Project on Cybercrime
www.coe.int/cybercrime

and the

Lisbon Network
www.coe.int/lisbon-network

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Department of
Information Society and
Action against Crime
Directorate General of
Human Rights and Legal
Affairs
Strasbourg, France

8 October 2009

Cybercrime training for judges and prosecutors: a concept

Project funded by contributions from Romania, Microsoft and McAfee and by the Council of Europe

This paper has been prepared by a multi-stakeholder working group within the framework of the Project on Cybercrime and the Lisbon Network of Judicial Training Institutions of the Council of Europe.

Contact:

For further information please contact:

Department of Information Society and Action against Crime
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

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

Disclaimer:

This technical report does not necessarily reflect official positions of the Council of Europe or of the donors funding this project or of the Parties to the instruments referred to in this document

Contents

1 Executive summary

Given the reliance of societies worldwide on information and communication technologies, judges and prosecutors must be prepared to deal with cybercrime and electronic evidence. While in many countries, law enforcement authorities have been able to strengthen their capacities to investigate cybercrime and secure electronic evidence, this seems to have been less the case for judges and prosecutors. Experience suggests that in most cases, judges and prosecutors encounter difficulties in coping with the new realities of the cyber world. Particular efforts are therefore required to enable judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence through training, networking and specialisation.

The present concept is to support such efforts. It has been developed by the Council of Europe's Project on Cybercrime and the Lisbon Network of judicial training institutions in cooperation with a multi-stakeholder working group in the course of 2009.

The purpose of the concept is to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training (that is, to institutionalise it). It will furthermore facilitate networking among judges and prosecutors to enhance their knowledge as well as consistent – rather than ad hoc – support to training initiatives by interested partners.
The concept consists of the following elements:

Objectives

Current initial and in-service training generally does not provide judges and prosecutors with the level of knowledge required to deal with cybercrime and electronic evidence.

Thus, the objectives of a training concept for judges and prosecutors should be:

- To enable training institutes to deliver initial and in-service cybercrime training based on international standards
- To equip the largest possible number of future and practicing judges and prosecutors with basic knowledge on cybercrime and electronic evidence
- To provide advanced training to a critical number of judges and prosecutors
- To support the continued specialisation and technical training of judges and prosecutors
- To contribute to enhanced knowledge through networking among judges and prosecutors
- To facilitate access to different training initiatives and networks.

The following measures should help achieve these objectives:

1. Institutionalising initial training

- In countries where initial training is practical training on the job it is recommended that at least part of such training is related to cybercrime and electronic evidence
- In countries where initial training is provided by judicial training institutions their curriculum should contain as a minimum one basic level module on cybercrime and electronic evidence. These issues should in addition be covered in mandatory modules covering substantive and procedural law. Optional modules for advanced knowledge on cybercrime and electronic evidence should be offered
- The specific training modules should be standardised to the point that they are replicable and allow candidates to progress from basic to advanced levels

2. Institutionalising in-service training

- In-service training institutions should offer at least one basic level module on cybercrime and electronic evidence in order to equip those practising judges and prosecutors with basic knowledge who had not such training in their initial training
- They should furthermore offer courses for advanced knowledge.

3. Standardised and replicable courses/modules

- Standardised courses or modules should be developed that can be replicated at a broad scale in a cost-effective manner and that allow candidates and practising judges and prosecutors to progress from basic to advanced
- Existing basic courses that could be integrated into the curricula of initial or in-service training programmes, should be evaluated. A standard course could subsequently be recommended to initial and in-service training institutions
- A similar evaluation could be carried out for advanced level courses and a standard advanced course could subsequently be recommended
- Trainers would need to be trained in the delivery of such courses to the point that training can be delivered by local trainers in local languages and only limited needs of international trainers.

4. Access to training/self-training materials

- Training materials need to be developed reflecting common international standards and good practices. They should be made available to training institutions in a cost effective manner for the purpose of being delivered locally
- While judges and prosecutors need to be trained primarily in the application of domestic legislation, it is nevertheless possible to develop standardised training materials in a way that leaves sufficient room to take into account domestic systems and legislation
- On-line courses should be developed and made available.

5. Pilot centres for basic and advanced training

- A number of pilot centres for basic and advanced training of judges and prosecutors on cybercrime and electronic evidence should be established to test and further develop standardised courses and materials, disseminate good practices, carry out research on training, maintain a register of trainers, offer training of trainers, provide training to other countries with similar systems and languages
- Pilot centres should coordinate their work with each other with the support of the Council of Europe
- Judges and prosecutors who are prepared to become specialists should consider participating in training through the centres of excellence for law enforcement and industry.

6. Enhancing knowledge through networking

- In addition to training, peer-to-peer interaction, networking among judges and prosecutors, but also networking with a range of other stakeholders will be of crucial importance
- Judges and prosecutors should make use of existing networks for judges or prosecutors (such as GPEN)
- The creation of an international network of cybercrime or e-crime judges should be discussed (similar to GPEN for prosecutors) by the Council of Europe
- The networking among European institutions offering training on cybercrime and electronic evidence should be supported by the Council of Europe and the European Judicial Training Network

- In order to facilitate access by judges and prosecutors to these and the many cybercrime-related networks, the Council of Europe should map initiatives and networks and establish a portal with links, brief information and contact details on different networks. This should also facilitate coordination among networks. It should furthermore facilitate access to existing training materials and initiatives.

7. Public private cooperation

- The support of the private sector to the training of judges and prosecutors would be beneficial given that the private sector disposes of relevant subject matter expertise. At the same time, judges and prosecutors must remain independent and impartial
- Judicial training institutions may make use of private sector expertise when designing training programmes, developing training materials and delivering courses
- The support from industry to training institutions must not be conceived to potentially secure favourable decisions in court or to generate business, but to ensure that judges and prosecutors are given adequate information which enables them to make informed decisions
- The private sector could support in a transparent manner international or national organisations, academia, training initiatives or other third parties which then support independent training institutions
- While judges and prosecutors should have an overview of the Internet and cybercrime, it is also important to provide them with platform specific information. Industry could provide materials for specific modules (rather than full courses) on the functioning of relevant platforms.

The Lisbon Network of the Council of Europe approved this concept in September 2009 and recommended that it be widely disseminated and implemented by judicial training institutions. It decided to bring it to the attention of the Consultative Council of European Judges and the Consultative Council of European Prosecutors as well as the European Commission for the Efficiency of Justice (CEPEJ) to ensure broadest possible support to the concept.

2 Introduction

In recent years, societies worldwide have made tremendous advances towards becoming information societies. Information and communication technologies (ICT) now permeate almost all aspects of people's life. The increasing reliance and thus dependency on ICT makes societies vulnerable to threats such as cybercrime, that is, crime committed against or through computer data and systems.

In addition to the large number of offences against or through ICT, an increasing number of other cases ending up in court involve electronic evidence stored on a computer system or other devices.

Therefore, judges and prosecutors must be prepared to deal with cybercrime and electronic evidence. As stated by the Consultative Council of European Judges[1], "it is essential that judges, after having done full legal studies, receive detailed, diversified training so that they are able to perform their duties satisfactorily" (para 3), "Such training is also a guarantee of their independence and impartiality" (para 4), and training should "take into consideration the need for social awareness and an extensive understanding of different subjects reflecting the complexity of life in society" (para 27). The importance of ICT in today's societies is such, that judges and prosecutors must have at least a basic understanding of such technologies and related problems.

While in many countries, law enforcement authorities have been able to strengthen their capacities to investigate cybercrime and secure electronic evidence, this seems to have been less the case for judges and prosecutors who nevertheless play an essential role in the criminal justice process. Experience suggests that in most cases, judges and prosecutors encounter difficulties in coping with the new realities of the cyber world.

Particular efforts are therefore required to enable judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence through training, networking and specialisation.

The expertise of the private sector in respect to new technologies has been essential for law enforcement training. It will also be beneficial for judicial training[2] but this potential has so far been underused. At the same time, the independence and impartiality of judges and prosecutors must be maintained. Innovative approaches are therefore required that ensure the independence of judges and prosecutors while allowing them to have access to private sector expertise and understand the functioning of industry and technology. The concept proposed here shows how judicial training institutions can benefit from support by industry and academia through standardised training programmes and other means.

The purpose of the concept presented in this report is to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training (that is, to institutionalise it).

[1] Opinion no. 4 on appropriate initial and in-service training for judges at national and European levels (CCJE (2003) Op no 4)

[2] See the study published in March 2009: "Co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel"

The concept is based on information received from training institutions in Belgium, Croatia, Georgia, Germany, France, Netherlands, Poland, Portugal, Romania, Spain, "the former Yugoslav Republic of Macedonia" and the United Kingdom (replies to a questionnaire received in June 2009), a workshop held in Portugal in July 2009 with representatives from Belgium, Ireland, Italy, Portugal, Netherlands and the United Kingdom, as well as the private sector and a workshop held in Strasbourg on 3 and 4 September 2009 with the participation of representatives of training institutions, judges and prosecutors of the above countries, the private sector as well as the European Judicial Training Network and the Lisbon Network of the Council of Europe[3].

