COUNCIL OF THE EUROPEAN UNION

Brussels, 27 April 2011

9258/11

TELECOM 46
DATAPROTECT 36
JAI 256
PROCIV 51

NOTE

From :	Presidency
To:	Delegations
No Cion. prop.:	8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV38
No prev doc.	8806/11 TELECOM 44 DATAPROTECT 28 JAI 228 PROCIV 43
Subject:	Draft Council Conclusions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" (CIIP) - Presidency text

Delegations will find attached draft Presidency conclusions on CIIP. This draft takes into account the delegations' comments as well as the outcome of the Ministerial Conference on Critical Information Infrastructure Protection held in Balatonfüred on 14-15 April 2011 and the respective Presidency Statement.

DRAFT COUNCIL CONCUSIONS

On Critical Information Infrastructure Protection
"Achievements and next steps: towards global cyber-security"

THE COUNCIL OF THE EUROPEAN UNION,

I. WELCOMES

The Commission communication of 31 March 2011 on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security"; [1]

II. RECALLS

1. **The Council Conclusions of 20 April 2007 on a European programme on critical infrastructure protection;** [2]
2. The Council Directive of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection; [3]
3. The Commission **C**~~c~~ommunication of 30 March 2009 on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and cyber-disruptions: enhancing preparedness, security and resilience" setting out an action plan to strengthen the security and resilience of vital Information and Communication Technology (ICT) Infrastructures; [4]
4. The Presidency **C**~~c~~onclusions on CIIP of the Tallinn **M**~~m~~ministerial **C**~~c~~onference of 27-28 April 2009;

[1] Doc 8548/11
[2] **Doc 7743/07**
[3] OJ L 345, 23.12.2008, p. 75–82
[4] Doc 8375/09

5. The Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security;[5]
6. The Commission **C**~~c~~ommunication of 19 May 2010 on "a Digital Agenda for Europe" underlining the need to increase security in the digital society and thus enhance trust in networks ; [6]
7. The Council Conclusions of 31 May 2010 on **the** Digital Agenda for Europe;[7]
8. The Commission **C**~~c~~ommunication of 22 November 2010 on "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe"; [8]
9. The Presidency **S**~~s~~tatement on CIIP of the Balatonfüred **M**~~m~~ministerial **C**~~c~~onference of 14-15 April 2011[9].

III. RECOGNISES

1. The **growing** importance of ICT **systems, infrastructures and services and of the Internet in particular** for European citizens, businesses and for the European economy at large, which highlights Europe's social, political and economic dependencies of ICT~~,~~ ~~but~~ **and** also underlines the need to make IT systems and networks resilient and secure to all possible **disruptions,** ~~threats~~ **whether accidental or voluntary**;
2. **That** ~~The link between security of networks and the trust it creates in users, allowing them~~ **beside severe disruption of networks and information systems, security incidents can also undermine the trust that users have in technology, networks and services, thereby affecting their ability** to exploit the full potential of ICT ~~thus boosting~~ **to contribute to** economic growth ~~and contributing~~ **as well as** to a better quality of life;

---

5 Doc 15841/09
6 Doc 9981/10
7 Doc 10130/10
8 Doc 16797/10
9 http://www.eu2011.hu/document/presidency-statement-en-ministerial-conference-critical-information-infrastructure-protecti

3. The increasing risks coming from new and more sophisticated threats to ICT **networks and services** and the Internet **in particular**, which make the need to ensure their effective protection more ~~obvious~~ **pressing** than ever;
4. The ~~potential~~ major damage **that** ~~for the European economy in case of destruction~~ **vulnerabilities of** or disruption **to** ~~of~~ information and communication technology systems, infrastructures and services **could cause to the European economy**, taking into account that ~~an attack~~ **disruption** in one Member State may also affect other Member States and the EU as a whole;
5. The need to stimulate and support the development of a high level of preparedness, security and resilience capabilities ~~in Europe with the objective~~ **to allow Europe to face the challenge of networks and information protection;**
6. **The need of developing widely recognised minimum requirements, basic principles and standards in the field of network and information security to promote security by design and products and services that are secure by default as much as possible;**
7. **The need** to stimulate trust and security **among all involved stakeholders which constitutes a condition for fostering reinforced cooperation in the protection of vital infrastructures and for making every European digital, as pursued in the Digital Agenda for Europe;** ~~as much as possible ICT created benefits and minimize as much as possible ICT related damages~~;
8. ~~The geo-political dimension of ICT that makes the objective to ensure effective protection not only a national and European challenge but also an international one;~~
9. That the ~~wide~~ **broad** use of **ICT and** the Internet by all kinds of users **and** for all kinds of purposes necessitates a collaborative approach to network and information security, involving all stakeholders **in order to raise users' awareness and increase consciousness in use**;

10. The need for public and private stakeholders to join forces and share responsibility for developing their capabilities and preparedness to prevent, detect and respond to cyber-security challenges;
11. The interconnectedness of information and communication technology systems, infrastructures and services that **makes the objective of preventing any disruption** ~~put the prevention and reaction challenges in a global context~~ **not only a national and European challenge but also an international and global one**.

