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 9 November 2011

Specialised cybercrime units

- Good practice study -

Prepared jointly by

CyberCrime@IPA project of the Council of Europe and the European Union

Global Project on Cybercrime of the Council of Europe

European Union Cybercrime Task Force

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

Content

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: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Disclaimer:

This technical report does not necessarily reflect official positions of the Council of Europe or of the European Union or of the parties to the agreements referred to.

Executive summary

Purpose and justification of specialised units

This study is to help public authorities create or further strengthen specialised cybercrime units as a key element of the response to cybercrime. It is recognised that both law enforcement and prosecution authorities require a specialised response to the issues raised by cybercrime. While the law enforcement requirement is often catered for, the needs of prosecution departments have to be identified and implemented to ensure the effectiveness and fairness of criminal justice systems. This study concentrates on the development of police type of law enforcement specialised units; however it is of value to prosecution departments that are seeking to create their own units or seeking to up the skill of staff within existing offices to deal with cybercrime.

The study is based on the actual experience of cybercrime units not only in Europe but also other regions of the world. Information in the form of replies to questionnaire have been received from Australia, Austria, Belgium, Brazil, Croatia, Cyprus, Czech Republic, Finland, France (Gendarmerie and Police), Ireland, Kosovo,[*] Luxembourg, Mauritius, Montenegro, Romania, Serbia (Specialised Prosecutors Office), Spain and "the former Yugoslav Republic of Macedonia".

There is no single solution that will be appropriate for all countries and it is vital that the development of cybercrime units evolve in accordance with the needs of each country based upon its legislation, reliance on IT, prevalence of different types of criminal activity and other matters that are dealt with in this study.

The evolution of information and communication technologies (ICT) and the Internet are transforming societies worldwide. The more societies depend on computer networks, the more vulnerable they become to threats such as cybercrime.

Following the concept of the Budapest Convention on Cybercrime, cybercrime is considered to cover:

- Offences against computer systems
- Offences by means of computer systems, in particular those that have acquired a new quality through the use of ICT such as forgery and fraud, child pornography and offences related to intellectual property rights.

Any offence may involve important evidence located on a computer (including mobile devices), even if this offence is otherwise un-related to computer systems. While this is not cybercrime, the criminal justice system nevertheless needs to be able to recognize and handle electronic evidence.

Therefore the primary role of specialised cybercrime units is:

- Investigating and/or prosecuting offences against computer data and systems
- Investigating and/or prosecuting offences committed by means of computer data and systems
- Carrying out computer forensics with respect to electronic evidence in general.

In relation to digital forensics, it is important to recognise that some jurisdictions are moving away from the model where all forensic activities are undertaken by cybercrime units. Separation of the

[*] 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

investigation and evidence examination functions has gained impetus. Incorporation of digital forensics into mainstream forensic structures, introducing standards and accreditation of providers is something that should be considered, while recognising that cybercrime units need to retain a capability to deal with the capture and analysis of vulnerable data during investigations. It does of course depend on the size of the country, the number of cases and the response capacity, but pushing all digital evidence to cybercrime units may not be sustainable and creates the type of backlog seen in many countries.

In addition to the role described above the cybercrime units may also contribute to the formulation of: national cybercrime strategies, national cybersecurity strategies, cybercrime legislation and others.

Specialised cybercrime units are a crucial part of the law enforcement and prosecution response to cybercrime and to the proper handling of electronic evidence. The creation and allocation of resources to such units is justified by:

- The growth in cybercrime in all regions of the world
- The transnational and fast evolving nature of technology and cybercrime
- The large amount of crime proceeds generated (most cybercrime is aimed at illicit gain) and the impact and damage caused
- The need to protect citizens, including children against sexual exploitation and abuse
- The fact that cybercrime may affect economic, social and other national interests as well as national security and international relations
- The increasing demand for computer forensics, including collection and analysis of electronic evidence on computer systems, including mobile devices.

Types of specialised units

The following types of specialised cybercrime units are found:

- "Cybercrime units" that tend to be services investigating all types of cybercrime committed against and by means of computer data and systems and also have computer forensic functions
- "High tech crime units" that are mainly competent for investigating offences against computers and include computer forensic functions
- "Computer forensic units" as separate units which are responsible for collecting and analysing electronic evidence
- "Central units" without investigative functions but responsible for coordination, strategic and intelligence functions
- Crime-specific units
- Specialised prosecution units.

In most countries, the function, responsibilities, organisational structure and other features keep evolving in the light of the changing threat or policy or law enforcement priorities.

Institutional set up and organisation

The key considerations to be taken into account when setting up a cybercrime unit are the:

- national legislation that provides the legal basis
- internal orders and regulations governing the functioning of the unit
- police department to which the unit is attached (organisational setting)
- premises of the unit

- internal organisation and structure.

However, the most important prerequisite is that a government understands the nature and impact of the threat of cybercrime and thus the need for a specialised unit that is equipped with the necessary authority and resources. In addition, there is a necessity that the government prepare a cybercrime strategy which would provide the general direction and guide the institutions in their activities against cybercrime. The overall objective of this strategy would be to ensure that the rule of law is applied and that the legitimate rights are protected also in the ICT and online environment.

From the analysis of the current types of cybercrime units it appears that a cybercrime unit should be structured in three sections, that is, investigation, data and information analysis and computer forensics. One unit at the central level coordinating a number of field offices seems to be an efficient formula. However, the units should remain flexible enough to respond to the evolution of cybercrime and technology and to changes in the environment in which it operates.

Functions and responsibilities

Functions and responsibilities may include all or a combination of:

- Investigations
- Collection of data and forensic analysis
- Intelligence collection, analysis and dissemination
- Assessment and analysis of cybercrime phenomena
- Contribution to drafting national legislation on cybercrime
- Contribution to defining national cybercrime strategy
- Coordination of regional/territorial units
- Specialised support to other police units
- Cooperation with the private sector
- International cooperation
- Prevention
- Defining internal procedures
- Training programmes
- Development of national reporting systems.

Interagency, public/private and international cooperation

Cybercrime is not a clear-cut, stand-alone type of crime but requires inter-agency cooperation with the Ministry of Interior, other law enforcement services, the prosecution, the Ministry of Justice, intelligence services, incident response teams (CSIRT/CERT) and others for information exchange, common projects, common operations, prevention measures, training and other activities.

Cooperation with the private sector (including service providers, the finance and other sectors, the ICT industry, academia) is essential not only in terms of securing electronic evidence but also for prevention, threat assessments, the formulation of policies and strategies, training and other measures.

Considering the transnational nature of cybercrimes, effective international cooperation is a priority. In this regard having the 24/7 point of contact within the specialised cybercrime unit provides a great advantage to the unit when handling cases that require the preservation of data pursuant to article 29 and 30 of the Convention on Cybercrime and the collection of evidence, the provision of legal information and location of suspects as foreseen in article 35 of the Convention with the goal of assisting in an ongoing investigation. The use of mutual legal assistance treaties is key to evidence being transferred between jurisdictions; however there are issues with the speed with which requests are processed.

Steps towards the creation of a specialised unit

Ideally steps would include:

1. Assessing needs and making a decision
2. Establish the legal basis
3. Appointment of the manager of the cybercrime unit
4. Staffing the unit
5. Equipment and other resources
6. Training programme for the unit
7. Independence of and knowledge about the unit
8. Action plan and evaluation mechanisms.

Assessment and conclusions

A growing number of countries have a separate specialised unit that investigates cybercrime and carries out forensic investigations. Such units have evolved gradually since the early 1990s.

A key factor has been the recognition by governments of the impact and relevance of cybercrime and electronic evidence. The increased financial impact on the governments, corporations and individuals as well as the potential impact on the Critical National Infrastructure has justified the investments in cybercrime units.

A thorough analysis of the units shows that each unit has its specific strong points while they seem to share similar challenges, that is, a lack of personnel, limited budgets, limited resources for training, as well as slow and time-consuming cooperation with third countries.

The performance of the specialised cybercrime unit depends to a large extent on:

- the quality of its staff and the determination and motivation of its leadership
- cooperation with prosecutors, courts and other agencies at the domestic level
- cooperation with the private sector
- international cooperation.

A cybercrime unit justifies its existence and the resources allocated if it can be positively assessed against the following indicators:

- knowledge of the phenomenon of cybercrime, including typologies, risks and trends
- enforcement of national and international law in the area of cybercrime
- investigations carried out and leading to prosecution and conviction of offenders
- visibility, credibility and trust in the unit.

1 Introduction

The intention of the present study is to help public authorities create or further strengthen specialised cybercrime units as a key element of the response to cybercrime.

The study is the result of a cooperative effort of the:

- CyberCrime@IPA joint project of the Council of Europe and the European Union on regional cooperation against cybercrime in eight countries/areas of South-eastern Europe
- Global Project on Cybercrime of the Council of Europe which supports countries worldwide in the implementation of the Budapest Convention and related tools and good practices
- European Union Cybercrime Task Force (EUCTF) which was established in 2010 and gathers the heads of high-tech crime units of the 27 Member States of the European Union. The secretariat of the EUCTF is provided by Europol.

In June 2011, the Council of Europe and the EUCTF had sent out a common questionnaire to cybercrime units in Europe and other regions of the world.

Information in the form of replies to questionnaire was subsequently received from Australia, Austria, Belgium, Brazil, Croatia, Cyprus, Czech Republic, Finland, France (Gendarmerie and Police), Ireland, Kosovo[*], Luxembourg, Mauritius, Montenegro, Romania, Serbia, Spain and "the former Yugoslav Republic of Macedonia". The study is thus based on the actual experience of cybercrime units not only in Europe but also other regions of the world.

Most of the information received was related to police-type units and thus the present study covers primarily police-type units. Nevertheless, it is essential that prosecutor enhance their specialisation or follow the example of countries such as Romania or Serbia where specialised prosecution units have been established.

Between July and September 2011, replies were analysed and the study was prepared by:

- Virgil Spiridon, Head of Cybercrime Unit, Romanian National Police, Romania
- Yasmine Ourari, Legal Adviser, Federal Computer Crime Unit, Belgium
- Marjolein Delplace, Strategic Analyst, Federal Computer Crime Unit, Belgium

In September 2011, the draft study was discussed at a CyberCrime@IPA regional workshop on specialised cybercrime units in Budva, Montenegro.

Between September and November 2011 further information was gathered from specialised services of additional countries to enhance the report. Detailed comments were also provided by Nigel Jones (United Kingdom).

In November 2011, the study was presented at the global Octopus Conference on cybercrime (Council of Europe, Strasbourg, France, 21-23 November 2011).

[*] 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

Table 1: Units analysed

Name	Year established	Organisational setting
Albania: Sector against cybercrime	2009	Directorate against Financial Crime under the Department against Organised and Serious Crime, General Directorate of State Police
Australia: Cybercrime Operations	2008	Australian Federal Police - High Tech Crime Operations
Austria: Unit 5.2 Computer Crime of the Criminal Intelligence Service	2002	Director of the Criminal Intelligence Service, Federal Ministry of Interior
Belgium: Federal Computer Crime Unit	2001	Federal Judicial Police, Direction economical and financial crime, Ministry of Home Affairs
Bosnia and Herzegovina (Republika Srpska): Department for High-tech Crime	2010	Criminal Police Administration, RS Ministry of Interior
Brazil: Computer Forensic Unit of the Federal Police	1996	Brazilian Federal Police, Forensic Institute, Technical & Scientific Directorate, Ministry of Justice
Croatia: specialised officers of the Organised Crime Department and Economic Crime and Corruption Department (not a separate specialised unit)		General Police Directorate, Ministry of Interior
Cyprus: Office for Combating cybercrime	2007	Police Headquarters, Department C (Criminal Investigation Department), Ministry of Justice and Public Order
Czech Republic: Information Technology Crime Section	2005	Bureau of Criminal Police and Investigation Service, Police Presidium
Finland: Cybercrime Intelligence Unit, Cybercrime Investigations Unit, Crime Laboratory		National Bureau of Investigation, Ministry of the Interior
France: Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication - OCLCTIC (Police)	2000	General Directory of National Police, Central Directory of Judicial Police, Sub directory of Fighting against Organized Crime and Financial Delinquency
France: Cybercrime division (Gendarmerie)	1998	Pôle judiciaire de la gendarmerie nationale, Ministry of Interior
Ireland: Garda Computer Crimes Investigation Unit	1991	Garda Bureau of Fraud Investigation, National Policing Service
Kosovo*: Cybercrime Investigation Unit	2011	Directorate for Investigation of Organised Crime
Luxembourg: Section Nouvelles Technologies	2003	Police Grande Ducale - Service of Judicial Police, Ministry of Public Force
Mauritius: Information Technology Unit -IT Unit	2000	Central Crime Investigation Division, Mauritius Police Force
Montenegro: cyber-crime specialists of Division for Combating Organised Crime and Corruption (not a specialised unit)	2004	Criminal Police Department
Romania: Cybercrime Unit (Police)	2003	General Inspectorate of Romanian Police, Organised Crime Department, Ministry of Administration and Interior
Romania: Service for Combating Cyber Criminality-Cybercrime Unit (Prosecution)	2003	Directorate for Investigating Organized Crime and Terrorism Offences, Prosecutor's Office attached to the High Court of Cassation and Justice
Serbia: Special Prosecution Office for High Tech Crime	2006	Higher Public Prosecutor's Office Belgrade, Appointed by the Public Prosecutor of the Republic
Spain: Brigada de Investigación Technologica (BIT)	1995	Criminal Police General Directorate, Cuerpo Nacional de Policia
"The former Yugoslav Republic of Macedonia": Cybercrime Unit	2004	Department for Financial Crime under the Centre for Suppression of Organised and Serious Crime, Ministry of Interior

2 The purpose of specialised cybercrime units

The evolution of information and communication technologies (ICT) and in particular the Internet is transforming societies worldwide. It offers unique opportunities not only in terms of social, economic, cultural and scientific development but also in terms of human rights and democracy. Societies rely on ICT. The more they are dependent on computer networks, the more vulnerable they become to threats such as cybercrime.

Research shows an increase in cybercrime in all regions of the world. Offenders exploit the opportunities offered by the Internet by illegally accessing computer systems, intercepting communications and stealing or manipulating data, or interfering with computer systems. Most cybercrime is now aimed at generating illicit gain through different types of fraud – ranging from phishing and identity theft to payment card fraud, account take-over, auction fraud, investment fraud, and mass-marketing fraud – through offences related to intellectual property rights or counterfeit pharmaceuticals. Also other "traditional" types of crime have increased in scope through ICT, such as extortion and other activities carried out by organised criminal groups. The cost of cybercrime reportedly exceeds 100 billion Euros globally.

The sexual exploitation and abuse of children, including child pornography, has obtained a new quality through the use of ICT and the Internet, and is a particular concern.

An "underground economy" has evolved that provides the tools and infrastructure to commit such forms of crime, including, malware and services to deploy malware and anti-forensics, botnets for taking over computer systems, sending spam, spreading malware or carrying out denial of service attacks, bullet-proof hosting of criminal domains, markets for credit card, bank account, and other personal details that can be used for identity-related fraud, or money mules to move crime proceeds and launder criminal money. These "underground market places" used to be accessible for a select public with the proper connections, but these days they are more and more accessible for everyone with bad intentions.

The impact of a cybercrime unit - UK example

A Metropolitan police unit claims to have saved the economy more than £140m in the past six months and is on course to exceed its four-year "harm reduction" target, the force said on Sunday.
The Met said the central e-crime unit had delivered nearly 30% of its £504m target during this period.
The figure relates to the amount of money the UK has been prevented from losing through cyber crime and follows a number of successful prosecutions and operations.
Funding of £30m has been provided over four years to support the development of the unit as it tackles computer intrusion, denial of service attacks and internet fraud.

Excerpt from an article published in "The Guardian" on Sunday 2 October, 2011 for more details follow the link: http://www.guardian.co.uk/uk/2011/oct/02/cyber-crime-unit-met-police/print

Most types of crime now involve computers in one way or the other, either in that computer data and systems are the target of the offence, or in that the offence is committed through computers or in that electronic evidence on a computer that may be important in relation to an offence that otherwise is un-related to computer systems.

Criminal justice authorities need to be able to deal with all three aspects:

- Offences committed against computer data and systems (such as those defined in Articles 2 to 6 of the Budapest Convention on Cybercrime)
- Offences committed by means of computers (such as those defined in articles 7 to 10 of the Budapest Convention but also others)
- Electronic evidence on a computer related to any type of offence (see article 14).

The criminal justice system of a country must therefore be capable of coping with a very large number of offences and cases.

Data provided by countries responding to the questionnaire suggests that if 100 offences against computer data and systems are investigated by a cybercrime unit, 1,000 offences by means of computers may be investigated and 10,000 devices may need to undergo computer forensic examinations.

The concept of cybercrime according to the Budapest Convention

The Budapest Convention is based on a concept of cybercrime that covers not only offences against but also a number of offences by means of computer data and systems:

- Offences against the confidentiality, integrity and availability of computer data and systems, that is, offences against computer data and systems, including illegal access, illegal interception, data and system interference, misuse of devices
- Offences committed by means of computer systems. This list is limited to those “old” forms of crime that obtain a new quality through the use of computers, that is, computer-related forgery and fraud, child pornography and offences related to infringements of copyright and related rights on a commercial scale. An additional Protocol covers the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189).

This concept is capable of capturing cases that consist of a combination of different types of conduct.

The Budapest Convention contains furthermore a set of procedural law and international cooperation measures. These apply to any crime involving electronic evidence or committed by means of a computer system. This concept is thus very wide scope in scope (see article 14).

However, the replies also show that while specialised cybercrime units are nearly always responsible for investigating offences against computers, in some countries offences by means of computers are investigated by other units or departments. This is particularly true for credit card fraud, child pornography or other forms of sexual exploitation and abuse of children, or for intellectual property rights-related offences. In such cases, cybercrime units may have a technical support function. This support function also applies to the forensic examination of electronic devices.

In any country, a sufficient level of specialist skills and specialised services must be available with the primary purpose of:

- Investigating and/or prosecuting offences against computer data and systems
- Investigating and/or prosecuting offences committed by means of computer data and systems
- Carrying out computer forensics with respect to electronic evidence in general.

Specialised cybercrime units need to take into account that and address the following needs:

- cybercrime often involves a combination of offences against and by means of computers and that therefore different law enforcement and other services share a responsibility. Interagency cooperation is thus essential and a specialised cybercrime unit may provide technical support and know how to other agencies
- all law enforcement officers, prosecutors and judges must have at least basic understanding of issues related to cybercrime and electronic evidence. The specialised unit may therefore provide training and advice to other services
- cybercrime is often transnational crime with offenders, victims, computer systems or evidence located in different countries. The specialized unit may therefore engage in international cooperation
- ICT technology and techniques used by criminals evolve constantly. The specialised unit may therefore engage in research and analysis. Cybercrime reporting systems as well as statistics on cases investigated, prosecuted and adjudicated should be maintained
- investigative powers need to be subject to conditions and safeguards to ensure that fundamental rights are protected and that the rule of law applies.

Specialised cybercrime units cannot be effective in isolation. The creation or strengthening of specialised cybercrime units should be part of an effective cybercrime strategy in which the police unit on national level can be a driving force. The cybercrime strategy should aim at crime prevention and criminal justice on the Internet covering measures such as:

- cybercrime prevention
- cybercrime reporting systems
- legislation harmonised with international standards such as the Budapest Convention
- institutional development and training of personnel
- public-private partnerships and cooperation (service providers, ICT companies, financial sector and credit card companies, and others)
- international cooperation.

The prevention and control of cybercrime, including the strengthening of specialised cybercrime units, requires substantial resources.

The allocation of resources seems justified given:

- the large amount of damage caused and criminal proceeds generated through cybercrime, that is, offences against and by means of computers. A cybercrime unit my save society large amounts of money and prevent major damage
- that, in societies dependent on computer networks, cybercrime may become a question of economic, social and other national interests as well as national security:
    - protection against terrorist attacks and terrorist use of ICT
    - protection of computer systems for the operation of critical infrastructure (energy network, health system, etc.)
    - involvement of organised criminal networks
    - protection of the business environment;
    - enhancing trust in the financial systems and communication networks of a country
    - protection of citizens when using electronic payment tools and other services through the Internet
- that attacks from one country may affect crucial interests of another country.

Specialised cybercrime units thus have a specific purpose but cover a wide range of offences and serve the larger interests of a country and of the international community.

3 Types of specialised units

Specialised cybercrime units have been established and have evolved during the past twenty years in response to the evolution of crime and within the specific context or criminal justice system of a country. This explains differences in types, organisation and functioning of specialised units.

When child pornography through the Internet became an issue, governments started to concentrate on this phenomenon and began to develop administrative and investigative capacities to address it.

In Romania, credit card fraud in relation to online purchases was the initial concern. Legislation criminalising electronic payment frauds and Internet fraud followed and a specialised unit within the police was created afterwards. Initially, the officers of this specialised unit were specialised in money counterfeiting and electronic payment frauds.

In Mauritius, the IT Unit was created in 2000 in the Mauritius Police Force, at the Police Headquarters and the objective was to regroup police offices for the development of Information Technology in the Mauritius Police, and also to combat ICT related crimes. In 2006, the IT Unit came under the Central Crime Investigation Division of the Police Headquarters. At that point, the investigation of cybercrime became a core function of the unit and a digital forensic laboratory was created.

In Spain, the Unit was created in 1995 as a small group of officers, and in 2000 was transformed to a Brigade for cybercrime. In Ireland, the Unit was established in 1991 with two staff and now has 16 staff.

This suggests that specialised units will further evolve in response to the evolution of cybercrime, and new types or combination of different types of units will emerge. The following is a basic typology of specialised units.

3.1 Cybercrime units

"Cybercrime units" tend to be services investigating all types of cybercrime, that is, offences against and by means of computers, including computer frauds, cyber-attacks, electronic payment frauds, online child pornography, and others. Examples are the specialised units within the police forces of Cyprus, the Czech Republic, France (Gendarmerie), Mauritius, Romania, or Spain.

In some countries, similar functions are carried out by a group of specialised investigators without them being organised as a separate specialised unit. This is, for example, the case of Croatia and Montenegro.

3.2 High-tech crime units

"High tech crime units" on the other hand are mainly competent for investigating offences against computers. They are not competent for other crimes committed through computer systems, such as electronic payment frauds, Internet frauds, and similar, but may provide technical support to investigations carried out by other units or agencies. Examples are the units of Austria, Belgium, Ireland or Luxembourg.

Given that most cybercrime against computers is related to offences by means of computers (such as identity-related crime combining illegal access or illegal interception with fraud), such a limitation to crimes against computer systems may not be the most effective approach.

3.3 Computer forensic functions/units

Both types of units often have computer forensic functions, which means that they analyse the evidence related to their own investigations or to investigations of other services. For example the Cybercrime Unit in Romania has within itself the "Forensics Unit" which is not the case with the unit in "the Former Yugoslav Republic of Macedonia" where the forensic analysis is handled by another Specialised Unit for Computer Forensics.

"Computer forensic units" may also be created as separate units and be responsible for collecting and analysing electronic evidence and possibly for providing technical support to investigative units. An example is the Brazilian Federal Computer Forensic Unit.

