network devices, LAN and WIFI).
  - Advanced training for Internet and Network investigation
  - Advanced techniques and tools for internet and network investigations;
  - Advanced training for computer viruses and malware
  - To know what is a computer virus and malware;
  - To know how to find them and identified type of virus and malware, to discover effect on computer and computer systems;
  - Live data forensic training
  - To know to collect evidence from live computers and computer systems;
  - Advanced training for computer forensic
  - Mobile phone forensic (XRay,XAct);
  - Computer Forensic (Encase, XWays, FTK);
  - Forensic using Linux tool (Bash scripting, Backtrack)
  - Training for making final report for computer crime investigations and forensic analyses to present them in front the Court.

3.6.4 Training capabilities and resources

According to the level of training required, the following level of delivery will be applied:

- For first responder level, the Ministry of the Interior training centre will provide the training with support from the Cyber Crime Unit (CCU) representatives
- For intermediate level, the training will be provided by the experts from the CCU and the computer forensic unit with support from trainers from the training centre
- The advance level training will be delivering different experts, at the national level (PhD Professors from the technical university) or experts from international organisations and police services.

3.6.5 Other considerations

Macedonia is in a somewhat fortunate situation in that it is currently undertaking a review of all training and has the opportunity to incorporate cybercrime training within this review and to provide the training opportunities that have been identified.

3.6.6 Implementation of the strategy / next steps

Macedonia should take advantage of the fact that it is currently conducting a review of law enforcement training to develop the underpinning cybercrime training strategy that will support the necessary training at all levels and consider a regime of assessment for each course. Consideration should be given, to engaging with academia to incorporate accreditation and qualifications into the programme for the specialist investigator and with industry partners, who may be able to help deliver the more technical levels of training and provide information about technology advances, which will inform the continued development of the strategy.

Macedonia should consider to what extent they are able to incorporate existing resources such as the training material available through ECTEG into a structured training programme. It is important to develop a training strategy that incorporates the requirements of staff at all levels of law enforcement and work towards incorporating training into existing programmes, where appropriate.

Macedonia is already a member of ECTEG and should register as interested parties with 2CENTRE in order to pursue the discussions and potential collaboration with others in terms of developing a centre of excellence.

It is important that the report on progress made by the country in the incorporation of cybercrime into its new overall training strategy, and final progress should be reviewed during the CyberCrime@IPA project with a report on developments at the final project meeting.

3.7 Turkey

3.7.1 Justification for training strategy

Technology related crime is affecting many fields of life in Turkey. Money is becoming digital data in the daily life of citizens and institutions. Government, industry and citizens use money transactions via electronic channels. The difference between imports and exports of Turkey in 2010 is approximately 70 billion US dollars. Turkey is expecting to cover majority of this gap with through tourism incomes from the tourism industry. Tourism expenses are being paid mainly by credit card. It is known that many credit card fraud gangs are targeting tourists being easier targets. Therefore, Turkey should invest enough to combat credit card fraud to ensure confidence in tourism and economic stability.

Turkey has 35 million Internet users and 114 million credit and debit cards according to 2010 data. E-commerce is increasing exponentially in recent years.

Cybercrime is causing severe damage to the digital economic world, affecting the economy, education, politics, business, information and the digital divide, communication, privacy, transportation, justice, security, national security and defence as well as the lives of citizens in Turkey.

There are two primary ways envisaged to decrease the risks; firstly, prevention and secondly, proactive investigations. A further issue for Turkey is the increase in mobile Internet connections. According to recent statistics, this is likely to reach 63%. This will make it more difficult and more technical to investigate IP related crimes.

There is no doubt that only officials who are specially and technically trained can investigate cybercrime. There are many sub fields and expert profiles that need to receive specific training. As it is well known training requires time, money and continued efforts. There is strong need to distribute training at proper levels to proper fields of experts.

3.7.2 Objectives of the training strategy

The aim and objectives of the training strategy should be as follows;

- The overall aim is to make all Turkish law enforcement officers aware of cybercrimes and stage by stage provide the required level of training for different levels of expertise, for cybercrime unit officials and the other stakeholders.

