COUNCIL OF THE EUROPEAN UNION

Brussels, 3 July 2013

11147/13

GENVAL 36

NOTE

From :	Presidency
To :	Working Party on General Matters including Evaluations (GENVAL)
Subject :	Orientation debate on the seventh round of Mutual Evaluations - possible topics

Introduction

1. The sixth round of mutual evaluation, dedicated to the practical implementation and operation of the Decisions on Eurojust and the European Judicial Network in criminal matters, is well underway. Since it started in May 2012, 15 Member States have been evaluated, and so far seven reports have been adopted. The last evaluation visit will take place in spring 2014, and this means that the final report should be adopted in autumn 2014.

2. Taking into account the length of the preparatory work: choosing a topic, drafting, discussing and adopting a questionnaire, it is time to start debates on the topic and to take a decision during the Lithuanian Presidency. According to Article 2(1) of Joint Action 97/827/JHA[1], adopted by the Council on 5 December 1997, the Presidency shall propose a "*specific subject of the evaluation as well as the order in which Member States are to be evaluated*". The first evaluation visits could then take place around May/June 2014.

[1] Joint Action 97/827/JHA of 5 December 1997 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, establishing a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organized crime (OJ L 344, 15.12.1997, p. 7).

To initiate the discussion on the topic for the seventh round of mutual evaluation, the Presidency would suggest the following topics, which were both already discussed, when deciding on a topic for the current sixth evaluation round:

A) Cybercrime; and
B) Special investigative techniques.

Topic A: Cybercrime

3. A topic that received the support of a large number of Member States during discussions in 2011 was the fight against cybercrime. For the same reason part of the text and arguments below will be well-known and mainly updated.

4. "Cybercrime", even as only part of the broader "cybersecurity", is indeed a multidisciplinary topic, covering a multi-faceted range of issues, involving different policy areas. Exactly for this reason a Friends of Presidency Group (FoP) on Cyber Issues was established at the end of 2012[2]. According to the Terms of Reference for this FoP Group, agreed by COREPER in November 2012, this group should ensure horizontal coordination of cyber policy issues in the Council, serve as a cross-cutting working platform and develop an EU integrated approach. Member States were requested to designate national focal point(s) on cyber policy issues who have met twice during each Presidency. The Group has been initially set up for one year. It was considered to of utmost importance to establish better cooperation also in view of upcoming the Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "*The Cybersecurity Strategy of the European Union: An open, safe and secure Cyberspace*[3], issued on 7 February 2013 by the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy.

---

[2] 15686/12 POLGEN 183 JAI 750 TELECOM 198 PROCIV 170 CSC 72 CIS 6 RELEX 988 JAIEX 91 RECH 398 COMPET 659 IND 181 COTER 107.

[3] 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.

"Cybercrime" is defined in footnote 5 of this Joint Communication, as follows: "*Cybercrime commonly refers to 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)*".

Council Conclusions welcoming this Commission communication were adopted in June this year[4]. These Council Conclusions contain, among other things, in its point 30-36 recommendations and invitations to stakeholders in the area of cybercrime, and in the Annex to the Annex an updated (non-exhaustive) enumeration of legislative and non-legislative initiatives within the field. All the above-mentioned initiatives stress the importance of coordination and a comprehensive policy framework.

5. Considering the legislative framework, the Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[5] will be replaced by the Directive of the European Parliament and of the Council on Attacks against Information Systems, which is likely to be adopted in July or at the latest in September this year. Member States will have a transposition period of two years from adoption, meaning autumn 2015. Apart from an approximation of the criminal law of Member States by establishing minimum rules concerning the definition of criminal offences and the sanctions in the area of attacks against information systems, the objective of this Directive is to improve cooperation between competent authorities, including the police and other specialised law enforcement services of the Member States, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its recently established European Cyber Crime Centre (EC3), and the European Network and Information Security Agency (ENISA).

---

[4] 11357/12 JAI 432 DAPIX 77 CRIMORG 71 ENFOPOL 184 ENFOCUSTOM 56.

[5] OJ L 69, 16.3.2005, p. 67.

The Directive builds upon an important Council of Europe Convention on Cybercrime of 23 November 2001 (the Budapest Convention)[6], which has been supplemented by an Additional Protocol of 28 January 2003 concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems[7]. So far, the Convention has been ratified by 20 Member States, and the Additional Protocol by 10 Member States. Completing the process of ratification of that convention as soon as possible has long been considered a priority, and Member States have repeatedly been asked to do so.