3.4 Central cybercrime units

Some countries have established "central cybercrime units" whose power is limited to collecting information or assisting other police structures in computer forensics, cybercrime investigations or other types of criminal investigations.

For example, in the United Kingdom, the Cybercrime Unit from SOCA has primarily an intelligence function (collection of data), with the purpose of defining national policies and threat assessments, and for initiating major investigations. In these police systems, the actual cybercrime investigation is a task of the local police, with the assistance of the specialised unit.

In countries where the central cybercrime unit provides support and assistance to local or territorial structures, such support is mainly provided to Internet investigations or to computer forensics.

3.5 Crime-specific units

In some countries, units have been created with responsibility for specific types of crime, or a cybercrime unit may have sub-sections responsible for specific crimes. This is often true for child pornography and other forms of sexual exploitation and sexual abuse of children, but it may also apply to IPR-related offences or specific types of fraud.

An example is CEOP (Child Exploitation Online Protection) of the United Kingdom which has primarily responsibilities for responding to online child abuse.

CEOP follows a broad approach and takes responsibility not only for investigations but also for prevention and international cooperation.

3.6 Specialised prosecution units

This study is documenting good practices of police-type specialised units. However, some countries have gone beyond the specialisation of prosecutors and have created specialised units. Examples are Romania and Serbia.

In Serbia, the Special Prosecutor's Office for the suppression of high-tech crime was established in 2006 within the Higher Public Prosecutor's Office in Belgrade but with jurisdiction over the territory of

Serbia and with respect to offences against and by means of computers. The Special Prosecutor can also engage in international legal cooperation. For computer forensics the Special Prosecutor relies on the Ministry of Interior. In January 2010 the competencies of this office were redefined with responsibility for a broader range of offences but lesser responsibility for minor criminal acts. The Special Prosecutor cooperates directly with the specialised Department for Suppression of High-Tech Crime within the Ministry of Interior.

In Romania, the cybercrime unit of the general Prosecutor's Office was created in line with article 62 of Law 161/2003, and functions also as a 24/7 contact point. The main responsibilities of this unit are:

- provides specialised assistance to foreign authorities
- orders the expeditious preservation of computer data or traffic data
- executes or facilitates the execution of letters rogatory or other mutual legal assistance requests in cases of cybercrime requesting:
  - identification of persons
  - criminal records
  - IP addresses or providers
  - house or computer searches
  - interception of all types of communication
  - seizing or blocking assets, etc.
- investigates and prosecutes complex, technical cybercrime cases.

In countries such as Romania where a prosecutor is in charge of or supervising an investigation, specialisation of prosecutors or specialised prosecution services will enhance the effectiveness of cybercrime law enforcement.

Another approach consists of joint units of prosecutors and police officers. However, this is subject to the specific criminal justice system of a country. The system of Nordic countries such as Norway, allows for prosecutors and police officers to operate within the same structure, and an example is the Cybercrime Investigation Section within the High-Tech Crime Department of the National Criminal Investigation Service of Norway.

4 Institutional set up and organisation

The key considerations to be taken into account when setting up a cybercrime unit are:

- the national legislation that provides the legal basis
- the internal orders and regulations for the functioning of the unit
- the police department to which the unit is attached
- the premises of the unit (the personnel, training and equipment)
- the internal organisation and structure.

4.1 National legislation

The national legislation provides important aspects to be observed when setting up any police unit, including cybercrime unit, such as:

- police units organisation, reorganisation and setting up of new units
- material and territorial jurisdiction of police units
- procedural powers and tools to be used by police units in their investigations or in specific activities.

The legal framework states the moment to set up the cybercrime unit, the department to which it is attached to, its components, jurisdiction, tasks and relationship with other police units.

In countries, where the national law provides that a 24/7 contact point for international cooperation is set up according to article 35 of the Budapest Convention on Cybercrime operate within police units, this must be taken into consideration and resources must be allocated for that.

4.2 Internal orders and regulations

The duties of the specialised units are usually defined by an Internal Act. They mainly regulate the following issues:

- the organisation and functioning of a police unit
- its jurisdiction (defined and clearly separated from other units)
- definition of the limits of jurisdiction between police units and collaboration and hierarchical relation between them
- staff positions in the unit (number of officers, number of management positions, etc.)
- tasks of the police unit.

The orders and regulations are issued and approved by the managers of the police and the responsible ministry, in accordance with and completing the national law.

Whenever a police unit/department is set up, it must have its own internal regulation for organisation and functioning.

In Belgium, for example, the Federal Computer Crime Unit is based on a Directive of the General Director of the Federal Judicial Police of 2002. Additional internal regulations and circulars provide more detailed instructions regarding procedures to be followed and the assistance to be provided by the FCCU.

4.3 The organisational setting

Regarding the most appropriate place of a new cybercrime unit within the police structure several aspects need to be considered: the jurisdiction, legislation and national tradition and in particular the specific tasks and jurisdiction of the unit, before making the final decision about the place of the unit.

This is especially true with regard to the central versus local/regional organisation but also with respect to the horizontal support function, that is, the assistance that the cybercrime unit has to provide to other law enforcement units.

Cybercrime units have not yet found a firm place within the organisational structure of law enforcement. They seem to be often placed in a department where they "support the most". Common examples are (in no particular order):

- Economical and financial Crime Unit, e.g. in Belgium (Directorate of economic and financial crime)
- Intelligence Services Unit, e.g. Austria (Directorate of the Criminal Intelligence Service)
- Organised Crime Unit, e.g. Montenegro (Division for Combating Organised Crime and Corruption)
- Forensics Unit, e.g. Brazil (Technical and Scientific Directorate)
- Criminal Investigation Department, e.g. Cyprus, Czech Republic, Finland.

The facts that cybercrime is increasingly organised and that it is transnational in nature would argue for having them close to organised crime departments. The fact that much cybercrime is profit-driven would argue for a close link to economic and financial crime departments. However, one could also argue that they play a transversal role and thus be established as a separate structure with their own budget.

Allocation of funds

In most countries, the budget for the specialised unit is part of the general police budget. In Belgium the Federal and Regional Computer Crime Units (circa 175 staff members) have an annual budget of approximately € 720 000 at their disposal for material and software. In addition to that they have an annual budget of € 220 000 from the Ministry of Justice for the purchase of hard disks and cd-rom/dvd-rom that are used to make forensic copies, or used as evidence budget.

In a number of countries where cybercrime is of great concern, territorial cybercrime units have been created to enable more efficient investigations at local or regional levels.

At the same time, the existence of specialised police units at central level and at territorial or regional level may generate communication problems as well as duplicating or overlapping activities or even parallel investigations. Therefore, criteria and mechanisms need to be put in place for defining competencies and ensuring collaboration and exchange of information and data. For example, Belgium has a directive of the General Director of the Federal Judicial Police on the organisation and functioning of the Regional Computer Crime Units and the Federal Computer Crime Unit.

It would seem that the most efficient model is to have a centralised cybercrime unit with subordinated territorial or regional specialised units that are coordinated from the central level.

Some cybercrime units have deployed "satellites" (key personnel with technical skills similar to cybercrime investigators) within other crime units. These satellites are supported by the cybercrime unit which in return is less often called upon to provide horizontal support.

In some countries several national police structures with similar – possibly competing – competencies in the area of cybercrime may co-exist.

In Brazil or Australia, both the Federal Police and the State Police can handle offences by means of computer systems. In France, the National Police and Gendarmerie have both specialised units for cybercrime.

In order to ensure an efficient approach and best use of resources, the efforts of units need to be coordinated according to their respective strategic priorities. A task-force could help ensure cooperation and efficient exchange of information with regard to national threats and effective and immediate responses.

4.4 Premises

The offices and other premises of a cybercrime unit need to have certain features. Separate office space is needed for officers dealing with cybercrime investigations and computer forensic.

The space where different applications or database servers are located must be suitable for the safe storage of equipment. The access to the premises where servers are located will be restricted. Space is needed furthermore for seized computers or equipment and other digital evidence.

Where the forensic capacity is the cybercrime unit itself, specific conditions (laboratory environment) need to be provided for the personnel responsible for forensic tasks. Dealing with digital forensics is often only seen as performing an autopsy on computers. However, uncovered computer components are very sensitive in general and especially vulnerable to shocks and static electricity. Even if resources for a specific and pure laboratory environment are not available, precautions must be taken and a clear policy must be established on how to ensure the careful handling of electronic devices and digital media.

4.5 Internal organisation and structure

The organisation and functioning of a cybercrime unit depend on many internal conditions and a perfect blue print is not feasible. However, the basic organisation principles to be fulfilled are that a cybercrime unit should:

- have a clearly defined legal statute
- function at central level and possible coordinate territorial or regional units under responsibility
- have its own management
- be visible and credible.

The arguments for having a cybercrime unit at central level are:

- to address the phenomenon at a national level
- to come to a better understanding of transnational threats (new types of crimes, new developments of operating methods, etc.)
- to follow and link up with international initiatives (international concept and strategies, international work groups, international legislation, etc.)

- to ensure proper cooperation with relevant domestic institutions and stakeholders (develop partnerships and prevention measures)
- to contribute to the creation of a national strategy and to the evaluation of the phenomenon at the national level.

The internal organisation of a cybercrime unit should reflect the material jurisdiction (crimes it is responsible for) and tasks of the unit. The internal organisation of the cybercrime unit depends on the following issues:

- the crime phenomenon as registered in the country
- national legislation, international requirements and standards
- available financial resources.

The cybercrime unit should be a separate and specialised part of a police department, not a unit combining several other tasks (e.g. not a cybercrime and money counterfeiting), and have a manager with decision-making and representation powers.

Experience shows that a cybercrime unit, no matter its size or material jurisdiction, may be organised in three sections:

- investigation
- data and information analysis
- computer forensics.

The question as to whether a forensic unit should be part of the cybercrime unit or a separate entity is a controversial one. It can be argued that computer forensics should be separated from investigative functions in order to avoid incompatibilities or a compromising of evidence. On the other hand, it may be more efficient if computer forensics and cybercrime investigations are within the same unit. In fact, given the large need for forensics, every police unit should possibly have trained officers capable of carrying out basic forensic tasks, such as analysing evidence on social networks, e-mail and others.

Different solutions have proven to function in practice:

- If the forensic unit is part of the cybercrime unit, it could functions as a separate section, so that some staff can focus on investigation and other staff on the forensic analysis. That is the case in e.g. Romania. This will also reduce the risk of incompatibilities.

- Another option is to have a separate dedicated forensic unit that works in close collaboration with the cybercrime unit. That is the case, for example, in the Czech Republic and "the former Yugoslav Republic of Macedonia". The Brazilian Federal Police Computer Forensic Unit with 21 forensic examiners in headquarters and some 170 forensic examiners in about 50 field offices is only covering forensics, while a separate cybercrime unit of the Federal Police is carrying out investigations.

It is essential that sufficient resources (staff, equipment) are allocated for forensic functions as it is here that huge backlogs are accumulated.

Table 2: Personnel and software available

Name	Number of staff	Qualifications	Field offices	Software available
Albania: Sector against cybercrime	5 officers at HQs, 12 officers in 9 regional offices	No, special training. The head of the Unit is currently attending the UCD Masters Course	Yes, 9	HELIX3, Live Detector, Paraben forensic tool
Australia: Cybercrime Operations	3 investigators and 1 support. 7 investigators and 2 specialists work from our regional offices	Various	Yes	Not mentioned
Austria: Unit 5.2 Computer Crime of the Criminal Intelligence Service	17 experts	Criminal Investigation and technical education, specification in network and computer forensic and ECTEG	No	Encase, FTK, X-WAYS, X-RAY, Cellebrite
Belgium: Federal Computer Crime Unit	35 FCCU and 140 RCCU's	Bachelors and masters in ICT + administrative staff	Yes, 26	Open Source Linux Tools, X-WAYS, FTK, XRAY, UFED, virtualisation software
Bosnia and Herzegovina (Republika Srpska): Department for High-tech Crime	7 Officers		No	
Brazil: Computer Forensic Unit of the Federal Police	26 CFU and 170 in the field offices	Bachelors and masters in Computer Science or similar	Yes, ca. 50	FTK, Encase, Cellebrite UFED, XRY, Distributed Network Attack (DNA), CellDEK, Logicube Forensic Dossier, IDA Pro, VMWare, X-WAYS
Croatia: specialised officers of the Organised Crime Department and Economic Crime and Corruption Department	2 police officers at the central level and 30 police officers in the field offices	Bachelor of Economics, law and criminology	No	forensic computers, EnCase software, other software for data recovery
Cyprus: Office for Combating cybercrime	6 (and 7 in the lab)	Experience in investigative issues (computer technicians in the lab)	No	FTK
Czech Republic: Information Technology Crime Section	7 + 1 police officers (+50 police officer in regional IT groups)	internal police training of seizing data and external training of investigation cyber crime	No	Encase, DEFT
Finland: Cybercrime Intelligence Unit, Cybercrime Investigations Unit, Crime Laboratory	14 Intelligence, 10 Investigations, 3 Crime laboratory	National/international training	No	Encase, FTK, X-WAYS, Blackpack, Oxygen, Cellebrite
France: OCLCTIC (Police)	50 in the Central Unit and 283 investigators trained in Cybercrime	Most of the officers have computer related qualifications before receiving in service training and attending various training programs that are recognized by the Ministry of National Education.	No field offices but utilises services of trained investigators	X-ways Forensic and Encase.

Name	Number of staff	Qualifications	Field offices	Software available
France: Cybercrime division (Gendarmerie)	21 people at the central level and 220 investigators in the field offices	The gendarmerie's bachelor degree on cybercrime, advanced training in law, computer science, computer and network security.	No	Various Internet connections, computers adapted for Internet investigations. Forensic equipment (forensic laptops, XWays, mobile phone analysis tools. Specialised software for Internet surveillance (P2P, Web). Various software for the collection of evidence online.
Ireland: Garda Computer Crimes Investigation Unit	16 people (forensic and investigators)	Most have a Masters Degree in Forensic Computing and Cybercrime investigation from University College Dublin, Centre for Cybersecurity and Cybercrime Investigation. (UCD CCI)	No	Forensic network, most normal CF tools and a separate internet network
Kosovo*: Cybercrime Investigation Unit	5 Officers		No	
Luxembourg: Section Nouvelles Technologies	4 engineers, 4 operators 2 police investigators, 1 secretary	Medium to very high. Members of the unit follow training given abroad	No	Open source software, X-Ways, FTK, XRY and CELLEBRITE
Mauritius: Information Technology Unit -IT Unit	35 police staff	Diploma in Computer Science, degree in computer science, MSC Computer Security & Forensics training in cyber crime investigation from collaboration with other countries or private companies	No	Encase, FTK and Cellebrite
Montenegro: cyber crime specialists of Division for Combating Organised Crime and Corruption	No separate specialised unit	No separate specialised unit	Yes, 21	Forensic Centre: Encase
Romania: Cybercrime Unit	28 in the central unit and 150 in the field offices	Law degree and computer degree	Yes	EnCase, FTK, X-ways, Mobile Edit
Romania: Cybercrime Unit (Prosecution)	5 in the central office and one prosecutor within each territorial structure	Law degree	Yes	
Serbia: Special Prosecution Office for High Tech Crime	3 prosecutors, 2 advisers and 2 administrative staff			
Spain: Brigada de Investigación Technologica (BIT)	45 people. 20 in every operative section and 5 in the support section	Not any special requirement is needed to join the unit. People with university studies in computing have preference.	Yes	Forensic duplicators, write blocking devices, analysis workstations
"The former Yugoslav Republic of Macedonia": Cybercrime Unit	7 staff		No	X-ray tool kit and various other tools

5 Functions and responsibilities

This section of the study examines the different functions and responsibilities that exist in the creation of a capability to combat criminal use of technology, and in particular the development of a cybercrime unit. The functions of such a unit will be at both the strategic and tactical levels. The role of the cybercrime unit should be clearly identified within a national cybercrime strategy, now seen as a key requirement to be developed in all countries.

At the strategic level a cybercrime unit may have an ongoing role in the development of:

- National legislation on cybercrime
- National cybercrime strategy
- National cybercrime prevention programmes
- Development of national system for reporting of criminal activity.
- Cooperation at the national and international level, both with public and private partners
- Intelligence analysis and dissemination
- Defining guidelines for investigations
- Developing training strategies at the national level
- Assessment and analyses of cybercrime phenomena, which informs the above.

At the tactical level, the unit may be responsible for the following activities either as a core function or a secondary function based upon the requirement for the use of the knowledge and skills of the staff of the unit:

- Coordinating and conducting Investigations
- Collection, examination and analysis of digital evidence within the forensic science framework of the country
- Coordination of regional/territorial units.
- Specialised support to other non cybercrime police units
- Practical Interagency Cooperation
- The private sector
- Internal cooperation
- Delivering training to other LE staff and those within the wider CJS (Criminal Justice System).
- Identifying equipment requirements of the primary and regional units

5.1 Strategic responsibilities

As can be seen from table 3 below, the common denominator for all countries is that the cybercrime unit has a role to play in the development of strategies, policies and legislation at the national level, while some of the tactical matters are dealt with in different locations within police organisations depending on the national requirement and capability.

5.1.1 Contributing to national legislation on cybercrime

Developing the correct levels of cybercrime legislation is the foundation upon which all other national and cooperative activities described elsewhere in this study are based. Without the legislation being in place, the other activities will not be able to be implemented. The specialists of the cybercrime unit should contribute to the drafting of national legislation in the area of cybercrime. As an example of the need for this involvement, in many countries, due to a lack of understanding of the issues, by legislators, certain cybercrime offences are not considered predicate offences for organised crime conditions to be met. This subsequently creates problems in countries where law enforcement relies on organised crime provisions to investigate or prosecute cybercrime.

A good example of the inclusion of cybercrime specialists in the drafting the legislation is Montenegro, where officers of the Police Directorate can give proposals to the amendments of the Criminal Procedure Code and Criminal Code, participate in working groups and participate in round tables to contribute to the shaping of the proposed national legislation governing issues relating to cybercrime.

Similarly the cybercrime unit of the Brazilian Federal Police contributed to the Brazilian cybercrime law proposal at the Congress and to the Internet regulatory act for civil purposes. In the Czech Republic, the ITCS contributes to the preparation of legal regulations.

In short, the practical experience of specialists from cybercrime units needs to be taken into account when legislation is drafted.

5.1.2 Contributing to a national cybercrime strategy

In order to protect Critical National Infrastructure, other assets as well as the well being and safety of citizens against the threats offered by cybercrime and other technology related criminality, it is essential that national cybercrime strategies be developed. The practical knowledge and experience of cybercrime personnel, is also essential to be included in the development of national policies and strategies on the prevention and control of cybercrime, as well as when defining strategic cyber security objectives to ensure the protection of critical infrastructure.

In Mauritius, the representatives of IT Unit participated in the task force/working group for the preparation of the security chapter of the National ICT Strategic Plan for Mauritius, conducted by the Ministry of ICT.

The Attorney General’s Office, the Ministry of Defence and the Ministry of Communications of Australia are currently working on the “white paper”, that is, a document that is to serve as a "comprehensive blueprint" to allow Australians to be confident online. The document will be released in the first half of 2012. The paper would look at consumer protection, cyber-safety, cybercrime, cyber security and cyber defence, and will build on the government's existing 2009 Cyber Security Safety Strategy.

The Council of Europe – under its Global Project on Cybercrime – in 2011 prepared a discussion paper that proposes the elements that should typically be part of a national cybercrime strategy.

5.1.3 Prevention

Any national strategy for cybercrime should include prevention as one of the key aspects. The practical experience of cybercrime units should inform this activity in order that the correct information and countermeasures may be delivered to those affected. The specialised unit should pay special attention to the prevention of cybercrime, by joint activities with mass media or the private sector, or by specific projects that help the public and private companies better understand the phenomenon and protect themselves.

Phenomena of cybercrime spread rapidly and affect societies around world and so does information about these types of crime. However, there are a lot of types of cybercrime that are less well known to the public but still have major impact. Prevention and public education is therefore essential.

Prevention campaigns should be set up as a cooperative effort of cybercrime units, other governmental departments and the private sector.

For example, in Belgium, police units for cybercrime and trafficking in human beings carry out prevention measures for the safety of internet users in collaboration with Child Focus (European centre for missing and sexually exploited children). The cybercrime unit undertakes also campaigns with the economic department of the government and with Western Union and the Association of Banks for the prevention of credit card fraud and other types of fraud on internet.

In Cyprus, the Office for Combating Cyber Crime gives lectures and seminars to different social groups and schools for the purpose of educating the public and preventing crime. Similar measures are taken in Belgium, Romania, Ireland and Montenegro and certainly other countries.

In France, the specialised unit in the Gendarmerie is working mainly on crime they identify on the Internet. In this respect the work is innovative, in line with the evolutions of the practices on the Internet and preventive more than reactive.

Prevention programmes should provide assurance that police units are able to deal effectively with cybercrime issues that may be reported to them by the public as well as businesses and other who may be affected.

5.1.4 Development of national systems for reporting of criminal activity

Systems for cybercrime reporting are useful instrument to allow victims to report crime in a fast and efficient manner, it is a way of ensuring that crimes are directed to the correct unit for investigation and it reduces the time needed to initiate investigations. It furthermore allows cybercrime units to understand and react to emerging threats.

The system must be advertised, known and easily accessible. It must be part of the promotion activity of the cybercrime unit. It is essential for assessing awareness of the phenomenon and for providing feedback to victims.

This system may include e-mails, telephone numbers, fax numbers, online reporting systems, which have to be acknowledged by the national law as a means of notification/reporting, so that the data received can be means for initiating investigations.

For example www.ecops.be (Belgian governmental contact point for internet abuse) is a point of reporting. The appropriate services are informed and reply to the person reporting.

5.1.5 Cooperation at the national and international level

The transnational nature of cybercrime means that for any national response to be effective, national and international cooperation must be a major part of the role of a cybercrime unit. Working within national and international legislation, agreements and protocols, the unit should establish relationships with other law enforcement agencies as well as other criminal justice and industry players. In particular, it is essential for effective working relationships to be created with Internet Service and content providers. Further detailed information on relationship building is provided in the section of the report dealing with tactical issues (p. 29). The importance of enabling these relationships and the building of trust in the fight against cybercrime cannot be overstated.

An example of the importance placed on this may be shown by the fact that in 2008, the Octopus Conference of the Council of Europe adopted "guidelines[1] for the cooperation between law enforcement and internet service providers against cybercrime". These guidelines contain:

- Common measures (including protection of rights and freedoms), such as:
  - Develop a culture of cooperation
  - Develop written procedures for cooperation with each other
  - Cooperate for the protection of rights and freedoms of individuals
  - Respect each others' roles, rights and limitations
  - Mindful of cost of cooperation
- Measures to be taken by law enforcement, such as:
  - Broad and strategic cooperation with ISP
  - Procedures for legally binding requests
  - Designated and trained personnel for cooperation
  - Verification of source of requests
  - Standard request format
  - Specificity and accuracy of requests
  - Follow preservation orders with production/disclosure orders
  - Criminal compliance programme
- Measures to be taken by service providers, such as:
  - Report criminal incidents
  - Assist LEA with training and other support
  - Procedures for responding to requests
  - Designated and trained personnel for cooperation
  - Emergency assistance outside business hours
  - Criminal compliance programme
  - Verification of source of requests
  - Standard response format
  - Explanation for information that is not provided.

