COUNCIL OF THE EUROPEAN UNION

Brussels, 3 February 2014

5335/1/14 REV 1

LIMITE

GENVAL 3 CYBER 3

NOTE

From :	Presidency
To :	Working Party on General Matters including Evaluations (GENVAL)
Subject :	Seventh round of mutual evaluations - Questionnaire

Delegations will find enclosed the questionnaire for the seventh round of mutual evaluations, as agreed following the discussions at the meetings of the Working Party on General Matters including Evaluations (GENVAL) on 27 November 2013 and 22 January 2014.

In line with Article 2 of the Joint Action 97/827/JHA of 5 December 1997, GENVAL decided at its meeting of 3 October 2013 that the seventh round of mutual evaluations will be devoted to the practical implementation and operation of the European policies on prevention and combating cybercrime.

ANNEX

7th round of Mutual Evaluations

The practical implementation and operation of European policies on prevention and combating Cybercrime

One of the consequences of the rapid growth in global connectivity is the increasing growth of computer crime, which figures amongst the current ten "eurocrimes" (Article 83(1) TFEU). For the same reason, the number of initiatives and activities aiming at preventing and combating cybercrime at EU-level is also growing.

The Stockholm Programme[1] includes a number of measures to counteract cybercrime in the context of the fight against organised and serious crime among the strategic guidelines for legislative and operational planning within the area of Justice, Security and Freedom for the period 2010 - 2014. The Europol 2013 Serious and Organised Crime Threat Assessment (SOCTA)[2] considers cybercrime an ever increasing threat to the EU in the form of large scale data breaches, online fraud and child sexual exploitation, while profit-driven cybercrime is becoming an enabler for other types of criminal activity. The JHA Council on 6-7 June 2013[3], within the framework of the Policy Cycle, designated cybercrime as one of the nine EU priorities in the fight against serious and organised crime between 2014 and 2017.

The Council Conclusions on the EU Cybersecurity Strategy of June 2013[4] reiterate the objective of ratification of the Council of Europe Convention on Cybercrime(the Budapest Convention)[5] of 23 November 2001 as soon as possible and emphasise in their preamble that "the EU does not call for the creation of new international legal instruments for cyber issues". This Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems[6].

---

1 OJ 2010/C 115/01 of 4.5.2010.

2 7368/13 JAI 200 COSI 26 ENFOPOL 75 CRIMORG 41 CORDROGUE 27 ENFOCUSTOM 43 PESC 286 JAIEX 20 RELEX 211.

3 12095/13 JAI 611 COSI 91 ENFOPOL 230 CRIMORG 98 ENFOCUSTOM 118 PESC 843 RELEX 630.

4 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

5 CETS no. 185; opened for signature on 23 November 2001, entered into force on 1 July 2004.

6 CETS no. 189; opened for signature on 28 January2003, entered into force on 1 March 2006.

Cyber security, including online child abuse, fraud attacks on information systems and cloud security and e-crime prevention in the EU will continue to be among the priorities of the Post-Stockholm Process in the JHA area[7] .

The choice of cybercrime as the subject for the 7th Mutual Evaluation round was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation will focus primarily on three specific areas: cyber attacks, child sexual abuse/pornography online and online card fraud and will provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU-agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[8](transposition date 18 December 2013), and Directive 2013/40/EU[9] on attacks against information systems (transposition date 4 September 2015), are particularly relevant in this context.

In order to facilitate Member States in providing their responses, the present questionnaire builds upon a questionnaire used by the United Nations Office on Drugs and Crime (UNODC) for the preparation of a recent study on Cybercrime[10], but with a clear focus on EU legislation, cooperation between Member States and reflecting in particular the role of the EU Agencies active in the cybercrime field, namely Europol/EC3, ENISA (European Union Agency for Network and Information Security) and Eurojust. Their expert input will be sought both for the final drafting and completion of the questionnaire in so far as they consider it appropriate.

---

7 doc. 17808/1/13 REV 1.
8 OJ L 335, 17.12.2011, p. 1.
9 OJ L 218, 14.8.2013, p. 8.
10 http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

When answering the questionnaire, delegations are invited to observe the following guidelines:

- one single completed questionnaire per MS combining the contributions of all appropriate authorities should be returned;
- organisation charts or alternatively brief description of the competences and the place within the national system of the respective judicial, Law Enforcement Agencies (LEAs) and other authorities that participated in completing the questionnaire, should be provided.
- practitioners (judicial and LEAs), as well as technical experts should be consulted as much possible, especially where a detail of practical expertise is sought;
- answering simply by "*yes*" or "*no*" should be avoided as far as possible;
- supporting information, including examples, both positive and negative, which may assist the evaluation team in its work should be provided, as appropriate;
- personal data relating to individual cases where specific examples are required should not be provided.