In particular, attention must be paid to help them to appreciate the cybercrime phenomena, deliver standardised and sustainable training, deliver the correct training for the different levels of individual or groups of individuals, help create different expertise related to computer related cases, increase the capability to conduct cybercrime investigations, prevent or decrease cybercrimes, and to support and advise other investigative units and other governmental bodies.

Turkey has two police services that have similar but different requirements based upon their structure and responsibilities.

3.7.3 Training requirements (needs analysis)

The stakeholders and their learning requirements identified as relevant to the Turkish National Police are:

- First responders
  - Legal codes CMK134, Arama ve El Koyma Yönetmeliği
  - Types of court orders
  - Modus operandi of cyber crime types
  - Evidence: integrity and stability
  - Data storage capacity of electronic devices
  - Computer and systems basics
  - Live system analysis tools
  - Data imaging tools (Hardware and Software)
  - Requirements of evidence storage devices
  - Anti-forensics techniques
  - Investigation description and preparation
  - Security of crime scene
  - Crime scene interviews
  - Running systems response techniques
  - Static computer system response techniques
  - Rechargeable mobile device Response
  - Labelling, packaging and Transport

- Cybercrimes investigators
  - Legal codes CMK 134, TCK 142/2-e, !58/1-f, 243, 244, 245 Arama ve El Koyma Yönetmeliği
  - Awareness in cyber crimes
  - Modus operandi of cyber crimes
  - Internet architecture
  - Information gathering techniques
  - Basic Internet investigation techniques
  - Command line interpreter
  - Network live investigation techniques
  - IRC, P2P investigations techniques
  - Server response analysis
  - Crime analysis
  - Report writing
  - Computer forensics for investigators
  - Skimming investigation techniques
  - Carding investigation techniques
  - Phishing, Vishing, Smishing investigation techniques
  - Covert investigation techniques
  - Wireless investigation techniques

- Computer forensics examiners
  - 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 (Silent Runner, Prodiscover network etc)
  - Malware analysis
  - Steganography
  - Live data forensics
  - EnCase
  - FTK
  - Xways

- Data Recovery Tools - Software/Hardware (PC3000,DataCompass, HDDoctor, FlashDoctor etc.)

– Decrypters
  - 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 (Silent Runner, Prodiscover network etc)
  - Malware analysis
  - Steganography
  - Live data forensics
  - Password Recovery Tools (PRTK, Passware etc.)

– Mobile examiners
  - 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 (Silent Runner, Prodiscover network etc)
  - Malware analysis
  - Mobile Forensics Tools (CelleBrite, Paraben, XRY, Tarantula etc.)

– Data carvers
  - 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 (Silent Runner, Prodiscover network etc)
  - Malware analysis
  - EnCase
  - FTK
  - Xways
  - Payment systems (MSR, skimmer, ATM)
  - Password Recovery Tools (PRTK, Passware etc.)
  - Data Recovery Tools - Software/Hardware (PC3000,DataCompass, HDDoctor, FlashDoctor etc.)

– Analysts
  - Awareness in cyber crimes
  - Modus operandi of cyber crimes
  - Internet architecture
  - Basic Internet investigation techniques
  - Computer forensics for investigators
  - Crime analysis 4 x 4
  - Information gathering techniques
  - Database programming
  - Crime analysis tools
  - Visualization of analysis reports

- Cybercrimes trainers
  - Trainer development course
  - Training management
  - Internet investigator course
  - Analyst course
  - Basic computer forensics course
  - Awareness in cyber crimes
  - Modus operandi of cyber crimes
  - Internet architecture
  - Basic Internet investigation techniques
  - Training field topics

- Senior staff
  - Legal Codes
  - CMK 134, TCK 142/2-e, !58/1-f, 243, 244, 245
  - Arama ve El Koyma Yönetmeliği
  - Modus Operandi of Cyber Crime Types
  - Evidence: Integrity and Stability
  - Data Storing Capacity Electronic Devices
  - Computer Forensics For Investigators
  - Cyber Crime Personnel Management
  - Awareness in Cyber Crimes
  - Modus Operandi of Cyber Crimes
  - Internet Architecture
  - Basic Internet Investigation Techniques

- Very senior managers
  - Cyber Crime Trends
  - Cyber Crimes Modus Operandi Examples
  - Awareness in Cyber Crimes