This multi-stakeholder process led to the preparation – for the first time – of a concept for the training of judges and prosecutors in cybercrime and electronic evidence matters. The participatory nature of this process will certainly facilitate the cooperation of different stakeholders and the consilience of knowledge and expertise in the implementation of the concept.

The Lisbon Network of the Council of Europe approved this concept in September 2009 and recommended that it be widely disseminated and implemented by judicial training institutions. It decided to bring it to the attention of the Consultative Council of European Judges and the Consultative Council of European Prosecutors as well as the European Commission for the Efficiency of Justice (CEPEJ) to ensure broadest possible support to the concept.

[3] Lisbon Network for the Exchange of Information between Persons and Entities in Charge of the Training of Judges

3 Training institutions[4] and systems

In Europe – and similarly in other regions – systems for the training of judges and prosecutors are rather diverse.[5]

With regard to initial training, systems typically consist of one or a mix of the following[6]:

- System A: Candidates – after having completed university level law studies and often after having succeeded in an entry examination – receive specific training at a judicial training centre to become judges and/or prosecutors. Sometimes future judges and prosecutors are trained together, sometimes in different institutions.
- System B: Candidates – after having completed university level law studies – gather practical experience on the job (sometimes in a formalised apprenticeship) in prosecution services, courts, law offices or other institutions – before passing an examination that qualifies them to work as lawyers, prosecutors and judges. No centralised specific training institution is involved[7].

In-service training, that is, continued professional training of serving judges and prosecutors, is offered either by public judicial training institutions which are also responsible for initial training (e.g. France, Georgia, Netherlands, Poland, Portugal, Romania, Spain, "the former Yugoslav Republic of Macedonia", Croatia), by training institutions that have been specifically established for in-service training (e.g. Germany), or by other public institutions, non-governmental organisations, international organisations or the private sector. In some instances this is foreseen in annual training plans or may be delivered ad hoc. In most cases, in-service training is optional, unless judges or prosecutors perform their duties at specialised courts (e.g. Romania).

The curricula for initial and in-service training in most cases require a formal review and approval process, although there is greater flexibility with regard to optional in-service training. For example:

- In France the curricula are established following consultations between the judiciary, legal staff and departments of the Ministry of Justice. The training programme is then submitted to the Board of Directors of the school for approval.

[4] The term training institution, for the purposes of this paper, refers to any entity responsible for training.

[5] As stated by the Consultative Council for Judges of the Council of Europe in 2003: "There are great differences among European countries with respect to the initial and in-service training of judges. These differences can in part be related to particular features of the different judicial systems, but in some respects do not seem to be inevitable or necessary. Some countries offer lengthy formal training in specialised establishments, followed by intensive further training. Others provide a sort of apprenticeship under the supervision of an experienced judge, who imparts knowledge and professional advice on the basis of concrete examples, showing what approach to take and avoiding any kind of didacticism. Common law countries rely heavily on a lengthy professional experience, commonly as advocates. Between these possibilities, there is a whole range of countries where training is to varying degrees organised and compulsory."
Opinion No. 4 of the Consultative Council of European Judges (CCJE) to the attention of the Committee of Ministers of the Council of Europe on appropriate initial and in-service training for judges at national and European levels (CCJE (2003) Op. N° 4; November 2003).

[6] See Appendix for further information.

[7] The specificities of common law systems should be mentioned. In the UK, for example, judges are appointed from the ranks of experienced practitioners. There is also a possibility for practitioners who are not full-time judges to sit as part-time judges for at least one month each year, after which a great majority is appointed as full-time judges. In addition, there are many part-time lay appointments to sit as members of Tribunals (civil) and Magistrates Courts (mainly criminal). Separate training programmes exist prior to any appointment and during the tenure.

- In Germany, the Programming Conference of the German Judicial Academy – comprising representatives of the different administrations of the justice systems as well as of the professional associations of judges and prosecutors – is responsible for the preparation of the curricula for in-service training of the academy.
- In Poland, by 30 April each year, proposals are submitted by departments of the Ministry of Justice, presidents of courts, and prosecution services. Based on these proposals, the Director of the National School presents to the Programming Board the schedule of training activities for the following year for approval by 30 July. Following approval by the Minister of Justice, the training schedule is sent to the relevant departments of the Ministry of Justice, presidents of courts of appeal and appellate public prosecutors.
- In Romania, the strategy for initial and in-service training is approved by the Scientific Council of the National Institute of Magistrates and the Superior Council of Magistrates.
- In Spain, the curricula and training programmes are prepared by a pedagogical committee consisting of experts in legal matters in consultation with judges associations or individual judges. Curricula for both initial and in-service training for judges are finally approved by the General Council for the Judiciary.
- In Portugal, a training programme is elaborated and developed each year by the Center for Judiciary Studies. While the initial training curriculum is provided for by law, the in-service training changes every year according to the needs identified in practice. The training programme is established after consultations with the Superior Councils of the Judiciary, the Tax and Administrative courts and of the Prosecution Service.
- In Belgium, general and more specific formations programs are developed by or under the supervision of the « Institut de formation judiciaire » every year. This Institute is newly created by law (31/01/07) and it has been active since the beginning of 2009. Cybercrime can be included in the (often optional) in-service training.
- In the Netherlands the Council of Judges and the Council of Procurators-General (who together form the instructing organization for the training institution SSR) decide whether or not there is budget for a training proposed. Propositions can be made by for instance prosecutors or judges or by the lectors of the SSR and if budget is available and awarded, the training will then be developed by the relevant experts from the SSR, the prosecution service, judges and where useful third parties, including private ones.
- In Croatia, curricula for initial training and the plans for in-service training are established in cooperation with the Advisory Council and the Programme Council of the Judicial Academy. The Programme Council identifies the training priorities and submits the proposal for the draft annual curricula of professional training. The Advisory Council adopts the document and provides guidelines for defining the strategy of professional training. Members of both Councils are prominent legal experts and representatives of all target groups of the Judicial Academy.

Training institutions can make use of external expertise, in particular if the subjects are specific and technical as is the case with cybercrime and electronic evidence. For example:

- In Germany, the German Judicial Academy makes extensive use of external lecturers who are mostly legal professionals or researchers but occasionally also industry experts.
- In the Netherlands, consultants and industry experts are involved in the development of training courses and in the actual delivery of training sessions.
- In Romania, the National Institute of Magistrates relies on external trainers and lecturers in specialised field such as cybercrime (e.g. Council of Europe, US Department of Justice, FBI, US Secret Service as well as the private sector such as eBay, Visa, American Express, Amazon, PayPal, Microsoft) and in particular for the training of trainers.
- In Spain, the General Council of the Judiciary has signed agreements with private sector companies (CYBEX, Logality) to provide training on cybercrime and cyberforensics. In addition, private sector experts take part in judicial training.
- In Portugal, most of the trainers of the Center for Judiciary Studies are judges or prosecutors. For in-service training (e.g. seminars or short courses) trainers from the private sector and other experts can be involved.

- In Croatia, specialists from the police units who fight organized and economic crime are involved in developing and delivering the training.
- In Belgium, a major percentage of the budget allocated for the training of judges and prosecutors is to be organised by universities. It is, however, possible to involve experts of the private sector in some training programmes.

The implication for the training for judges and prosecutors on cybercrime/electronic evidence are:

- Judges and prosecutors – as a rule – begin their training with university-level law studies. It can be assumed that the more cybercrime and electronic-evidence related issues are regulated by legislation, the more these issues will be reflected in text books and curricula for law studies. However, it may be useful to make suggestions in this respect to those responsible for preparing materials for university-level courses.
- In countries where initial training is carried out by judicial training institutions, it should be possible to insert cybercrime/electronic evidence training into curricula.
- This is less the case, where initial training takes place on the job.
- In most countries, judicial training institutions that offer in-service training are available and it should be possible to insert cybercrime/electronic evidence issues into the curricula.
- While in-service training is possible ad-hoc, formal procedures and approvals are required to insert cybercrime/electronic evidence training into formal curricula, and thus to institutionalise such training.
- In-service training is usually optional. The challenge will be to convince judges and prosecutors to undergo training in a technical area such as cybercrime/electronic evidence[8].
- External public and private sector expertise is required and can be used for the development of training courses, the training of trainers and the delivery of training courses.

[8] In Portugal, in service training is an obligation (i.e. each judge and prosecutor must attend, at least, two training events per year) or in Romania it can be compulsory in some instances.