It should be noted that in accordance with Article 9 of the Joint Action 97/827/JHA of 5 December 1997, the experts of the evaluation teams are required to respect the confidentiality of the information they receive in connection with their task.

In case you have any questions related to this questionnaire or to the evaluation process in itself, please do not hesitate to contact the General Secretariat of the Council (secretariat.mutual-evaluation@consilium.europa.eu (functional mailbox)).

For the purposes of this questionnaire the following terms are used:

Table 1[11]	
"cybercrime"	a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware) [12]
"information system"	a device or a group of interconnected or related devices, one or more of which, pursuant to a program, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance[13]
"computer data"	representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function[14]

[11] The definitions included in Table 1 are only for the purposes of providing clarification and serving as a guidance where needed in filling in the questionnaire. The scope of the 7th round of evaluation is defined in Table 2.

[12] Definition contained in Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 7 February 2013 "The Cybersecurity Strategy of the European Union: An open, safe and secure Cyberspace ", footnote 5.
doc. 6225/13 POLGEN 17 JAI 87 TELECOM 20 PROCIV 20 CSC 10 CIS 4 RELEX 115 JAIEX 14 RECH 36 COMPET 83 IND 35 COTER 17 ENFOPOL 34 DROIPEN 13 CYBER 1.

[13] Article 2 (a) of Directive 2013/40/EU on attacks against information systems.

[14] Article 2 (b) of Directive 2013/40/EU on attacks against information systems.

"service provider"	any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service[15]

For the purposes of this questionnaire cybercrime is limited to the following three groups of criminal acts:

Table 2	
Acts unique to information systems, in particular those related to cyber attacks	• Illegal access to information system • Illegal system interference • Illegal data interference • Illegal interception of computer data • Misuse of devices - production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools
Content-related acts, in particular those related to child sexual abuse online and child pornography	• Computer-related production, distribution or possession of child pornography • Computer-related solicitation or "grooming" of children
Acts where computer/IT systems were involved as tool or target, in particular online card fraud	• Computer-related fraud or forgery • Computer-related identity offences • Sending or controlling sending of Spam

[15] Article 1(c) of the Council of Europe Convention on Cybercrime (ETS No. 185).

QUESTIONNAIRE[16]

1. General matters

1. Please indicate whether your MS has a national cyber security strategy. If so, please explain whether and how it addresses cybercrime. Provide a copy or web link to its full text, and if possible, translation in English or in French.
2. Briefly outline your national priorities with regards cybercrime, particularly in the area of prevention, legislation, capacity building, training, public awareness and international cooperation. Are the national priorities linked to the strategic goals and operational action plans elaborated for the EU "Cybercrime" Priority[17]?
3. Please indicate which governmental institutions are responsible for the prevention of and fight against cybercrime. Briefly outline their roles as well as their way of collaboration, cooperation and coordination with other institutions/bodies?
4. Please specify the main trends in your MS with regard to cybercrime in the recent years. If possible, provide in % the share of cybercrime in the total criminality picture in your MS.
5. Please describe how your statistics on cybercrime are compiled in terms of: participating institutions/bodies; are they integrated ; input from the private sector; are judicial statistics kept separately from the LEA statistics?. If possible, specify the share of input both of LEA and private sector into your national statistics.
6. Please provide any available statistics on the number of registered cases, investigations, prosecutions , final convictions, as well as the number of persons investigated, prosecuted for and convicted of cybercrime acts in the last 2 years.
7. How does your MS protect Fundamental rights/freedoms and Internet? (privacy, protection of personal data, freedom of expression) when tackling cybercrime?

---

[16] Note: this questionnaire will also be addressed to the European Cyber Crime Centre (EC3), Eurojust and the European Network and Information Security Agency (ENISA); they should reply in so far as they consider it appropriate.