6. Combating cybercrime was also established as a priority also in the Council Conclusions adopted by the JHA Council on 6-7 June 2013 setting the EUs priorities for the fight against serious and organised crime between 2014 and 2017. The Europol 2013 Serious and Organised Crime Threat Assessment (SOCTA)[8] considers cybercrime a crime area posing 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 criminal activity.

7. Solicitation of children for sexual purposes is a threat with specific characteristics in the context of the Internet. The fight against child pornography and the prevention and combating of sharing of child pornography images, spreading through the use of new technologies and the Internet, could be dealt with as a separate element of such an evaluation. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography[9], to be implemented by 18 December 2013. In particular, its Article 25, is relevant in this context.

---

6 CETS no. 185; opened for signature on 23 November 2001, entered into force on 1 July 2004.
7 CETS No. 189; opened for signature on 28 January2003, entered into force on 1 March 2006.
8 7368/13 JAI 200 COSI 26 ENFOPOL 75 CRIMORG 41 CORDROGUE 27 ENFOCUSTOM 43 PESC 286 JAIEX 20 RELEX 211.
9 OJ L 335, 17.12.2011, p. 1.

Also the Global Alliance against Child Sexual Abuse Online, a joint initiative by the EU and the US launched by the Commission on 5 December 2012, and now comprising 50 countries from around the world, deserves mentioning. All participants commit to four key policy targets, among others to investigate cases of child sexual abuse online and to identify and prosecute offenders and to reduce the availability of child pornography online and the re-victimization of children.

In relation to the investigation of commercial distribution of child abuse images, also the International Child Sexual Exploitation Database at Interpol could be looked at. Participation 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") could also be looked at. The existence of specialized units and the use of joint investigation teams (JITs) in the fight against cybercrime would be another important element. Training, and in particular the question of national centres of excellence is also an important topic here. The same goes for public-private partnership, in view of the fact that cooperation between the public authorities and the private sector and civil society is of great importance in preventing and combating cyber-attacks.

8. The Cybersecurity Strategy explicitly recognises protection of privacy and of personal data as core values, and in the same vein, the just adopted Council Conclusions stress the need for protection of fundamental rights or, in the words of the conclusions in the preamble "*reaffirming the EU's position that the same norms, principles and values that the EU upholds offline, notably the EU Charter of fundamental rights, should also apply in cyberspace*".

9. Apart from the legal issues, a number of other issues could be considered in the context of an evaluation. In general, an evaluation should look at best practices on technological investigation techniques in the police, judicial and forensic authorities. Statistical data and anti-cyber crime policy would need to be evaluated as well as knowledge on modus operandi and the ways in which this knowledge is shared with other Member States. Practical forms of cooperation should be studied: the way in which Member States set up their national cybercrime reporting systems or adapted them to be able to report to Europol's European Cybercrime Platform (ECCP); how they handle a cross-border cyber-incident in practice, etc.

Topic B: Special investigative techniques

10. Special investigative techniques were suggested as an alternative topic in spring 2011. Some of the special investigative techniques have already been dealt with as a sub-aspect of other previous mutual evaluation rounds, i.e. the second round of mutual evaluations on "Law enforcement and its role in fighting drug trafficking". The ongoing sixth evaluation round touches upon "controlled deliveries". Others (e.g. cross-border surveillance, hot pursuit, controlled deliveries of drugs), which are dealt with in the Schengen Convention and the Schengen Implementation Convention, are being evaluated in the context of the Schengen evaluations.

11. Special investigative techniques are regulated by the domestic law of Member States. No internationally agreed definition seems to exist. Reference to special investigative techniques has been increasingly made in recently adopted EU criminal law instruments, e.g. the abovementioned Directive on child sexual abuse, the Directive on cyber-attacks and the Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims[10]. Also the draft proposal on a Directive on protection of the euro and other currencies[11], currently being discussed within the Working Party of Substantive Criminal Law, could be mentioned in this context.

12. Cross-border operation regarding some techniques is to a certain extent regulated by the EU Convention of 29 May 2000 on mutual assistance in criminal matters between the Member States[12]. Its purpose was to encourage and modernise cooperation between judicial, police and customs authorities in the EU. The 2000 Convention was supplemented by a Protocol in 2001[13]. The Convention includes a number of special investigative measures, such as controlled delivery, covert investigations and interception of telecommunications. For other special investigative techniques, such as the use of undercover agents, the use of informants, access to private computer files, measures for identification of computers and telephones users in internet cafes and other public communication business (registration logs, security cameras), there appear to be no "EU standards".