4 Skills and knowledge required by judges and prosecutors

It is obvious that an increasing number of criminal cases, but also many civil and administrative matters before court will in one way or the other be related to information and communication technologies, and that the majority of criminal judges and prosecutors will be confronted if not with cybercrime with matters involving electronic evidence. It is thus not sufficient to train specialised judges and prosecutors only.

Broad mainstreaming of cybercrime and electronic evidence knowledge is required: all or the largest possible number of judges and prosecutors, therefore, need to obtain at least basic training in matters related to cybercrime and electronic evidence. Such basic knowledge should be provided through initial training for future judges and prosecutors, and through in-service training for serving judges and prosecutors.

At the same time, these are highly technical and constantly evolving issues and it cannot be expected that judges and prosecutors in general are able to keep up with technological developments at all times. It is therefore necessary to provide advanced knowledge to a sufficient number of judges and prosecutors who become specialised in cybercrime and electronic evidence.

4.1 Basic knowledge

In the majority of judicial systems it cannot be predicted which judge will deal with a particular case (principle of the natural judge) so, eventually, all judges, investigative judges and prosecutors should have a basic knowledge of matters related to cybercrime and electronic evidence. "Basic knowledge" means that they should be able to understand the following:

- Computers and networks: how do they work, basic notions of the functioning of the internet, role of service providers, particular challenges to judges and prosecutors
- Cybercrime: how information and communication technologies are used to commit crime
- Cybercrime legislation: domestic legislation (including case law) and international standards
- Jurisdiction and territorial competencies
- Electronic evidence: technical procedures and legal considerations.

As a result of such basic training judges and prosecutors should be in a position to:

- Relate criminal conduct to provisions in domestic legislation
- Approve investigative techniques
- Order the search and seizure of computer systems and the production of electronic evidence
- Expedite international cooperation
- Question witnesses and experts
- Present/validate electronic evidence.

The following is an example of a typical basic training course for judges and prosecutors.

Example: Cybercrime and electronic evidence training - a typical module to provide basic knowledge

Course objective	By the end of the course judges and prosecutors should have basic knowledge of what are cybercrime and electronic evidence, how judges and prosecutors can deal with them, what substantive and procedural laws as well as technologies can be applied, and how urgent and efficient measures as well as extensive international co-operation can be taken
Session 1	About cybercrime
	➢ Why worry about cybercrime? ➢ What is cybercrime? ➢ Challenges for judges and prosecutors ➢ National law and international standards
Session 2	Technology
	➢ Functioning of the internet (basic notions) ➢ Glossary of terms ➢ Protocols
Session 3	Cybercrime as a criminal offence in domestic legislation
	➢ Offences against computer data and systems ➢ Computer-related fraud and forgery ➢ Content-related offences (child pornography, xenophobia, racism) ➢ Intellectual property-related offences ➢ Court decision/case law
Session 4	Electronic evidence
	➢ About electronic evidence: definitions and characteristics ➢ Requirements of electronic evidence ➢ Computer Forensics
Session 5	Procedural law/investigative measures
	➢ Jurisdiction and territorial competencies ➢ Expedited preservation of computer data ➢ Production orders/warrants ➢ Search and seizure of computer data ➢ The interception of traffic and content data ➢ Safeguards
Session 6	Interaction with the private sector
Session 7	International co-operation
	➢ The Convention on Cybercrime as a framework for international co-operation ➢ General principles ➢ Provisional measures and the role of 24/7 points of contact ➢ Mutual legal assistance and the role of competent authorities
Session 8	Evaluation and conclusion
Logistics and materials	The training could be provided online or in classroom. If provided in classroom: ➢ Training room with a PC and projector for presentations is sufficient (as this course does not include practical exercises such as the demonstration of forensic software or investigative techniques, a computer laboratory is not required) ➢ Relevant extracts of domestic substantive and procedural legislation ➢ Budapest Convention on Cybercrime including explanatory report ➢ Reader with glossary of terms and other background information ➢ If lectures are provided in a foreign language, interpretation should be foreseen and materials should be translated.

4.2 Advanced knowledge

Sometimes, basic knowledge is not sufficient to carry a judicial case of cybercrime. To face these kind of situations, it would be required that a considerable number of judges, investigative judges and prosecutors to have advanced knowledge in order to investigate/prosecute/judge complex cases related to cybercrime and electronic evidence, or to provide support to other prosecutors and judges.

In some countries, specialised prosecution units or departments have been established (e.g. Romania, Serbia), in others larger prosecution services dispose of a number of specialised prosecutors. In the Netherlands, the programme "intensiveringsprogramma" is underway to ensure among other things that there is at least one specialised prosecutor on cybercrime in each of the eleven largest offices. In Italy, under the new cybercrime legislation 29 prosecution offices now have jurisdiction in cybercrime matters. In Portugal, the Lisbon District Prosecution Service has a specialized section on computer crime, where these investigations are distributed.

In some countries, specific prosecutors may supervise the work of high-tech crime units of the police. In most countries, prosecution services are hierarchically organised so that a senior prosecutor could assign a case to a specialised prosecutor. Thus, it is possible to identify prosecutors that should have an advanced level of knowledge.

With regard to judges, in some countries, it is possible that cybercrime cases are assigned to a specialised judge at a court dealing with particular types of crime, such as organised crime. An example (possibly the only one in Europe) is Serbia where a special department at the district court of Belgrade is dealing with cybercrime cases. However, given the principle of the natural judge in most judicial systems, a different approach is necessary. In the Netherlands, perhaps unique in Europe, five centres with specialised judges have been established that serve as a resource to other judges. In Spain, a similar proposal is being discussed by the General Council of the Judiciary under which a group of judges specialised in cybercrime and electronic evidence would assist and advise other judges. In Belgium, there is no specialization requested by law but most of the courts have the possibility of requiring one or more of their members to specialize. The fact that those cases are attributed to such specialized judges is however only a question of internal organization of the court. Sometimes the competence for judging some cases is given by law to specific courts of the country (Brussels). However, in most of the cases the competence is determined by the place of the criminal act and a specialized judge/prosecutor is not always there. In many countries there may be courts dealing with cybercrime cases more often than others, thus requiring a higher level of specialisation than others.

"Advanced knowledge" means that judges and prosecutors should have practical understanding and are able to apply their knowledge with regard to the following:

- Computers and networks:
  - Glossary of computer and cybercrime terms
  - Functioning of the internet
  - Protocols and technology
  - Role of service providers

- Cybercrime:
  - Trends in cybercrime
  - Typologies: Particular types and techniques of cybercrime (eg phishing, botnets and other malware, child pornography)
  - Practical examples and simulations

- Cybercrime legislation:
  - Domestic legislation and case law

  - International cooperation: international and bilateral agreements, judicial cooperation channels and practical means for expedited cooperation

- Investigation and electronic evidence:
  - Jurisdiction and territorial competencies
  - Procedural law provisions and their practical application
  - Steps to search, seize and preserve electronic evidence
  - Features of forensic software
  - Identifying suspects
  - Following criminal money
  - Safeguards and conditions
  - Presenting electronic evidence in court.

Example: Cybercrime and electronic evidence training - a typical module for advanced knowledge[9]

Course objective	By the end of the course judges and prosecutors should have advanced knowledge that can be applied in practice on the functioning of computers and networks, what is cybercrime, cybercrime legislation, jurisdiction, investigative means and electronic evidence, and international cooperation
Session 1	Computers and networks
	➢ Glossary of computer and cybercrime terms ➢ Functioning of the ICTs/Internet infrastructure - Protocols and technology - How computers communicate - IP Investigation and electronic evidence -numbers and computer names - Role of service providers ➢ Information on the internet - Gathering of information - Use of (hidden) internet databases ➢ Profiles of social groups - Manners of communication - Manners of anonymity ➢ Detection/identification of the location and identity of computers, companies and persons on the internet
Session 2	Cybercrime and security risks
	➢ Trends in cybercrime ➢ Typologies: Particular types and techniques of cybercrime (eg phishing, botnets and other malware, child pornography) ➢ How criminals use information and communication technologies ➢ Offenders ➢ Impact of cybercrime ➢ How to enhance the security of ICTs ➢ Practical examples and simulations
Session 3	Cybercrime legislation: Substantive criminal law
	➢ Offences against computer data and systems ➢ Computer-related fraud and forgery ➢ Content-related offences (child pornography, hate crime) ➢ Intellectual property-related offences ➢ Court decision/case law
Session 4	Investigation and electronic evidence
	➢ Electronic evidence - Traces/footprints on computers, the internet, digital communication

[9] Based on replies to the questionnaire and the example provided by the Netherlands.

