COUNCIL OF THE EUROPEAN UNION

Brussels, 23 April 2013

8767/13

POLGEN 50
CYBER 8
JAI 308
COSI 39
TELECOM 82
PROCIV 50
CSC 39
CIS 10
RELEX 320
JAIEX 26
RECH 118
COMPET 233
IND 113
COTER 39
ENFOPOL 119
DROIPEN 43
COPS 166
POLMIL 25
DATAPROTECT 48

NOTE

from:	Presidency
to:	Friends of Presidency Group on Cyber Issues
No. prev. 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
Subject:	Draft 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 attached a Presidency proposal for draft Council conclusions on the above mentioned joint communication.

The Cybersecurity Strategy covers a multi-faceted range of issues; therefore the matter has been considered by a number of Council Working parties for the matters within their remits. Some of theses groups provided their views to the Friends of Presidency Group on Cyber Issues (FoP) but Member States also wished to coordinate their views on a national basis for submission to the FoP. The attached draft Council conclusions have been drafted in light of these views.

Draft 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, and that it has an enormous impact on all aspects of the daily life of the general public, and is an indispensable asset for economic growth in the EU and that it plays a vital role in societal development,

2. UNDERLINING the importance of cybersecurity and measures to fight cybercrime for our economies, administrations and society and for the smooth functioning of the internal market and RECOGNISING the need to preserve the availability, integrity of networks and infrastructure and the confidentiality of the information contained therein,

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

4. REAFFIRMING the EU's position that the same norms, principles and values that the EU upholds offline, should also apply online,

5. RECOGNISING that many international standards such as the Budapest Convention, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights and International Humanitarian law provide a legal framework applicable in cyberspace. Efforts should therefore be made to ensure that these instruments are enforced in cyberspace; therefore the EU does not call for the creation of new international legal instruments for cyber issues,

6. 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,

7. RECALLING the numerous EU and international initiatives in the cyber field, including those set out in annex I of this document,

8. 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,

9. WELCOMING the objectives of the Commission proposal for a Directive laying down measures to enhance

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

HEREBY

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

11. 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 improved cyber security across the EU and beyond,
- advances the efforts to bridge the global divide and promotes international cooperation in cybersecurity,
- reflects the roles and rights of individual citizens, of the private sector, and civil society in cyber issues; including a strengthening of public-private cooperation and exchange of information,

AND

12. 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

13. UNDERLINES that the rights of individuals to freedom of speech and to privacy must always be respected in developing policy and practice on cyberspace issues and takes note of the ongoing negotiations to agree an EU Data Protection Regulation that can operate effectively in the cyber era,

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

15. CALLS UPON the EU and its Member States

- to develop a unified and strong position regarding the 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,
- to promote digital literacy and help to raise users' awareness regarding their individual responsibility when placing personal data on the internet,

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

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

Prosperity

18. INVITES the Commission to make specific efforts to take these issues forward within the Union, and international fora (e.g. the World Trade Organisation (WTO), and the International Trade Administration (ITA) -negotiations) as well as to ensure market access in these sectors when negotiating free trade area agreements with third countries,

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

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

21. EMPHASIZES

- the importance of a vibrant EU Information and Communication Technology (ICT) Security Sector 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 cyber security should foster innovation and growth, and focus on the protection of infrastructure that Member States judge to be critical,

Improving Network and Information Security

22. CALLS UPON all EU institutions, bodies and agencies to take the necessary action to ensure their own cybersecurity, through cooperation with ENISA to achieve best practice and in coordination across the EU on incident response,

23. INVITES Member States

- to take steps to ensure they have reached an appropriate national level of cybersecurity,
- to engage with industry in public-private partnerships to enhance cybersecurity,
- to support awareness-raising on the nature of the threats and the fundamentals of good digital hygiene, at all levels,
- to engage in pan-European cybersecurity exercises,
- to ensure effective cooperation and coordination at EU level,

Cybercrime

24. COMMENDS the creation of the European Cyber Crime Centre (EC3) at EUROPOL and INVITES Member States to use EC3 to enable the strengthening of cooperation between national agencies,