[17] Council Conclusions on setting the EU's priorities for the fight against serious and organised crime between 2014 and 2017 (doc.12095/13)

8. Are there dedicated budget allocations for the prevention of and fight against cybercrime? Do you benefit from EU funding to tackle cybercrime?
9. Are you party to the CoE Convention on Cybercrime? If not yet, please explain the reasons and indicate when you are planning to complete the ratification process.

2. Legal aspects

2.A. Criminalisation

In respect of legislation and other rules, please provide copies in the original language and, if possible in English or in French, of relevant laws and explanatory memoranda, as well as any guidelines or instructions (ministerial or from the judiciary) to prevent/tackle cybercrime, as addressed as a subject to this evaluation.
In cases where the questions of this chapter relate to the implementation of the Directive 2013/40/EU on attacks against information systems and the implementation-process is not yet complete in your MS (transposition date 4 September 2015), please indicate (i) what you have already in place following the implementation of the Council Framework Decision 2005/222/JHA and (ii) how you plan to implement Directive 2013/40/EU.

1. Which cybercrime acts (among those listed in Table 2) are criminalised? Please indicate for each one of them:
   - the title and relevant provisions in your legislation
   - the definition used;
   - intent/recklessness;
   - aggravating/mitigating factors;
   - minimum and maximum penalties.;
   - multiple crimes/recidivism
   - incitement, aiding and abetting, and attempt

2. Does you legislation provide for liability of legal persons for cybercrime? Specify the nature (criminal/non-criminal) and scope of the liability (the offences), and the sanctions provided.

3. Does your legislation provide for specific criteria e.g. high economical, political or social impact or number of affected systems, level of damages , which would classify the cyber attack as a "serious" or "large scale" cyber attack?
4. How are minor cases treated?
5. Are there other types of cybercrime covered by your national legislation which are not mentioned in Table 2 above?
6. Do you plan to amend your existing legislation or introduce new legislation on cybercrime? If so, for what reason? If relevant, indicate any provisional planning in this regard? Are there any difficulties already foreseen in this respect? If so, how you plan to overcome them?
7. Please indicate any other binding or non-binding rules/ministerial or judiciary instructions relevant for the application of the cybercrime specific legislation.

2.B. Procedural issues

1. According to your legislation can fundamental rights and freedoms, in particular privacy, personal data, freedom of expression be limited for the purposes of cybercrime investigation/prosecution? If so, please briefly describe.
2. Please specify which of the following investigative techniques are permissible under your national law, including the relevant legal provisions and any specific conditions, such as derogations from the general regime:
    - search and seizure of information system/computer data;
    - real-time interception/collection of traffic/content data;
    - preservation of computer data;
    - order for stored traffic/content data;
    - order for user information.
3. Are the following defined in your legislation or practice: computer data, content data, traffic data, order for search/seizure of information system, networks managed or controlled by suspects of cybercrime?

4. Please explain how e-evidence, as defined under your legislation or practice (specify what is considered as e-evidence according to your law or working definition) is collected, stored and transferred to the prosecutor or the court to be used in a trial.

5. What are the admissibility rules for e-evidence, if any? Do they differ if the e-evidence is obtained outside your Member State?

6. Do you perform electronic or remote forensic examination? If so, please provide details.

7. With regard to encryption, please describe the following

   - possible problems you have encountered with encryption;
   - in which areas and how were those problems addressed;
   - how do the authorities involved cooperate with each other;
   - are there specialist centres;
   - is decryption carried out in cooperation with private companies;
   - in which areas has it not yet been possible to deal with the problem of encryption effectively;
   - what is done to address any security concerns that may arise in that context?

8. Please describe the special investigative techniques used for the purpose of cybercrime investigation in your MS. Which ones are most commonly used?

9. Please describe a good practice/lesson learned in respect to the use of a cybercrime investigation technique, if any.

2.C. Jurisdiction

1. Does your national law provide for jurisdiction with regard to cybercrime acts committed partially/entirely outside the territory of your MS? If so, please describe the criteria used (e.g. active/passive personality principle).

2. How do you resolve conflicts of jurisdiction when two or more MS can investigate and prosecute the same perpetrator for cybercrime acts committed outside their respective territories? Please provide details of any experience you have had in this area.

3. Indicate specific problems and solutions found as regards the establishment of jurisdiction for cybercrime acts committed in the "cloud" or collecting related e-evidence that is stored in the "cloud"?

4. Have you used provisions related to the Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings in relation to cybercrime cases[18]? Have you referred cases to Eurojust in order to solve conflict of jurisdiction? Please provide details about your specific experience.