	- Steps to search, seize and preserve electronic evidence - Features of forensic software - Identifying suspects - Following criminal money - Safeguards and conditions - Case management/preparation - Presenting electronic evidence in court ➢ Organisation of law enforcement with respect to cybercrime/electronic evidence ➢ Case studies
Session 5	Cybercrime legislation: procedural law
	➢ Expedited preservation of computer data ➢ Production orders ➢ Search and seizure of computer data ➢ The interception of traffic and content data ➢ Safeguards ➢ Interaction with internet service providers/private sector ➢ Case studies
Session 6	Jurisdiction and territorial competencies
	➢ General principles ➢ Cybercrime jurisdiction - challenges ➢ The jurisdiction provisions in the Convention on Cybercrime ➢ Case studies
Session 7	International co-operation
	➢ The Convention on Cybercrime as a framework for international co-operation ➢ General principles ➢ Provisional measures, the role of 24/7 points of contact and police co-operation ➢ Mutual legal assistance and the role of competent authorities ➢ Case studies
Session 8	Evaluation and conclusions
Logistics and materials	The training could be provided online or in classroom. If provided in classroom: ➢ Training room with a PC and projector for presentations ➢ It would be useful that trainees have a computer with internet access (but this is not a condition) ➢ Relevant extracts of domestic substantive and procedural legislation ➢ Budapest Convention on Cybercrime including explanatory report ➢ Reader with glossary of terms and other background information ➢ If lectures are provided in a foreign language, interpretation should be foreseen and materials should be translated.

Judges and prosecutors usually will not need the type of technical skills and knowledge required by high-tech crime or forensic investigators. Nevertheless it may be useful to recall the efforts made to arrive at a systematic training programme for law enforcement officers.

With funding from the European Commission (Falcone Programme 2002), a project led by the Irish Garda Siochana and with the participation of experts from ten EU Member States developed a standardised basic ("Level 1") cybercrime training programme for law enforcement officers. Since 2004 a two-week course is available and has been delivered in many European and non-European countries. The course was accredited by University College Dublin (UCD) in 2006.

Under further projects led by the Irish Garda in partnership with UCD additional intermediate and advanced modules were developed with the overall aim of a fully accredited Masters Degree programme in Forensic Computing and Cybercrime Investigation for law enforcement officials globally. Existing intermediate-level modules for law enforcement include:

- Internet Investigations
- Network Investigations
- NTFS Forensics
- Linux Forensics
- Mobile Telephone Forensics
- Wireless LANS and VOIP
- Advanced Scripting
- Live Data Forensics
- Microsoft Vista Forensics.

These modules are constantly updated and additional modules are in preparation.[10]

In July 2007, Europol set up the Cybercrime Investigation Training Harmonisation Group which has the primary objective of coordinating the efforts within the EU on high tech crime training in order to establish a certified training curriculum for law enforcement investigators within Europe and to disseminate this beyond the EU to assist other law enforcement agencies who wish to do the same. Partners include the European Commission, OLAF, Eurojust, CEPOL, Interpol, Council of Europe, United Nations, UCD Centre for Cybercrime Investigation, University of Troyes, Canterbury Christchurch University, University of Bologna, as well as the industry.

4.3 Specialist knowledge

Some judges and prosecutors may acquire specialist knowledge through post-graduate studies, self-training, networking or professional experience. Such knowledge would not be part of regular training programmes. Judges and prosecutors with such specialist knowledge are a valuable resource for others and as trainers.

[10] Other examples include the high-tech crime programmes of the UK National Policing Improvement Agency.

5 Current training on cybercrime and electronic evidence

5.1 Initial training

“Initial training” means the training that candidates – after having completed university level law studies – receive in order to become judges and/or prosecutors. In many systems, the initial training is provided by a judicial training institution over a one to three year period; in some others such initial training consists of more or less formalised practical training on the job without a specific curriculum.

In most countries, cybercrime and electronic evidence are not foreseen in initial training or to a very limited extent. For example:

- In France, the procedural law training at the Ecole Nationale de la Magistrature (ENM) includes a three-hour lecture by an IT specialist on the search for electronic evidence and on technology; cybercrime matters are not covered.
- In Georgia, it is not foreseen in the initial training for prosecutors, but in the training for judges and court staff where a half day course in the form of a lecture is taught.
- In Germany it is not a requirement in the practical on-the-job training.
- In Croatia, Poland and Romania these topics are not included in initial training.

However, in some countries cybercrime and electronic evidence is a regular feature of initial training. For example:

- In the Netherlands, initial training contains a basic one day course on cybercrime which is taught by the Education Institution for Prosecutor and Judges (SSR) in Utrecht or Zutphen and includes a reader and other background information. The course involves interactive seminars and case studies. In addition to this basic one-day course and in-depth four-day training, a two-day masterclass is offered.

- The Spanish Judicial School provides initial training on cybercrime and electronic evidence to newly appointed judges, in both procedural and substantive matters. It is part of the mandatory training on procedural law and evidence taking. Cybercrime and electronic evidence are covered by seminars over four afternoons and include national law, international cooperation instruments, demonstration of forensic software and investigative techniques, seizure of electronic evidence and case studies. In addition, once a year a special seminar on electronic evidence is organised and another seminar on substantive law (crimes committed by electronic means). These seminars are taught by legal as well as IT specialists. Moreover, judges have access to a virtual library on e-crime. The aim of this initial training is to provide basic knowledge.

- In “the former Yugoslav Republic of Macedonia”, the Training Academy for Judges and Prosecutors provides initial training on cybercrime and electronic evidence as part of the training on criminal law, IT and searches. Ten hours are foreseen for cybercrime and electronic evidence.

- In Portugal cybercrime is not a specific and autonomous subject part of the curricula. However, within the area of criminal investigation there is a specific seminar (one and half hour of training time) on cybercrime and digital evidence. During the training on criminal law and criminal procedural law, 9 hours are dedicated to computer crimes and procedural measures for obtaining digital evidence and 9 hours to ICT.

The courses are delivered by permanent trainers, judges, prosecutors or lawyers with experience in the matter, specialised police officers, IT experts or specialists from private sector companies.

Information available suggests:

- Given the goal of providing all judges and prosecutors with a basic level of knowledge of cybercrime and electronic evidence, the training on offer is far too limited.
- With very few exceptions, initial training covers basic levels only and advanced training is not foreseen.
- Standardised training materials for replicable training are usually not available.

5.2 In-service training

In-service training, that is, continued professional training of serving judges and prosecutors, is offered either by public judicial training institutions but may also be provided by a range of other organisations. For example:

- In France, the Ecole Nationale de la Magistrature holds a five day advanced-level seminar at the school, and in addition offers two-day internships at the high-tech crime office of the Ministry of the Interior (OLCTIC). Cost (some Euro 5,000 per course) is covered by the school. Trainers are judges, prosecutors, police officers, IT experts, or selected experts from industry.

- In Georgia, the High School of Justice is the only institution in charge of in-service training for judges. They carried out a basic two-day course on cybercrime, funded from the State budget. Trainers are members of the faculty and judges of the Supreme and appellate courts. Prosecutors are trained by the training unit of the Ministry of Justice but courses on cybercrime and electronic evidence have not been organised so far.

- In Germany, in-service training for judges and prosecutors is provided by the Deutsche Richterakademie which organises some 150 events per year. In 2009, two of these were aimed at cybercrime and had a duration of four-days each. Trainers are usually prosecutors and judges with experience in cybercrime matters, but can be also from police, customs, tax authorities or others. The cost is shared between the Federal and State Governments. These courses provide basic and advanced knowledge.

- In the Netherlands, although in-service training is optional every judge is obliged to spend a specific number of educational hours per year. Each judge can decide which course(s) to follow. The Educational Institution for Judges and Prosecutors (SSR) but also several other institutions and post-graduate education facilities offer in-service training on cybercrime and electronic evidence covering both basic and advanced levels. The SSR offers every year three basic and three in-depth courses and one masterclass. Trainers are cybercrime specialists from the national prosecution service as well as experts from private companies and industry. However, the SSR also offers a wide range of other training courses and covering both legal and practical aspects (totalling around 400 courses). Thus, cybercrime training must compete with all these courses.

- In Poland, the Polish National School of the Judiciary and Public Prosecution offers basic and advanced level courses in the form of conference with a duration of four to five days. In 2009, two such events were organised ("Methodology of crimes committed with the use of information systems", "Electronic proof in trial").

- In Romania, the National Institute of Magistrates provides in-service training but only at the basic level. For example, from 2006 to 2009, two two-day seminars, each for some 25 judges/prosecutors, were organised each year, mostly from the budget of the NIM, some with European Commission (PHARE) funding, and some (in 2006) with the support of eBay.

Trainers are Romanian magistrates, IT specialists as well as foreign experts funded by organisations such as the Council of Europe. Cybercrime is furthermore a mandatory subject of the decentralised training at the level of the prosecution offices attached to courts of appeal. This training is also coordinated by the NIM.