5.1.6 Intelligence analysis and dissemination

Collecting data and information not only serves strategic and intelligence purposes, in that it helps understand crime phenomena and trends but also operational, investigative purposes.

The information to be collected, analysed and disseminated for use in the area of cybercrime prevention and detection shows specific characteristics.

The means and sources for data collection are primarily those specific to the police, to which open sources are added, such as mass-media or the Internet. It should be considered that other sources of information such as government and industry sources are extremely valuable and should be utilised. In the case of cybercrime, the data and the places from which it may be retrieved are different from other types of crimes.

When collecting intelligence and information about cybercrime it is important to take into consideration new forms of cyber crimes, new modes of operating, new computer systems and tools, or new payment services.

[1] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/lea_isp/default_EN.asp

The creation and maintenance of databases related to cybercrime as well as statistical analyses by specialised units serves operational and intelligence functions.

Statistical reports provide indicators on the evolution of the crime phenomenon during specific periods of time. They also serve as a tool for an assessment of the performance of cybercrime units.

5.1.7 Defining guidelines for investigations

Although guidelines for investigations are often drawn up at the local level, the transnational nature of cybercrime and traditional crimes in which digital evidence is involved, mean that it is important that guidelines incorporate plans that will enable evidence to be exchanged between jurisdictions with no impact on their admissibility. For this reason it is necessary for guidelines to be developed at the national level for the conduct of investigations. The experience of the cybercrime unit should be heavily utilised in the creation and maintenance of these guidelines, which should be revisited at least once a year.

These guidelines are in addition to national legislation – in particular substantive law and the investigative measures foreseen in the criminal procedure code (some of which are rather specific as to the handling of electronic evidence such as in Montenegro).

These guidelines and procedures take the form of practical manuals and guidelines for performing various types of investigations. They need to be drafted by experienced investigators from cybercrime units. Examples of these types of guidelines are:

- Luxembourg, where the cybercrime unit elaborated a "Vademecum" for seizing electronic evidence that is handed out to every investigator
- France, where the specialised unit of the Gendarmerie is responsible for drafting internal procedures.

The work procedures are based on the national legislation and the practical experience accrued in carrying on investigations. They should provide the steps to be followed during investigations or the collection and analysis of digital evidence (computer forensics).

The defined procedures are helping tools for observing the legal framework, for ensuring proper performance during investigations and the safe collection of electronic evidence, as well as for training and protecting personnel.

Another important procedure is how to define which demands or cases get priority. As many countries suffer a lack of staff, they need to set priorities. A clear procedure and criteria for ranking cases by priority would be very helpful.

5.1.8 Delivering training programmes

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.

Training should therefore not be limited to the officers of the cybercrime unit. It should be in the interest of the unit that also officers of other departments have at least basic knowledge of cybercrime investigations. Furthermore, the training of judges and prosecutors in cybercrime is something that staff of the cybercrime unit should become actively involved in.

The continuous training of its own staff but also of other services should be considered an essential function of a cybercrime unit.

Different countries have their own approaches to cybercrime training for other units. As an example, in Cyprus the educational programmes on cybercrime are integrated in the basic training at the Cyprus Police Academy. According to the same principle Belgium set up a response reference network at the different local police units. Besides organising and teaching of these courses, they also participate themselves in national and international courses e.g. from private security firms or training programmes from Interpol, Europol, OLAF, FBI, IACIS, etc.

Best practice from Croatia

The Ministry of the Interior of Croatia, the Ministry of Science, Education and Sports of Croatia and the Croatian Academic and Research Network – **CARNET** have concluded an Agreement on Cooperation in Prevention and Resolving Computer Incidents and other Aspects of Cybercrime. Some of the benefits of the agreement are the organisation of training events, workshops and other types of education with the content adapted to the needs of the Ministry of the Interior.

Other examples of how countries have dealt with training are:

- Spain has developed his own training programme for the police officers working in the cybercrime area.
- In Mauritius there is a training centre that runs training programmes around the year in small batches on the handling of cybercrime cases and of digital evidence to all ranks of police officers and to all units/ braches of the Mauritius Police Force.
- Luxembourg gives short training to the local police unit on how retrieves evidence on the internet (yahoo, messenger, Microsoft), so they can handle on their own offences by means of computer systems.

In order to ensure a coherent approach, each country should develop a training strategy to create a workforce that is able to fulfil its functions at each level within an organisation. Within the framework of the CyberCrime@IPA project such law enforcement training strategies are being developed for countries and areas of South-eastern Europe.

Any training strategy should comprise a number of elements. The first one should be the justification for such a strategy. This 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

The objective of the training strategy is to be defined. It could typically be formulated as:

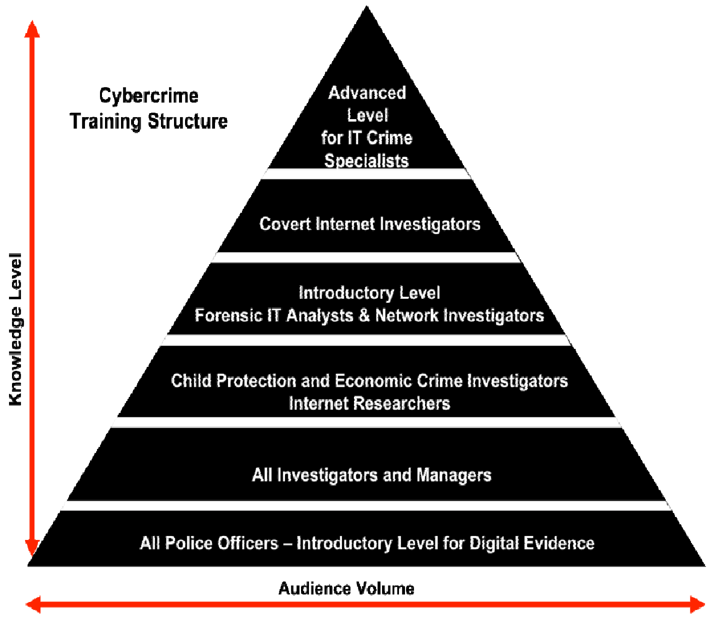
- To ensure that LEA agencies/officers have the skills/ competencies necessary for their respective functions to
  - investigate cybercrime,
  - secure electronic evidence
  - and carry out computer forensics analyses for criminal proceedings
  - assist other agencies
  - as well as contribute to network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

Considerations should include sustainability, standardisation, certification, institutionalisation, efficiency, scalability etc.

The next part of a strategy should deal with training requirements (training needs analysis).

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.

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 in cybercrime 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.


Cybercrime Training Structure
Advanced Level for IT Crime Specialists
Covert Internet Investigators
Introductory Level Forensic IT Analysts & Network Investigators
Child Protection and Economic Crime Investigators Internet Researchers
All Investigators and Managers
All Police Officers – Introductory Level for Digital Evidence
Knowledge Level
Audience Volume

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.

The cybercrime unit will have a key role in advising training academies on the development of training programmes at all levels, as well as using their knowledge and expertise in delivering training to members of staff.

5.1.9 Assessment and analyses of cybercrime phenomena

Understanding the cybercrime phenomena is essential for national strategies and policies to be effective. The cybercrime unit must be able to present analyses and assessments of cybercrime phenomena at the request of decision makers.

Such analyses and assessments will help decision makers and legislators understand the phenomenon and raise awareness of the risks of cybercrime. Parts of the assessment and analysis provided by the unit can also be used in public campaigns aimed at the education of citizens and other preventive measures.

In addition, based on these assessments and analyses, the unit can contribute proposals aimed at reducing risks, increasing counter-measures and creating the legal and institutional basis to fight cybercrime. Changes in technology may require new legislation to be introduced and this requirement may be properly informed by analysis of the effect of these changes on cybercrime by the police cybercrime units.

The following sections deal primarily with issue that relate to the tactical considerations of establishing a law enforcement cybercrime unit and the practical aspects of the work that the unit will undertake.

5.2 Tactical responsibilities

The following sections deal primarily with issues that relate to the tactical considerations of establishing a law enforcement cybercrime unit and the practical aspects of the work that the unit will undertake.

5.2.1 Coordinating and conducting investigations

One of the main tasks of the specialised cybercrime unit is the investigation of cybercrime. In this regard most of the cybercrime units that were analysed as part of this study are capable of carrying out investigations of crimes committed against and/or through computer systems, including crimes such as online child pornography and copyright offences.

This includes:

- Identification and investigation of criminal facts
- Identification and investigation of cybercrime suspects
- Identification of the source and target computer systems in criminal activities
- Investigation through the Internet, including undercover operations.

Table 3: Responsibilities

Name	Investigating offences against computer systems	Investigating offences by means of computer systems	Forensic analysis	CERT responsibilities	Other tasks
Albania: Sector against cybercrime	Yes	Yes	No, the Forensics is within another department	No	Takes part in the Joint Investigation Units
Australia: Cybercrime Operations	Yes. But also specialist units within State and Federal Police Law Enforcement in accordance with the attached schedule of legislation	Yes. But also specialist units within State and Federal Police Law Enforcement in accordance with the attached schedule of legislation	Separate branch of the Australian Federal Police	No. CERT at the Attorney General's Department	Yes. Policies, internal procedures, international cooperation, training
Austria: Unit 5.2 Computer Crime of the Criminal Intelligence Service	Yes	No. This is with Criminal Intelligence Service Austria Department 3 and 7	Department 5 Computer Crime Unit	No	Yes. Policies, internal procedures, international cooperation
Belgium: Federal Computer Crime Unit	Yes. But also Regional Computer Crime Units	All police units supported by FCCU & RCCU's	Federal Computer Crime Unit + Regional Computer Crime Units	No. CERT.be, Belgian Milcert	Yes. Policies, internal procedures, , international cooperation, training etc.
Bosnia and Herzegovina (Republika Srpska): Department for High-tech Crime	Yes	Yes	Yes, also done by the Forensic Centre	No. CERT is being established within Agency for IT society	Policies, internal procedures, international cooperation
Brazil: Computer Forensic Unit of the Federal Police	No. Responsibility with BFP Cybercrime Unit	No. Responsibility with BFP Cybercrime Unit + other BFP or state police units	Yes. And with field offices and State police or State Forensic Institute	No. CERT.Brazil, National Government CSIRT	Yes. Policies, internal procedures, international cooperation, training
Croatia: specialised officers of the Organised Crime Department and Economic Crime and Corruption Department	Yes	Yes	Yes	Yes	Yes. policy, internal procedures, training, international cooperation, etc
Cyprus: Office for Combating cybercrime	Yes	Yes	No. With Computer Forensic Examination Lab	No. Implementation of a CERT is the responsibility of the commissioner of Telecommunications and Postal Regulations	Yes. Policies, international cooperation, training
Czech Republic: Information Technology Crime Section	Yes, but also local police units according to a procedure code	Yes, but also local police units according to a procedure code	No. Forensic institute of Prague or an external private forensic expert	No	Yes. Contribution to legal regulation and internal rules, when in preparation, coordination of the international cooperation, etc

Name	Investigating offences against computer systems	Investigating offences by means of computer systems	Forensic analysis	CERT responsibilities	Other tasks
Finland: Cybercrime Intelligence Unit, Cybercrime Investigations Unit, Crime Laboratory	Cybercrime Investigations Unit, Local police units	Cybercrime Investigations Unit, Local police units	Cybercrime Investigations Unit or Crime laboratory, Local forensic units	No. CERT-FI	Yes. Policies, internal procedures, training, international cooperation, training
France: Police Nationale	Yes	Yes (except Child pornography, racism and xenophobia).	Yes	No	Yes. Contribute to National Policies, international cooperation, training of other LEA etc.
France: Cybercrime division (Gendarmerie)	Cybercrime Division	Cybercrime Division	Cybercrime Division	No	Yes. policy, internal procedures, training, international cooperation, etc
Ireland: Garda Computer Crimes Investigation Unit	Garda Computer Crimes Investigation Unit	Garda Computer Crimes Investigation Unit and other units The specialised unit does not carry investigation on IP offences and child pornography	Garda Computer Crimes Investigation Unit	No	Yes. policy, internal procedures, training, etc
Kosovo*: Cybercrime Investigation Unit	Yes	Yes	No, the forensics is done by IT forensics Section	No	N/A
Luxembourg: Section Nouvelles Technologies	Section nouvelles technologies	every police unit	Section nouvelles technologies	No but strong collaboration with the Luxembourg CSIRT/ CERT	Yes. Internal procedure, internal cooperation, training
Mauritius: Information Technology Unit -IT Unit	IT Unit	IT Unit	IT Unit	No	Yes
Montenegro: cyber crime specialists of Division for Combating Organised Crime and Corruption	Division for Combating Organised Crime and Corruption	Division for Combating Organised Crime and Corruption	Forensics Centre at Danilovgrad	No. Planned at the Ministry for Information Society and Telecommunication	Yes. Policies, internal procedures, training
Romania: Cybercrime Unit	Cybercrime Unit	Cybercrime Unit	Cybercrime Unit	No	Yes. policy, internal procedures, training, international cooperation, etc
Romania: Cybercrime Unit (Prosecution)	Yes	No. Only internet fraud, intellectual property right violations, misuse of credit card information, credit card fraud, credit card forgery offences if committed by the organised crime groups and child pornography on the Internet	No	No	Yes. policy, internal procedures, international cooperation, etc

Name	Investigating offences against computer systems	Investigating offences by means of computer systems	Forensic analysis	CERT responsibilities	Other tasks
Serbia: Special Prosecution Office for High Tech Crime	Yes	Yes	No, forensic analysis is done by other institutions in accord with the CPC.	No	Yes, policy, internal procedures, training, international cooperation, etc.
Spain: Brigada de Investigación Technologica (BIT)	BIT - Intern policing. There is a specialised group on investigation of hacking, defacements, damages on computer data	BIT - There are groups specialised on the investigation of frauds, child pornography, piracy, and threats.	Brigada de Investigación Technologica - in the investigations conducted by the unit and cooperates with other units if it is necessary	No	Yes. policy, internal procedures, training, international cooperation, etc
"The former Yugoslav Republic of Macedonia": Cybercrime Unit	Yes	Yes	No, the forensic analysis is done by another Unit in the MoI	No	Yes, policies, internal procedures, training, international cooperation etc.

Depending on the legal system, a prosecutor may be supervising or leading the investigation. While the actual activities of the police are the same, they should be approved by the prosecutor.

Cybercrime investigations bring their own challenges to the Criminal Justice System. One example of a practical problem arising in the course of an investigation is that several offences may be investigated in one case, but not all of these may be in the responsibility of the cybercrime unit. In this case the prosecutor is the one to decide about who will continue the investigation.

In other cases, an offence may start as a non-cybercrime investigation, but later on additional offences against computer systems or data are discovered. Again, it is the prosecutor who decides who will be in charge to continue the investigation, unless there are clear provisions in law.

A further responsibility for cybercrime units is to coordinate investigative activities that take place in different parts of the country or involve other jurisdictions.

5.2.2 Collection, examination and analysis of digital evidence within the forensic science framework of the country

As in any other investigation of criminal offence the investigation of cybercrimes usually involves collecting evidence and its analysing it under controlled forensic conditions. The difference is that during the investigation of cybercrimes (computer crimes) the evidence that is collected is often digital evidence that may be compromised if not handled correctly and in a timely fashion. It is therefore essential that law enforcement develops and maintains the ability to collect and analyse electronic/digital evidence. It is for each country to decide if it wishes to create a specialised unit within its core forensics institute or department, or whether it gives the task of dealing with all forms of digital evidence to the cybercrime unit.

In some countries there is a move to further professionalise the way in which digital evidence is dealt with and introduce a requirement for traditional forensic methods and structures to be used. For example, in the United Kingdom, a forensic regulator has been appointed to introduce forensic science standards for all evidence, including digital evidence that is used in the criminal justice system. This also involves the accreditation of any organisation involved in that work. More information about the work of the regulator may be found at: www.homeoffice.gov.uk/agencies-public-bodies/fsr/

There is no doubt that cybercrime units will always require a capability to collect and deal with evidence that emanates from their investigations. This is particularly so in cases where volatile or other vulnerable evidence is present at the scene of an investigation and which needs dealing with to prevent compromise or destruction of potential evidence. There are questions as to the advisability of digital evidence from all types of investigation being sent to a cybercrime unit for processing. The extent of backlogs in some countries where this policy is adopted should be considered a potential downside.

In practical terms, the focal point of computer forensics is the computer system, either the computer as the target, the one used to commit crime or in the possession of a witness to a crime involving technology. For that reason, law enforcement must have the appropriate resources for computer forensics, with adequately trained personnel having access to appropriate specialised software and hardware.

For its own investigations, the unit should develop its capacity to examine compromised computer systems in order to identify logs and traces of perpetrators, as these are often the only ways to identify them. The identification of the computer used for crimes must be quick because the logs and the traces are volatile and maintained only for a short period of time. The examination of computers belonging to suspects is helpful for the identification and clarification of the way the crimes were committed.

Furthermore, the technical ability for authorised and lawful access and interception of computer systems is a technical component that needs to be created. Technical solutions and operational methods for such activities need to be developed as these are ways to collect evidence, sometimes the only ways, in case of cybercrime. In Romania, there are a large number of cases (illegal computer access and internet fraud offences) in which the wire tapping of internet connections was the best technique applied to identify a suspect and his criminal activities and associates.

Law enforcement agencies (LEA) use a number of special investigative techniques including techniques such as the wiretapping/interception of communications (phone, email, Skype, VOIP etc) in their investigations. In many case these special investigative techniques are an essential instrument for the investigators.

The swift development of the ICT has turned the technology into the main communication tool for criminal groups. Internet, mobile phone, SMS, MMS, VoIP, is often the only means the criminals use to communicate.

The border between mobile phones and devices and computers is disappearing. This generates increasing demands to analyse mobile phones. Most specialised units carrying out computer forensics also do mobile forensics with specialised software. In Cyprus mobile phones (and CCTV) are analysed by a different department (Scientific and Technical Support Department), while computers are being analysed by the Office for Combating Cyber Crime (Criminal Investigation Department).

In case of offences against computer systems, interception of communications and access to the victim's computer by LEA can provide crucial information on the way the system was attacked (malware, Trojan, which can continue to work after the attack). In cases of child pornography, access to the offender's computer can give information on the contacts of the offender, the network he or she is part of, the websites visited etc.

Interception of Internet communications is a specific and very technical area, and the investigator must be able to interpret the results and depending on the tools used, the data intercepted must be made readable and workable for the investigator.

Every country should put in place appropriate legislation to govern the use of special investigative techniques regardless of how important these techniques are and the results they provide for the investigation. It is very important that actions by law enforcement is authorised by the law and subject to supervision. The Budapest Convention on Cybercrime has set a number of safeguards (article 15) which aim to protect the human rights and liberties based on the domestic law of each party.

In addition to the legal possibility for such activities, the technical capabilities need to be created to deploy such investigative means.

There are situations where these activities are technically carried out by separate specialised services of different authorities (Ministry of the Interior, Intelligence Services, National Police).

In Belgium, it is the responsibility of the Central Technical Interception Facility (CTIF) within the Directorate of the Special Unit, to execute an interception. This Unit collaborates with the operators (phone, IAP, ISP) to put in place the interception. But it's the unit in charge with the investigation who has to analyse the results. The CTIF is just in charge of technical aspect.

5.2.3 Coordination of regional/territorial units

The coordination of regional/territorial units is an important responsibility.

From an operational perspective it is important to coordinate territorial structures in order to avoid parallel investigations and inefficient use of human, financial and logistical resources.

Countries with territorial cybercrime units include Australia, Belgium, Brazil, Montenegro, Romania and Spain. The Cybercrime Unit in Romania has 15 field offices. The field offices are administratively subordinated to the central unit but they are independent in terms of initiating and conducting the investigations.

Central units usually have a coordinating function, but the role of central units can also be limited to providing training and equipment.

5.2.4 Specialised support to other non cybercrime police units

With most "traditional" offences containing elements of electronic evidence or involving computer systems, law enforcement officers investigating these offences often require technical support from cybercrime units.

This may include assistance in computer forensics, identification and localisation of IP or e-mail addresses, authorised lawful access to computer systems or computer data interception.

For cybercrime units which do not themselves have investigative competencies, such technical support is a primary part of their work.

The IT Unit in Mauritius assists and provides digital forensic expertise to other governmental agencies (such as the Information and Communication Technology Authority - ICTA, the Independent Commission Against Corruption - ICAC, The Mauritius Revenue Authority - MRA) to attend to the scene of crime and execution of search warrants where electronic equipment is suspected to be found.

In Brazil, the most frequent cases in which the Computer Forensic Unit provides technical support are bank fraud, child abuse, calumny/slander by means of computer systems (especially using social networks such as Orkut or Facebook).

5.2.5 Practical interagency cooperation

Effective cooperation among all institutions involved in preventing and controlling cybercrimes is a key factor for success as operational and strategic levels. The cybercrime unit has a key role to play in ensuring such cooperation among public institutions.

The main objectives of interagency cooperation are:

- identification of criminal groups/subjects
- crime reduction
- efficient use of resources
- rapid channels of communication
- successful prosecutions and convictions.

Cooperation is required with many public private and international organisations. The following information seeks to provide some practical advice on how cooperation my take place with different bodies.

Other departments of the police force

Internal regulations within each police force provide for responsibilities of and relations between different units. However, often the jurisdiction of units is not clearly defined and it is difficult to decide which one is responsible for continuing the investigation of a given case.

The goal of cooperation is to exchange information and provide support to each other. When a cybercrime unit is not allowed to use special investigative means, other units that have the authorisation may need to come to perform them. Or conversely, if another unit requires a computer forensic analysis, the cybercrime unit may perform this specific task in support of another unit. Or different units carry out joint investigations.

The Ministry of Interior

In most cases, a cybercrime unit is part of the police which in turn is subordinated to the ministry of interior. A cybercrime may thus contribute to the drafting of national strategies or legislation through the ministry of interior.

The ministry may also make additional resources available for a specific investigation, provide access to databases and strategic information or coordinate preventive activities.

Prosecution Service

Cooperation with the prosecution services is essential, not only in systems where prosecutors are leading the investigation. In the final analysis, it is less the number of investigations, but that of successful prosecutions and adjudication that serves as performance indicator.

In some countries, governments have set up specialised prosecution units for cybercrime or have appointed prosecutors with subject-matter knowledge, such as in Serbia or Romania. In Belgium, a network of ICT and cybercrime reference magistrates was set up, one at the Federal Prosecutor’s office and one per local Prosecutor’s office. In this way the cyber crime cases are mostly handled by a magistrate with knowledge and experience in the matter.

Joint training programmes for police and prosecutors not only increase skills, but also facilitate practical cooperation. Law enforcement specialised units should collaborate with prosecution departments in their efforts to create specialised prosecution units, where this is considered appropriate.

Ministry of Justice

Cooperation between cybercrime units and ministries of justice facilitate the drafting of legislation harmonised with international standards, the preparation of other regulations or the drafting of national cybercrime policies and strategies. It is essential with respect to international judicial cooperation.

The judiciary

The role of the judges during the investigation differs from one judicial system to another. They are usually involved in the investigation by issuing authorisation for certain investigation activities, such as searches, interception of communications and other measures.