---

10 OJ L 101, 15.4.2011, p.1.
11 6152/13 DROIPEN 11 JAI 81 ECOFIN 92 UEM 18 GAF 3 CODEC 268 (COM(2013) 42 final).
12 OJ C 197, 12.7.2000, p.1.
13 OJ C 326, 21.11.01, p. 2.

13. The United Nations' Convention against Transnational Organised Crime, approved by the Council of behalf of the Community[14], contains in its Article 20 a provision on "special investigative techniques". Its paragraph 1 makes reference to controlled delivery and other special investigative techniques, such as electronic or other forms of surveillance and undercover operations. Each State party is asked to take the necessary measures to allow for the appropriate use of the mentioned measures, however only "*if permitted by the basic principles of its domestic legal system*" and "*within its possibilities and under the conditions prescribed by its domestic law*" .

Same wording and safeguards can be found in Council Decision of 25 September 2008 on the conclusion, on behalf of the European Community, of the United Nations Convention against Corruption[15], Article 50.

14. Also the Naples II Convention[16], of which the objective is to regulate particular forms of cooperation involving cross-border actions for the prevention, investigation and prosecution of certain infringements of both the national legislation of Member States and Community customs regulations, contains provisions on special investigative techniques; inter alia controlled deliveries (Article 12 - see also art 22 of the Naples II Convention), covert investigations (Article 14 - see also Article 23 of the Naples II Convention) and interception of telephone communications (Articles 17 to 22).

15. One argument for not choosing "special investigative techniques" as a topic for the sixth evaluation was that three Member States had still not ratified the 2000 Convention, since this implied that there would be no real EU legal benchmark by which the domestic situations of Member States could be assessed. These ratifications are still missing. However, taking into account that reference to "special investigative techniques" are increasingly made in post-Lisbon instruments, it might be worth to have a closer look at. In addition, practical experience in relation to some special investigative techniques has, as mentioned in point 10, already formed an important part of two evaluations and getting a fuller picture could be of interest.

---

14 Council Decision of 29 April on the conclusion, on behalf of the European Community, of the United Nations Convention Against Transnational Organised Crime (OJ L 261, 6.8.2004, p. 69).

15 OJ L 287, 29.10.2008, p. 1.

16 OJ C 24, 23.1.1998, p. 1.

16. The proposed evaluation could for instance focus on legal and practical obstacles within the field of special investigative techniques, in particular in relation to practical cross-border cooperation, including cooperation and coordination between the services/actors involved and their counterparts in other Member States. Developments and adaptation to changing technologies, and the balance between fundamental rights and the need to efficiently investigating crimes, should also be included.

17. An area which is similar to B above is cross-border cooperation; an evaluation could focus on how this cross-border co-operation work in practice. Although the Schengen evaluation would examine this, the idea here is that all types of law enforcement cooperation having a cross-border dimension be evaluated. The evaluation would therefore not only be focused on hot pursuit, cross-border surveillance and on controlled deliveries, but also on joint investigation teams (JITs), police custom cooperation centres (PCCC), permanent JITs and investigations without the formal setting up of JITs (mirror investigations). Issues such as common equipment, joint patrolling and exchange of training and best practices could also be looked at.

Concluding remarks

18. What is stated above under A and B is first and foremost a compilation of relevant instruments, documents and ideas for what could be looked at during an evaluation. The mandate of the evaluation will of course have to be clearly defined.

19. Member States are invited to propose additional topics for the 7th evaluation.

20. When the rounds of mutual evaluations started in 2003, they involved 15 countries; today it is almost the double. Due to the fact that mutual evaluation rounds now include 28 countries, the Presidency will suggest a tightening of the existing procedure, which would not require any change of the Joint Action. This could for instance include suggestions to shorten the length of country reports and to change, the form of presentations of the reports in GENVAL in order to put more emphasis on discussions. A separate document dealing with this issue will be circulated. Concerning the follow-up, minor changes were already agreed at the latest GENVAL-meeting, see doc. 9154/1/13 REV 1 GENVAL 25.

At its meeting on 10 July 2013, GENVAL is invited to:

- *agree on conducting a seventh round of Mutual Evaluation;*

- *have an initial discussion of the topics for this evaluation round, including suggesting others than those included above.*