- In Spain, the Spanish Judicial School under the General Council of the Judiciary provides in-service training for judges on cybercrime and electronic evidence. For prosecutors such training is offered by the Centre of Legal Studies under the Ministry of Justice. In both cases, the training is organised in cooperation with CYBEX, a private company specialised in these matters. The Judicial School has a budget of some Euro 42,000 for cybercrime training. Private sector funding and support is possible. The in-service training covers basic levels, and the courses have a duration of three to four days and include lectures and analyses of practical cases. The materials are published and normally available for every judge. In 2008 and 2009 two such seminars were held each year. Although some matters are dealt with in some depth, a systematic advanced level training programme is not available.

- In Portugal, the in-service training on cybercrime is provided by the Center for Judiciary Studies that organizes around 30 events per year. Two of them are regularly on basic cybercrime matters. Sometimes there are other seminars on related matters, such as copyright online or technology and the courts. The trainers are judges and prosecutors, lawyers, police officers and experts from public and private sectors. The seminars are well received having a large number of participants (mostly prosecutors, but also lawyers and judges from criminal courts).

- In Belgium the programme for in-service training is still under construction due to the recent creation of the ”Institut de Formation Judiciaire”. The purpose is obviously to organize such training taking into account the results and recommendations of several think tanks and among them the observations of the Council of Europe. The participation of Belgian magistrates in training abroad can be financed by the Institute at the request of the magistrate (e.g. one judge and one prosecutor followed the European certificate on cybercrime and e-evidence organized in Paris in February of 2009).

- Currently, in Croatia there is no in-service training on cybercrime and/or electronic evidence. This matter was addressed only due to CARDS programme in which Croatia participated.

- In “the former Yugoslav Republic of Macedonia” no in-service training is offered.

- Training offered by the Academy of European Law (ERA). ERA, formally established on the initiative of the European Parliament in 1992 aims at providing in-depth knowledge and analysis of European and Community law by organising practically oriented seminars and courses for practitioners of law. The Academy is also a forum for the exchange of experience and views about European law and policies. The ERA organises on a regular basis open events on cybercrime attended by participants coming from all over the EU. For the period 2009-2010 ERA is also cooperating with TAIEX, implementing a series of seminars for Romania, Bulgaria, the candidate countries and potential candidate countries that will present the main European and international instruments to fight cybercrime.
  All seminars are intended as a platform to debate and assess how European legislation in the field of cybercrime is applied in the different Member States and candidate countries as well as the perspectives for an effective Europe-wide campaign against illegal use of the internet. The most recent European legal acts and instruments such as the Council of Europe Convention on Cybercrime (2001), Council Framework Decision 2005/222/JHA on attacks against information systems and Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography are debated. Ongoing co-operation with service providers and web societies such as Google, Microsoft and Yahoo! is also discussed.

Each seminar offers a mixture of training methods, varying from introductory and more in-depth lectures to case studies and other types of interactive learning. Particular attention is devoted to discussion in small working groups. Lectures and workshop sessions are presented by EU and national experts.

- In a number of countries training events are supported by industry. For example:

  In Germany, eBay has supported the New Media and Criminal Law training course for judges and prosecutors organised by the Deutsche Richterakademie by providing a speaker to present the eBay Marketplace, the related criminal activity, the countermeasures in place and how eBay works with law enforcement. eBay has also participated in several 'one time' trainings organised by the Berlin Senate of Justice with around 100 prosecutors participating each time.

  In Romania, eBay has conducted numerous trainings for judges, prosecutors and law enforcement. In particular, eBay worked with the US Secret Service at the US Embassy to offer training for 25 prosecutors from different DIICOT (Directorate for Investigation Organised Crime and Terrorism) offices, 15 judges and 20 police officers in Sibiu. Furthermore, eBay participated in additional training opportunities for judges in Targu Jiu as well as for 60 judges from different courts under the appeal court Craiova.

As indicated earlier, in almost all cases, changes or additions to the curricula on judicial institutional training would require a formal validation and approval process.[11]

Although it is clear that many initiatives are taking place to address the need for delivering adequate training on cybercrime to judges and prosecutors, there is an evident lack of consistency between the approaches described above.

Even in taking into consideration the national specificities in law and the fact that education systems vary greatly, cybercrime issues are international by nature and demand a minimum level of coordination and consistency among countries. A similar understanding across borders of what is cybercrime can only improve consistency in court decisions and prevent the creation of safe havens for criminals, while providing training institutes with quality training content at a reduced cost.

Information available suggests the following:

- Most in-service training on offer covers basic levels.
- Only very few courses are offered, reaching only a very small number of judges and prosecutors.
- In most cases, the basic courses appear not to be standardised. They thus do not seem to be replicable and do not allow a judge or prosecutor to progress from basic to advanced levels in a systematic manner. The Netherlands seems to be an exception in this.
- Training materials appear to be scattered and prepared ad-hoc.

[11] Against this background, the project of the "European Certificate on the fight against cybercrime and the use of electronic evidence" implemented by CYBEX with funding of the European Commission (JPEN) is of interest. It includes a four-day standardised basic level course for judges, prosecutors and lawyers. Between early 2009 and late 2010 the course will be tested in 14 pilot countries in Europe and Latin America. Participants will receive a certificate showing that they have acquired a basic-level theoretical and practical, legal and technical knowledge on electronic evidence and cybercrime related issues.
The Council of Europe – under the Project on Cybercrime – has also begun to develop a training manual for judges and prosecutors for a two-day basic level course with a focus on cybercrime legislation.

- Given that eventually all judges and prosecutors need at least basic knowledge of cybercrime and electronic evidence, the training on offer is largely insufficient, in particular considering that the current generation of practicing judges and prosecutors has in all likelihood not received any initial training nor covered these topics during university studies.
- With few exceptions, training offering knowledge at advanced levels for judges and prosecutors is not available.
- Given the international nature of cybercrime, a minimum level of coordination and consistency among countries would be necessary.

6 The approach proposed

6.1 The objective

As demonstrated in the previous section, in general, current initial and in-service training does not provide judges and prosecutors with the level of knowledge required to deal with cybercrime and electronic evidence.

Thus, the objectives of a training concept for judges and prosecutors should be:

- To enable training institutes to deliver initial and in-service cybercrime training based on international standards
- To equip the largest possible number of future and practicing judges and prosecutors with basic knowledge on cybercrime and electronic evidence
- To provide advanced training to a critical number of judges and prosecutors
- To support the continued specialisation and technical training of judges and prosecutors
- To contribute to enhanced knowledge through networking among judges and prosecutors
- To facilitate access to different training initiatives and networks.

The following measures should help achieve these objectives.

6.2 Institutionalising initial training

- In countries where initial training is practical training on the job (a type of apprenticeship or series of internships) without a formalised curriculum, it is recommended that at least part of such training (e.g. one internship or similar) is related to cybercrime and electronic evidence.

- In countries where initial training is provided by judicial training institutions:
  - their curriculum should contain as a minimum one basic level module on cybercrime and electronic evidence
  - these issues should in addition be covered in mandatory modules covering substantive and procedural law
  - optional modules for advanced knowledge on cybercrime and electronic evidence should be offered.

The specific training modules should be standardised to the point that they are replicable and allow candidates to progress from basic to advanced levels. Replicable means that they can be repeated at least within the same country for different trainees, so that participants in different training events have a similar level of knowledge. This also means that the methods of delivering the training are standardised. In order to ensure that the quality of the training is consistently high an evaluation should be carried out at the end of each course.

6.3 Institutionalising in-service training

- In-service training institutions should offer at least one basic level module on cybercrime and electronic evidence in order to equip those practising judges and prosecutors with basic knowledge who didn’t have such training in their initial training.

- They should furthermore offer courses for advanced knowledge.

- Again: the specific training modules should be standardised to the point that they are replicable and allow candidates to progress from basic to advanced levels. It may therefore be necessary to harmonise the in-service training modules as much as possible with those of the initial training. The methods of delivering the training should also be standardised including quality control through evaluations at the end of courses.

- In order to train specialist judges and prosecutors internships in high-tech crime units or post-graduate courses/studies could be encouraged.[12]

6.4 Standardised and replicable courses/modules

- Standardised courses or modules should be developed that can be replicated at a broad scale in a cost-effective manner and that allow candidates and practising judges and prosecutors to progress from basic to advanced.

- Existing basic courses[13] that could be integrated into the curricula of initial or in-service training programmes, should be evaluated. A standard course could subsequently be recommended to initial and in-service training institutions.

- A similar evaluation could be carried out for advanced level courses and a standard advanced course could subsequently be recommended.

- Finally, trainers would need to be trained in the delivery of such courses to the point that training can be delivered by local trainers in local languages and only limited needs of international trainers.[14]

6.5 Access to training/self-training materials

- Training materials need to be developed reflecting common international standards and good practices. They should be made available to training institutions in a cost effective manner for the purpose of being delivered locally. Obviously, while for law enforcement training focusing on technology and forensics at a high level of standardisation is possible, this is less the case with regard to the training of judges and prosecutors who need to be trained primarily in the application of domestic legislation. Nevertheless, it is possible to develop standardised training materials in a way that leave sufficient room to take into account domestic systems and legislation.

