COUNCIL OF THE EUROPEAN UNION

Brussels, 22 July 2013 (OR. en)

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

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	11357/13
Subject:	Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

Delegations will find enclosed the Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace as agreed by the General Affairs Council on 25 June 2013.

ANNEX

Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy joint communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

The Council of the European Union,

1. RECOGNISING that cyberspace, inherently transnational in nature, consists of interdependent networks and information infrastructures, including inter alia the Internet and telecommunications networks, constitutes one of the most important present and future channels for fulfilling the needs, interests and rights of EU citizens and member states and provides an indispensable asset for economic growth in the EU,

2. UNDERLINING the roles and rights of individual citizens, the private sector, and civil society in cyber issues and the important role of the EU in supporting and maintaining an open, secure and resilient cyberspace based on the core values of the EU such as democracy, human rights, and the rule of law, for our economies, administrations and society and for the smooth functioning of the internal market,

3. RECOGNISING the need to improve the confidentiality, availability, and integrity of networks and infrastructure and of the information contained therein,

4. RECOGNISING that safeguards have to be put in place and measures taken to prevent threats associated with or harmful to interdependent networks and information infrastructures and to protect the cyber domain, in both the civilian and military fields,

5. 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,

6. RECOGNISING that international law, including international conventions such as the Council of Europe Convention on Cybercrime (Budapest Convention) and relevant conventions on international humanitarian law and human rights, such as the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights provide a legal framework applicable in cyberspace. Efforts should therefore be made to ensure that these instruments are upheld in cyberspace; therefore the EU does not call for the creation of new international legal instruments for cyber issues,

7. AFFIRMING that cybersecurity needs to be addressed in an integrated, multidisciplinary and horizontal way and that measures should cover a multifaceted range of issues that affect cyberspace,

8. RECALLING the numerous EU and international initiatives in the cybersecurity field, including those set out in the annex of this document,

9. RECALLING the provisions of Article 222 of the Treaty on the Functioning of the European Union and takes into account the ongoing discussions on its implementation,

10. BEING AWARE that both the efforts to raise cybersecurity and the fight against cybercrime must be led not only within the European Union but also in third countries, including those from where cybercriminal organisations operate,

HEREBY

11. WELCOMES the Joint Communication of the Commission and the High Representative of the EU on a Cybersecurity Strategy of the European Union,

12. REGARDS it essential and urgent to develop further and implement a comprehensive approach for EU cyberspace policy that:

    - protects and promotes enjoyment of human rights and is grounded in the EU's fundamental values of democracy, human rights and the rule of law,

    - advances European prosperity and the social and economic benefits of cyberspace including the Internet,

- promotes effective and improved cyber security across the EU and beyond,

- advances the efforts to bridge the global digital divide and promotes international cooperation in cybersecurity,

- reflects the roles and rights of individual citizens, the private sector, and civil society in cyber issues; including a strengthening of public-private cooperation and exchange of information,

AND

13. INVITES Member States, the Commission and the High Representative to work together, respecting each others' areas of competence and the principle of subsidiarity, in response to the strategic objectives set out in these Conclusions.

Values

14. UNDERLINES that individuals' human rights, including the freedom of expression and privacy must always be respected in developing policy and practice on cyberspace issues as well as in legislation and takes note of the ongoing negotiations to agree an EU legal framework on the protection of personal data that can operate effectively in cyberspace,

15. RECOGNISES that the values and interests promoted and protected within the Union should be also promoted in its external policies related to cyber issues,

16. CALLS UPON the EU and its Member States:

- to defend their unified and strong position regarding the universal applicability of human rights and fundamental freedoms, including the freedoms of opinion, expression, information, assembly and association in cyberspace,

- to establish how existing obligations can be enforced in cyberspace,

17. INVITES the EU and its Member States to promote digital literacy and help users raise their awareness regarding their individual responsibility when placing personal data on the Internet,

18. UNDERLINES the EU's important role in maintaining the multistakeholder model for governance of the Internet,

19. INVITES Member States to take all reasonable steps to ensure that all EU citizens are able to access and enjoy the benefits of the Internet,