Cooperation of a cybercrime unit with the judiciary can help improve reports on an investigation and electronic evidence and help judges obtain a better understanding cybercrime issues. It may be practical to draw up some guides or glossaries explaining phenomena of cybercrime and technical terms.

Specialists of the cybercrime may contribute to the training of judges. And both judges and staff of cybercrime units should be trained regarding the presentation and admissibility of electronic evidence in court.

Intelligence services

Intelligence services in many cases have access and can provide key information on cybercrime for both operational and strategic purposes. They may also provide additional resources in an investigation.

In Romania, for example, expertise on cloned credit cards is provided by a research institute of the intelligence service.

Intelligence services also have an important role in the drafting and implementation of cyber security strategies aimed at the protection of critical infrastructure.

Incident response teams (CERT/CSIRT)

Computer Emergency or Computer Security Incident Response Teams (CERT/CSIRT) and specialised cybercrime units have distinct roles when it comes to questions of cybercrime and cyber security.

The role of the CERT/CSIRT is to respond to cyber threats especially when these threats are directed at critical national infrastructure, while a cybercrime unit has criminal justice functions. The role of a CERT/CSIRT in a country can be complementary to the activities and responsibilities of a cybercrime unit. Thus, cooperation between a cybercrime unit and a CERT/CSIRT is important at several levels, including the sharing of information and know how, monitoring of trends in cyber attacks and incidents, or support during joint actions. Cooperation may also include prevention, training and national security measures.

However, CERT/CSIRT functions are different and independent from those of a cybercrime unit.

CERT-s

For **example** the CERT of Australia is attached to the Attorney General’s Department, while in Brazil the National Government CSIRT is attached to the President’s office.

In Mauritius, the CERT is found under the National Computer Board of Mauritius which does not actually have investigative powers, thus cases where criminal actions are suspected, are referred to the Police specialised cybercrime unit.

The methods of cooperation, exchange of information and response to requests should be defined by the heads of the CERT/CSIRT and the cybercrime unit.

5.2.6 The private sector

One essential factor for the success of a cybercrime unit is cooperation with the private sector. Partnerships must be created to the benefit of both parties. In most of the countries surveyed. cybercrime units have contacts and cooperate with private partner, on a case-by-case basis rather than by memoranda of understanding.

A more structured approach to cooperation with the private sector should be sought. For example, the cybercrime unit in Belgium has quarterly meetings with the Belgian card issuing banks. Other examples include the Irish Bankers Federation High Tech Crime Forum, or Information Sharing and Analysis Centres (ISAC) for the financial sector in the USA, Netherlands and other countries.

Such cooperation not only helps investigate cybercrime but also contributes to prevention of cybercrime and trust in ICT to the benefit of both sides.

Cooperation between cybercrime units and service providers is crucial since both play essential roles in building trust and confidence in information and communication technologies, in protection users and their rights, and in minimising the use of services for illegal purposes. Cybercrime investigations are often not effective without the cooperation of service providers.

At the same time both have different roles: law enforcement must uphold the law while providers are to provide users with the ability to communicate. Cooperation must therefore respect their different roles and in particular must be designed to protect the rights of users.

A culture of cooperation between law enforcement and service providers will help the private sector understand the limits and the necessity of investigations, as well as how cybercrime units operate.

It will allow cybercrime units receive data and information that are necessary for efficient operations as well as obtain a better understanding of attack trends.

And finally, the knowledge, experience and technology of private sector companies may help train and equip cybercrime units.

5.2.7 International cooperation

Cybercrime and electronic evidence often have a transnational dimension. International cooperation is thus a priority task of a cybercrime unit but at the same time one of the most difficult areas.

From the perspective of a cybercrime unit, international cooperation comprises the following:

- creating channels and mechanisms of cooperation
- ensuring efficient preservation and exchange of data
- understanding trends and evolution of transnational cybercrime
- establishing the unit as a reliable and trusted counterpart of foreign partners
- participating in international cybercrime efforts, including regulatory efforts
- preparation of guidelines to overcome the obstacles and facilitate cooperation
- ensuring efficient utilisation of existing channels of cooperation
- ensuring cooperation with institutions responsible for judicial cooperation (prosecution service, ministry of justice).

A cybercrime unit should not only cooperate with foreign law enforcement bodies, but also with international organisations and multinational private sector organisations.

At the operational level, international cooperation should allow exchange of data and information, evidence provided by other countries and joint operations. It relies on the legal procedures and instruments of cooperation, but also very much on trust between partners.

Channels of cooperation most often used include Interpol, Europol, foreign liaison officers based in one's country, and 24/7 points of contact.

Cybercrime units need to be flexible and use the channel that is most suitable in a given situation.

24/7 points of contact should be used in cases of urgency, in particular for the preservation of data in a foreign country. In many countries, the cybercrime unit is the 24/7 point of contact. A network of contact points has been established by the G8 High-tech Crime Sub-group, and has also been included in the Budapest Convention on Cybercrime (article 35).

It should be underlined that police to police cooperation is essential, but it cannot replace the formal mechanisms of judicial cooperation. Cybercrime units must therefore also interact at the domestic level with the competent authorities for international legal cooperation (prosecution services and ministries of justice).

24/7 points of contact

According to the Budapest Convention, 24/7 points of contact should have the following functions and responsibilities:

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network

Table 4: 24/7 point of contact

	Does the Unit serve as 24/7 point of contact?	If the Specialised Unit serve as 24/7 point of contact, can the following measures be directly carried out by the Specialised Unit?						
		Provision of technical advice to foreign authorities	**Preservation of data**	**Collection of evidence**	**Provision of legal information**	**Locating of suspects**	**Sending/receiving/ execution of judicial cooperation/mutual legal assistance requests**	**Other**
Albania: Sector against cybercrime	Yes	No answer	No answer	No answer	No answer	No answer	No answer	
Australia: Cybercrime Operations	Not the Unit, but the AFP has a 24/7 point of contact to facilitate cooperation	Only within 5 eyes community (Australia, Canada, New Zealand, UK and US)	Only with MAR	Only with MAR	On a case by case basis	If warrant exists and extradition is sought	On a case by case basis	
Austria: Unit 5.2 Computer Crime of the Criminal Intelligence Service	Yes	Yes	No	Yes	Yes	Yes	No (BK SPOC single point of contact)	
Belgium: Federal Computer Crime Unit	Yes	Yes	Yes	Yes	Yes	Yes. Requires international assistance request	No. Via magistrates, Ministry of Justice	
Bosnia and Herzegovina (Republika Srpska): Department for High-tech Crime	No	Not applicable	No applicable	No applicable	No applicable	No applicable	No applicable	
Brazil: Computer Forensic Unit of the Federal Police	Yes	Yes	Can be facilitated	Yes	Can be facilitated	Can be facilitated	Can be facilitated	
Croatia: specialised officers of the Organised Crime Department and Economic Crime and Corruption Department	Yes	Yes	Yes	Yes	Yes	Yes	Yes. Only through the proper channel	
Cyprus: Office for Combating cybercrime	Yes	Yes	Yes	Yes. Requires official request	Yes	Yes. Only for intelligence purposes	Yes. Only through the proper channel	

	Does the Unit serve as 24/7 point of contact?	If the Specialised Unit serve as 24/7 point of contact, can the following measures be directly carried out by the Specialised Unit?						
		Provision of technical advice to foreign authorities	**Preservation of data**	**Collection of evidence**	**Provision of legal information**	**Locating of suspects**	**Sending/receiving/ execution of judicial cooperation/mutual legal assistance requests**	**Other**
Czech Republic: Information Technology Crime Section	Yes	Yes	Partly(1)	No. Any collection of evidence can be provided only via MLA	Yes	Partly(1)	No	Not applicable
Finland: Cybercrime Intelligence Unit, Cybercrime Investigations Unit, Crime Laboratory	No. Contact point is SIRENE office with who they have constant communication	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
France: OCLCTIC(2) (Police)	Yes	Yes	Yes		Yes	Need rogatory letter	Yes	
France: Cybercrime division (Gendarmerie)	No	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Only through the proper channel	
Ireland: Garda Computer Crimes Investigation Unit	No	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	On a case by case basis, MLAT is needed	
Kosovo*: Cybercrime Investigation Unit	No	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	
Luxembourg: Section Nouvelles Technologies	Yes	Immediately	An order of a national magistrate is necessary. Foreign authorities have to contact our magistrates.	An order of a national magistrate is necessary. Foreign authorities have to contact our magistrates.	An order of a national magistrate is necessary. Foreign authorities have to contact our magistrates.	An order of a national magistrate is necessary. Foreign authorities have to contact our magistrates.	An order of a national magistrate is necessary. Foreign authorities have to contact our magistrates.	Not applicable
Mauritius: Information Technology Unit -IT Unit	Yes	They act by responding promptly	Yes, on a case to case basis	Yes, on a case to case basis	Yes, on a case to case basis	Yes, on a case to case basis	Yes, on a case to case basis	
Montenegro: cyber crime specialists of Division for Combating Organised Crime and Corruption	No. Contact person at the Dep. for the fight against org. Crime	Until now, there were no requests from foreign	(*)	(*)	(*)	(*)	(*)	(*)

	Does the Unit serve as 24/7 point of contact?	If the Specialised Unit serve as 24/7 point of contact, can the following measures be directly carried out by the Specialised Unit?						
		Provision of technical advice to foreign authorities	**Preservation of data**	**Collection of evidence**	**Provision of legal information**	**Locating of suspects**	**Sending/receiving/ execution of judicial cooperation/mutual legal assistance requests**	**Other**
	and corruption	authorities. (*)						
Romania: Cybercrime Unit	Yes	Yes	Yes	Yes	Yes	In cooperation with other units of the national police if the proper request exists	No	
Romania: Cybercrime Unit (Prosecution)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Serbia: Special Prosecution Office for High Tech Crime	Yes	No. This is done by MoI	Yes in cooperation with Investigative Judge and ISP	No. It is done by MoI	Yes	No	Yes	
Spain: Brigada de Investigación Technologica (BIT)	Yes	Yes	Yes	Yes	Yes	If possible and in cooperation with other units of the national police	No	
"The former Yugoslav Republic of Macedonia": Cybercrime Unit	Yes (recently nominated)	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	

(1) From the end of March 2011 the data related to electronic communications are not available, by reason of a decision of the Constitutional Court of the Czech Republic

(2) Office Central de Lutte contre la Criminalité Liée aux Technologies de l'information et de la Communication (OCLCTIC)

6 Steps towards the creation of a specialised unit

6.1 Step 1: Assessing needs and making a decision

The first step for the setting up of a cybercrime unit is that decision makers understand and recognise the phenomenon and impact of cybercrime. The benefits of having a well functioning cybercrime unit and its expected results should be recognised and included in a national cybercrime strategy, in order that the creation of the unit is a key aspect of the strategy.

An assessment or needs analysis should be carried out of the type of unit required, of the functions it should have and of the most suitable institutional setting and internal structure (see the previous chapter of this study).

6.2 Step 2: Establish the legal basis

It is necessary to have provisions in the national law as well as internal norms for the creation of the cybercrime unit as stated earlier.

It is recommended that the national legislation define the criminal offences and the procedures for investigations in accordance with international standards in this field. The Budapest Cybercrime Convention could serve any country as a guideline in this respect (www.coe.int/cybercrime).

Countries must ensure that the legislation provides for the investigation of cybercrime offences as such. This means that all forms of cybercrime can be prosecuted on their own, and not only as predicate or secondary offences of organised or other types of crime.

Due to the nature of the tasks that specialised units need to perform, there is a need for a specific legal basis which provides the mandate and the authority of this unit and precisely describes the role and responsibilities of this unit in the investigation of various crimes in accordance with the national legislation or on the basis of international conventions to which the country is a Party.

Due to the nature of cybercrime and the fact that many of the crimes are regional or international in nature it is required that the legislation foresees a number of safeguards and conditions that protects the users of computer networks against arbitrary law enforcement actions but also protects the officers that are acting in their official capacity during the investigation of cybercrime.

Furthermore, procedural law should regulate special investigative means or techniques to be used by police units. Thus, for the investigation of some offences, communications can be intercepted or undercover investigators can be made use of. If such techniques are foreseen for cybercrime, specialised units need to have access to such resources.

It may also be necessary to set up rules for the cooperation with the private sector: Are they obliged to cooperate by law? Is cooperation free of charge or may they claim compensation (such as for preserving data)? What type of data do they need to retain or preserve and what are the conditions for law enforcement requesting the production of data or other evidence?

The law should provide for the admission of electronic evidence in court. Procedures need to be put in place on the handling of electronic evidence. Investigators and forensic experts need to adhere to these regulations to make evidence admissible in court proceedings.

The legislation should in addition enable international cooperation and authorise the unit to cooperate with similar units of other countries.

Finally, the legislation in place should provide guidelines and define the relationship of the unit with the prosecution, the judiciary, service providers, academia and others.

6.3 Step 3: Appointment of the manager of the cybercrime unit

The person appointed must be able to understand the phenomenon, have managerial skills and experience in law enforcement activities, and preferably have experience in the investigation of cybercrime or cases connected to cybercrime or electronic evidence.

It is advisable that this person has knowledge of computer technology and speaks foreign languages given the need to represent the unit at international levels and given the transnational nature of cybercrime.

6.4 Step 4: Staffing the unit

The assessment carried out at the outset may have determined the number and type of staff required, but this may subsequently be subject to modification by decision makers and to the availability of resources. Experience also shows that units may be small in the beginning but evolve over time.

The officers working in the cybercrime unit will need to be carefully selected and included in ongoing training programmes. The officers need to have knowledge of computers, Internet, police investigations, legislation governing cybercrime, and foreign languages. Depending on their function they have specific qualifications, mostly in criminal investigation and ICT.

Depending on the size of the cybercrime unit and its jurisdiction and tasks, the selection process must take place within a reasonable period of time and have as criteria the skills and integrity of candidates.

The structure of the cybercrime unit has to be considered and a distinction is to be made between the officers who will perform investigations in various areas and the officers who must not only have knowledge about computers and legislation, but also subject-matter knowledge.

For example, the personnel to investigate child pornography on the Internet will have to also have knowledge of psychology and investigations related to minors or those following intellectual property crime knowledge about intellectual property rights.

A practical problem that arises is the method for recruiting and the source for recruiting the personnel for investigations or computer forensics. The private sector may have many qualified experts. However, public salaries are usually not competitive enough to attract them to serve in a cybercrime unit. On the other hand, many young police officers may know about computers and be motivated, but they may not have sufficient investigative experience.

Fluctuation of personnel is a major problem affecting cybercrime units. Over time, the best investigators often move to private companies with much higher salaries. This is a reason to keep selecting new officers, preferably young ones that are computer passionate, and to provide them with ongoing training courses.

For staff dealing with computer forensic different selection criteria apply. They must be specialised in this work, but they do not necessarily have to be police officers.

Thus, the following should be considered:

- Specialists vs. generalists: national units tend to employ more specialised personnel. In a local unit a specialised generalist is often preferred
- Employed civilian experts vs. police officers: is it easier to train a technician to think like a police officer or vice versa?
- Programmers: on a daily basis there is a need for quick-and-dirty one time solutions e.g. for extraction of non-standardised data using customised scripts
- Analysts: especially for intelligence purposes close cooperation between cybercrime specialists and analysts is proven gainful
- Technicians: offloads the specialists by managing the internal networks and equipment
- Administrative personnel: offloading administrative duties from specialists will obviously lead to the most cost-effective utilisation of their expertise
- Outsourcing/consultants: is it legal in your country to outsource investigative or forensic tasks? Beware of sensitive data and possibly illegal content, such as related to child abuse.

Employing the right mix of staff and roles in a unit and finding the right individuals is a challenge for any branch. Clear job descriptions and proper evaluation of candidates, including practical tests, are recommended.

6.5 Step 5: Training programme for the unit

This section deals specifically with the training needs of the specialised unit rather than the national training strategy and support for other players within the criminal justice system. These are dealt with in section 5.1.8 above.

Most specialised units organise training on cybercrime and digital forensics for their staff. Some countries offer training on related crimes e.g. falsified credit cards (Montenegro), skimming devices (Belgium), child pornography (Montenegro), selling of psychoactive substances on the Internet (Montenegro), or advanced internet investigation training of Interpol (Cyprus). Brazil even has e-learning courses. All these countries work towards and need the staff of the specialised units to be well informed and educated.

The success of any specialised unit that is created will depend on the knowledge, skills, education, and the hard work of the people who will staff the unit. In the area of cybercrime, the level of training required to become an effective operative is lengthy, continuing and sometimes expensive.

Staff of the unit will have varying requirements for training depending on their roles within the organisation, for example a digital forensics technician will require different training than an investigator responsible for cyber-attacks.

There are, however, some similarities in the training and it is appropriate for each to have an understanding of the others’ work. At the introductory stage, it is appropriate for all unit staff to receive basic training on digital forensics and network investigations. Once the unit is established it will be necessary to identify a training path for each member of staff that will support the needs of the unit.

These initial training courses should be organised for the personnel right after the selection process and even in a partnership with private companies, financial institutions and law enforcement agencies from abroad. There are training courses developed by various police structures and it is better to use them at this training stage rather than try to develop new courses.

It is recommended that a learning portfolio be created for each member of staff that will enable a full record of an individual's learning and training to be maintained. One of the main reasons for this is to provide evidence during judicial proceedings of an individual's competence in this area of work.

It is vital that each member of staff follows a program of continuing professional development (CPD) once their core training has been completed. The changes in technological advance are so great that it is not possible to assume that someone trained in year one is still competent in year three, if they have not followed a CPD program. This may take the form of additional training, attendance at relevant conferences and workshops and exchange visits with other similar units in other jurisdictions.

6.6 Step 6: Equipment and other resources

The tasks and priorities of the unit will determine the equipment needed. The rapid evolution of software and hardware on the one hand and techniques for committing cybercrime on the other hand; means that the equipment needs to be at the cutting edge of technology and continually updated. This requirement often exceeds the financial resources allocated to a police unit. As the user base for cybercrime specific software is rather small, commercial software tends to be expensive. Thus, OSS (open source software) and software created by law enforcement for law enforcement only e.g. via the international law enforcement cybercrime community should be considered.

Once the manager of the cybercrime unit has been appointed, it is his or her task to establish a 'business plan' for the setting up of the unit. The manager can perform a SWOT-analysis, prepare up a mission statement, and describe the tasks, the equipment, staff and training required.

A reasonable budget has to be allocated to this unit, based on the personnel costs, costs of the necessary equipment and software, as well as the costs of using special techniques of investigation (undercover investigations, etc) and a provisional budget for the update of the software and equipment.

The budget must also include prevention activities, cooperation with the private sector and international cooperation as well as the training of the members of the unit.

There is a clear incentive for criminals to commit cybercrimes as well as their potential to purchase sophisticated equipment for the commission of these crimes. This shows and justifies the great needs for equipment and its continuous updating for the cybercrime unit.
The technical nature of cybercrime makes it impossible to perform investigations without the appropriate equipment and knowledge.

It is important to have in place the minimum equipment necessary before the unit begins its operations, so it is able to perform its tasks (equipment for computer investigations, equipment for digital forensic and Internet connections).

The equipment required for the use of special investigation techniques, prevention projects, creation of databases, applications needed for certain investigations, could be acquired after the date of the unit set up.

The allocated budget must be uninterrupted and regular, so the unit can plan ahead and make previsions to follow the technical evolution.

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

- adequate space for computer equipment;
- secure storage for exhibits
- sufficiently powerful computers for workers;
- overt and covert Internet connections;
- necessary software and devices for forensically processing computer systems and other devices;

The necessary equipment and software should be related to computer systems investigations, digital computer forensic activities, undercover operations through the Internet, lawful access to computer systems, databases operation, lawful interception of computer systems, etc. For example:

- Workstations are not the same as that an IT-department normally provides. Users must have full administrator access on their workstations
- Digital forensic examinations require special hardware e.g. write-blocking devices.
- Extreme storage capacity is needed
- UPS (Uninterruptable Power Supply) is required to avoid possible data corruption or loss in case of power outages.

A normal lifecycle for the IT-equipment organisations is around three years. Equipment for digital forensic examinations have a shorter lifecycle; around 12 to 18 months for digital forensic workstations. Hard drives, internal or external, should be treated as consumables similar to CDs.

During an examination there is often a need for certain adaptors, special cables etc. These are relatively small expenses and it is advised to keep petty cash available for the immediate purchase of these items.

6.7 Step 7: Independence of and knowledge about the unit

Similar to other police units, the cybercrime unit must be efficient and able to react to the realities of cybercrime. For that it has to be independent in deciding upon the investigations to be performed and the operating means.

It has to be able to decide which tools to use for the collection of data and information, how it organises controls and how it works with other institutions, such as police, prosecutor, courts, etc.

To achieve all these, they should be provided in the internal norms and procedures of the police department where the cybercrime unit is included.

The role of the cybercrime unit needs to be known by other police departments and by the public.

This unit must be visible and credible for its role in supporting other police units and for developing a relationship of trust with the public, in particular so that confidence is created in the unit as an effective resource for the reporting of crimes by victims.

6.8 Step 8: Action plan and evaluation mechanisms

From the very beginning of the cybercrime unit, a plan should be designed covering the activities to be performed by this unit. Priorities and key areas of activity should be established in a way that they can be evaluated and that the achievement of goals can be assessed.

The process of setting up the cybercrime unit must follow a plan that states the main goals to be achieved within a reasonable time frame.

After the creation of the unit, other areas must be developed to respond to operational or strategic needs.

The evaluation of this unit should be periodic, assessing the achievement of objectives and the response to cybercrime.

The managers of a cybercrime unit must pay permanent attention to the need of adjusting the cybercrime unit’s size, competences, responsibilities, in order to have it in line with the development of cybercrime.

For example, there can be an arising need for developing the computer forensic capacity, the investigation of child pornography, credit cards fraud investigations or to develop subordinated territorial units. In Ireland, the issue of having territorial units is under consideration.

The more decisions makers understand about the need for the creation of the specialised unit, the more they will support the unit.

If the main steps - legislation, personnel, training, equipment – are taken before the unit is to be operational, the actual organisation of the unit will be more efficient.

7 Practical issues affecting the functioning of cybercrime units

There are day to day issues that impact on the ability of cybercrime units to function effectively. The report gives a number of instances where this occurs. These issues are not solely in the domain of the cybercrime unit and will require action by others within the cyber world, such as legislators and those responsible for international cooperation to solve. The following are such examples.

Non-criminalisation of "criminal" activities

Since there cannot be a crime without a law, units are only allowed to investigate conduct criminalised under domestic legislation.

There are cases where the law does not criminalise certain conduct, either because the conduct is new or linked to existing criminal offences. For example, phishing and identity theft are not criminalised in the Romanian legislation, other types of offences are used in order for investigations to be conducted, such as computer fraud attempt.

The non-criminalisation of some offences makes the initiation and performing of investigations more difficult and the collection of necessary evidence more difficult.

Legal procedures not corresponding to practical realities

There are instances identified in certain countries where the procedural law in place does not allow for the specific challenges that are encountered in technology related crime.

As an example, in Romania, the procedure for computer searches requires the presence of witnesses and the owner of the computer.