25. INVITES Europol to continue to strengthen its 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,

26. CONSIDERING that the Europol 2013 Serious and Organised Crime Threat Assessment (SOCTA) states that the Internet enables organised crime groups to access a large pool of victims, obscure their activities and carry out a diverse range of criminal acts in a shorter period of time and on a much larger scale than ever before, and 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,

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

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

29. INVITES the Commission to

- use the Internal Security Fund (ISF) to support law enforcement 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,

CSDP

30. WELCOMES the strong focus in the EU Cyberspace Strategy on cyber defence in the framework of the CSDP, as part of the multidimensional array of EU policies and Policies and within the Multi-stakeholder model and highlights the following issues:

- 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 strengthen a comprehensive approach fostering the cooperation between EU civilian and military actors, including between public and private sector, in raising EU-wide resilience of critical infrastructures. Reinforcing close cooperation and coordination 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,
- 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

31. UNDERLINES that Research and Development in the area of cybersecurity is essential to strengthen the competitiveness of the European Information and Communication Technology (ICT), service and security industries, and their ability to develop trustworthy and secure solutions, and encourages the Commission to make the best of leverage the Horizon 2020 Framework Programme for Research and Innovation to achieve this,

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

33. 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 cyber defence with the collaborative involvement of the private sector and academia,

International Cyberspace Cooperation

34. REITERATING 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,

35. CALLS UPON the Commission and the High Representative, in accordance with agreed Council positions:

- to promote fundamental rights in cyberspace in all international engagements on cyber,

- to secure a mandate from the Council before important international engagements on cyber issues, seeking out Member States' cyber policy expertise and their experience from bilateral engagements/cooperation and to use the relevant working group to develop common EU messages on cyberspace issues and work closely with the Member States on the operational aspects,
- to promote the adoption of the Budapest Convention by third countries in order to improve international cooperation against cybercrime,
- in cooperation with Member States to make full use of relevant EU aid instruments for ICT capacity building, including cybersecurity,
- to have full recourse to 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,

36. CALLING ON the Member States, the Commission and the High Representative to work towards achieving a coherent EU International cyberspace policy by:

- increasing engagement with key international partners and organisations, to mainstream cyber issues into CFSP, in a manner that ensures that all Member States can benefit fully from such cooperation,
- improving coordination of global cyber issues and mainstreaming cybersecurity 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,
- Supporting capacity-building in third countries, through training and assistance for the creation of relevant national policies, strategies and institutions, in view of both supporting the development of resilient systems in those countries and mitigating cyber risks for the EU institutions and Member States,

Respective roles and responsibilities

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

AND

38. CALLS UPON the Commission and High Representative to produce an Action Plan on the basis of their Communication and these Conclusions; to assign responsibility for, and map delivery against, the objectives set out in these Conclusions; and PROPOSES periodic formal review of the Action Plan by the competent Council preparatory body/bodies,

39. 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.

References

1) 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,

2) Council

- The Stockholm Programme - an open and Secure Europe serving and protecting citizens[1],
- Internal Security Strategy for the European Union: "Towards a European Security Model"(ISS) [2],
- Council conclusions on the Commission Communication on the European Union internal security strategy in action[3],
- Council conclusions on the Commission Communication on Critical Information Infrastructure Protection ("Achievements and next steps: towards global cybersecurity (CIIP)") [4],
- European Union's priorities in the fight against organised crime between 2011 and 2013[5] within the framework of the EU Policy Cycle for organised and serious international crime,
- Council conclusions on the establishment of a European Cybercrime Centre[6],
- General approach on the proposal for a Directive on attacks against information systems[7],
- Council conclusions on the European strategy for a Better Internet for Children[8],