Prosperity

20. INVITES the Commission to make specific efforts to promote the Digital Single Market and to take related issues forward within the Union, and international fora (e.g. the World Trade Organisation (WTO), and the Information Technology Agreement (ITA) -negotiations) as well as to ensure market access in these sectors when negotiating free trade area agreements with third countries,

21. UNDERLINES the importance of legislation in this sector being technology neutral and encourages net neutrality as much as possible so as not to hamper competition by discriminating against cross-border online trade and new business models,

22. WELCOMES the recognition given to the need to invest in research and development in the area of cyberspace, as an important field that could provide high-quality jobs and economic growth,

23. EMPHASIZES:

- the critical importance of a vibrant EU Information and Communication Technology (ICT) and ICT Security Sector with regards to the reinforcement of cybersecurity and INVITES Member States and the Commission to explore and report on what steps can be taken to support its development,

- that legislation in support of cybersecurity should foster innovation and growth, and focus on the protection of infrastructure and vital functions that Member States judge to be critical,

- that the digital economy is a major driver of growth, innovation and employment, and that cybersecurity is key to protecting the digital economy,

- the importance at national level of CIIP (Critical Information Infrastructure Protection).

Achieving cyber resilience

24. WELCOMES the objectives of the Commission proposal for a Directive laying down measures to enhance:

    - network and information security across the EU,
    - cybersecurity preparedness and capabilities at national level,
    - cooperation between the Member States and across the EU and to stimulate a culture of risk management in the public and private sector,

25. CALLS UPON all EU institutions, bodies and agencies, in cooperation with Member States, to take the necessary action to ensure their own cybersecurity, by reinforcing their security according to the appropriate security standards, in cooperation with ENISA to achieve best practice, in accordance with Regulation (EU) No 526/2013[1],

26. RECALLS that a CERT (Computer Emergency Response Team) for the EU institutions, bodies and agencies has been set up following a pilot phase of one year and successful assessment of its role and effectiveness,

27. UNDERLINES the utmost importance of ENISA in supporting Member States and Union efforts in achieving a high level of network and information security, in particular by supporting Member States capacity building, and developing strong national cyber resilience capabilities, European cyber exercises as well as Union's efforts on R&D and standardisation and INVITES ENISA to cooperate with other Union institutions, bodies and agencies on NIS related matters, in accordance with Regulation (EU) No 526/2013,

[1] OJ L 165, 18.6.2013

28. HIGHLIGHTS the need to raise EU wide resilience of critical infrastructures and reinforce close cooperation and coordination between relevant actors, also between EU civilian and military actors, including between public and private sector in responding to cybersecurity incidents and challenges, through initiatives such as the development of common standards, awareness-raising, training and education and ongoing review and testing (or development) of early warning and response mechanisms. Reinforcing close co-operation and co-ordination in responding to cyber incidents by defence actors, law enforcement, private sector and cyber security authorities is also necessary to effectively tackle cyber challenges, including incident management,

29. INVITES Member States

- to take steps to ensure they reach an efficient national level of cybersecurity, by developing and implementing the proper policies, organizational and operational capacities in order to protect information systems in cyberspace, in particular those considered to be critical,

- to engage with industry and academia to stimulate trust as a key component of national cybersecurity for instance by setting up public-private partnerships,

- to support awareness-raising on the nature of the threats and the fundamentals of good digital practices, at all levels,

- to support the owners and providers of ICT systems in protecting their own systems and the vital services that they provide,

- to foster pan-European cybersecurity cooperation, in particular by enhancing pan-European cybersecurity exercises,

- to ensure effective cooperation and coordination between Member States at EU level, towards a common threats' assessment,

- to strengthen and expand cooperation between Member States and EU users, building on existing structures.

- to take into account cybersecurity issues in light of ongoing work on the solidarity clause.