5. Do you consider the existing legal framework sufficient for investigation and prosecution of cybercrime committed outside your national territory? If not, describe the main shortcomings and provide ideas how in your opinion those could be overcome.

3. National structures

3.A. Judiciary (prosecution and court)

1. Are cybercrime acts dealt in your country by a general or specialised prosecution/court? Please indicate respectively their number, place within the internal judiciary structure, special powers related to cybercrimes.
2. What measures have been taken or are planned to strengthen the capacity to investigate/prosecute cybercrimes in your MS?
3. Please specify the main obstacles to successful prosecution of cybercrimes in your MS. Have you experienced particular difficulties in prosecuting and/or obtaining conviction for any specific offence? Could you describe the reasons.

[18] OJ L 328, 15.12.2009, p. 42.

3.B. Law enforcement authorities

1. Please describe the law enforcement structure for preventing and combating cybercrime, specifying its composition and powers.
2. Do you have a specialised body to investigate cybercrime? If so, please provide details. If not, please explain which general entities/bodies are responsible for the investigation of cybercrime and whether they have specialised officers. Are there special posts for IT forensic examiners?
3. Please specify the main obstacles to successful investigation of cybercrimes in your MS.
4. Do you have operational 24/7 contact point for urgent requests? Please describe their organisational structure and competences. Please indicate the procedural steps which are followed in handling the requests (see Preamble, paragraph 22 and Article 13 of Directive 2013/40/EU and Article 35 of the Budapest Convention) .

3.C. Other authorities

1. Are there other national authorities besides judiciary and LEA responsible involved in the prevention of and fight against cybercrime? If so, please provide details on their structure and powers.
2. Please explain how the coordination between the various national authorities with a role in the prevention of and fight against cybercrime is organised in your MS.

4. Cyber attacks

1. Has your MS transposed into national legislation Directive 2013/40/EU[19] on attacks against information systems (transposition date 4 September 2015)? If so, did you experience any difficulties in implementation?
2. Could you indicate the nature and number of recent cyber attacks your MS has been subject to? Please provide specific details, as appropriate or share lessons learned or valuable conclusions that might be of interest to the other MS.
3. Is the private sector under any obligation to report cyber attacks in your MS? If so, please provide details on the procedure used, channels and scope of reporting.
4. Does your MS dispose with a coordinated multidisciplinary mechanism to respond to a serious cyber attack? If so, please describe the respective roles of the participating bodies, their responsibilities and procedures.
5. What is the role of operators of critical infrastructure and information systems in minimizing cyber attacks threats and mitigating their effects?
6. What are the obstacles that LEAs face when responding to cyber attacks (e.g. inability to analyze high volume of data, lengthy proceedings, different data retention periods, preserving evidence, limited knowledge/skills/capacity)? Please describe.
7. As cyber attacks often involve criminals from outside EU, do you make use of mutual legal assistance (MLA) instruments to successfully tackle this issue? If not, provide details on how you tackle this issue/deal with those cases?

[19] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

5. Offences related to child sexual abuse online and child pornography

1. Has your Member State transposed into national law Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography[20] (transposition deadline 18 December 2013)? If so, did you experience any difficulties in implementation?

5.A. Specific questions related to the act/victim

1. Are there any software databases specifically designed to identify victims in your MS?
2. What measures you have in place to avoid re-victimisation if images/videos are not deleted?
3. What measures you have in place to prevent child sex tourism? (Article 21 of Directive 2011/93/EU requires Member States to establish measures against advertising abuse opportunities and child sex tourism).
4. Have you developed specific measures to counteract real time web-based child pornographic performance?
5. Have you undertaken specific preventive actions, such as:
    - making hotlines available and providing specific information on how to make complaints,
    - developing information tools for children for safe use of Internet;
    - developing information tools on harmful/illegal behaviour online?
6. Have you put in place any measures to address the following: sex exploitation/abuse online, sexting, cyber bulling?

[20] OJ L 335, 17.12.2011, p. 1.