- In some countries, training materials are available online for judges and prosecutors.[15] This practice should be followed by other countries.

- On-line courses should be developed and made available.**[16]**

- Access to training courses (national and international) should be facilitated as much as possible through simplified approval procedures.

[12] For example, the basic two-week course developed by the Irish Garda and University College Dublin should be of interest also for judges and prosecutors.

[13] For example the ECCE-course developed and currently piloted by CYBEX.

[14] A "train the trainer" course has been developed by UCD and INTERPOL and could be made available. The course covers training skills, course development, etc. It is NOT a law-enforcement only course and can be delivered to anyone.

[15] Examples are the Netherlands and the CYBEX e-evidence library. As part of the 2CENTRE project, UCD will be developing online resources for the delivery of some of the AGIS/ISEC training material.

[16] For example, UCD currently offer two MSc programmes, portions of which are delivered entirely online. The CEJ of Portugal intends to organise an online course on Courts and ICTechnologies, with modules on cybercrime and on electronic evidence. It will be in Portuguese and the possibility to be expanded it to other Portuguese speaking countries (e.g. Brazil, Cape Verde, Angola, Mozambique, Guinea-Bissau, São Tomé or Timor) is considered.

6.6 Pilot centres for basic and advanced training

- A number of pilot centres for basic and advanced training of judges and prosecutors on cybercrime and electronic evidence should be established. Such centres could:
  - Test and further develop standardised courses and materials
  - Disseminate good practices
  - Carry out research on training
  - Maintain a register of trainers
  - Offer training of trainers
  - Provide training to other countries with similar systems and languages.

- Pilot centres should coordinate their work with each other with the support of the Council of Europe.

- Judges and prosecutors who are prepared to become specialists should consider participating in training through the centres of excellence for law enforcement and industry.[17]

6.7 Enhancing knowledge through networking

While initial and in-service training will provide judges and prosecutors with a foundation, peer-to-peer interaction, networking among judges and prosecutors, but also networking with a range of other stakeholders will be of crucial importance.

Thus:

- Judges and prosecutors should make use of existing networks for judges[18] or prosecutors (such as GPEN).[19]
- The creation of an international network of cybercrime or e-crime judges should be discussed (similar to GPEN for prosecutors) by the Council of Europe.
- The networking among European institutions offering training on cybercrime and electronic evidence should be supported by the Council of Europe and the European Judicial Training Network.
- In order to facilitate access by judges and prosecutors to these and the many cybercrime-related networks, the Council of Europe – on its www.coe.int/cybercrime site - should map initiatives and networks and establish a portal with links, brief information and contact details on different networks. This should also facilitate coordination among networks. It should furthermore facilitate access to existing training materials and initiatives.

[17] The 2Centre initiative (Cybercrime Centres of Excellence Network for Training Research and Education) was launched in March 2009 (during the Council of Europe's Octopus Conference). 2Centre "examines the current methods of training law enforcement and industry in IT forensics and cybercrime investigation. It reviews the activities undertaken by members of law enforcement and relevant industry personnel to gain knowledge and skills in an area which currently has a diverse range of levels of professional training, in-house training, cross training and on-the-job learning". University College Dublin is the first centre of excellence; the University of Troyes is to become the second in 2010.

[18] It seems that an international network for judges covering cybercrime and electronic evidence does not yet exist. An example for a national initiative is what has been developed in the Netherlands where a wiki-type intranet resource has been created.

[19] The Global Prosecutor's E-Crime Network, GPEN, is an initiative established in 2008 and is hosted by the International Association of Prosecutors (IAP). The network is to facilitate information exchange and cooperation among prosecutors in cases involving e-crime or cybercrime while taking into account the Convention on Cybercrime, to develop and deliver training programmes, to provide on-line resources to prosecutors. GPEN is a network of specialist e-crime prosecutors and each IAP organisational member has been invited to nominate at least one prosecutor to be registered as the GPEN national contact point. The network is managed by the GPEN Development Board drawn from the IAP membership.

6.8 Public private cooperation

Structured and regulated cooperation between law enforcement and the private sector (ICT industry, including internet service providers) is essential for the investigation of cybercrime and securing electronic evidence[20], and the private sector contributes expertise and other support to law enforcement training initiatives.

The support of the private sector to the training of judges and prosecutors would be beneficial given that the private sector disposes of relevant subject matter expertise. At the same time, judges and prosecutors must remain independent and impartial.

Thus:

- Judicial training institutions may make use of private sector expertise when designing training programmes, developing training materials and delivering courses.

- The support from industry to training institutions must not be conceived to potentially secure favourable decisions in court or to generate business, but to ensure that judges and prosecutors are given adequate information which enables them to make informed decisions.

- The private sector could support in a transparent manner international or national organisations, academia, training initiatives or other third parties which then support independent training institutions.

- While judges and prosecutors should have an overview of the Internet and cybercrime, it is also important to provide them with platform specific information. Industry could provide materials for specific modules (rather than full courses) on the functioning of relevant platforms.

[20] See for example the Guidelines for law enforcement – ISP cooperation adopted by the Council of Europe's Octopus Conference in April 2008.

7 Supporting the implementation of this concept

The implementation of this concept is primarily the responsibility of judicial training institutions but should be supported by public and private sector institutions and partners, including international organisations. In view of the significance of information and communication technologies for society, funding for such training measures will be a valuable investment and every effort should be made to provide training institutions with the necessary resources.

The Council of Europe and the European Judicial Training Network as well as other bodies should promote the implementation of the concept throughout Europe and beyond.

The EJTN and the Council of Europe could organise a joint conference on this concept in the near future.

The Council of Europe and the EJTN should regularly assess the progress made.

The implementation of this concept in practice should also be supported by donors. Interested donors and organisations could partner up to develop projects to assist training institutions and other stakeholders that are prepared to assume responsibility for the measures proposed in this concept.

In order to reduce the risk of conflicts of interest or compromising the impartiality of judges and prosecutors, donors – rather than offering direct support – could provide resources to neutral third parties such as international organisations who would then interact with training institutions.

8 Appendix

8.1 Lisbon Network: Links to judicial training institutions

Forty-four of the forty-seven member States of the Council of Europe are represented within the Lisbon Network. The Lisbon Network's members are relevant national institutions in charge of the initial and continuous training of judges and prosecutors. They can also be, depending on the cases, Schools of Magistrature, Centres for Legal training or magistrates' training units within the Ministries for Justice.

For the information available for each of the Network's member countries (including in certain cases associated training programmes), see:

- Albania
- Andorra
- Armenia
- Austria
- Azerbaijan
- Belgium
- Bosnia and Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Georgia
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Moldova
- Montenegro
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Russian Federation
- Serbia
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- "the former Yugoslav Republic of Macedonia"
- Turkey
- Ukraine
- United Kingdom
  - England and Wales
  - Scotland

Observer

- UNMIK

8.2 Examples of basic training courses: structure and topics covered

8.2.1 Netherlands example

<u>Basic training</u> – 1 day

Programme:

1 General orientation:

- What is cybercrime?
- Manifestation of cybercrime
- Legal framework for law enforcement and prosecution

2 Law enforcement:

- Digital law enforcement as daily practice
- Methods of law enforcement

3 Law enforcement (part 2):

- Internet and law enforcement under Act on special law enforcement privileges

Conclusions + evaluation

8.2.2 Germany (German Judicial Academy) example

<u>Basic training:</u> *„Forms of appearance and strategy for combating cybercrime*" – 4 days

Programme:

<u>Day 1:</u>

- Material German Penal Code
- Use of the German Penal Code in the context of computer- and internet criminality
- Problems of daily experience in prosecution office and in court

Speaker is a judge of Munich Court specialized in financial and economic crime, some years ago being a prosecutor working with cases of cybercrime, spying data, corrupting date etc.