In practice this activity can take much time due to the complexity of the case or to the size of a digital storage device. The activity may have to cease or new authorisations obtained over and over again for the same activity. Therefore, the proposed new penal legislation excludes the requirements of witnesses under certain circumstances.

Another example is authorised, lawful access to a computer system or online searches. In some situations, a computer searched is online and the connected system or the data are located in a foreign jurisdiction where it is not clear in which one or where the location is known, the legal requirements in that country are not known. Also, it may be unclear whether an authorization is issued for a single access or for multiple accesses and also for a future period.

Unclear competencies

It is important to have regulations that define the criteria for the jurisdiction or competencies of police units with cybercrime duties. This is to avoid parallel investigations and inefficient use of resources by different departments.

For example, in Croatia, the investigative competence for intellectual property right violation and computer fraud belongs to different units of the Economic and Corruption Department and of the Organised Crime Department.

In Romania, it is not clearly regulated at the police level which unit is responsible for the investigation of credit card fraud when the police receive a case, except for cases of fraud involving organised criminal groups. With regard to the prosecution of such offences, the situation is clear.

The departments responsible therefore took internal decisions to assign the competencies (Criminal Investigation Department and Organised Crime Department) within the police.

Another practical issue relates to actions through the Internet which are not considered as offences, such as spam, posting personal data, calumny, etc. In such cases, the victims do not know exactly who to address in order to have this information removed and to identify those responsible.

Although there are national agencies with competences in these areas, most of the times the police is notified to investigate such cases, although it often doesn’t have such competence.

Insufficient or out of date equipment

A frequent practical situation which influences the results of the investigations is related to the absence of necessary software or equipment for performing some computer searches over new types of storage devices, mobile phones, IPAD, IPHONE, etc or to proceed with some special investigative technique, like authorised access of computer systems and interceptions.

On-line reporting system

The online reporting instrument like www.efrauda.ro from Romania is very helpful not only for domestic reports but also for the victims from other countries that submit their complaints to the appropriate agency and receive a feedback that somebody investigates the case.

Cost of the investigations

Some jurisdictional systems are based on the principle of compulsoriness – i.e. all reports must be investigated, irrespective of the prejudice or the cost of investigation (e.g.: the Romanian jurisdictional system). Others are based on the principle of opportunity – i.e. investigations will take place only for deeds of certain gravity or with a high prejudice (e.g.: the UK jurisdictional system).

The main reason for the distinction between these jurisdictional systems is the cost of the investigations.

Both systems have weaknesses, as huge amounts of resources might be required for investigating minor facts or some investigations are not initiated at all, even though one may never know the importance or the complexity of an investigation from the very beginning.

The differences between the national jurisdictions systems also affect international cooperation, because there are situations when requests for cooperation sent to a country will not be investigated because it does not fulfil the legal requirements (e.g. UK will not provide assistance for investigations on internet fraud on cases in which the cost is less than 5000 Pounds).

Form and content of the first report

The content, form and evidence supporting the reported facts, are very important for the first steps of the investigations.

When the reports are incomplete or are received by untrained officers, time and essential evidence are wasted and it is possible to misunderstand the nature of illegal activities.

For example, in case of a computer attack against the servers of a company, the logs have to be obtained and access must be granted to the compromised system. The victims should provide the necessary information in order to identify the traces left by the perpetrators.

In such cases, the first issues to be cleared are the place where the logs are kept and the administrator of the servers. There has to be cooperation with the person responsible for logs administration, for the purpose of establishing exactly what computer systems, software applications were targeted or used for the illegal activities.

When the report is received by an untrained person, all the above aspects are not known to him and there is danger to lose evidence.

It can be practical to draw up some prototype reports with a clear explanation of the phenomenon e.g. botnet, command & control-server, that can be put at the disposal of all cybercrime investigators.

Cooperation with victims

Whenever illegal activity in the area of cybercrime is identified and victims need to be contacted for obtaining data, reports and other pieces of evidence, it must be taken into account that sometimes individuals of companies do not wish to file reports because the effect on their reputation.

For example, in a case of unauthorised access followed by blackmail for not publishing personal data, victims are reluctant to work with the police as they do not wish to be identified as having insecure systems.

It is useful if it is possible to reach an agreement between authorities and victims (as in the UK), where the authorities are bound to keep data concerned in the case or discovered during investigation, in a confidential manner, in order to avoid media or business impact.

Letter of request for public institutions and private companies

The format and transmission of letters of request to institutions or companies must follow legislation and legal reasoning; otherwise difficulties may arise in understanding the importance of the request or of the information to be provided.

There may be a situation where a request, which doesn’t observe the legal form of addressing, is not answered by the institution or the private company. It will have to be reformulated, wasting time and resources or even losing evidence.

In the relation with these institutions, it is important to have a prioritisation of the requests according to the nature of requested information and importance of the case.

For example Microsoft as well as Google and Facebook have an urgency procedure wherein a request for identification/ip-localisation can be provided within a few hours (in normal circumstances it takes a few days). This procedure is foreseen for cases with threat of life or risk of injury. Several countries e.g. Belgium and France use this urgency procedure.

Sometimes, companies wish to have a single point of contact from which request can be sent. So, they are sure that its origin is known. In that case, local units send their request to the contact point (which should be the cybercrime unit), so it can make a quality control on the request before resending it to the companies.

The Guidelines for the cooperation of law enforcement authorities with service providers developed by the Council of Europe is a useful tool to be implemented at domestic level. (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp)

Collection of electronic evidence

When computer data storage units, servers, mobile phones etc. have to be collected for analysis of the content, attention must be paid to the fact that this should be done in a manner which does not affect their condition and that there is no additional alteration to the data. They must be sealed and safely transported. The environment and the storage room is important for not compromising the seized equipment.

At the moment of collecting such evidence, photos should be taken, for identifying the place where they were found, their functioning status and even the existence of fingerprints or DNA, which can be later used for identifying the users.

An internal procedure for this process has to be drafted and distributed to all investigators who are required to follow this procedure as well as to the training institutions for the training purposes to all the police units.

Often, in cybercrime and other cases, the evidence identified within computer systems is the only direct evidence identifying certain facts or persons.

Presentation of electronic evidence to the prosecutor/judge

A key aspect of the successful investigation is the way of drafting and presenting the documents concerning the administration of digital evidence to the prosecutor/judge by the police officers.

The way of drafting the documents and presenting the results of computer forensic examinations must observe the rules about the format and content provided by the law. For example the log files from a compromised computer server may not be readable by everyone.

There is need for computer knowledge in order to be able to read and understand if a computer was the source of the attack or it was used as proxy, or other machine in a botnet investigation.

The situation is more complicated when you have to present them to the prosecutor/judge in order to make some decisions within the case.

The results of the forensic activities/digital evidence should be presented in a clear manner, with the needed technical explanations, in a logical sequence, without interpretations. They have to be easy to understand by the prosecutors and judges who have usually less technical knowledge.

Evidence from foreign jurisdictions

An important challenge in the cyber investigation is to obtain the traces left by criminals in computer systems from abroad, as well as to obtain documents and exhibits. For investigation purposes they need to be provided in a very short period of time and through a direct and fast channel, but this is actually not happening very often.

We can offer the example of a phishing attack where the source and the target are in the same jurisdiction. Even so, there may be servers used for the attack or for data storage located in another jurisdiction.

The issue arising here, that is probably the most frequent one in cybercrime investigation concerns the channel and the form to get the needed information and evidence from another jurisdiction as quickly as possible.

For ensuring the exchange of information and evidence there are international instruments (rogatory commission, preservation requests, Police cooperation, etc.) but sometimes they require a long period of time before receiving an answer. Therefore, the long time required for drafting and sending rogatory letters, often makes it impossible for the beneficiary authority to use the information, as the evidence is no longer in the system.

Preservation requests

The 24/7 contact points, established according to article 35 of the Budapest Convention on Cybercrime, that are functioning in some countries (Croatia, Romania, Spain, Brasilia, Cyprus, etc.) are mainly used for sending preservation request in urgent cases.

Even within this network there are difficulties, due to the fact that the procedure of preservation requests is regulated differently in various countries and in most of the countries there is need for rogatory letters to be sent in order to obtain the information.

A specific problem is that a foreign preservation request is not followed up by a rogatory letter. This undermines the willingness of domestic authorities and service providers to cooperate in future cases.

8 Assessment and conclusions

8.1 Assessment

An increasing number of countries have separate specialised units that investigate cybercrime and carries out computer forensics. Units that were already created in the early 1990s have evolved over time. With cybercrime and other types of crime involving electronic evidence growing exponentially, it can be expected that more countries will establish such units and their size and scope of work will increase substantially in the future.

A key factor is the recognition by governments of the impact and relevance of cybercrime and electronic evidence and as well of the threat of cybercrime and cybercriminals to critical national infrastructure, national security, the functioning of corporations, and the well-being of citizen and protection of their rights. Governments realise that the rule of law needs to apply also in cyberspace that societies are dependent upon. Decision makers increasingly understand that investment in cybercrime units is justified.

Cybercrime units are increasingly called upon to assist other law enforcement and criminal justice authorities that are responsible for handling offences such as trafficking in human beings, sexual exploitation and abuse of children, drug trafficking and in fact any type of crime that involves computer systems, data or electronic evidence in one way or the other.

All of this implies that cybercrime units will need to evolve faster than other types of units. They need to become effective very quickly, remain pro-active and flexible and need to be well managed.

The units analysed as part of this study have all their strong points:

- Belgium has developed a strong recruitment and selection procedure. They have good experience in forensic ICT investigations in large environments and network and data analysis. They also have experience with cases of e-banking fraud and money mules. They undertook several botnet investigations and took down a number of botnet servers
- Brazil tries to process evidence as fast as they can to be compliant with legal deadlines
- Cyprus has located and transmitted information concerning the possession, offering or distribution of child pornography material on the internet to other countries and brought many cases before courts. They have good experience in giving lectures and seminars to different social groups and schools with the goal of educating the public and preventing crime. They also traced and saved four juveniles who expressed through the internet their intention to commit suicide
- Finland has a wide national and international mandate and they work with very qualified officers.

Weak points that are common to most units include:

- lack of personnel which results in a large back-log of cases
- lack of budget for training
- time-consuming and sometimes frustrating cooperation with third countries.

8.2 Conclusions

The purpose of this study is to help public authorities create or further strengthen specialised cybercrime units. The study is based on the actual experience of cybercrime units not only in Europe but also other regions of the world.

The following general conclusions may be drawn:

- The reliance of societies on computer networks, the evolution of technology, the realities of law enforcement and the evolution of the phenomenon of cybercrime underline the necessity of specialised cybercrime units

- The role and the way a cybercrime unit is organised and is functioning very much depend on how decision-makers understand and formulate the response to cybercrime

- Specialised cybercrime units are one important element of the response to cybercrime. Governments should formulate a comprehensive response to cybercrime possibly in the form of a cybercrime strategy. Cybercrime units can contribute to such a strategy http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf

- Personnel, equipment and training will remain challenges that cybercrime units of all countries have to face

- Cybercrime units need to be able to apply special techniques for investigations

- The performance of the specialised cybercrime unit depends to a large extent on:

  - quality of its staff and determination and motivation of its leadership
  - cooperation with prosecutors and courts and other agencies at the domestic level
  - cooperation with the private sector
  - international cooperation

- A cybercrime unit justifies its existence and the resources allocated if it can be positively assessed against the following indicators:

  - knowledge of the phenomenon of cybercrime, including typologies, risks and trends
  - enforcement and observance of national and international law in the area of cybercrime
  - investigations carried out and leading to prosecution and conviction of offenders
  - visibility, credibility and trust in the unit.

- Special cybercrime units will not be able handle all offences against or by means of computer systems or the analysis of electronic devices related to any crime on their own. Increasingly, cybercrime units will need to assist other police units and to provide them at least with basic know in cybercrime investigation and securing electronic evidence.

9 Appendix: Profiles of specialised units

9.1 Albania: Sector Against Cybercrime

9.1.1 Name and contact details

Sector Against Cybercrime
Ministry of Interior of Albania
Bulevardi "Bajram Curri"
Tirana, Albania
Fax +355 4 24 7156
Web: www.moi.gov.al

9.1.2 Functions, responsibilities and legal basis

The legal basis of the unit is Law nr. 9749 of 4 June 2007 "For State Police".

The unit is responsible for the investigation of offences committed against computer systems and data. The unit is responsible for the investigation of certain crimes committed by means of computer systems but not all types of crimes. For example the unit can investigate cases relating to child pornography on the internet, child abuse on the internet and computer fraud.

The sector does not have forensic responsibilities/capacities. This role lays within the Sector for Digital Evidence Examination in the Forensic Directorate.

The unit does not have CERT or CSIRT responsibilities.

The unit can also contribute to national policies on cybercrime and to design and implement training programmes for other police officers on cybercrime and electronic evidence.

The unit can engage in international police cooperation through Interpol channels, through liaison officers or on the basis of cooperation agreements.

9.1.3 Institutional set up and resources

The Sector Against Cyber Crimes is placed under the Directorate Against Financial Crimes at the Department Against Organized Crimes and Serious Crimes of General Directorate of State Police.

It was first established in June 2009 in the General Directorate of State Police and at that point was staffed by 3 police officers.

In June 2010, the number of specialists in this Sector was increased by two other police officers. At the same time, capabilities to investigate cybercrime were created in nine District Police Directorates, that is, in Tirana with three police officers and in Durres, Elbasan, Fier, Gjirokaster, Vlora, Lezha, Shkodra and Korca with one police officer respectively.

There are no special training programmes for the members of the Unit in Albania.

9.1.4 Interagency, public/private and international cooperation

Since 2009 in Albania were established seven Joint Investigative Units (JIU) which are operating in 7 major cities. These units are responsible for the investigation of corruption, economic and financial crimes and consist of representatives of the Prosecution office, police officer, tax representative, customs representative and a representative from the Intelligence Service. These JIU units also have the responsibility to investigate cases of cybercrime. As result when the Sector Against Cybercrime is carrying out an investigation relating to cybercrime the members of the JIU from other law enforcement departments are available to assist the Sector against cybercrime on any matter.

The sector against cybercrime is cooperates with other LEA in their investigations however this is regulated by internal procedures.

9.2 Australia: Specialist Units within the State and Federal Police

9.2.1 Name and contact details

Specialist Units within the State and Federal Police

Web: http://www.afp.gov.au/policing/cybercrime.aspx

9.2.2 Functions, responsibilities and legal basis

All units are part of policing agencies with mandate defined in legislation and by various State and Commonwealth Ministerial directions (see page 60 below for a schematic presentation of the structure in which the unit belongs). State and Federal Police are currently drafting guidelines on training and education requirements.

Each specialised unit within states and federal police is competent for offences against computer systems and for offences by means of computer system (fraud, identity crime). Each state get his own legislation, and the offences cover by the legislation are not always the same (for example, the use of false ID to commit offence is only included in the legislation of North Territory, Tasmania, Western Australia and South Australia).

The Units in Australia are authorised to contribute to the national cybercrime policies and have been involved in the drafting of a Government Cyber White Paper. In addition the Units are authorised to draft internal procedures, to coordinate field offices, take part in international judicial cooperation and to cooperate with International Organizations and LEA. The Units can design and implement training programmes relating to cybercrime for other police officers.

Each agency is responsible for its own computer forensic examination. None have their own laboratory but the Australian Federal Police houses dedicated forensics labs.

The CERT function in Australia rests with the Attorney General’s Department.

9.2.3 Institutional set up and resources

The Australian Federal Police has a specialist High Tech Crime Operations portfolio (HTCO) under an Assistant Commissioner, separate to the crime department. The investigations unit within the HTCO portfolio is called Cybercrime Operations.

Currently, there are three investigators and one support personnel in the Head Office, and seven investigators and two specialists that work from the regional offices. These regional/field offices are located in Sydney and Melbourne. The National Coordinator has the office located at the Headquarters in Canberra and the competencies of this coordinator are national.

9.2.4 Interagency, public/private and international cooperation

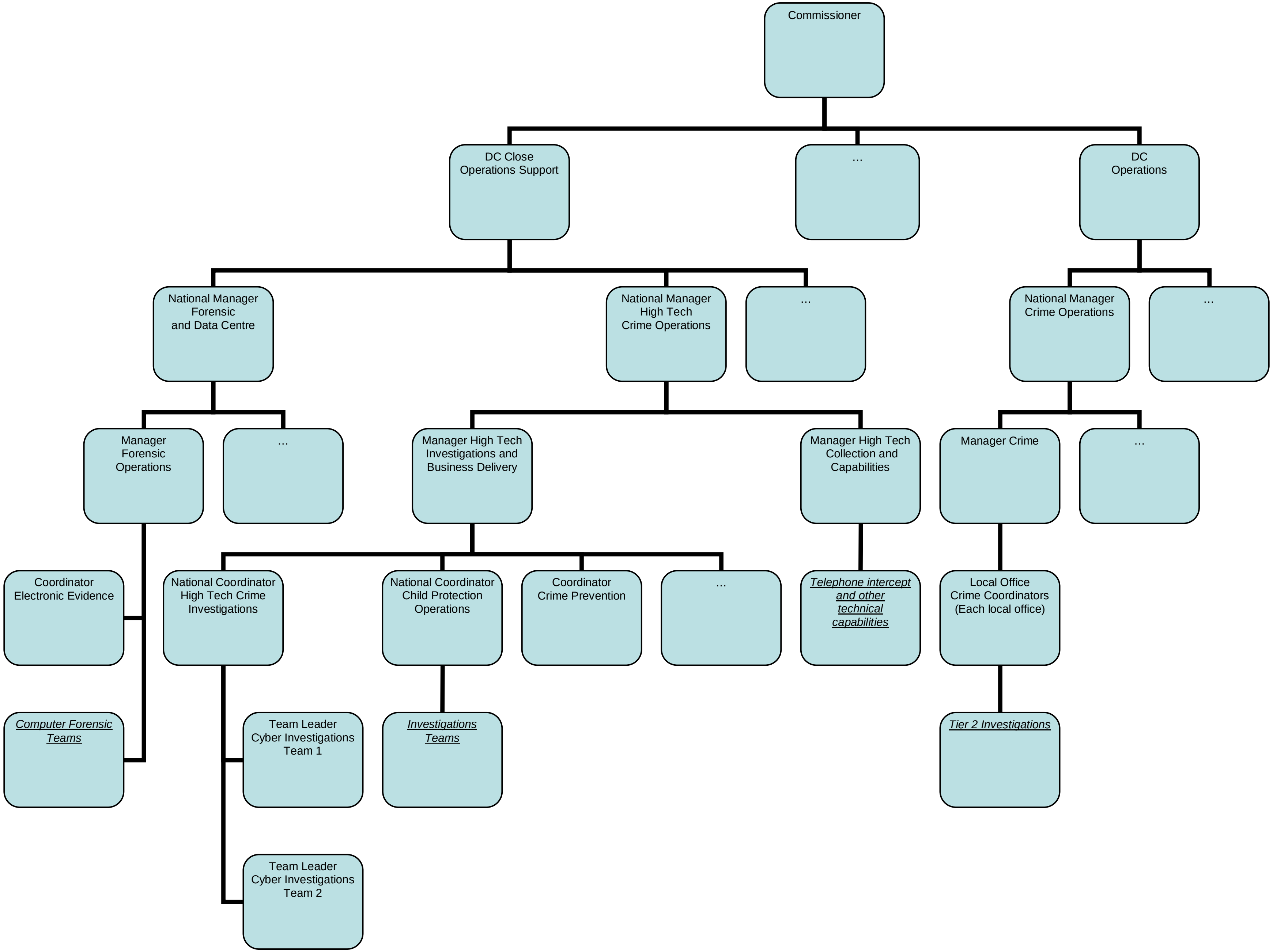
Australia is currently drafting protocols for law enforcement collaboration in Cybercrime.

The unit is not the 24/7 point of contact, but the Australian Federal police has her own 24/7 operations centre that acts as a facilitator for the international collaboration.

The Australian Government has not ratified the Budapest Convention on Cybercrime, however Australian authorities have taken steps towards changing legislation and the proposed new legislation is currently under review by the Parliament, these changes are in line with the Convention and foresee the requirement for preservation of data, improved international cooperation etc. Currently the only mean for international cooperation in this field is mutual legal assistance request, although in some cases there is sharing of intelligence on a case by case basis.

Currently the units have MOU with the Australian Bankers Association and have cooperation with the Internet Industry Association of Australia through the Child Protection Operations of the HTCO. There are ongoing negotiations with the financial institutions in relation to information sharing.

The Cybercrime Operations Unit (Investigations Unit within HTCO) cooperates with the members of the working groups on cybercrime within the 5 eye community (Australia, Canada, New Zealand, UK and USA).


Commissioner
DC Close Operations Support
…
DC Operations
National Manager Forensic and Data Centre
National Manager High Tech Crime Operations
…
National Manager Crime Operations
…
Manager Forensic Operations
…
Manager High Tech Investigations and Business Delivery
Manager High Tech Collection and Capabilities
Manager Crime
…
Coordinator Electronic Evidence
National Coordinator High Tech Crime Investigations
National Coordinator Child Protection Operations
Coordinator Crime Prevention
…
Telephone intercept and other technical capabilities
Local Office Crime Coordinators (Each local office)
Computer Forensic Teams
Team Leader Cyber Investigations Team 1
Investigations Teams
Tier 2 Investigations
Team Leader Cyber Investigations Team 2

9.3 Austria: Unit 5.2 Computer Crime

9.3.1 Name and contact details

Criminal Intelligence Service Austria - Unit 5.2 Computer Crime
Email: ccu@bmi.gv.at

9.3.2 Functions, responsibilities and legal basis

Functions and responsibilities

The Unit is responsible for the investigation of crime committed against computer systems, but not for the crime by means of computer systems (unlawful access, privacy of telecommunication, unlawful interception of data, damaging of data, interference in the functioning of a computer system, misuse of computer program, falsification of data, fraudulent misuse of data processing). The offences committed by the means of computer systems are investigated by the Criminal Intelligence Service Austria Department 3 and 7.

In 2010 the unit investigated a number of cases related to offences committed against computer systems. The table below shows the data based on the Austrian legislation

Criminal Offence		
Section		**2010**
§ 118a	Unlawful Access to a Computer System	79
§ 119	Infringement of the Privacy of Telecommunications	8
§ 119a	Unlawful Interception of Data	9
§ 126a	Damaging of Data	85
§ 126b	Interference with the Functioning of a Computer System	25
§ 126c	Misuse of Computer Programs and Passwords	78
§ 148a	Fraudulent Misuse of Data Processing	159
§ 225a	Falsification of Data	17

The unit is competent for the collection and analyze of the electronic evidence, and has its own forensic laboratory. The Unit coordinates and contributes to investigations led by other LEA (the regional police authorities).

The unit is also authorised to contribute to national policies on cybercrime, to draft internal procedures, to coordinate field office etc. The unit can take part in international judicial cooperation and can cooperate with International Organizations and other national LEA.

The legal basis for the functioning of the unit is the Federal Criminal law (Bundeskriminalamt Gesetz)

9.3.3 Institutional set up and resources

The Unit was set up in 2002 with the goal of the implementation of the criminal intelligence services. There are 3 subunits:

1) network crime,
2) computer crime and
3) mobile forensics.

The unit does not have field offices and is currently staffed by 17 experts who are qualified for criminal investigations, computer forensics. The personnel has also experience from ECTEG trainings.