Cybercrime

30. RECOGNISES the Council Conclusions adopted by the JHA Council on 6-7 June 2013 setting the EU's priorities for the fight against serious and organised crime between 2014 and 2017 which establish combating cybercrime as a priority,

31. UNDERLINES that the Europol 2013 Serious and Organised Crime Threat Assessment (SOCTA) considers cybercrime as a crime area which poses 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,

32. COMMENDS the creation of the European Cyber Crime Centre (EC3) at Europol and INVITES Member States to use EC3 as a means of strengthening cooperation between national agencies within its mandate,

33. INVITES Europol and Eurojust to continue to strengthen their cooperation with all relevant stakeholders, including EU agencies, Interpol, the CERT community and the private sector in the fight against cybercrime, including by emphasising synergies and complementarities in accordance with their respective mandates and competences,

34. ANTICIPATES the swift ratification of the Budapest Convention on Cyber Crime by all Member States,

35. CALLS UPON the Commission, Europol, CEPOL and ENISA, to support the training and up-skilling of Member States whose governments and law enforcement authorities need to build cyber capabilities to combat cybercrime,

36. INVITES the Commission to:

- support Member States, at their request, to identify gaps and strengthen their capability to investigate and combat cybercrime,

- use the Internal Security Fund (ISF), within its budget limit (while considering its other priorities), to support relevant authorities fighting cybercrime,

- use the Instrument for Stability (IfS) to develop the fight against cybercrime as well as capacity-building initiatives including police and judicial cooperation in third countries from where cybercriminal organisations operate,

- facilitate coordination of capacity building programmes in order to avoid duplication and provide for synergies,

- provide information relating to the progress of the Global Alliance against Child Sexual Abuse Online,

- continue to facilitate the monitoring of the EU policy environment related to the fight against cybercrime, in particular in light of the results and strategic information provided by Europol (EC3),

- continue to facilitate cross-community cooperation, in particular by supporting Europol (EC3).

Common Security and Defence Policy (CSDP)

37. In the framework of the CSDP, HIGHLIGHTS:

- the urgent need to implement and take forward the CSDP related cyber defence aspects of the Strategy to develop a cyber defence framework, as appropriate, and define concrete steps in this regard, also in view of the European Council debate on security and defence foreseen in December 2013. A single point of contact should be designated within the EEAS to steer these efforts,

- the need to enhance Member States' cyber defence capabilities, including through the development of common standards, and raising awareness through training and education in cyber security, making use of the European Security and Defence College and further improving training and exercising opportunities for Member States,

- using the existing mechanisms for Pooling and Sharing and utilising synergies with wider EU policies to build the necessary cyber defence capabilities in the Member States in the most efficient manner,

- the need for research and development. Priority is given to encourage Member States to develop secure and resilient technologies for cyber defence with strong involvement of the private sector and academia, and to strengthen cyber security aspects in EDA research projects on the basis of a collaborative approach and as a good example of a dual use capability to be coordinated between EDA and Commission under the European Framework Cooperation,

- that early warning and response mechanisms should be reviewed and tested in the light of new cyber threats, through dialogue between the EEAS, ENISA, EC3, EDA, Commission and Member States, with a view to seeking synergies and links with the defence community,

- the need to pursue and strengthen EU-NATO cooperation on cyber defence, identifying priorities for continued EU-NATO cyber defence cooperation within the existing framework, including reciprocal participation in cyber defence exercises and training,

- embedding cyber defence aspects in wider cyberspace policy.

Industry/Technology

38. RECOGNISING the necessity for Europe to further develop its industrial and technological resources to achieve an adequate level of diversity and trust within its networks and ICT systems, the Council strongly WELCOMES the call in the EU Cybersecurity strategy for Europe, to support a strong industrial policy, in order to promote trustworthy European ICT and cybersecurity industries and boost the internal market through R&D,

39. INVITES the Member States, the Commission and ENISA to strengthen efforts on Research and Development in the area of ICT and cybersecurity, as well as the availability of well-prepared professionals on cybersecurity, essential to boost the competitiveness of the European Information and Communication Technology (ICT), service and security industries, and their ability to develop trustworthy and secure solutions, hence the Council ENCOURAGES the Commission to leverage the Horizon 2020 Framework Programme for Research and Innovation,