- Industry and academia awareness training
  - Cyber Crime Trends
  - Cyber Crimes Modus Operandi Examples
  - Awareness in Cyber Crimes
  - Cooperation Possibilities

- Police investigators
  - Modus Operandi of Cyber Crime Types
  - Evidence: Integrity and Stability
  - Data Storing Capacity Electronic Devices
  - Computer Forensics For Investigators
  - Information Gathering Techniques

- All police personnel
  - All police officers at Police School or Police Academy need to receive basics of cybercrime investigators and volatile digital evidence before they join Turkish National Police.
  - Modus Operandi of Cyber Crime Types
  - Evidence: Integrity and Stability
  - Data Storing Capacity Electronic Devices

The Turkish Gendarmerie also has a group of staff that need to be catered for in their strategy. These are identified along with the learning requirements as follows:

- First Responders

– (Introductory training on the following subjects)
  - Electronic evidence related devices, hardware etc.
  - Network related hardware (modem, switch, WAP etc.)
  - Tools/devices for imaging
  - How to secure a crime scene
  - Officer health and safety
  - How to seize electronic evidence
  - Operating systems
  - Mobile phones
– (Advanced knowledge needed in addition to the above)
  - Computer related hardware in detail
  - RAID types (either software/hardware)
  - Database systems
  - Live forensics
  - Operating systems Windows/Linux/Unix (if possible in detail)
  - Encryption methods/programs/hardware
  - Servers (how to deal with)
  - Anti-forensic techniques

– Cybercrime Investigator/specialists
  - Internet structure in detail
  - How it works in detail?
  - All internet protocols
  - Internet activity monitoring and analyzing
  - File sharing technologies (P2P applications)
  - Video technologies
  - Social engineering

– Digital Forensic Examiners/specialists
  - Digital forensics tools (software, hardware)
  - Open source DF tools
  - Imaging
  - Operating systems
  - File systems
  - Mobile phones (imaging, Operating Systems)
  - Database systems, Data mining
  - Malware Analysis
  - Data concealing/disguising techniques
  - Reverse engineering

3.7.4 Training capabilities and resources

The Turkish National Police has a number of resources available to deliver training. These include TNP experts, local or international academia, local or international industry, international organisations, international governmental agencies who could deliver different level of training.

TNP has some trainers to develop and deliver training at introductory and intermediate levels at present. There are currently no dedicated, full time cybercrime trainers. It is recognised that there is strong need to increase the number of trainers and plan for an increase in cybercrime unit personnel in 81 regional police directories. TNP recognises that it needs assistance in developing and delivering in specific issues and is already in contact with several academics for cooperation. It is envisaged that the training material need to be updated by trainers and subject matter experts 2 months before any planned training and that once a year there should be an evaluation of previous training and future needs.

The Gendarmerie has its own structure for the delivery of training for the staff that are dealing with all of the procedures concerning crime identification, determining the type of intervention, the scope of the investigation, planning the operation, imaging of digital evidence, executing crime-scene investigation and delivering all of the evidence acquired to judicial authorities. These roles are fulfilled by specialised units (First Responders and Cybercrime Investigators/Specialists) that are part of KOM (Anti-Smuggling and Organized Crimes) units within the structures of all Provincial Gendarmerie Commands.

- In terms of technical competencies, trainers from KOM Department (HQs) are assigned to deliver training courses. At a introductory and intermediate level these trainers have adequate knowledge, but for the advanced level training is provided by recognised foreign institutions, private sector companies and academics/universities.
- In terms of judicial and procedural aspects, trainers from KOM Department (HQs) and Gendarmerie Schools Command are assigned. More specific trainings (i.e. Informatics and Internet Law) fare provided by academics from universities.
- Also in order to combat credit card fraud, support is provided through a course on "Combating against Forgery and Fraud in the Credit Card Payment System" provided by the Interbank Card Center (BKM).

The Turkish National Police has a substantial training capability consisting of 1 Police Academy (PA), 9 Police Profession Training Centres, (POMEM), 23 Police Schools (PMYO), 1 Turkish National Police Training Department (TNPTD), the Turkish International Academy Against Drugs and Organized Crime (TADOC) and the Crime Research and Investigation Training Centre (SASEM). TADOC, which is a regional organized crime academy, has two computerised class available with all necessary technical equipment and connectivity. On the other hand PA and many of the PMYO and POMEM's have computer classes available although there could be connectivity issues or strict filtering rules in place that may affect the ability to deliver some levels of training.