In Austria, investigators use this software: ENCASE, X-WAYS, FTK, XRAY, CELLEBRITE

9.3.4 Interagency, public/private and international cooperation

The specialised unit contribute or coordinate investigation led by another regional police authority but they give no technical support.

The cooperation modalities with public and private sector are regulated by national law, and by the criminal code.

The international cooperation of the Austrian Specialised Cybercrime Unit is done through Interpol, Europol and Liaison-officers.

The unit is participating in ECTEG, ISEC, Interpol Working Party on Cybercrime, Europol, EUCTF.

9.4 Belgium: Federal Computer Crime Unit (FCCU)

9.4.1 Name and contact details

Federal Computer Crime Unit – FCCU
Direction economical and financial crime
Federal Judicial Police
Notelaarstraat 211 - 1000 Brussels – Belgium
Tel +32 2 743 74 74 - Fax +32 2 743 74 19
Head of unit: Luc Beirens

9.4.2 Functions, responsibilities and legal basis

Belgium has one Federal Computer Crime Unit (FCCU) at Central level and 26 Regional Computer Crime Units (RCCU's) at district level.

- In normal circumstances all offences committed against computer systems and data (e.g. illegal access) are handled by the RCCU's. FCCU can support and assist them whenever they need specialised competences or centralised equipment. The FCCU can handle autonomously cases whenever there is an urgent intervention needed or whenever there is an attack on critical information infrastructure.
- FCCU/RCCU's do not handle offences committed through/by means of computer systems (e.g. child pornography) but can give support (sometimes to a very large extent) for forensic ICT analysis and internet investigations.
- FCCU/RCCU's do collect and analyze the electronic evidence for the cases they investigate themselves and the cases in which they are in support of other law enforcement departments.
- FCCU is responsible for the training on cybercrime and/or electronic evidence for police officers, but also gives information session to magistrates, high schools, enterprises, …
- FCCU is responsible for the equipment of FCCU/RCCU's.
- FCCU is responsible for the online hotline www.ecops.be, a site where internauts can report online offences.
- FCCU gathers intelligence on cybercrime and creates an image on the phenomenon
- FCCU does not include a CERT but interact with it.
- FCCU does not have a specialised dustfree lab.

A Directive of the General Director of the Federal Judicial Police of 2002 on the organisation, requirements of the unit and administrative rules of the functioning of the Federal Computer Crime Unit and the Regional Computer Crime Units describes the two main functions: (1) combating ICT and telecommunication crime and (2) assistance for legal analysis of information and telecommunication systems in the framework of judicial cases.

A permanent note of the General Director of the Federal Judicial Police of 2005 describes the services and procedural rules in operational assistance of FCCU/RCCU's.

The College of General Prosecutors released two circulars on the theme, one about research and treatment of digital evidence (2004) and one on the cooperation between the federal prosecutor and the central directions of the judicial police (which describes that the FCCU in some cases can lead autonomously an investigation, 2009).

9.4.3 Institutional set up and resources

In 2001, 1 FCCU and 17 RCCU's were established based upon the integration of former central units in FCCU, and consolidation of existing regional specialists in RCCU's.

The Regional Computer Crime Units hierarchically and operationally do not depend on the FCCU but on the Judicial director of the district. They do depend on the FCCU for equipment and training. They must report all important cybercrime cases to FCCU.

There is a cooperation on ad hoc basis between FCCU and RCCU's. Annually there are 2 to 3 meetings with FCCU and all heads of CCU's. The FCCU has 35 staff members, RCCU's at the moment 140.

Every investigator disposes of equipment and software to make forensic copies and analyze them: Open source Linux tools, virtualisation software, XWAYS, FTK, XRAY, UFED and a pilot case backup station.

The Belgian police is hierarchically attached and accountable to the Ministry of Home affairs. The Federal Computer Crime Unit depends on the central direction of financial and economical crime of the federal judicial police. The regional CCU's depend on and report to the judicial director of the district, that in turn depends on the federal judicial police.

At the Federal Prosecutor's office there is 1 specialised cybercrime magistrate that is responsible for the serious cybercrime offences.

At the Local Prosecutor's offices there has been set up a network of ICT and cybercrime reference magistrates.

9.4.4 Interagency, public/private and international cooperation

A form for demand of assistance of RCCU/FCCU exists and needs to be filled in by the agency that needs the support of RCCU/FCCU. Different departments of police can ask assistance e.g. a local police department, at central level mainly department of corruption, organised economical and financial fraud, internal police investigations demand support

FCCU doesn't coordinate, lead or contribute to investigations involving LEA, but they do give them technical support.

Public partners are: BelNIS (Belgian information network security), IBPT (Institut Belge de services postaux et telecommunications), FSMA (Autorité des services et marches financiers), PNCT (Plat-forme nationale de concertation Télécommunication), CERT.be – Milcert.be.Private partners are: ISPA Belgium (identifications and localisations, traffic data, legal intercept, locking domain name DNS), Microsoft, Google, Facebook, credit card companies, Febelfin, Online auction and shopping websites, Child Focus, Netlog, Team CYMRU, Shadowserver.

International partners are: EU Cybercrime task force, ECTEG (European Cybercrime Training and Education Group), Europol cybercrime expert meeting, Interpol European working party on IT crime, EC Expert group on data retention, AWF Terminal, AWF Cyborg, CIRCAMP Project, EU-US WG Cybercrime Cybersecurity, MMFWG Mass Marketing Fraud Working Group.

FCCU has a national 24/7 permanency and is contact point for cybercrime incidents.

9.5 Bosnia and Herzegovina (Republika Srpska): Department for High Tech Crime

9.5.1 Name and contact details

Department for High Tech Crime
Criminal Police Administration,
RS Ministry of Interior,
Jug Bogdana 108, 78000 Banja Luka,
Republic of Srpska, Bosnia and Herzegovina
+387 51 331 289; fax: +387 51 331 287;
E-mail: vtk@mup.vladars.net
Website - www.mup.vladars.net; www.cyber-vtk.net

9.5.2 Functions, responsibilities and legal basis

The department for High Tech Crime is authorised to investigate crimes committed against computer systems and data as well as offences committed through the use of computer systems.

The department does not have CERT or CSIRT authority but works closely with the Agency which will take this role in the near future (CERT is currently being established in the Agency for IT Society in the Republika Srpska).

The unit doesn't have 24/7 responsibilities but is part of the ongoing reform in Bosnia and Herzegovina in relation to the 24/7 point of contact.

9.5.3 Institutional set up and resources

The High-Tech Crime Department was established on 1st of January 2010, but it become fully operational in July 2010 when the amendments of the Criminal Code in Republika Srpska were adopted in order to criminalise cyber crime in accordance with Council of Europe Convention.

The Department has three sections: Internet Investigations, Misuse of Digital Communication and Software, and the Digital Forensic (with laboratory).

Currently the department is staffed by 7 people who have been trained by participating in major international trainings and seminars. However it is considered that training is needed for further development of the department.

9.5.4 Interagency, public/private and international cooperation

The department has good cooperation with other departments in the law enforcement as well as with the prosecution services based on the criminal procedure law.

The department has concluded MOUs for cooperation with the major ISPs in the country.

The department mainly cooperates with other Law Enforcement agencies through the Interpol when it comes to international Law enforcement cooperation. In addition the unit has international cooperation that goes informally (directly) and formally through mutual legal assistance.

9.6 Brazil: Brazilian Federal Police Computer Forensic Unit – BFP CFU

9.6.1 Name and contact details

Brazilian Federal Police Computer Forensic Unit – BFP CFU
Phones: +55 61 2024 9813 / +55 61 2024 9810
Fax: +55 61 2023-9358
Email: sepinf.inc@dpf.gov.br
Head of Unit: Marcos Vinicius G. R. Lima

9.6.2 Functions, responsibilities and legal basis

The Brazilian Federal Police has established two units that are responsible for the investigation of cybercrimes and analysis of forensic evidence. The Computer Forensic Unit (presented here) is responsible, for the analysing of forensic evidence, its collection and in many cases for providing support to the Cybercrime Unit in its investigations.

The Cybercrime Unit is the primary agency responsible for the investigation of offences against computer systems and data as well as for the investigation of offences by means of computers.
The BFP CFU was officially created in 1996 and its duties are defined by an Internal Act from the General Director Office.

9.6.3 Institutional set up and resource

The BFP CFU is attached to the BFP Forensic Institute, which is subordinated to the Technical & Scientific Directorate, which is directly attached to the General Directors Office.

The BFP CFU was officially created in 1996, since 2002 they have had a strong increment of human and material resources due to the rising demand from BFP investigative teams.
At this moment the CFU (central office) has a team of 21 forensic examiners and 5 administrative personnel and counts 3 specialised sections:

- an operational section, which runs forensic examinations and supports investigations;
- a training section and
- a Research & Development section.

Every computer forensic investigator receives specialised training during Police Academy. They are equipped with FTK, Encase, Cellebrite UFED, XRY, Distributed Network Attack (DNA), CellDEK, Logicube Forensic Dossier, IDA Pro, VMWare and X-Ways.

Since 2007 BFP CFU had an investment of about USD 13.5 million in lab improvement, which means equipment, software and training for the BFP forensic examiners. Each BFP forensic field office (around 50) has a forensic toolkit that varies based on the field office size.

In 2010 around 9500 forensic examinations were done on electronic evidence related to various offences.

There are around 50 field offices with 170 forensic examiners in total. Most of the field offices have operational competence only. Some bigger field offices cooperate with the CFU for tool developing, training support and procedures

Some Brazilian states don’t have specialised cybercrime and computer forensic units. The state police and their forensic labs are also authorised to investigate cybercrime and analyse electronic evidence.

The Federal or State Prosecution Offices (depending on the fact if the crime is state or federal level) are responsible for the prosecution on cybercrime.

9.6.4 Interagency, public/private and international cooperation

There are no formal agreements or procedures directly with BFP CFU. Cooperation varies case by case.

The BFU CFU does not coordinate/lead investigations involving other law enforcement agencies. They have had cases in which they contributed to the investigation led by the state police and international LEA.

The BFU CFU participates at the Interpol Latin-Caribbean cybercrime Working Group and Interpol’s crimes against Children Working Group. They also join ICANN LEA meetings and Microsoft Child Exploitation Tracking System tool.

The BFP CFU has acts as the national 24/7 point of contact..

9.7 Croatia: Specialised officers

9.7.1 Name and contact details

ECONOMIC CRIME AND CORRUPTION DEPARTMENT
ORGANISED CRIME DEPARTMENT
www.mup.hr

9.7.2 Functions, responsibilities and legal basis

Croatia doesn't have a specialised police unit for cybercrime. Police officers specialised for this type of investigations are part of the Economic Crime and Corruption Department and the Organised Crime Department.

Therefore, for some crimes the competence to investigate lays with the Economic Crime and Corruption Department (Intellectual property right violation, Infringement of secrecy, integrity and accessibility of computer data, programs and systems, Computer Forgery and Computer Fraud) and for other crimes the responsibilities belong to Organised Crime Department (Intellectual property right violation and Computer Fraud) or other departments.

There were not enough data available to determine the responsibilities of the two departments.
The Economic and Corruption Department has also computer forensic functions in its investigations, although it doesn't have a specialised lab for this.

The specialised investigators of the Economic and Corruption Department have responsibilities in defining the national policy, drafting internal procedure norms and defining training courses. Police officers in Economic Crime and Corruption Department are also responsible for cyber incidents and emergency responses, but there is no CERT in the Ministry of the Interior.

9.7.3 Institutional set up and resources

In the Economic Crime and Corruption Department, General Police Directorate (state level) there are two police officers who are responsible for cyber crime and violations of IPR. In 20 Police Districts there are also Economic Crime Departments/Groups in which, depending of category, there are 2 – 4 police officers who are responsible for cyber crime and violations of IPR.

The training of the personnel is ensured through regular annual workshops on network forensics, which are organised in cooperation with CARN – Croatian Academic and Research Network (on the basis of Agreement of Cooperation).

9.7.4 Interagency, public/private and international cooperation

There is cooperation with other agencies and private entities for activities related to data collection and development of their own investigations, based on existing police regulations.

It also carries on international cooperation activities by participating in international events, and for the operative exchange of information it uses the cooperation channels of the Europol and Interpol.

9.8 Cyprus: Office for Combating Cyber Crime

9.8.1 Name and contact details

Office for Combating Cyber Crime
cybercrime@police.gov.cy
Nicosia

The official site of Cyprus Police is:
www.police.gov.cy
(Contains useful information regarding the Office for Combating Cyber Crime, prevention measures and other links for further information)

9.8.2 Functions, responsibilities and legal basis

Cyprus has an Office for Combating Cyber Crime and a Computer Forensic Examination Lab.

- The Office for Combating Cyber Crime investigates offences committed against computer systems and data (e.g. illegal access) and offences committed through/by means of computer systems (e.g. child pornography).
- The Office for Combating Cyber Crime is also responsible for the collection of electronic evidence. During investigations of serious cases the office is supported by the Computer Forensic Examination Lab for the collection of evidence. This lab does the forensic analysis of electronic evidence related to any crime.
- The Office for Combating Cyber Crime does not have CERT responsibilities, but reacts immediately with the investigation of cyber crime.
- The Office for Combating Cyber Crime gives lectures and seminars to different social groups and schools with the purpose of educating the public and preventing crime.
- Educational programs in the Cyprus Police Academy have started and are addressed at members of the Police. These programs will be integrated in the basic training.
- The Office also organises the Advance Internet Investigation Training of Interpol in the Cyprus Police Academy once a year.

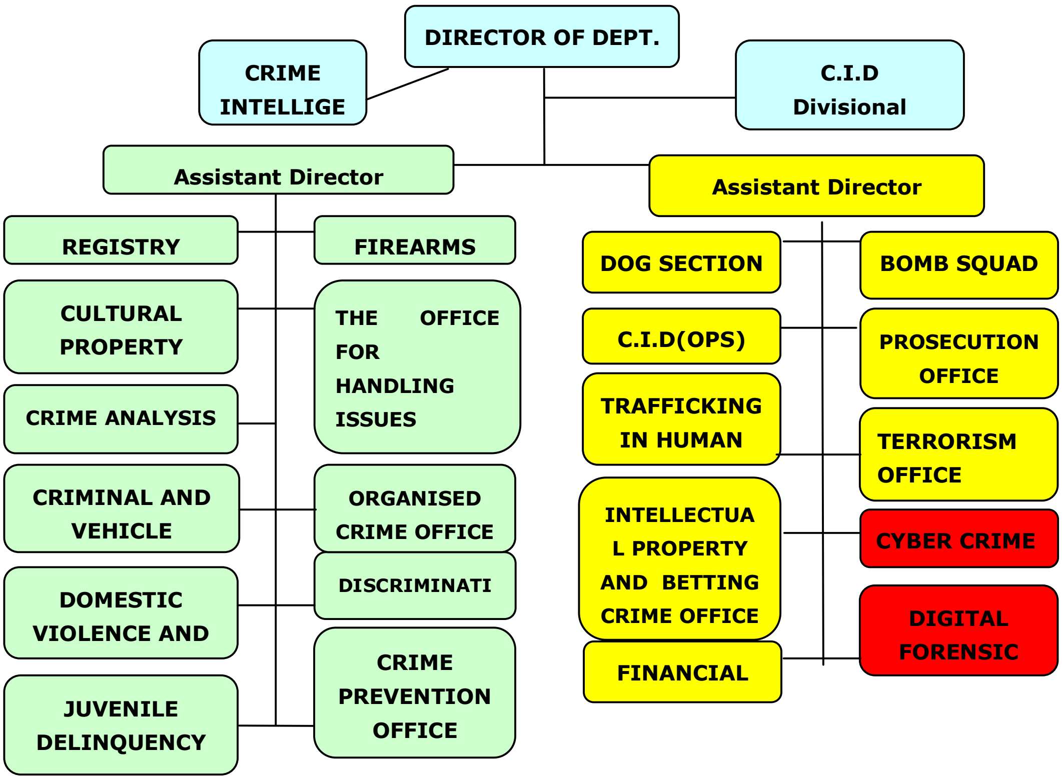
The functioning of the Office for Combating Cyber Crime is regulated / governed by the Police Standing Order 3/45.

Besides, the Office investigates cases that concern internet offences and offences related to Computers, according to L. 22(III)/2004, the Law on the Convention against Cyber Crime (Ratifying). The Office namely deals with cases of unlawful intervention – interference in IT systems and IT data, as well as cases of child pornography.

9.8.3 Institutional set up and resource

The Office for Combating Cyber Crime was established in 2007. The Computer Forensic Examination Lab was established in April 2009 with the responsibilities for the examination of all digital exhibits except CCTV (Closed Circuit TV or camera surveillance) and mobile phones exhibits.

CYPRUS POLICE HEADQUARTERS STRUCTURE DEPARTMENT C'



The Office for Combating Cyber Crime is staffed by five investigators and one duty senior officer. The main forensic tool used by the personnel is the FTK forensic tool.

The Computer Forensic Examination Lab consists of seven expert computer technicians.

Cybercrime is prosecuted by the prosecution office of the Cyprus Police. This office falls under the direction of Attorney General, for serious cases the prosecution office of the Attorney General itself does the case.

9.8.4 Interagency, public/private and international cooperation

The Office of Cyber Crime does not have field offices.

The Office of Cyber Crime has close cooperation with governmental and non-governmental organisations at a national level. Furthermore, the Office sustains close cooperation with International organisations, Europol, F.B.I. etc. in investigating relevant cases.

The Office is member of the following Working Groups: EUCTF (European Union Cyber Crime Task Force), AWF CYBORG of Europol, ICROS project of Europol, AWF TWINS of Europol, European annual expert meeting on child abuse – project or AWF TWINS, Cyber Crime Training & Education Group (ECTEG) of Europol, ICSE project of Interpol (internet child sexual abuse database), OLAF.

The CCTV and mobile phones exhibits of the Department D (Scientific & Technical Support Department) of Cyprus Police Headquarters are also authorised to investigate cybercrime and analyze electronic evidence.

The office for combating cybercrime as well as the computer forensic examination lab make part of the Department C (Criminal Investigation Department), responsible for the investigation and detection of serious crimes.

The specialised unit cooperates with other Law Enforcement Agencies through the official channels such as official requests, rogatory letters.

The Office of Cyber Crime is the 24/7 point of contact.

9.9 Czech Republic: Information Technology Crime Section

9.9.1 Name and contact details:

Information Technology Crime Section
Tel: + 420 974 834 754
fax + 420 974 834 795

Contact point 24/7 (Cybercrime Convention)
+42603190057contact@mvcr.cz , oik@mvcr.cz

9.9.2 Functions, responsibilities and legal basis

The main tasks and the legal mandate of Information Technology Crime Section are as follows:

- performs the tasks of police authorities in criminal proceedings in the criminal information
- searches, monitors and evaluates information crime and other emerging forms of crime in the area of information technology
- performs professional or technically challenging forensic technical work (seizing electronic data) , including consequential analysis of the data
- a contact point for direct communication with foreign police units and LEA in the prevention, detection and investigation of crime information
- a methodological and coordinating activities in the prevention, investigation, identifying, clarifying and documenting information crime
- a preparation of legal regulations and internal management in training and education of police officers

In addition to the above mentioned task the ICTS can contribute to the preparation of legal regulations, contribute to the preparation of the internal procedures in the drafting phase, as well as to design and implement training programmes for other law enforcement in the country.
The ICTS acts as the national coordinator for international LEA cooperation in the Czech Republic.

In the broader general sense the unit is authorised to investigate offences against or by means of computer systems, these investigations have to be done in accordance with a procedure code. In all cases the investigation of a crime has to be carried by a local police unit (from the place where the crime was committed) without regard to the type of crime. .

The unit doesn’t have a forensic laboratory. Electronic evidence is analysed by the Forensic Institute of Prague or by an external private forensic expert.

9.9.3 Institutional set up and resources

Information Technology Crime Section (ITCS) is part of the Bureau of Criminal Police and Investigation Service, which is highest institution of Criminal Police in the Czech Republic. ITCS is not authorised to investigate (generally).

Bureau of Criminal Police and Investigation Service is a part of the Police Presidium.

An internal organisation of ITCS can be described this way (informal organisation chart)

- a technician section - police officers mainly with technical skills and background focusing on attack against data or computer system

- a detective section - staffed by officers with legal background; the section focuses on child pornography, e-business, economic crime (credit card, fraud, phishing)
- a service section - with focus on operational activity

ITCS does not have field offices, but closely cooperates with regional police IT groups within the Czech Police. There are 8 police officers in the ITCS unit and 50 police officers in the regional police IT groups. All police officers in the ITCS and in the IT groups have participated in internal training for seizing of data and have also participated in external training for investigation of cybercrime (basic course).

The Czech Republic is divided into 13 police regions + 1 region of the capital. A small IT group was established during 2010 within each region. ITCS cooperates with these groups during searching of houses, seizing of data, questioning of witnesses; and also provides a connection with international LEA for them. It is important to emphasise that these IT groups (1-3 police officers) are not field offices of ITCS (they are not a part of ITCS. Within the organisation of each police region, they are a part of a Regional Police Analyse Section).

9.9.4 Interagency, public/private and international cooperation

ITCS does not have the authority to cooperate itself. ITCS can cooperate with other institutions only as part of the Bureau of Criminal Police and Investigation Service.

Only the Czech police is authorised to investigate cybercrime. The ICTS can coordinate investigation with different regional police units, or can give its contribution to the investigation by supporting them in the seizure, analysing of data, and communication with international LEA etc.

It is important to note that since end of March 2011, as a result of a decision by the Constitutional Court of the Czech Republic, data related to electronic communications is not available anymore.

The unit is part of the 24/7 Contact point set up by the Convention, the Interpol 24/7 Contact point and the AWF Cyborg.

ITCS handles all requests sent/received, related to Cybercrime, approximately. 1900 requests a year (including requests related to child pornography, phishing, and other computer related crimes, etc.).

9.10 Finland: Cybercrime Investigations Unit

9.10.1 Name and contact details:

Cybercrime Investigations Unit

9.10.2 Functions, responsibilities and legal basis

The cybercrime investigations unit within the National Bureau of Investigations (NBI) has the authority for the investigations of offences committed against computer systems and data as well as for the investigation of offences committed through computer systems. However the leading role in the investigations is given to the local police units, similarly to the case in the Czech Republic. Every unit with law enforcement powers can investigate cybercrimes.

The legal basis for the functioning of the specialised unit is the law for policing in Finland which gives the NBI the authorization to function nationwide as well as to participate in international cooperation.

The specialised unit in Finland does not have CERT/CSIRT responsibilities but closely cooperates with the CERT of Finland. In addition the unit employs personnel with the appropriate training to act as CERT in cases when needed.

The unit takes charge of coordinating the efforts of investigations that involve multiple LEA such as customs officers and border guards.

The Cybercrime Investigations Unit in Finland is authorised to contribute to national policies in the field of cybercrime and is authorised to draft internal procedures, to participate in international judicial cooperation and to take part in international cooperation with other LEA. The Unit may design and implement training programs for law enforcement.