40. EMPHASIZES that the development of public-private partnerships will be a relevant instrument to enhancing cybersecurity capabilities; and therefore CALLS UPON the Commission to foster synergies within H2020 between operators of critical infrastructures, ICT and Security research for cyber security and cyber crime related issues and with Union's policies for internal and external security,

41. CALLS UPON Member States and the Commission to take specific measures to support cybersecurity in small and medium-size businesses which are particularly vulnerable to cyber attacks and encourages Member States to develop secure and resilient technologies for cybersecurity with the collaborative involvement of the private sector and academia,

42. INVITES the Commission to take into consideration standards existing in the area of cybersecurity and UNDERLINES that cooperation and exchange of information on standards – e.g. on risk management – should be developed further, in cooperation with MS and industry and other relevant stakeholders.

International cyberspace cooperation

43. REITERATES the EU's commitment to supporting the development of confidence building measures in cybersecurity, to increase transparency and reduce the risk of misperceptions in state behaviour, by promoting the establishment of international norms in this field,

44. CALLS UPON the Commission and the High Representative, in conformity with the relevant Treaties procedures:

- (a) to promote the Budapest Convention as a model for drafting national cyber crime legislation and a basis for international cooperation in this field, (b) to promote respect of fundamental rights in cyberspace and (c) to make full use of all available international cooperation tools to develop the fight against cybercrime as well as related police and judicial cooperation in third countries from where cybercriminal organisations operate,

- to seek Member States' cyber policy expertise and their experience from bilateral engagements/cooperation to develop common EU messages on cyberspace issues and work closely with the Member States on the operational aspects,

- in cooperation with Member States and relevant private organisations and civil society to make full use of relevant EU aid instruments for ICT capacity building, including cybersecurity,

45. CALLS ON the Member States, the Commission and the High Representative to work towards achieving a coherent EU international cyberspace policy, in conformity with the relevant Treaties procedures, by:

- increasing engagement with key international partners and organisations in a manner that ensures that all Member States can benefit fully from such cooperation,

- incorporating cyber issues into CFSP,

- improving coordination of global cyber issues and mainstreaming cybersecurity including confidence and transparency building measures into the overall framework for conducting relations with third countries and with international organisations, including through enhanced coordination between Member States, Commission and the EEAS in relation to the conduct of dialogues and other activities on cyber security,

- improving coordination through the relevant Council preparatory bodies (including FoP on Cyber Issues),

- supporting capacity-building in third countries, through training and assistance for the creation of relevant national policies, strategies and institutions, in view of enabling the full economic and social potential of ICTs, supporting the development of resilient systems in those countries and mitigating cyber risks for the EU institutions and Member States, while making use of existing networks and forums for policy coordination and information exchange.

Respective roles and responsibilities

46. CALLS UPON the other stakeholders - private sector, technical and academic communities, civil society, and individual citizens to assume their respective roles and responsibilities towards an open, free and secure cyberspace,

47. CALLS UPON the Commission and the High Representative that the European activities should be designed to be compatible with national structures, constitutional law and initiatives concerning cybersecurity, to ensure an integrated approach and avoid duplication,

AND

48. CALLS UPON the Commission and High Representative to produce a progress report on the Cybersecurity Strategy to be presented at the High Level Conference to be held in February 2014; and PROPOSES to hold regular meetings of the competent Council preparatory bodies, (in particular the FoP on Cyber Issues) to assist in setting EU cyber priorities and strategic objectives as part of a comprehensive policy framework and review and support ongoing implementation of the Strategy,

49. In the implementation of these Council conclusions, only existing funds and financial programmes will be used, without prejudice to the negotiations on the future financial framework and therefore the Council INVITES the Commission to present the financing of the Strategy, taking into account the upcoming negotiations with the European Parliament.