It is expected that training will be delivered in Turkish, with some course potentially able to be delivered in English.

- "First Responder", "Cyber Crime Investigator", "Computer Forensics Examiner" and "Analyst" trainings will be delivered at TADOC, TNPTD, SASEM or POMEM Centres. TADOC, SASEM or the respective departments will coordinate it. Training mentioned above already have assessment and successful trainees receive a certificate valid for three years. This will continue as it is described.
- "Trainer" Trainings may be delivered at any TNP training facility when needed. It should be coordinated by TADOC, TNPTD or SASEM. Academic involvement is highly encouraged. "Trainers" also need certification by assessment before being able to undertake a training capacity.
- "Senior Staff Awareness" trainings will be delivered at TADOC, TNPTD classes or POMEM Centres. TADOC, SASEM or the respective department will coordinate it.
- "Very Senior Staff Awareness" training and "Industry and Academia Awareness" training may be delivered any place where the necessary presentation tools are available.
- "All Police" trainings for police candidates should be delivered at PA, POMEMs and PMYO's. Police officers who are not investigators but already in service will be trained at any of the TNP training facilities.
- "All Police Investigators" trainings will be delivered will be coordinated by TADOC, TNP Training Department and Respected Investigative Departments. Any of the available TNP training facility can be use for this purpose.

Training centres or respected departments mentioned above should coordinate any training available and possible to deliver outside of mentioned training facilities.

For the Gendarmerie, domestic resources, in existing facilities, using trained personnel, can deliver most of the basic and intermediate level trainings. Trainees are certified by giving them an Institutional Certificate.

3.7.5 Other considerations

Turkey is in a considerably different position than the other project areas, in that in terms of population, infiltration of technology and cybercrime, it has more experience in dealing with these matters. Within the TNP, for example, there are some 250 trained cybercrime personnel already and a requirement for some further 850 to be trained. This is in stark contrast to some of the other countries, whose experience is quite short-lived.

Turkey is therefore in a position to further its existing capability and has recognised the benefits of working with others from academia and industry to develop and deliver training. Council of Europe encourages Turkey to consider creating a national centre of excellence in cybercrime training, research and education as a focal point for its development of a sustainable capacity for cybercrime training and enhancing its capability to combat cybercrime. It is recognised that the Turkish National Police and Gendarmerie have a strong need for subject matter experts in cybercrime investigations and computer forensics examinations, and that increasing awareness of decision makers is required to ensure they build their capability in a standards based and structured manner. Turkey has been the recipient of a number of cybercrime support initiatives and should be careful to maximise the benefits of these activities.

3.7.6 Implementation of the strategy / next steps

Turkey has already incorporated a great deal of cybercrime training into the programmes of both the Turkish National Police and the Gendarmerie; however there is no overarching training strategy that informs the requirement. There is the potential that this gap is hindering the effectiveness of the programmes that have been developed. There is a very clear path set out for success and in order for this to be achieved, it is necessary that the strategy should be developed to support the necessary training at all levels and consideration given to a regime of assessment for each course that is developed. Consideration should be given, to engaging with academia to incorporate accreditation and qualifications into the programme for the specialist investigator and with industry partners, who may be able to help deliver the more technical levels of training and provide information about technology advances, which will inform the continued development of the strategy.

Turkey is a member of ECTEG and should examine existing resources such as the training material available through them with a view to incorporating them into a structured training programme. It is important to develop a training strategy that incorporates the requirements of staff at all levels of law enforcement and work towards incorporating training into existing programmes, where appropriate.

Turkey has sufficient training requirement to enable it to consider the development of a national centre of excellence in cybercrime training, research and education, and should work towards the creation of such a centre. They have a strong expertise and are recipients of other cybercrime based funding that provides training to law enforcement staff. Turkey should consider the potential of supporting the other countries in the region that do not have the same level of requirement but do need a small number of staff trained to a high level. On this basis, Turkey is well placed to create a regional centre of excellence. Turkey should

register as interested parties with 2CENTRE in order to pursue the discussions and potential collaboration with others in terms of developing a centre of excellence.
Progress should be reviewed during the Cybercrime@IPA project with a report on developments at the final project meeting.