5.B. Filtering/Blocking of access /Removal of content/Take down of web pages containing or disseminating child pornography (Article 25 of Directive 2011/93/EU requires Member States to establish measures against websites containing or disseminating child pornography)

1. Does your MS apply any of the following measures: filtering, blocking of access , removal of content, take down of web pages? If so, please specify in which cases.
2. What tools are used to filter websites for child pornographic materials?
3. Which authority can authorise or coordinate blocking of access/removal of content/take down of web pages? What is the role and responsibility of private sector?
4. Please specify how this is done in practice (e.g. has this power been exercised in agreement with the competent authority). Is there a separate procedure for urgent cases? What is your experience in this respect (cases)?
5. How do you deal with cases where the server is located outside your MS? What EU or other mechanisms do you use in those cases?

5.C. International cooperation

1. Does your MS have any experience in using the International Child Sexual Exploitation Database at Interpol?
2. Does your MS participate in the European Union Strategic Group of the Heads of National High-Tech Crime Units at Europol and other forms of practical cooperation (including "cyber-patrols")?
3. Do you have specialized units dealing exclusively with child pornography? If so, please provide details regarding their composition, size, powers, etc.

6. Online Card fraud

1. Do citizens and private companies usually report online card fraud offences to LEAs? If not, please explain the main reasons why not, if known.

2. Is there sufficient/effective cooperation between industry, banks, private sector and LEAs to prevent and fight online card fraud in general terms and specifically to:
    - notify police/LEA if they become aware of any abuse of new payment tools developed by industry?
    - increase the security of non-cash payment and minimize the vulnerability of magnetic stripes?
    - strengthen the authorisation of online transactions and authentication of customers?
3. Is the LEA equipment (software and hardware), resources, capacity and knowledge at the necessary level to keep up with the pace of criminal development (newer and newer technologies being used by criminals)? Please provide specific examples, if any.
4. What concrete measures exist or are being developed in your MS to limit the access of organised criminal groups to:
    - financial data and credentials,
    - skimming devises and software,
    - know-how?
5. How does your Member State try to overcome obstacles to cross-border cooperation specifically regarding online card fraud?

7. International cooperation - tools (Mutual Legal Assistance (MLA), surrender/extradition)

7.A. Mutual legal assistance

1. Is there any specific legal basis in your MS for provision of Mutual Legal Assistance (MLA) for cybercrime.
2. Which authorities are responsible for receiving/sending requests for MLA in cybercrime investigations and for taking decisions on such requests? What communication channels are used to send/receive the request/decision and any additional information?
3. Please provide, if available, statistics on the number of requests sent/received, specifying under which instruments, , and as far as possible for which type of cybercrime acts as regards EU MSs and third countries respectively.

4. Are there any specific procedures or conditions that need to be fulfilled, as regards the various categories of MLA requests related to cybercrime? Please specify. How are urgent requests treated? What is the average response time?

5. What actions can be requested via MLA in respect to cybercrime? What are the most common reasons for MLA requests?

6. Do you use informal pre MLA consultation with the respective competent authorities of the other MS in relation to cybercrime? If so, through which channels?

7. Have you encountered specific problems in providing/requesting MLA assistance for offences committed in the "cloud"? If so, how did you address them?

8. Have you used a bilateral or multilateral treaty to which your MS is a party in order to execute/send a MLA request related to cybercrime with third states, Please provide details, including legal basis, which State, what type of MLA, results, any difficulties encountered.

7.B. Mutual recognition

1. Have you used any of the following EU mutual recognition instruments in relation to prevention, investigation and prosecution of cybercrimes?:
    - European protection order;
    - Mutual recognition of supervision measures;
    - Mutual recognition of custodial sentences and measures involving deprivation of liberty;
    - Recognition and execution of confiscation orders;
    - Mutual recognition of financial penalties;
    - Execution of orders freezing property or evidence.

7.C. Surrender/Extradition

1. According to your legislation which cybercrime acts:
   a/fall in the scope of the EAW list, so as to give rise to surrender
   b/are extraditable.

2. Which authorities are responsible for sending/receiving surrender/extradition requests and for deciding on such requests in relation to cybercrime? What communication channels are used?

3. Please provide, if available, statistics on the number of requests sent/received, specifying under which instruments, ,and as far as possible for which type of cybercrime acts as regards EU MSs or third countries respectively.

4. Are there any specific procedures or conditions that need to be fulfilled as regards the requests related to cybercrime.? How are urgent requests treated? Are provisional arrests possible? What is the average response time?

5. Have you used the surrender procedure provided in the Agreement on the surrender procedure between the EU Member States, Iceland and Norway in relation to cybercrime?

6. Have you sent/received requests to/from other third countries in relation to cybercrime? What legal instruments have you used?