9.10.3 Institutional set up and resources

In addition to the Cybercrime Investigations Unit, there are two other units in the NBI that work in the field of cybercrime, the Cybercrime Intelligence Unit and the crime laboratory.
The Cybercrime Intelligence Unit gathers all information related to cybercrime, for example tip offs, threats, new phenomena and investigations, while the crime laboratory is responsible for the forensics part especially in complicated cases that require high level of expertise.

The Cybercrime Investigations Unit is staffed by 10 officers while the Cybercrime Intelligence Unit and the Crime Laboratory have 14 respectively 3 officers in their rosters.

9.10.4 Interagency, public/private and international cooperation

The Cybercrime Investigations Unit has good cooperation within Finland and supports other LEA in their investigations of cybercrimes, including cooperation with the customs and border guards.

The unit has not reported on any cooperation with the ISPs or the private sector.

9.11 France (Gendarmerie Nationale): Cybercrime Division

9.11.1 Name and contact details:

Cybercrime division: Pôle judiciaire de la gendarmerie nationale,
STRJD/DLCC, 1 bld Théophile Sueur,
93111 ROSNY SOUS BOIS Cedex,
+33 1 58 66 54 13
judiciaire@gendarmerie.interieur.gouv.fr

9.11.2 Functions, responsibilities and legal basis

In France there are two Departments that deal with investigation of Cybercrimes: The Cybercrime Division within the Gendarmerie Nationale (presented below) and the France National Cyber Crime Investigation Unit - O.C.L.C.T.I.C.

The cybercrime division which is located at a national level within the Gendarmerie Nationale is given the mission to proactively monitor the Internet for illegal activities and investigate them. The division also assist local investigators and coordinates local Internet surveillance.

In France, National Police and Customs have investigative units dealing with cybercrime and forensic capacities. Tax or consumer protection investigators also have some missions in relation with cybercrime.

The Division coordinates the judiciary intelligence in relation with IT crime. They can be co-leads on specific investigations if a unit needs assistance on a case. On national cases with a large number of suspects, the cybercrime division can coordinate (usually only within the gendarmerie).

The Division has the authority to investigate crimes committed through or against computer systems and data. For this purpose the Gendarmerie has created a team of 250 investigators trained for the investigation of cybercrime offences, 220 of these 250 officers are members of the territorial units..
The Division has capacity and performs forensic activity for its own cases and whenever analysis requires additional resources, it is performed by the IT Forensics department within the national forensic lab (the IRCGN : Institut de recherche criminelle de la gendarmerie nationale).

The Division in the Gendarmerie does not have competencies for CERT. The division can contribute to national cybercrime policies; it has the authority to coordinate field offices, elaborates the internal procedures and provides support to other units by request, and has the authority to design and implement training programs on cybercrime and electronic evidence for other police officers. The Division also takes part in the international judicial cooperation (directly or indirectly through national offices), has the authority to take part in the international cooperation with other LEA. In addition the Division assists the local police forces in their cooperation with the local telephone and ISP companies.

9.11.3 Institutional set up and resources

The Division was originally created on 1998 and was reorganised in 2005

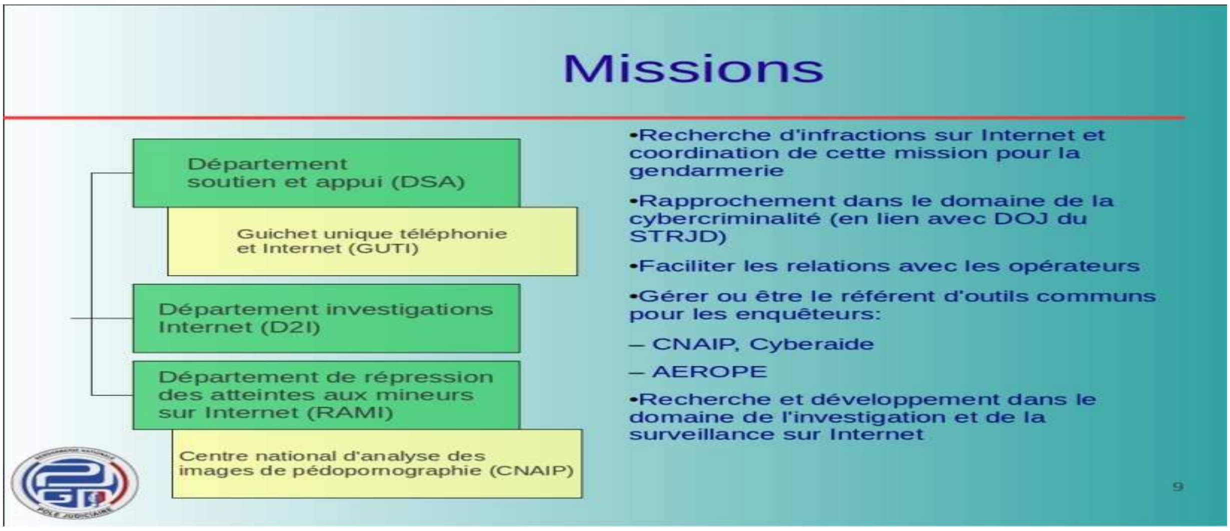
Currently the Division consists of three units:

- Support unit
- Internet investigations unit
- Crimes against children unit

The division does not have specialised cybercrime subordinated territorial units, but instead works with local specialised investigators.

Most investigators have graduated from the gendarmerie's bachelor program on cybercrime, which is developed in cooperation with the Université de Technologie de Troyessome members of the staff have advanced training in law, computer science, computer and network security.

Regular seminars on various topics are organised for investigators who also have access to Gendarmerie trainings for investigators.



Missions

Département soutien et appui (DSA)

Guichet unique téléphonie et Internet (GUTI)

Département investigations Internet (D2I)

Département de répression des atteintes aux mineurs sur Internet (RAMI)

Centre national d'analyse des images de pédopornographie (CNAIP)

- Recherche d'infractions sur Internet et coordination de cette mission pour la gendarmerie
- Rapprochement dans le domaine de la cybercriminalité (en lien avec DOJ du STRJD)
- Faciliter les relations avec les opérateurs
- Gérer ou être le référent d'outils communs pour les enquêteurs:
  - CNAIP, Cyberaide
  - AEROPE
- Recherche et développement dans le domaine de l'investigation et de la surveillance sur Internet

9

9.11.4 Interagency, public/private and international cooperation

There is cooperation with other agencies and private entities for activities related to data collection and development of their own investigations, but there are no signed cooperation protocols.

It is involved in international cooperation at operational level and also participates in international workgroups and meetings.

The Division remains in close contact with the National Cybercrime Unit through more than 10 staff from the gendarmerie who are embedded within the national cybercrime unit. Whenever needed, especially when a question involves an investigation under the responsibility of one of the gendarmerie's unit, these officers can provide assistance on the case.

They are part of EUCTIF, Europol AWF Twins / Terminal / Cyborg and Interpol working party on IT crime.

9.12 France (Police Nationale): OCLCTIC

9.12.1 Name and contact details

Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication (OCLCTIC)
Central High Tech Crime Unit
Central Directory of Judicial Police
101 rue des Trois Fontanot
92000 Nanterre
France.

00 33 (0)1 47 44 97 55
Fax : 01 47 44 97 99
oclctic-sec-dcpj@interieur.gouv.fr

9.12.2 Functions, responsibilities and legal basis

In France there are two Departments that deal with investigation of Cybercrimes: the France National Cyber Crime Investigation Unit - O.C.L.C.T.I.C (presented below) and the Cybercrime Division within the Gendarmerie Nationale.

The National Cyber Crime Investigation Unit has authority to investigate both crimes committed against computer systems and data and crimes committed by the use of computer systems except for crimes relating to child pornography, racism and xenophobia. The Unit has its own forensic laboratory but doesn't act as a CERT.

The unit can be in charge of supporting others law enforcement departments for the collection and analysis of electronic evidence. The unit supports the specialised police department for fighting terrorism, and the department for fighting illegal gambling.

The National Cybercrime Investigation Unit bases its activity on the decree n° 2000-405 of May 5th 2000.

9.12.3 Institutional set up and resources

The Unit was established in May 5th, 2000 by a decree. Before than the unit functioned under the name Brigade Centrale de Répression de la Criminalité Informatique, created in 1994, with less means and people; this unit didn't take in consideration all offences linked with computers.

OCLCTIC is attached to General Directory of National Police, Central Directory of Judicial Police, Sub directory of Fighting against Organized Crime and Financial Delinquency. The Unit has several sections such as:

- Operational section with groups investigating phishing, hacking and carding, fraud to phone providers, fraud to payment cards, fraud on Internet.
- Administration of report centres section: in charge of the web reporting platform, and the call centre on fraud;
- Operational documentation and Foreign Affairs Section: in charge of collecting operational information about cybercrime analysis. Also contact point for Interpol, Europol, 24/7; international cooperation with meetings Europol, Interpol, working groups, and partnerships with others countries, welcoming of foreign delegations.

- Technical Section: provides technical assistance to investigators, technologic watch and is in charge of professional training.

The unit has a central office but no field offices; however it utilizes the services of many trained police officers. The unit has 50 trained officers in the Central Unit and 283 investigators trained in cybercrime investigations. Most of the staff have had previous training on computer technologies while they have undergone in service training after joining the unit.

9.12.4 Interagency, public/private and international cooperation

The unit cooperates with all other Law Enforcement Agencies as part of the Unit's investigations. The Unit also acts as an institution that collects information on offences related to Cybercrimes. The unit cooperates with the prosecution services during the investigating of cases, as well as with the Treasury Service and the Tracfin when requiring information about domicile and funds of suspects, and financial transactions.

The unit cooperates with the CERT in France and has good cooperation with the ISPs and the credit card industries through the Groupement d'Intérêt Economique des Cartes Bancaires, which provides useful information for the unit's investigations, about cards transactions, amount of a prejudice etc. They can also monitor transactions of a certain card, for example.

OCLCTIC in many cases sends requests to phone companies, banks and any company when needed in investigations.

The unit cooperates with Specialised Cybercrime Units from other countries, including cooperation in joint investigations.

The unit acts as the 24/7 point of contact and is member of 24/7 Network, TCY committee, High Tech sub group in G8, Cyborg, Terminal with Europol, Cybercrime Task Force; OCTOPUS, European Working Party on Information Technology Crime with Interpol.

9.13 Ireland: Garda Computer Crimes Investigation Unit

9.13.1 Name and contact details

Garda Computer Crimes Investigation Unit
Harcourt Square, Harcourt Street,
Dublin 2.
Tel: 00353 1 6663708

9.13.2 Functions, responsibilities and legal basis

The Unit has responsibility to investigate crimes committed against computer systems (hacking, malware attacks, telecoms fraud etc.) but does not carry out investigations into crimes by means of computer systems, such as child exploitation online or IP rights. The unit investigates fraud where possible, but this can also be investigated by non specialist units.

The Unit is responsible for the collection and analysis of electronic evidence and has a Forensics lab staffed by 13 examiners, 2 supervisors and 1 manger (they receive more than 650 requests for this service annually, on average each request has 14 computers to be examined).

The Unit does not have CSIRT/CERT responsibilities.

The Unit can be asked to develop or contribute to policy and to the development of the internal procedures. Currently the unit does not have field office but there is an on-going discussion regarding the issue of field offices. The Unit is well known and has a leading role in Europe for the preparation and implementation of training programmes for other LEA in the field of cybercrime.

At this stage the Unit is only occasionally involved in international judicial cooperation whereas it has frequent and continuous international cooperation with other LEA. The Unit can contribute to investigations in other countries, including internet frauds, Malware/Botnets command and control server investigations.

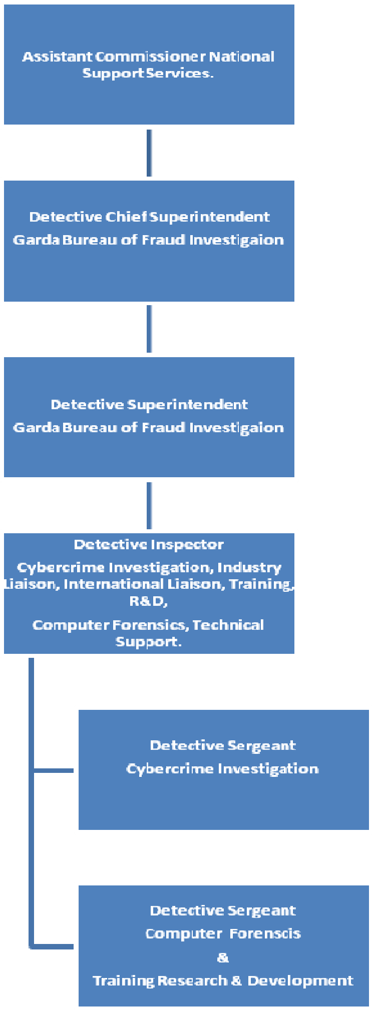
9.13.3 Institutional set up and resources

The Unit is part of the Garda Bureau of Fraud Investigation of the National Policing Service. The Unit was established in 1991 with two staff and currently has 16 staff.
The Unit has no specialised sections; the staff is both forensic specialist and cybercrime investigators that have graduated from the Master Program for Forensic Computing and Cybercrime Investigation at the University College of Dublin (UCD)

The unit has a forensic network, most of the usual Computer Forensic tools and a separate internet network at their disposal.

The Unit has a matrix of training developed for all staff. This training culminates in the Masters Degree in Forensic Computing and Cybercrime Investigation that most of the staff obtained at the Centre for Cybersecurity and Cybercrime Investigation at the University College Dublin.

The unit has no responsibilities for the coordination of the field offices at present, but that is actively under discussion. Following is a schematic presentation of the structure of the Unit:


Assistant Commissioner National Support Services.
Detective Chief Superintendent Garda Bureau of Fraud Investigaion
Detective Superintendent Garda Bureau of Fraud Investigaion
Detective Inspector Cybercrime Investigation, Industry Liaison, International Liaison, Training, R&D, Computer Forensics, Technical Support.
Detective Sergeant Cybercrime Investigation
Detective Sergeant Computer Forenscis & Training Research & Development

9.13.4 Interagency, public/private and international cooperation

The cooperation with other LEA is done mainly based on bilateral arrangement on a case by case basis.

Ireland doesn't have a 24/7 contact point for ensuring international cooperation and taking emergency actions. But the Garda Computer Crimes Investigation Unit has a 7 day service at 8 hours per day.

The Unit cooperates with foreign specialised Units in investigating criminal offences related to computer systems and data as well as in collecting and securing electronic evidence of a criminal offence, frequently through INTERPOL and EUROPOL and cooperate accordingly with the requesting jurisdiction.

The Unit takes part in specialised international networks, initiatives and committees/bodies, like ECTEG, EUCTF, INTERPOL WORKING PARTY ON IT CRIME.

9.14 Kosovo*: Cybercrime Investigation Unit

9.14.1 Name and contact details

Cybercrime Investigation Unit

Contact: cybercrime@kosovopolice.com ,

Website: www.KosovoPolice.com

9.14.2 Functions, responsibilities and legal basis

The Cybercrime Investigation Unit in Kosovo was established in August 2011 and is responsible for the investigation of offences committed against computer systems and data, as well as those committed by means of computer systems.

The Unit does not have forensic capacity. The forensic analysis of electronic evidence is done by the IT forensic section. The Cybercrime Investigation Unit does not have any CERT or CSIRT responsibility at this point.

The unit bases its activities on the law on cybercrime, while the internal regulations and the SOP (Standard Operating Procedures) are currently being developed.

The newly established unit does not have experience of having jointly investigated or assisted in the investigation of crimes by other departments within the law enforcement. The unit has limited experience in the field of cybercrime and to date have investigated only crimes relating to credit card fraud.

9.14.3 Institutional set up and resources

The cybercrime unit is part of the Directorate for Investigation of Organized Crime. Currently the Cybercrime Unit is staffed by 5 officers and is a centralised unit without field offices.

The unit has great need for training and needs additional equipment to be able to carry out their daily duties.

The unit is not the 24/7 point of contact at this point.

9.14.4 Interagency, public/private and international cooperation

The unit has good cooperation with the prosecutor’s office and with the IT forensics section. Due to the short time since it was established the unit has not had a chance to establish cooperation with the private sector and academia.

At this point the cooperation with the ISPs is done only through the execution of prosecutor or court orders.

[*] 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.

9.15 Luxembourg: Section Nouvelles Technologies

9.15.1 Name and contact details

Police Grande Ducale, SPJ Service de Police Judiciaire – Section Nouvelles Technologies
L-2957 Luxembourg
spj.nt@police.etat.lu

9.15.2 Functions, responsibilities and legal basis

The Unit has responsibility to investigate crimes committed against computer systems and data as defined in their criminal code (hacking, phreaking, phishing, - 78 cases in 2010) and give her support to every police unit for offences committed by means of computer system (673 request in 2010).

The Unit is responsible for the collection and analysis of electronic evidence in the cases investigated by them. In other cases, the investigator in charge is responsible, but can always ask for help to the specialised unit.

The unit has its own electronic forensics laboratory and currently relies on commercial and open-source products to collect and analyse electronic evidence. A technical report containing all the steps done and the results of their research is prepared.

The Unit can be reached 24/7, but does not have Computer Security Incident Response Team (CSIRT)/Computer Emergency Response Team (CERT) responsibilities.

The specialised unit can be asked to give training to other units of the police. In 2011, the Unit is providing the units with one hour training on how to get information from Microsoft, Yahoo, etc. These training are of more general approach to cybercrime and there is no proper forensic training is given to this unit. The main focus is to enable police units to deal on their own with offenses by means of computer systems.

The structure of the Police Grand-Ducale is defined by the law "Loi modifiée du 31 mai 1999 sur la Police et l'inspection générale de la Police" and subsequent texts.
http://www.legilux.public.lu/leg/textescoordonnes/compilation/code_administratif/VOL_2/POLICE_GRAND-DUCALE.pdf

The legal basis is the "Code d'Instruction Criminelle" , where the functions and the mandate are defined:
http://www.legilux.public.lu/leg/textescoordonnes/codes/code_instruction_criminelle/CodeInstrCrim_PageAccueil.pdf

9.15.3 Institutional set up and resources

The Unit is part of the Judicial Police. It was created in 2003 with one police officer, 1 engineer and 3 operators. Today, they are 4 engineers, 4 operators and 2 police investigator and 1 secretary. There is no field office. The Unit is competent for the whole country.

The staff participates in the trainings offered by Europol, Interpol, OLAF and private industry. Several staff members have passed the IACIS certification. Several staff members have received training on the software they used. The Unit also try to have an internal training periodically to pass the knowledge.

Every member has a recent PC and laptop with a connection to storage. The unit uses Linux and Windows XP/7 as OS and Open source software, X-Ways, FTK, XRY and CELLEBRITE.

Other software should be used by any specialised unit: GUYMAGER, XMOUNT.

9.15.4 Interagency, public/private and international cooperation

The unit has close cooperation with governmental and non-governmental organisations at a national level. The cooperation is defined by the law: "Entraide judiciaire internationale en matière pénale". The unit is available for technical support to all other police units in the country. In 2010 the unit received 673 requests for support to other units.

Europol is the only international body where the unit takes part.

There is no need for an agreement to provide for international cooperation for technical support (exchange of know-how), however a formal request should be addressed to the General Director of the Police Grand-Ducale. For every other request, the approval of a national magistrate is required before handing over judicial information.

9.16 Mauritius: Information Technology Unit

9.16.1 Name and contact details

Information Technology Unit (IT Unit)
Central Crime Investigation Division
Mauritius Police Force
Contact person: Narayan Gangalaramsamy

9.16.2 Functions, responsibilities and legal basis

When the Unit was created in 2000, one of its objectives was to attend to ICT related crimes, which was mentioned in a Circular (CP's Circular) from the Commissioner of Police. CP's Circular is a formal paper for information and instruction to members of the Police Force.

In 2006, after setting up of a digital forensic lab at the Police IT Unit, another CP Circular was issued about the role of the IT Unit in assisting investigation of computer related crimes/ cyber crimes, and examination of electronic/digital equipment (exhibits).

The Unit is responsible for investigations on crimes against computer systems and crimes by means of computer systems: illegal access, data and system interference, computer misuse, harassment/threat through emails, paedophiles, copy right offences, DOS attack, counterfeited bank notes, and unauthorised access to computer, etc.

They provide assistance to other police units or public agencies for the forensic examinations of the computers or digital media and if necessary house searches.

The CERT is found under the National Computer Board in Mauritius which does not actually have investigative powers, thus cases where criminal actions are suspected are referred to Police and IT Unit provide assistance.

The Mauritius Police Force has a training centre where the trainings on cyber crime and digital evidence are delivered for all police officers.

9.16.3 Institutional set up and resources

The IT Unit was created in 2000, in the Mauritius Police Force, at the Police Headquarters under the direct command of the Commissioner of Police. The objective was to regroup police offices for the development of Information Technology in the Mauritius Police, and also to combat ICT related crimes.

The national legislation on cybercrime from 2003 (Computer Misuse and Cyber Crime Act) is in line with the provisions from Budapest Convention on Cybercrime 2001.

The Digital Forensic Lab was created in 2006 within the unit; the staff of the Digital Forensic Lab is specialised on both forensic and cybercrime investigators.

In 2006, the IT Unit came under the Central Crime Investigation Division from the Police Head quarters, which investigates major crimes, and the criminal investigations (cyber crimes) became a core function of the Unit.

The IT Unit is composed of 35 Police officers (1 chief inspector, 2 Inspectors, 4 Sergeants, and remaining police constables – including 2 female staff). It has five important sections:

1. The Digital Forensic Lab (for computers, mobile phones, video/cctv examination)
2. Project Monitoring and Planning - System Administration team (System administrators/ DBAs for Police Servers,)
3. The Network Administrators and Computer maintenance workshop for Police Systems
4. Training (for IT awareness course and handling of E-crime cases for police officers)
5. Software Development Team (minor software developed in-house)

They have Encase, FTK and Cellebrite at their disposal as forensic tools.

However, though the staff are engaged in technical duties for support of IT in general in the Police Department, their expertise is used when attending to computer crimes/cyber crimes cases as all staff are deployed on cyber crime investigation and are on roster (on call) for assistance when the service of IT Unit is required.

At the central CID investigation, there are 5 officers (1 inspector, 1 sergeant, and 3 constables) responsible for investigations and there are no field offices, but there are investigators who are dealing with these types of investigations but are not dedicated only to cyber cases.

Next to the investigation teams at the central Crime Investigation Department (CID), there are also local CID's.

9.16.4 Interagency, public/private and international cooperation

At the national level the unit cooperates mainly with the Information and Communication Technology Authority, CERT-MU, ISPs, Independent Commission Against Corruption, Mauritius Revenue Authority etc.

The cooperation with other LE agencies are carried out mainly based on a case by case basis.

The Unit is member of the 24/7 High Tech Crime Network and can answer and provide support for all request received through 24/7 High Tech crime network, including the Interpol.

9.17 Montenegro: Specialised officers

9.17.1 Name and contact details

Police Directorate www.upravapolicije.com

Sector of Criminal Police
skp@t-com.me

Department for the fight against organised crime and corruption
org.krim@t-com.me
org.ekonomski@t-com.me

9.17.2 Functions, responsibilities and legal basis

In Montenegro there is no specialised police unit for cybercrime. Police officers specialised for this type of investigations are part of Department for the fight against organised crime and corruption.