References

1. European Parliament, Council and the Commission

   – Charter of Fundamental Rights of The European Union[2],

2. European Parliament and Council

   – Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency[3],

   – Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended by Directive 2009/140/EC[4],

3. European Parliament

   – European Parliament's resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy,

   – European Parliament's 2012 Report on Cyber Security and Defence,

4. Council

   – The Stockholm Programme - an open and Secure Europe serving and protecting citizens[5],

   – A secure Europe in a better world – European Security Strategy, 12 December 2003[6],

2 OJ C 364/1 of 18.12.2010,
3 OJ L 077 of 13.03.2004
4 OJ L 108 of 24.4.2002 and OJ L 337/37 of 18.12.2009
5 Doc. 17024/09 CO EUR PREP 3 JAI 896 POLGEN 229
6 Doc. 15849/03 PESC 783

– Internal Security Strategy for the European Union: "Towards a European Security Model"(ISS) [7],

– Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[8],

– Council conclusions on the Commission Communication on the European Union internal security strategy in action[9],

– Council conclusions on the Commission Communication on Critical Information Infrastructure Protection ("Achievements and next steps: towards global cybersecurity (CIIP)") [10],

– Council conclusions on setting the EU's priorities for the fight against serious and organised crime between 2014 and 2017[11],

– Council conclusions on the establishment of a European Cybercrime Centre[12],

7 Doc. 5842/2/10 JAI 90
8 OJ L 345 of 23.12.2008
9 Doc. 6699/11 JAI 124
10 Doc. 10299/11 TELECOM 71 DATAPROTECT 55 JAI 332 PROCIV 66. This Communication is a follow-up of COM Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (doc. 8375/09)
11 Doc. 9849/13 JAI 407 COSI 62 ENFOPOL 151 CRIMORG 77 ENFOCUSTOM 89 PESC 569 RELEX 434.
12 Doc. 10603/12 ENFOPOL 154 TELECOM 116

– Proposal for a Directive of the European Parliament and of the Council on attacks against information systems, replacing Council Framework Decision 2005/222/JHA 89. Approval of the final compromise text with a view to a first reading agreement with the European Parliament[13],

– Council conclusions on the European strategy for a Better Internet for Children[14],

– Council conclusions on combating sexual exploitation of children and child pornography on the Internet - strengthening the effectiveness of police activities in Member States and third countries[15],

– Council conclusions on the Global Alliance against Child Sexual Abuse Online[16],

– Council conclusions on a Concerted Work Strategy and Practical Measures against Cybercrime[17] and Council conclusions on an Action Plan to implement the Concerted Strategy to combat Cybercrime[18],

– Council's partial general approach on the Commission proposal for a Regulation establishing Horizon 2020 - The Framework Programme for Research and Innovation (2014-2020)[19],

– Council Joint Action on the establishment of the European Defence Agency[20],

13 Doc. 11399/12 DROIPEN 79 TELECOM 126 CODEC 1673
14 Doc. 15850/12 AUDIO 111 JEUN 95 EDUC 330 TELECOM 203 CONSOM 136 JAI 766 GENVAL 81
15 Doc. 15783/2/11 REV 2 GENVAL 108 ENFOPOL 368 DROPIEN 119 AUDIO 53
16 Doc. 10607/12 +COR 1 GENVAL 39 ENFOPOL 155 DROIPEN 69 AUDIO 62 JEUN 46
17 Doc. 15569/08 ENFOPOL 224 CRIMORG 190
18 Doc. 5957/2/10 REV 2 CRIMORG 22 ENFOPOL 32
19 Doc. 10663/12 RECH 207 COMPET 364 IND 102 MI 398 EDUC 152 TELECOM 118 ENER 233 ENV 446 REGIO 75 AGRI 362 TRANS 187 SAN 134 CODEC 1511.
20 Doc 10556/04 COSDP 374 POLARM 17 IND 80 RECH 130 ECO 121

– Joint proposal for a Council Decision on the arrangements for the implementation by the Union of the Solidarity Clause[21],

– Council conclusions on media literacy in the digital environment[22],

– Human Rights and Democracy: EU Strategic Framework and EU Action Plan[23],

– Report on the Implementation of the European Security Strategy[24],

5. Commission

– The Digital Agenda for Europe[25], which is one of the seven flagship initiatives of the Europe 2020 Strategy for smart, sustainable and inclusive growth[26], and the Digital Agenda for Europe - Driving European growth digitally[27] - which refocuses the Digital Agenda,