- Problems of daily experience in prosecution office and in court in the Netherlands
- Development and combating of cybercrime in Europe
- Problems with providers in the Netherlands and other European countries
- Cybercrime Convention of the Council of Europe
- Importance and significance of the Cybercrime Convention for Europe and the rest of the world (China, USA, Russia)

Speaker is Professor Dr. Henrik Kaspersen, Netherland

<u>Day 2</u>:

- Sabotage of computer systems
- Internet hacking
- Traps of internet orders
- Spying of data
- Computer fraud with credit cards
- Attacks against bank data
- Phishing and new types of crime in the internet
- Botnets
- Fraud by eBay or other selling platforms

Speaker is a policeman of the German Headquarter of Police (BKA) Wiesbaden

- Preventive internet searching for organised crime, terrorism, severe crime, money laundering, etc
- Internet searching for announcement of persons running amok (schools, etc.)
- Internet searching for children pornography
- International cooperation in searching the net

- On-line searching (problems with the constitution)

Speaker is the leader of a special department of Headquarter of Bavarian Police (LKA Munich)

Day 3:

- Backup and evaluation of data in Germany or other countries
- Searching of data in the internet and traceability of the data in the net
- Possibilities of forensic IT and limits of data analyses
- Systems of anonymising data in the net
- Using cryptograms by criminals

Speaker is a specialist of Munich Police Headquarter

- New legal problems with backup and evaluation of internet-data
- Competence for all legal measures of searching
- Competence getting evidence for investigations and for court
- New development of legal enforcement

Speaker is a judge of Bavarian penal High Court in Bamberg

Day 4:

- Russian business network
- Intercage
- Protection against sabotage of computers or data
- Positive „hacking"
- Influence and falsification of election machines
- Political influence in new laws
- Population sitting in a house of glass

The speaker is a member of the famous Chaos Computer Club (CCC) of Hamburg, members of the club are trying to get in the computers of the government, the White House, the CIA. The club demonstrate how to manipulate water supply of a city, etc**.**

8.2.3 Council of Europe examples

1. Cybercrime training workshop for prosecutors, Belo Horizonte, Brazil, 26 August 2008 (organised by the Ministério Publico Estadual Minas Gerais in cooperation with the Council of Europe)

Basic training – 1 day

Programme:

1 Opening session
- Opening remarks
- Current legislative reforms

2 Cybercrime: phenomena
- Overview of current threats
- Specific threats and cases investigated in Brazil

3 Substantive law: what offences?
- International standards
  - Typology, legal concepts
  - Convention on Cybercrime
- Provisions under Brazilian law
  - Current provisions
  - Legal reforms underway

4 Investigations and international cooperation

- Role of prosecutors in the investigation of cybercrime
- National procedural law
- Procedural measures and international cooperation under the Convention on Cybercrime

5 Public-private partnerships

- Examples of public-private partnerships in Brazil
- Law enforcement – Internet service provider cooperation in the investigation of cybercrime: guidelines
- Discussion: Law enforcement – ISP cooperation: experience in Brazil

2. Cybercrime: training for judges, Cairo, Egypt, 9 and 10 June 2008 (organised by Microsoft with the contribution of the Council of Europe)
This course was delivered twice for different groups of judges from commercial courts (these are responsible for e-crime matters as well)

Basic training – 1 day

Programme:

1 Opening session

2 Cybercrime: phenomena

- Overview of current threats
- Specific threats
  - Fraudulent use of online identities and information: examples
  - Credit card and other types of fraud

3 Substantive law: what offence?

- International standards (Council of Europe expert)
  - Typology, legal concepts
  - Convention on Cybercrime
  - Criminalising identity theft
- Provisions under national law
  - Current provisions
  - Legal reforms underway

Part 2 Evidence in cybercrime proceedings

4 Investigations and criminal proceedings

- Procedural measures under the Convention on Cybercrime
- Role of police, prosecutors, judges, specialized services
- National procedural law

5 International cooperation

- Convention on Cybercrime
- Provisions under national law and bilateral agreements
- 24/7 points of contact
- Role of judges

6 Obtaining, preserving, using electronic evidence

- Evidence on the accused person's computer: Presence of digital files used for the cybercrime
- Evidence identifying a network location: IP addresses
- Evidence obtained from Internet Service Providers

7 Court proceedings and case law: examples

8.3 Examples of advanced training courses: structure and topics covered

8.3.1 Netherlands example

<u>In depth training</u> – 4 days
Programme:

<u>Day 1 and 2</u>

The infrastructure of Internet

- Understanding how internet works
- How do computers communicate?
- What are IP-numbers and computer names?

Information on the internet

- How to gather information from the internet
- Searching (hidden) internet databases

Profiling of Social Networks

- communication
- anonymity
- determine location and identity of computers, companies and persons on the internet

Digital tracks

- what are "tracks"?
- which tracks are left behind on a computer?
- which tracks are left behind on the internet?
- which tracks can be found in digital communication?

Security

- the risks of the internet
- the importance of a sound digital security
- safe storage of information
- e-mail security

During these two days each participant has access to a computer connected to the internet and have hands on experience of the themes that are discussed. Participants will get a name of a certain individual and are asked to gather as much information as possible from open access sources on the internet concerning this person. They are also asked to track e-mail (through the e-mail headers) origins or to search for tracks in digital communication.

<u>Day 3 and 4</u>

The legal framework

- Which are the competences of police and prosecutors in investigating cybercrime
- Case study by the team High Tech Crime

The Organization of investigating and prosecuting cybercrime in the Netherlands;

Interception (this will not be in the new course, because it will be part of the basic programme);

Digital counter-plea's

- which counter-plea's are known
- case law concerning these plea's
- which counter-plea's are to be expected in the future and how to react to them
- case studies

Each participant is provided with training materials, a reader that contains all of the topics discussed in the training and that can be used as a reference book, the print out of the presentations by the trainers and the book Handboek Digitale Criminaliteit by Arjan Dasselaar.

8.3.2 Master class proposal from the Netherlands

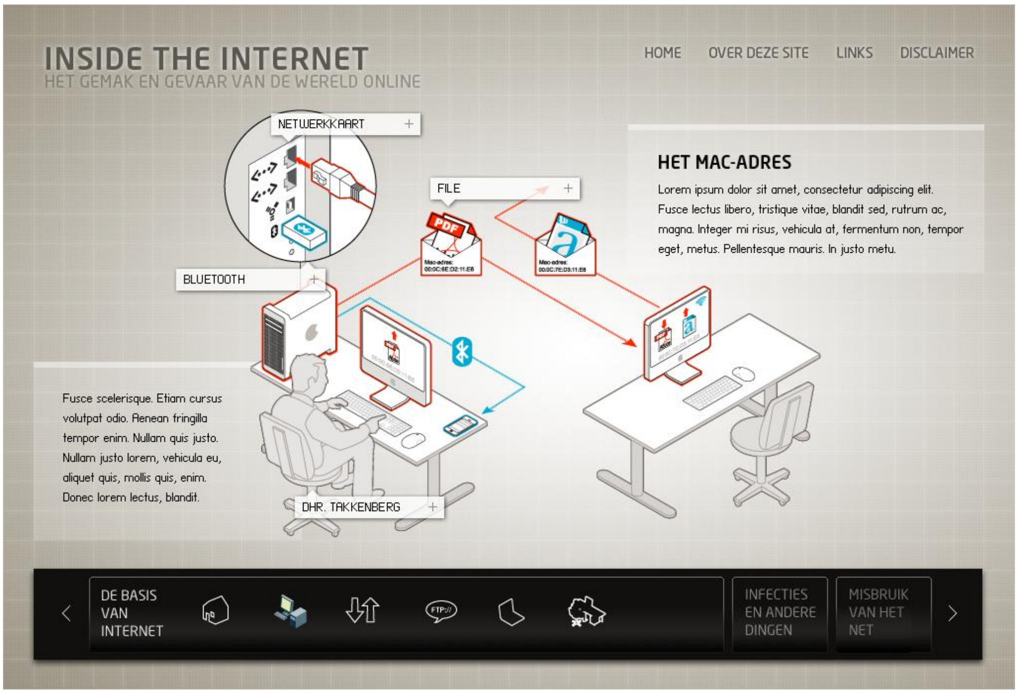
Developing a new course on cybercrime

The ‘Intensiveringsprogramma Cybercrime’, the National Prosecutor on Cybercrime and the SSR (the Dutch Judicial Training Centre) have been working on a new course on cybercrime which covers topics ranging from ‘interception’ to master classes cybercrime on specific themes (botnets).

There is no complete programme yet, but the first day will cover the basics of interception (wire and internet taps), the second day will be a basic course on cybercrime. Both these courses will be mandatory for *all* prosecutors in the Netherlands as a part of their permanent education. The second part of the course is for cybercrime specialists only (there will be strict conditions of admittance to these courses) and consists of an in-depth course (2 to 4 days) and a two day master class (yearly). These courses are given in cooperation with external partners, such as Fox-IT, Digital Intelligence Training and Hoffman Bedrijfsrecherche.

The reason for developing the course is not the dissatisfaction with the content of the training so far, but is to make sure that the parts of the course are more structured and better adjusted to each other, so that no overlap occurs. The appointment of cybercrime prosecutors at the eleven largest offices of the Dutch Prosecution Service as a part of the ‘Intensiveringsprogramma’ was also an important reason to develop / restructure the training. It is also vital to the new course that there is a build up; each participant is required to first take the two basis courses, before they are admitted to the in-depth training and master classes.