- The Department for the fight against organised crime and corruption is responsible for the investigation of offences against computer systems and data.
- This Department is also responsible for the offences committed through/by means of computer systems (e.g. child pornography).
- This Department does not do forensic analysis, however it does collect electronic evidence, similarly as other officers from the Police Directorate depending on the criminal offences which are investigated. After evidence is adequately collected, it is sent to Forensic Centre in Danilovgrad for further analysis and forensic examination.
- The Department for combating organised crime and corruption does not have CERT responsibility. The new Ministry for Information Society and Telecommunication is currently planning to establish a CERT Team. For the moment, the officers from the Police Directorate undertake operative actions regarding to emergency responses.

Working positions of officers in the Police Directorate are prescribed in an Act on organisation and systematisation of working places. The Act prescribes norms for the holder of a position such as years of working experience, education requirements etc.

The officers from the Police Directorate are authorised to provide proposals to the amendments of the Criminal Procedure Code and Criminal Code, to participate in roundtable discussions and working groups as well as to organize training seminars/workshops for other members of the law enforcement in Montenegro. The officers from this directorate can prepare internal procedures and have the authority to direct Police Officers from the field units of the Police Directorate.

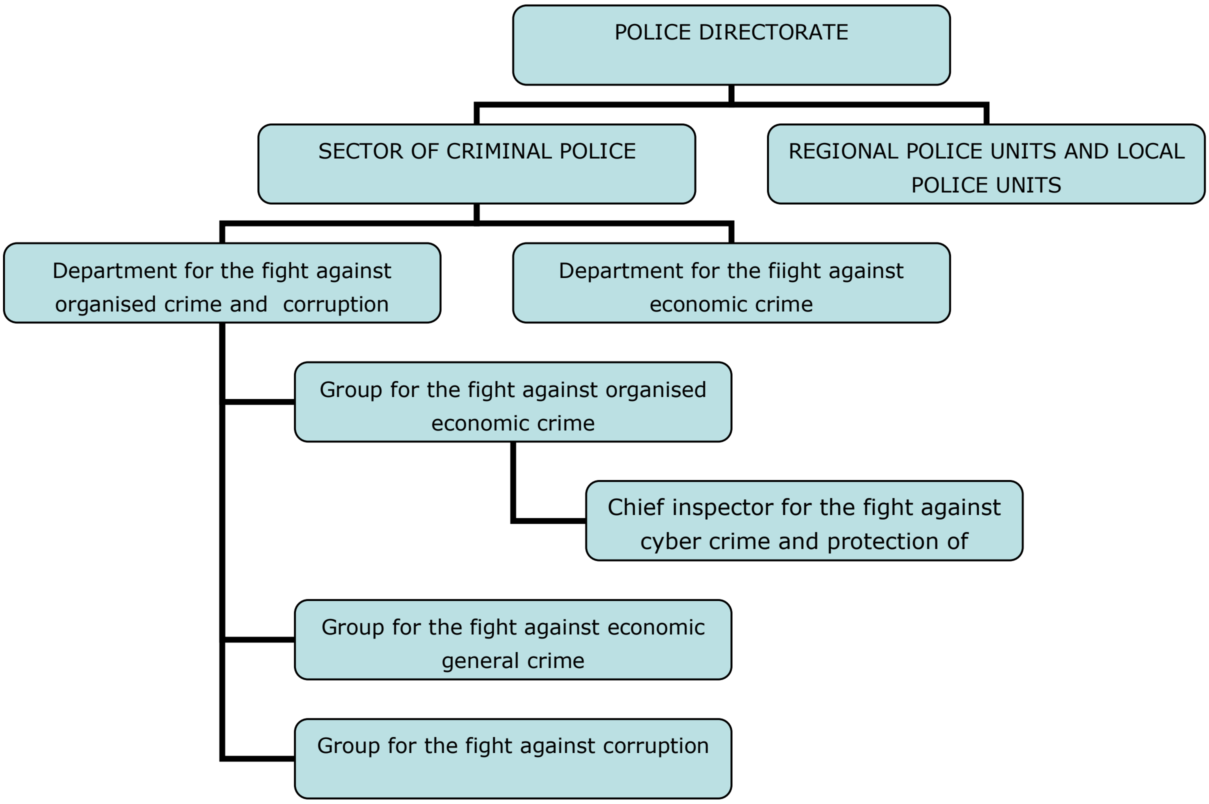
9.17.3 Institutional set up and resource

Within the Sector of Criminal Police at the Police Directorate of the National Police of Montenegro, there is a Department for Fight against Organised Crime and Corruption that was established in 2004. One of the divisions in this department is the Division for the fight against Organised Economic Crime. This division has a line of work for the fight against cybercrime and protection of intellectual property.

Besides the central level, there are regional units and local police units, in total 21, and in accordance with the Act on systematisation and organisation of working places, these units have groups for the fight against economic crime with highly qualified and adequately trained officers.

The line of work for the fight against cyber crime coordinates all activities in relation to the fight against cyber crime, also with the officers in the departments in the field.

In the Police Directorate there are no specialist programs or equipment. The Forensic Centre uses the software tool Encase.


POLICE DIRECTORATE
SECTOR OF CRIMINAL POLICE
REGIONAL POLICE UNITS AND LOCAL POLICE UNITS
Department for the fight against organised crime and corruption
Department for the fiight against economic crime
Group for the fight against organised economic crime
Chief inspector for the fight against cyber crime and protection of
Group for the fight against economic general crime
Group for the fight against corruption

Besides the Prosecutor office and the National police of Montenegro no other law enforcement agency are authorised to investigate cybercrime and analyze electronic evidence, except in specific cases where the Prosecutor office can ask for help of NGO or ISP in specific matter where there expertise and knowledge are necessary for efficiency of investigation .

9.17.4 Interagency, public/private and international cooperation

The officers from the Department for the fight against organised crime maintain contacts and have meetings with the representatives from Administration for the fight against money laundry, Municipal Police, Tax administration, Market inspection, Agency for the protection of intellectual property, University of Montenegro, Ministry for information society, Internet service providers, private banks, BSA (Business Software Alliance) and other relevant institutions.

In accordance with Criminal procedure Code and Criminal Code, the officers from Police Directorate are obliged to present their knowledge about committed offences to a competent prosecutor.

The officers from Police Directorate communicate and cooperate with other agencies from abroad through NCB Interpol as well as through liaison officer for countries of West Europe but are not allowed to take part in International Judicial Cooperation since this authority lays within the judicial system in Montenegro. In the Department for the fight against organised crime and corruption there is an officer that is contact person 24/7 in relation to cybercrime. Until now there were no requests from foreign authorities.

9.18 Romania: Cybercrime Unit

9.18.1 Name and contact details:

General Inspectorate of Romanian Police
Directorate for Countering and Organised Criminality
Cybercrime Unit
Bucharest, Stefan cel Mare Street, no 13-15
Tel: 00 41 21 3100419
cybercrime@politiaromana.ro
www.efrauda.ro

9.18.2 Functions, responsibilities and legal basis

The cybercrime unit is the only structure from the Police responsible with preventing and combating cybercrime.

The cybercrime unit has the following responsibilities:

- to perform investigations (computer offences, computer related offences and credit card offences)
- to perform computer forensic activities
- to provide support to other police units (computer forensic and internet investigations)
- to create a national training program for the entire staff
- to evaluate and analyze the phenomenon and make proposals for improved and more efficient activity
- to ensure cooperation with other institutions and the private sector
- to ensure international cooperation.

9.18.3 Institutional set up and resources

The unit was created in 2003, based on an order of the Minister of Interior and included 8 officers working at central level.

Currently, the unit employs 28 police officers at central level, operating in two sections:

- the section for cybercrime investigation (18 police officers) and
- the section for computer systems investigation and forensics (9 police officers).

The unit has a dedicated office space where the officers conduct the computer searches. The unit has the required equipment and software to conduct such activities (EnCase, FTK, Forensic duplicator, X-ways, Mobile Edit).

At territorial level, within the brigades for combating organised crime there are 15 units for combating cybercrime, as well as officers working in this field in the counties where there are no cybercrime units.

In total, the Romanian Police employs approximately 170 police officers working in the cybercrime area.

The territorial units are administratively and professionally coordinated by the central unit, but they are independent in initiating and performing their investigations together with the prosecutor responsible for the investigation.

The cybercrime unit doesn’t have a separate budget as the National Police is the only one to have its own budget.

9.18.4 Interagency, public/private and international cooperation

The cybercrime unit cooperates with CERT and other competent institutions in order to perform preventive actions in this area or to carry on investigations.

There are cooperation protocols signed with private companies and NGOs for cybercrime and online child protection prevention.

The cybercrime unit administers the portal efrauda.ro, for reporting complaints about cybercrimes.

Together with NGOs the cybercrime unit administers the hotline safernet.ro for submitting complaints about online child abuses.

The representatives of the cybercrime unit participate and organise annual training courses, seminars, round tables with representatives of other institutions responsible in the area of cybercrime prevention, including the bank sector.

The cybercrime unit is a 24/7 contact point together with the cybercrime unit of the General Prosecutor’s Office.

The cybercrime unit ensures the proper functioning of the international cooperation at operational level and territorial subordinated units.

The Unit cooperates with foreign specialised units in investigating criminal offences related to computer systems and data as well as in collecting and securing electronic evidence of a criminal offence, frequently through INTERPOL and EUROPOL and cooperates accordingly with the requesting jurisdiction.

9.19 Romania: Specialised Prosecution Unit - DIICOT

9.19.1 Name and contact details:

Service for Combating Cyber Criminality (Cybercrime Unit);
Directorate for Investigating Organized Crime and Terrorism Offences;
Prosecutor’s Office attached to the High Court of Cassation and Justice;
Bucharest, 12-14 Libertatii Blvd
www.diicot.ro

9.19.2 Functions, responsibilities and legal basis

The Service for Combating Cyber Criminality (Cybercrime Unit) within the prosecutor’s office is authorised to investigate offences committed against computer systems and data, the unit is authorised to investigate offences committed through computer systems only in cases when these are committed by an organized crime group. The prosecutor conducts the investigation while the specialized police unit carries out the prosecutor’s dispositions and gathers evidence. The unit can prosecute only crimes provided by Law nr.161/2003 which implemented the Budapest Convention provisions, and intellectual property right violations, misuse of credit card information, credit card fraud, credit card forgery if committed by an organized crime group.

The legal basis for the functioning of the Unit is Law 161/2003 - Art.62 - (1) In order to ensure an immediate and permanent international cooperation in the cyber-crime domain, within the Organised Crime Fighting and Anti-drug Section of the prosecutor’s Office belonging to the Supreme Court, a cyber-crime fighting service is created as a contact point available permanently.

The Law no. 508/2004 provided for the establishing of the Directorate for Investigating Organized Crime and Terrorism Offences. The Service for fighting against Cyber criminality was embedded in the above mentioned unit within Prosecutor’s Office attached to the High Court of Cassation and Justice

Collection of evidence including the electronic evidence is a part of the investigation carried out by the specialized prosecutorial unit (procedural dispositions, production orders etc. needed in order to prove the constitutive elements of the offences). The specialized police units execute the orders in this respect.

The Unit contributes to the national policies on cybercrime, is authorised to draft internal procedures, coordinate local offices and to participate in international judicial cooperation.

9.19.3 Institutional set up and resources

The Cybercrime Unit was established in 2003 as Service for Combating Cyber Criminality (Cybercrime Unit) within the Directorate for Investigating Organized Crime and Terrorism Offences, Prosecutor’s Office attached to the High Court of Cassation and Justice. Currently the unit is staffed by 5 prosecutors at the Central Level, at least one prosecutor within each territorial structure is to prosecute cybercrime offences as described above. The staff have Law degrees and have undergone basic training on cybercrime investigation, collection of electronic evidence. National Institute of Magistracy is national responsible for basic and in service training for magistrates, however for cybercrime there is no special training program designed for prosecutors. Nevertheless prosecutors assigned for cybercrime received training provided by different national/international institutions/projects (Phare, Isec)

The Central Service for fighting cyber criminality consists of three Bureaus (the Bureau for combating cybercrime; the Bureau for combating credit card fraud; the Bureau for combating IPR infringements). Within the territorial structure there are not specialised offices or bureaus. However specialised prosecutors are working in this particular field.

9.19.4 Interagency, public/private and international cooperation

The Cybercrime Crime unit cooperates with law enforcement and the private sector including the ISPs based on the legal provisions in Romania.

The unit acts as the 24/7 point of contact and is authorised to:

a) provide technical advice to foreign authorities
b) provide for the preservation of data
c) provide for the collection of evidence
d) can provide legal information
e) can facilitate the location of suspects and
f) can send/receive judicial cooperation/mutual legal assistance requests

9.20 Serbia: Special Prosecutors Office for High Technological Crime

9.20.1 Name and contact details:

Special Prosecutors Office for High Technological Crime,
Savska 17a str., 11000 Belgrade, Serbia,
Office Phone: +381.11.360.1431,
Mobile Contact Phone: +381.11.64.832.4057,
www.beograd.vtk.jt.rs

9.20.2 Functions, responsibilities and legal basis

The Special Prosecutors Office for High Technological Crime is authorised to investigate the following types of crimes committed against computer systems and data in accordance with the national legislation of Serbia:

- CC Article 298 (Damaging Computer Data and Programmes)
- CC Article 299 (Computer Sabotage)
- CC Article 300 (Generating and Introducing Computer Viruses)
- CC Article 301 (Computer Fraud)
- CC Article 302 (Unauthorised Access to Protected Computers, Computer Networks and Electronic Data Processing)
- CC Article 303 (Preventing or Restricting Access to Public Computer Networks):
- CC Article 304 (Unauthorised Use of Computer or Computer Networks)
- CC Article 304a (Manufacture, Procurement and Provision to others Means for the Committing Criminal Offences against the Security of Computer Data)

All years included starting in 2006 and until September 2011 the total number of cases is 1602.

In addition the Special Prosecutors Office for High Technological Crime is authorised to investigate offence committer through the use of computer systems:

- CC Article 138 (Endangerment of Safety)
- Old CC Article 171 (Fraud)
- Old CC Article 183a (Intellectual and Property Rights Abuse)
- CC Article 185 (Exhibition, Procurement and Possession of Pornographic Materials and Exploiting Juveniles for Pornography – Only from 01.01.2010)
- CC Article 199 Unauthorised Exploitation of Copyrighted Work or other Works Protected by Similar Rights)
- CC Article 208 (Fraud)
- CC Article 221 (Concealment)
- CC Article 353 (Unlicensed Practice of Profession)
- CC Article 355 (Counterfeiting Documents)

All years included starting in 2006 and until September 2011 the total number of cases is 1602

The Law on Organisation and Competence of Government Authorities in Suppression of High Technological Crime, CPC and Criminal Code of Republic of Serbia are main legal/regulatory basis. High technological crime for the purpose of those Laws is criminal offence committed using, as object or tool of committing the crime, computers, computer networks, computer data , including their products in tangible or electronic form.

Special Prosecutor's Office for suppression of high technological crime is established within the Higher Public Prosecutor’s Office in Belgrade (hereinafter the Special Prosecutor's Office) with jurisdiction of the territory of the Republic of Serbia to proceed in criminal offences of high tech crime.

The Special Prosecutor's Office is managed by a Special Prosecutor for suppression of high technological crime. The Special Prosecutor is appointed by the Republic Public Prosecutor

9.20.3 Institutional set up and resources

Law on Organisation and Competence of Government Authorities in Suppression of High Technological Crime was adopted by National Assembly in July 2005. Special Prosecutors Office for High-Tech Crime was founded during February 2006. On January 1st., 2010 competences of the Office were changed on one hand widening scope of the criminal acts under jurisdiction of the Office while on the other hand narrowing it’s capability to prosecute lesser forms of criminal acts then before. So far two Special Prosecutors took the Office.

The specialised Prosecutors Unit consists of 1 Prosecutor (Head of the Office), two Deputy Public Prosecutors, two Prosecutor Advisers and two administrative workers. The personnel has undergone basic training and continuously participates in training programmes organized by the Judicial Academy of Serbia, Council of Europe cybercrime programmes, OSCE, EUROPOL, U.S. DOJ, TAIEX etc.

The specialised Prosecutors Unit is authorised to: contribute to the national cybercrime policies
draft internal procedures, coordinate field offices, prepare and implement training programs for police officers, participate in international judicial cooperation and to cooperate with international organizations and LEA.

Regarding the budget the office budget is part of the main Public Prosecution budget handled at the moment by Ministry of Justice, however this will change on January 1st, 2012.

9.20.4 Interagency, public/private and international cooperation

The Special Prosecutor’s Office for High Technological Crime has direct cooperation with Specialized Department for Suppression of High-Tech Crime within Ministry of Interior. Direct communication with 24/7 Council of Europe network and other similar networks and authorities when need arises. International cooperation is supported by Republic Public Prosecutors Office through direct cooperation and support as well as by use of all International Agreements and MOU’s

The Office has direct communication and good cooperation with the ISP’s, Banks, Credit Card companies etc.

The Office serves as the 24/7 point of contact for Serbia.

9.21 Spain: Brigada de Investigación Tecnológica

9.21.1 Name and contact details

BRIGADA DE INVESTIGACIÓN TECNOLÓGICA
JULIAN GLEZ SEGADOR ST. 28043 MADRID
+34915822469/8
http://www.policia.es/org_central/judicial/udef/bit_alertas.html
http://www.facebook.com/BrigadaInvestigacionTecnologica

9.21.2 Functions, responsibilities and legal basis

The Cybercrime Unit from the Spanish Police was created according to National Law 1/86. It operates as a specialised structure for investigating crimes against computer systems and crimes through computer systems (frauds, child pornography, piracy and threats).

The unit has also forensic capacities and carries on activities related to the analysis and forensics of computer systems and computer data storage devices during their investigations. This structure is authorised to coordinate territorial units.

By request, the unit provides support to other police units for computer systems forensics in complex cases. The Unit can also provide technical or specialised support during the investigations of other police structures of the National Police.

The CERT responsibilities do not lie within the Cybercrime Unit.

The unit participates in developing the national strategy and internal procedures as member of different workgroups and is involved in international cooperation and participation in meetings and workgroups.

9.21.3 Institutional set up and resources

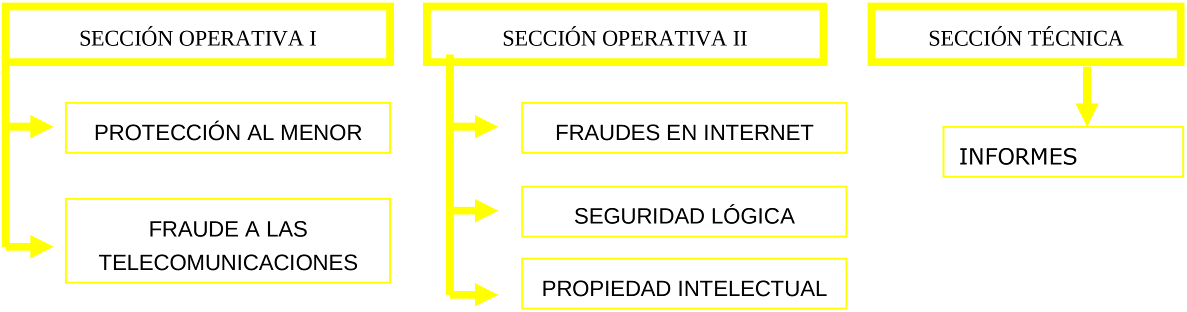
The unit has been developed from a small group, in 1995 to a Brigade in 2000.
At the present there are 45 people working in the central unit and specialised units consisting of 4-7 investigators, in the field offices.

The central unit has three sections:

- Section one is responsible with investigations related to crimes against person (child pornography, threats, etc)
- Section two is responsible for investigations of economic crimes (frauds, piracy, hacking, etc)
- Section third is responsible for forensic activities

The National Police is responsible for the training program, and there are two trainings for cybercrime every year the personnel take part.

The Unit has developed the own training program for the personnel.



9.21.4 Interagency, public/private and international cooperation

There is cooperation with other agencies and private entities for activities related to data collection and development of their own investigations, but there are no signed cooperation protocols.

They have a 24/7 contact point operating according to 2001 Cybercrime Convention, that takes emergency measures for data preservation.

The BIT unit is member of European and South American working parties in Interpol. They join the European Task Force and the ECTEG program in Europol.

9.22 “The Former Yugoslav Republic of Macedonia”: Cybercrime Unit

9.22.1 Name and contact details

Cybercrime Unit
Ministry of Interior
cybercrime@moi.gov.mk
http://www.moi.gov.mk

9.22.2 Functions, responsibilities and legal basis

The cybercrime unit is responsible for investigation of both offences against computer systems and data including illegal access, data interference and offences by means of computer systems, such as fraud, child pornography etc.

The functions and the mandate of the Unit are defined in “Rule for the work and organization of Centre for suppression of organized and serious crime”.

The mission of the unit is: “Conducting of criminal investigations, prevent, detect, document and report perpetrators of crimes of cybercrime, child pornography and abuse and falsification of credit cards. The unit monitors and promotes the distinctive methods for detection of essential and nonessential computer crimes in cyber space, continuously monitors internal and international standards for securing electronic evidence, participate in the coordination and harmonization of national legislation with international conventions and declarations, forms and proposes methods of education and professional training of personnel, establishing cooperation with all domestic institutions and especially with service providers in the Internet space as well as foreign legal entities and international organizations”.

The unit currently doesn’t have forensic capacities which lay with the Forensic Department in the Ministry of Interior. The unit does not have CERT responsibilities.

The Cybercrime Unit is authorised to contribute to national policies on cybercrime, to draft internal procedures, to coordinate field offices (although the unit has none to date), to design and implement training programmes for other police officers, to participate in international judicial cooperation and to cooperate with international organizations and LEA.

9.22.3 Institutional set up and resources

The Unit was established in December 2004. The unit firstly was organized as Section for cyber crime and forgery in Sector for financial crime. Than from 01 of September 2008 the unit was transformed in Unit for fight against cybercrime in Department for Organized Crime and beginning from January 2011 the unit is organised as Unit for Cybercrime in the Department for Financial Crime in Centre for Suppression of Organised and Serious Crime.

The unit currently employs seven people and does not have field offices.

There is no in-service specialised training programme for the unit within the MoI and the unit doesn’t have a separate budget.

The current needs of the unit are: specialised technical equipment specialised training courses for live data forensics and equipment and trainings on child pornography. Currently the unit uses X-ry tool kit software and various internet tools.

9.22.4 Interagency, public/private and international cooperation

The Cybercrime Unit has good cooperation with other departments in the Ministry of Interior which include providing support to investigations of other units and joint (mixed team) investigations with other units. The unit has ongoing discussions and consultations with the prosecution and judicial authorities about ongoing investigations. The cooperation with the ISP's and other private sector stakeholders (banks, phone companies, credit card companies) is good but in most cases limited to submitting of requests for the identifying users of IP addresses, phone numbers, request for information about suspicious online transactions and bank accounts etc.

Currently the Unit is not acting as the 24/7 point of contact although it is foreseen that the chief of the unit will be the 24/7 point of contact.

The unit cooperates with foreign specialized Unit through Interpol, Europol and in joint operations coordinated by SECI Centre in Bucharest – Romania. A strong point in the international cooperation of the unit is considered the vast cooperation with Interpol.