– Communication on Safeguarding Privacy in a Connected World, a European Data Protection Framework for the 21st Century[28],

– Communication "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre"[29],

21 Doc. 18124/12 CAB 39 POLGEN 220 CCA 13 JAI 946 COSI 134 PROCIV 225 ENFOPOL 430 COPS 485 COSDP 1123 PESC 1584 COTER 125 COCON 45 COHAFA 165

22 Doc. 15441/09 AUDIO 47 EDUC 173 TELECOM 233 RECH 380

23 Doc. 11855/12 COHOM 163 PESC 822 COSDP 546 FREMP 100 INF 110 JAI 476 RELEX 603

24 Doc. 17104/08 CAB 66 PESC 1687 POLGEN 139

25 Doc. 9981/1/10 TELECOM 52 AUDIO 17 COMPET 165 RECH 193 MI 168 DATA PROTECT 141.

26 Doc. 7110/10 CO EUR-PREP 7 POLGEN 28 AG 3 ECOFIN 136 UEM 55 SOC 174 COMPET 82 RECH 83 ENER 63 TRANS 55 MI 73 IND 33 EDUC 40 ENV 135 AGRI 74.

27 Doc. 17963/12 TELECOM 262 MI 839 COMPET 786 CONSOM 161 DATAPROTECT 149 RECH 472 AUDIO 137 POLGEN 216

28 Doc. 5852/12 DATAPROTECT 8 JAI 43 MI 57 DRS 10 DAPIX 11 FREMP 6

29 Doc. 8543/12 ENFOPOL 94 TELECOM 72

– Commission Communication on "Unleashing the potential of cloud computing in Europe"[30],

– Commission Communication on Critical Information Infrastructure protection (CIIP) "Achievements and next steps: towards global cyber-security"[31],

– Commission Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"[32],

6. UN

– UN General Assembly Resolution A/RES 57/239 on the Creation of a global culture of cyber security,

– UN Human Rights Council's Resolution A/HRC/20/L.13 of 29 June 2012 on the promotion, protections and enjoyment of human rights on the Internet,

– UN General Assembly Resolution A/RES 67/27 on developments in the field of information and telecommunications in the context of international security,

– Establishment of an open-ended intergovernmental expert group on Cybercrime with UNODC pursuant to UN General Assembly Resolution 65/230,

7. Council of Europe

– Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981,

– Council of Europe Convention on Cybercrime of 23 November 2001,

30 Doc. 14411/12 TELECOM 170 MI 586 DATAPROTECT 112 COMPET 585
31 Doc. 8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV 38.
32 Doc. 8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46

8. Organisation for Security and Cooperation in Europe (OSCE)

– Permanent Council Decision No. 1039, 26 April 2012: Development of Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies,

– Ministerial Decision Nº 4/12, 7 December 2012: OSCE's efforts to address transnational threats,

– Open-ended informal OSCE working group to elaborate a set of draft confidence-building measures CBM's to enhance interstate cooperation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation and conflict that may stem form the use of ICTs (OCSE perm. Council decision no. 1039, 26 April 2012),

9. Conferences, initiatives and events

– International Conference on Cyberspace, held in London on 1 and 2 November 2011 and followed up on 4 and 5 October 2012 by an International Conference on Cyberspace in Budapest,

– Joint EU-US cyber incident table top exercise "Cyber Atlantic 2011" and pan-European cyber incident exercises with the participation of all Member States (Cyber Europe 2010 and Cyber Europe 2012),

– Ad hoc Group on Nuclear Security, which discussed and elaborated on the issue of Computer Security / Cybersecurity in its final report[33],

[33] Doc. 10616/12 AHGS 20 ATO 84

10. Other

– Europol 2013 Serious and Organised Crime Threat Assessment (SOCTA)[34],

– The Information Assurance Security Policy[35] and Guidelines[36] on Network Defence.

---

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

[35] Doc. 8408/12 CSCI 11 CSC 20

[36] Doc. 10578/12 CSCI 20 CSC 34