3.8 Kosovo

3.8.1 Justification for training strategy

Kosovo recognizes that the cyber-attacks carried out against Estonia in the spring of 2007 served as a wake-up call to the potential damage that a large scale cyber-attack can have on a highly wired country. Although the resources of Kosovo are limited a strategy for combating Cybercrime is more than necessary to be developed. The impact of technology on crime in Kosovo is growing every day. Every day the number of people using computers for business (money transactions) and for other activities is growing, and with it, grows also the danger of technology being misused. The main problems for now in Kosovo are tax evasion and credit card fraud. However, economic, social, political, security and human rights are recognized as being at potential risk of being a target of cybercrime attacks. Attacks against computer data and systems, offences by means of computer systems (forgery, fraud, child pornography), are happening every day and they are causing damage to the economy.

Nevertheless, they still don't know the exact statistic of the impact of technology on crime because the section for fighting cybercrime is not established yet.

Kosovo needs to build its capability to counter cybercrime according to international standards, in order to be able to defend the citizens and the economy and to be able to help and support other countries in the fight against Cybercrime.

3.8.2 Objectives of the training strategy

The overall aim of the cybercrime training strategy for Kosovo is identified as: ensuring that all law enforcement officers have the skills necessary at their respective level to fight cybercrime. They should be trained at the level that is necessary regarding competencies and responsibilities they have in their respective institutions.

Overall objectives of the strategy will include implementing cybercrime laws, creating a specialised cybercrime unit, increasing citizen awareness of cybercrime and organizing law enforcement and judicial training regarding cybercrime.

Specific objectives relating to law enforcement training are to train first responders, cybercrime investigators and digital forensic examiners.

3.8.3 Training requirements (needs analysis)

In general, all Law enforcement members must have knowledge of cybercrime. However, they need to be specialised in the specific fields that impact on their daily work. The required levels of training and knowledge are therefore different. Some of the areas of knowledge are:

- All police officers should have a basic knowledge that should be part of the general curricula. The material should contain information how to deal with digital evidence at the crime scene and also how to respond to the complaints of citizens. Kosovo has already prepared a pocket manual, which contains basic information about dealing with digital crime scenes, and it will be provided to all Police Officers after it has been approved.
- All Investigators and managers should have knowledge of how to deal with crime scenes when digital evidence is involved.
- Child protection and economic crime investigators should have intermediate knowledge about Internet research.

- Forensic IT analysts, network investigators and Internet investigators should have intermediate to advanced level of knowledge.
- Advanced level IT Crime Specialists should have an advanced level of knowledge.

The training courses developed over a number of years by ECTEG are seen as being of use in Kosovo with the introductory IT forensics and network investigation course being of general use with the following courses being valuable for specifically identified staff:

- Core skills in Mobile Phone Forensics
- Applied NTFS Forensics
- Internet Investigations
- Network Investigations
- Linux as an Investigative Tool-Part One
- Linux as an Investigative Tool-Part Two
- Wireless LAN & VoIP
- Forensic Scripting using BASH
- Windows 7/Vista Forensics
- Intermediate Mobile Phone Forensics
- Databases & Data Mining
- Live data forensics
- Certified ethical hacker
- Computer Hacking Forensic Investigation

3.8.4 Training capabilities and resources

The Kosovo centre for public safety, education and development and licensed companies are seen as those capable of training delivery, along with accredited institutions for advanced training. In order for the Kosovo centre for public safety, education and development to deliver training, it requires at least two certified trainers, approval for the curricula and incorporation of training into the annual training programme. They are also anticipated to be able to work with the licensed organisations to update the ECTEG materials and to create new materials as required.

3.8.5 Other considerations

As Kosovo is one of the countries that does not have a long experience in dealing with cybercrime, it may benefit more than others from the creation of a regional centre of excellence.