---

1 Doc. 17024/09 CO EUR PREP 3 JAI 896 POLGEN 229
2 Doc. 5842/2/10 JAI 90
3 Doc. 6699/11 JAI 124
4 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)
5 Doc. 11050/11 JAI 396 COSI 46 ENFOPOL 184 CRIMORG 81 ENFOCUSTOM 52 PESC 718 RELEX 603.
6 Doc. 10603/12 ENFOPOL 154 TELECOM 116
7 Doc. 11566/11 DROIPEN 62 TELECOM 95 CODEC 1025
8 Doc. 15850/12 AUDIO 111 JEUN 95 EDUC 330 TELECOM 203 CONSOM 136 JAI 766 GENVAL 81

- 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[9],
- Council conclusions on the Global Alliance against Child Sexual Abuse Online[10],
- Council conclusions on a Concerted Work Strategy and Practical Measures against Cybercrime[11] and the Council conclusions on an Action Plan to implement the Concerted Strategy to combat Cybercrime[12],
- Council's partial general approach on the Commission proposal for a Regulation establishing Horizon 2020 - The Framework Programme for Research and Innovation (2014-2020)[13],
- Council Joint Action on the establishment of the European Defence Agency[14],
- Joint proposal for a Council Decision on the arrangements for the implementation by the Union of the Solidarity Clause[15],
- Council conclusions on media literacy in the digital environment[16],
- Human Rights and Democracy: EU Strategic Framework and EU Action Plan[17],
- Report on the Implementation of the European Security Strategy[18],

3) Commission

- The Digital Agenda for Europe[19], which is one of the seven flagship initiatives of the Europe 2020 Strategy for smart, sustainable and inclusive growth[20], and the Digital Agenda for Europe - Driving European growth digitally[21] - which refocuses the Digital Agenda,

---

9 Doc. 15783/2/11 REV 2 GENVAL 108 ENFOPOL 368 DROPIEN 119 AUDIO 53
10 Doc. 10607/12 +COR 1 GENVAL 39 ENFOPOL 155 DROIPEN 69 AUDIO 62 JEUN 46
11 Doc. 15569/08 ENFOPOL 224 CRIMORG 190
12 Doc. 5957/2/10 REV 2 CRIMORG 22 ENFOPOL 32
13 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.
14 Doc 10556/04 COSDP 374 POLARM 17 IND 80 RECH 130 ECO 121
15 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
16 Doc. 15441/09 AUDIO 47 EDUC 173 TELECOM 233 RECH 380
17 Doc. 11855/12 COHOM 163 PESC 822 COSDP 546 FREMP 100 INF 110 JAI 476 RELEX 603
18 Doc. 17104/08 CAB 66 PESC 1687 POLGEN 139
19 Doc. 9981/1/10 TELECOM 52 AUDIO 17 COMPET 165 RECH 193 MI 168 DATA PROTECT 141.
20 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.
21 Doc. 17963/12 TELECOM 262 MI 839 COMPET 786 CONSOM 161 DATAPROTECT 149 RECH 472 AUDIO 137 POLGEN 216

- Commission Communication on Safeguarding Privacy in a Connected World, a European Data Protection Framework for the 21st Century[22],
- Commission Communication on "Unleashing the potential of cloud computing in Europe"[23],

4) 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 June 2012 on the promotion, protections and enjoyment of human rights on the Internet,

5) 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,

6) 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),
- Establishment of an open-ended intergovernmental expert group on Cybercrime with UNODC pursuant to UN General Assembly Resolution 65/230,
- Ad hoc Group on Nuclear Security, which discussed and elaborated on the issue of Computer Security / Cybersecurity in its final report[24],

---

22 Doc. 5852/12 DATAPROTECT 8 JAI 43 MI 57 DRS 10 DAPIX 11 FREMP 6
23 Doc. 14411/12 TELECOM 170 MI 586 DATAPROTECT 112 COMPET 585
24 Doc. 10616/12 AHGS 20 ATO 84

7) Other

- Europol 2013 Serious and Organised Crime Threat Assessment (SOCTA)[25],
- The Information Assurance Security Policy[26] and Guidelines[27] on Network Defence that apply to the Council and Council members.

---

[25] Doc. 7368/13 JAI 200 COSI 26 E□FOPOL 75 CRIMORG 41 CORDROGUE 27E□FOCUSTOM 43 PESC 286 JAIEX 20 RELEX 211

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

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