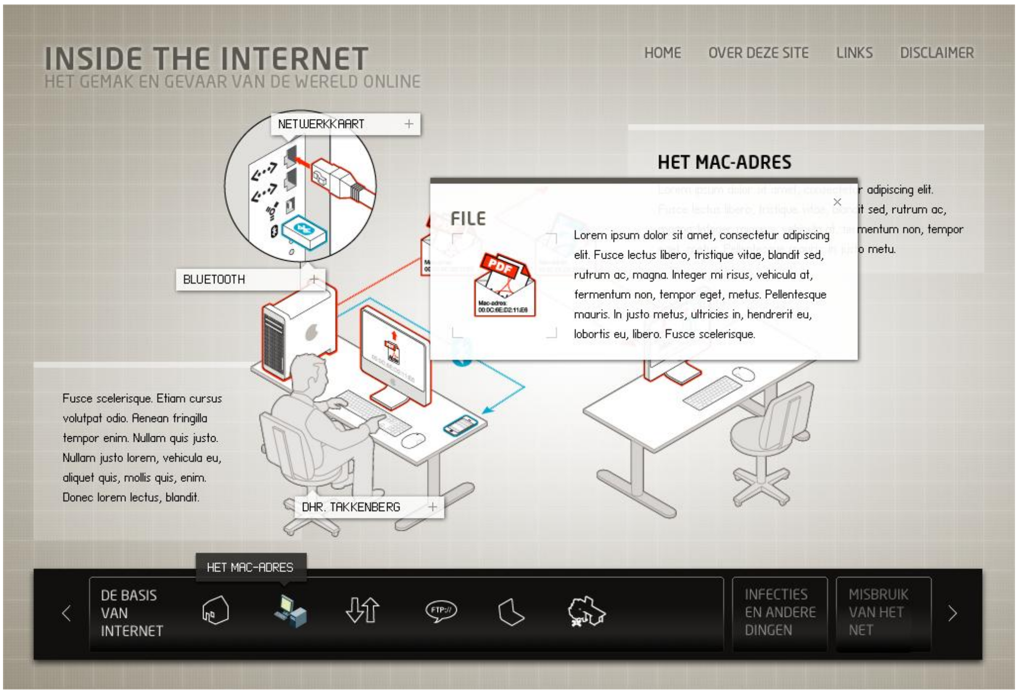
One of the new possible features of the new training will be an info graphic on the workings and risks of the internet. This info graphic is currently in the finishing stages of development and can also be used in trial presentations. Following are a few examples of how the info graphic will look.



HET MAC-ADRES

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce lectus libero, tristique vitae, blandit sed, rutrum ac, magna. Integer mi risus, vehicula at, fermentum non, tempor eget, metus. Pellentesque mauris. In justo metu.

Fusce scelerisque. Etiam cursus volutpat odio. Aenean fringilla tempor enim. Nullam quis justo. Nullam justo lorem, vehicula eu, aliquet quis, mollis quis, enim. Donec lorem lectus, blandit.



FILE

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce lectus libero, tristique vitae, blandit sed, rutrum ac, magna. Integer mi risus, vehicula at, fermentum non, tempor eget, metus. Pellentesque mauris. In justo metus, ultricies in, hendrerit eu, lobortis eu, libero. Fusce scelerisque.

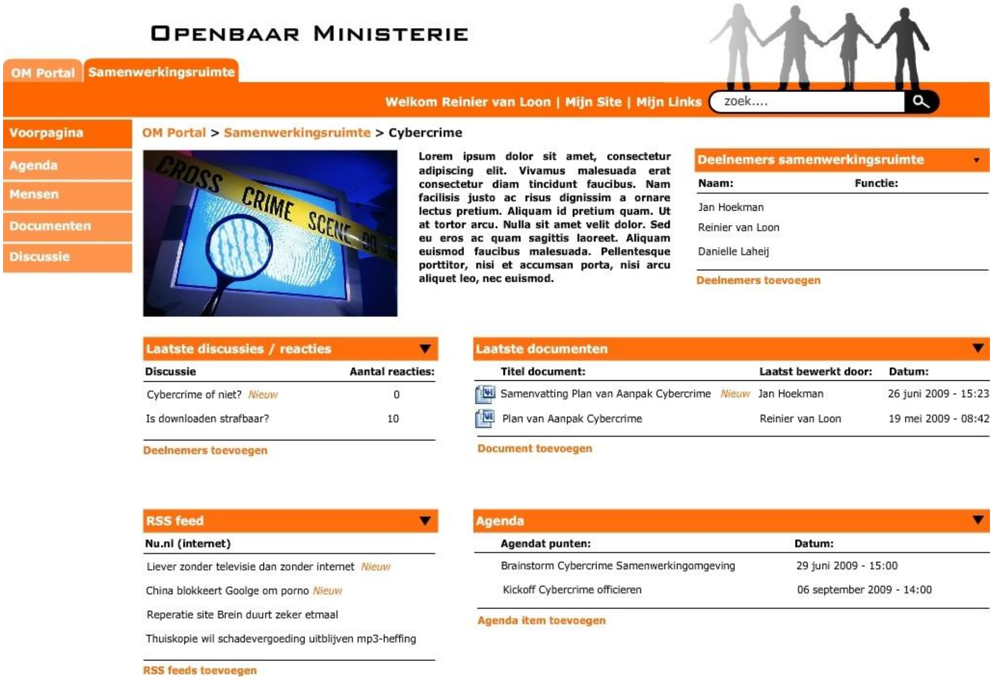
Fusce scelerisque. Etiam cursus volutpat odio. Aenean fringilla tempor enim. Nullam quis justo. Nullam justo lorem, vehicula eu, aliquet quis, mollis quis, enim. Donec lorem lectus, blandit.

Follow up

To ensure that the prosecutors that deal with cybercrime on a day to day basis will be able to keep up to date with developments in the fast moving world of cybercrime two additional programmes are currently on their way.

The first is the establishment of a Knowledge and Expertise Centre at the National Prosecutors Office in Rotterdam. This Centre will provide answers to questions of technical and judicial nature, will keep up with the latest case law and will disseminate this and other relevant information amongst all cybercrime professionals both with the police force and the Prosecution Service (the centre is a joint venture by both organizations).

Secondly and annex to this project a ‘digital cooperation room’ is developed, comparable to a sharepoint application. In this virtual room cyber professionals can discuss matters related to their work and find all kinds of information relevant to their jobs. An inventory of what should be the content and (technical) possibilities of such a digital room will take place in October of this year. This is an example of how the home page of the digital room could look:



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus malesuada erat consectetur diam tincidunt faucibus. Nam facilisis justo ac risus dignissim a ornare lectus pretium. Aliquam id pretium quam. Ut at tortor arcu. Nulla sit amet velit dolor. Sed eu eros ac quam sagittis laoreet. Aliquam euismod faucibus malesuada. Pellentesque porttitor, nisi et accumsan porta, nisi arcu aliquet leo, nec euismod.

Deelnemers samenwerkingsruimte

Naam:	Functie:
Jan Hoekman	
Reinier van Loon	
Danielle Laheij	

Deelnemers toevoegen

Laatste discussies / reacties

Discussie	Aantal reacties:
Cybercrime of niet? *Nieuw*	0
Is downloaden strafbaar?	10

Deelnemers toevoegen

Laatste documenten

Titel document:	Laatst bewerkt door:	Datum:
Samenvatting Plan van Aanpak Cybercrime *Nieuw*	Jan Hoekman	26 juni 2009 - 15:23
Plan van Aanpak Cybercrime	Reinier van Loon	19 mei 2009 - 08:42

Document toevoegen

RSS feed

Nu.nl (internet)
Liever zonder televisie dan zonder internet *Nieuw*
China blokkeert Goolge om porno *Nieuw*
Reperatie site Brein duurt zeker etmaal
Thuiskopie wil schadevergoeding uitblijven mp3-heffing

RSS feeds toevoegen

Agenda

Agendat punten:	Datum:
Brainstorm Cybercrime Samenwerkingomgeving	29 juni 2009 - 15:00
Kickoff Cybercrime officieren	06 september 2009 - 14:00

Agenda item toevoegen

Creating a sense of urgency: training at the managerial level

Given the relatively small capacity of the Dutch police force, choices have to be made as to which crimes are investigated and which are not (note: the Dutch legal system allows the Prosecution Service not to investigate and prosecute crimes, this is called the opportuniteitsbeginsel). It is usually at the managerial level where these choices are made.

It is recognized by the police and the Prosecution Service that at this level there is a lack of knowledge concerning the impact of cybercrime and importance of fighting it, so there is a risk that important cases will not be dealt with because other (conventional) crimes are deemed more important. Therefore a training course for police and Prosecution Service managers is currently being developed. According to schedule a pilot training will be given end of this year. This training will aim at creating a sense of urgency and will mostly confront the participants with the reality of cybercrime in today’s society. It will not deal with the topics on a content level (as the in-depth training does), but at a strategic, managerial level.