8. International cooperation - partners (EU Agencies, JITs/cyber patrols, third countries)

8.A. Cooperation with EU Agencies

1. Are there any formal requirements or specific procedures foreseen by your national law in respect of the cooperation between your national authorities and Europol/EC3, Eurojust, ENISA, in relation to cybercrime cases? If so, please specify.

2. Has your MS had any experience of cooperation in a concrete case with Europol/EC3, Eurojust, ENISA? If so, please describe.

3. What is your MS's overall assessment of Europol/EC3, Eurojust and ENISA in terms of their contribution in dealing with cybercrime ? How would you assess their added value in international cooperation in relation to cybercrime?

4. Would you recommend a better way of making use of Europol/EC3, Eurojust and ENISA in relation to cybercrime?

8.B. Participation in JITs and cyber-patrols

1. Has your MS participated in JITs in relation to cybercrime? If so, could you please describe your experience?
2. Was EU funding allocated to facilitate this cooperation? If so, please specify under which financial instrument.
3. Do you have experience with participation in cyber patrols? If so, please provide details as appropriate .
4. What is your overall assessment of these tools for cooperation? Have you any suggestions on how they can be improved?

8.C. Cooperation with third countries

1. Describe your policy, if any, with respect to third countries regarding cybercrime prevention and investigation.
2. In your experience has the involvement of Europol/EC3/Eurojust brought an added value to cases related to third countries? If so, explain how.
3. Can you explain your involvement with Interpol regarding cybercrime issues?

9. Co-operation with the private sector

1. Please explain how and on what basis the private sector is involved in the prevention of and fight against cybercrime, e.g. legal or policy obligations. Please describe how the private sector intervenes, e.g. by providing support in preservation of evidence, identifying of offenders, shutting down of information systems or functions that have been compromised or used for illegal purposes, etc. Please, describe your experience.
2. Are Internet service providers subject to any specific responsibility/liability under your national law? If so, please describe. How are requests for blocking the access/removal of the content or websites handled?

3. When the private companies have their main headquarters in a third State have you cooperated directly with the local branches? If so, has this affected the investigation and the prosecution of the case? Have private companies been subject to coercive measures, e.g. house searches?
4. Are resources allocated to enhancing/improving the co-operation with the private sector?
5. Does your MS use Public Private Partnership (PPP) in the prevention of and fight against cybercrime? If so, please provide details on their scope, composition, organisation and modalities of operation.

10. Prevention of cybercrime, training and awareness raising activities

10.A. Prevention

1. In what way is the issue of prevention addressed in your national legislation/policy? Does it include any specific measures or activities in this respect? If so, please specify.
2. Describe any recent or planned prevention activities undertaken by both governmental institutions and non-governmental organisations, including schools and academia.

10.B. Training

1. Do you provide cybercrime related training to your general and specialised LEAs and the judiciary? Describe the objectives, subject matters covered, and if possible the frequency and duration of this training.
2. Are there any specialised education modules targeted at IT-forensic examiners and cybercrime investigators?
3. Who is responsible for the provision of cybercrime related training? To what extent do CEPOL, ECTEG (European Cybercrime Training and Education Group) and Europol/EC3 contribute to the training of your LEAs ?
4. What are the annual costs for the training/education of your LEA's covered by your authorities (approximate annual budget)?

5. Is training in relation to cybercrime provided to those persons who have a role in the process of international cooperation? Describe the objectives and length of any such training provision. Is it proposed that refresher training be provided? If so, how frequently?
6. Describe the role of national centres of excellence (if any) in the provision of cybercrime specific training?
7. What is the role of academia? Are special cybercrime related courses provided in the curricula?

10.C. Awareness Raising

1. How does your MS generally raise awareness of cybercrime? What is the role of the private sector (campaigns, EU/national funding).
2. Given the level of ICT penetration and the early age of ICT tools used, have you considered introducing special courses in the Universities/classes in schools (if so, how early) to make the general public aware/improve their level of awareness of the cybercrime related threats?

11. General observations and final remarks

1. How do you assess the general capabilities of your MS to prevent and fight cybercrime?
2. Please provide examples of good practice in combating cybercrime, if any.
3. Do you have any suggestions (practical measures or legislative steps) with a view to strengthening prevention and counteracting cybercrime?
4. Are there any other comments that you would wish to be taken into consideration as part of this process of Mutual Evaluations?