3.8.6 Implementation of the strategy / next steps

It is necessary that the strategy in Kosovo should develop to support the necessary training at all levels and consider a regime of assessment for each course. Consideration should be given to engaging with academia to incorporate accreditation and qualifications into the programme for the specialist investigator and with industry partners, who may be able to help deliver the more technical levels of training and provide information about technology advances, which will inform the continued development of the strategy.

Kosovo should examine existing resources such as the training material available through ECTEG with a view to incorporating them into a structured training programme. It is important to develop a training strategy that incorporates the requirements of staff at all levels of law enforcement and work towards incorporating training into existing programmes, where appropriate. For higher-level training that doesn't already exist, this should be developed and delivered and where it is more relevant, staff should take advantage of

training offered at regional or international level. Kosovo should seek membership of ECTEG and register as interested parties with 2CENTRE.
Progress should be reviewed during the CyberCrime@IPA project with a report on developments at the final project meeting.

4 CONCLUSIONS AND RECOMMENDATIONS TO THE PROJECT AREAS

4.1 Conclusions

As identified in the situation report, none of the countries in the project region has a documented training strategy for law enforcement officers in the subjects of cybercrime investigation or digital forensics. None of the countries has a training centre dedicated to developing and delivering training in the subject matters.

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 in the region are:

- Croatia has provided information regarding what is a substantial input on the related subjects within its graduate and undergraduate studies on criminalistics and criminal investigation.
- Serbia currently has a project involving the Academy of Criminalistic and Police Studies and the Ministry of Interior which will incorporate the needs of the Ministry in relation to basic Masters and specialist studies as well as on-going training for members of the HTCU and other officers.
- Bosnia and Herzegovina - Republika Srbska has provided details of a high tech crime module that forms part of its professional undergraduate studies, specialised degree programme.
- Turkey has a range of cybercrime training courses and are planning to deliver more specialist training to staff under the current twinning project.

Most of the training delivered in cybercrime investigation and digital forensics is on an ad hoc basis by international organizations such as OSCE. Other training on digital forensics is almost exclusively restricted to product vendor training, which deals with how to use the tools provided.

There is no evidence of the involvement of academia or 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 region.

All countries in the region recognise the benefits of engaging in training activities with foreign specialist cybercrime units as well as with other members of the criminal justice system in their own countries. Activities such as joint training courses, workshops and conferences are considered to be those most likely to be of lasting benefit.

As the project is planning to utilise the accredited training model developed in the EU under the series of cybercrime training projects, it would be beneficial to coordinate the regional activities in this area.

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 status of the Police Academy in Croatia being able to offer academically accredited training programmes would enable the region to develop its programme, taking advantage of the existing training courses that have been developed in Europe and elsewhere, including modules already developed in the region. Assigning credit levels would be a more straightforward exercise and enable a programme that, with the support of the planned project training working group, to be an effective solution for the region. Having accreditation at the regional level would allow further modules to be introduced at the appropriate level.

Much work has also been conducted in Serbia, with the potential for the country to become a regional centre of excellence that may build on their previous activities. Turkey has a different position than the other countries as identified above. For those reasons it is capable of creating a national centre of excellence that may support others in the region. However it should not be considered as a single regional centre, mainly for the reason that language would be an issue and it is important that a regional centre is able to cater for the greatest number of students using compatible languages. For that reason it is believed that a regional centre in Croatia or Serbia is preferable. The regional working group should help identify how this should develop and thereby ensure the greatest benefits are accrued to the countries of the project area.

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 Dublin, 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 Dublin should be taken back to each project area and developed into national strategies that will be implemented and not just left once created. 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.

4.2 Recommendations

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

- The development at national and regional level of a cybercrime training strategy 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 such as existing with the European Cybercrime Training and Education Group (ECTEG) should be investigated for suitability at project area and regional 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.

- It is recommended that at least one regional centre of excellence in cybercrime training research and education is created to support the work being conducted at national level and to ensure that much needed training is available at regional level where each project area may not have such a requirement to support in project area training. Croatia and Serbia should be considered as potential countries for such a centre. Turkey should consider creating a national centre of excellence as it has a much different requirement than other countries and can sustain such a centre. It should become a partner of any regional centres that are created and all should consider the benefits of seeking membership of the Cybercrime Centres of Excellence Network for Training, Research and Education (2CENTRE).

- 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.