IV. UNDERLINES

1. The significant progress **made by** the European Forum of Member States (EFMS) ~~made~~ in fostering discussion and exchanges between relevant authorities on good policy practices related to security and resilience of ICT infrastructures;
2. The importance of multi-stakeholder **efforts** ~~work~~, in particular **within** ~~of~~ the European Public-Private Partnership for Resilience (EP3R)**,** ~~to launch~~ a Europe-wide governance framework for the resilience of ICT infrastructures;
3. **The importance of the development of National/Governmental Computer Emergency Response Teams (CERTs) and the elaboration of national cyber incident contingency plans as well as the organization of national cyber exercises;**
4. The important role of the European Network and Information Security Agency (ENISA) in relation to the activities performed by Member States in the field of network and information security, to the activities of EP3R and to the ~~activities~~ **establishment** of ~~the~~ **well functioning** National/Governmental CERT~~S~~**s**;
5. The **success of** ~~national cyber exercises for large-scale network security incident response and disaster recovery and~~ the first pan- European cyber exercise of 4 November 2010 demonstrating the **shared will for** cross-border collaboration between Member States;

6. The benefits that could arise for ~~the N~~**n**etwork and ~~I~~**i**nformation ~~S~~**s**ecurity from a national, European and global culture of risk management at all levels and by all stakeholders focused to promote coordinated actions to prevent, detect, mitigate and ~~react~~ **respond** to all kinds of disruptions;

7. The possible gains from further fostering cooperation between Member States and promoting, in relation with the private sector, a strong European IT security industry, for example by developing European incident cooperation mechanisms between Member States, organizing pan European exercises, encouraging dialogue on issues related to ICT security such as on ICT criteria of European Critical Infrastructures or on Internet stability and resilience;

8. The benefits **that could be drawn** from further promoting, with the ~~help~~ **support** of ENISA, a coherent and cooperative approach on ~~N~~**n**etwork and ~~I~~**i**nformation ~~S~~**s**ecurity in the Member States, **in the** EU Institutions and in the private sector.

V. STRESSES

The importance of rapidly modernising ENISA ~~so that it can~~ **to enable the Agency to** better assume its role and **to** further contribute to strengthening network and information security in Europe.

VI. INVITES THE MEMBER STATES TO

1. Increase their efforts in promoting a culture of risk management in the field of network and information security;
2. **Foster** ~~Reinforce~~ the cooperation between **already** established **or still to be established** **N**~~n~~ational **/Governmental** CERT**s**~~S~~ ~~or CERTS to be established,~~**;**
3. **Establish** ~~in particular by creating~~ a well functioning network of **N**~~n~~ational**/Governmental** CERT**s**~~S~~ ~~from all Member States~~ **by 2012**, ~~if needed~~ with the ~~help~~ **support** of ENISA **as appropriate**;

4. Establish, ~~if necessary~~ with the support of ENISA **as appropriate**, **their** national Information Sharing and Alert Systems **with a view to set up an integrated European Information Sharing and Alert System (EISAS) by 2013**;
5. Consider the adoption of national cyber-security strateg**y**~~ies~~ **where it does not exist**~~, including the establishment of national Public-Private Partnerships~~;
6. Consider developing ~~and implementing~~ national ~~and, in cooperation with the Commission, European~~ cyber incident contingency plans **and contribute, in cooperation with ENISA, to the development of a European cyber incident contingency plan by 2012**;
7. Organise national **or cross-border** cyber exercises to test preparedness to cope with cyber-disruptions, **contribute to** organis~~e~~**ing** and participate in European cyber exercises and other capacity building activities in the Union;
8. **Finalise within EFMS, and in cooperation with EP3R, the work on the criteria for identifying European Critical Infrastructures in the ICT sector, notably for fixed and mobile communication and for the Internet;**
9. **Further reflect on the possibility to introduce this work in the review of the Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection planned in 2012**[10]**;**
10. On the basis of solidarity among Member States, ~~help~~ **assist** each other in cross-border incidents;
11. **Work together** ~~Cooperate~~ with the ~~European Commission~~ **Union's institutions** ~~with the aim to~~ **towards** strengthen**ing** international cooperation in the field of global cyber-security **and towards establishing strategic international partnerships at bilateral and multilateral level**, for example by ~~supporting~~ **contributing to** the activities of the EU-U.S. Working Group on Cyber-security and Cyber-crime;
12. Stimulate and support the cooperation ~~of relevant Public-Private Partnerships~~ **with the private sector** both at national and European level**, in particular with the objective of developing a strong European IT security industry**.

[10] **Council Directive 2008/114/EC of 8 December 2008, referred to in footnote no. 3.**

VII. INVITES THE COMMISSION TO

1. Promote the resilience and stability of the Internet at all levels in collaboration with public and private stakeholders;
2. **Promote a coherent and efficient European approach of NIS, in order to avoid redundant efforts and to ensure a common understanding of the different challenges at stake;**
3. **Closely cooperate with Member States and** ~~S~~**s**upport ~~the~~ **their** efforts ~~of the Member States~~ resulting from these conclusions, as appropriate;
4. Engage the private sector as much as possible in ~~Commission~~ **its** activities aiming to promote global cyber-security;
5. **Define and d**~~D~~evelop, in cooperation with the Member States, a European cyber incident contingency plan **by 2012**;
6. Monitor the development of the best governance strategies for emerging technologies with a global impact, including cloud computing;
7. Enhance EU preparedness by establishing **a** CERT for the Union's Institutions;
8. Together with the Member States and ~~the EEAS~~ **relevant Union's bodies**, work towards strengthening international cooperation in the field of cyber-security, ~~in particular~~ **for example** with the **US, in the framework of the** EU-U.S. Working Group on Cyber-security and Cyber-crime ~~and~~ **as well as with** other international partners**;**
9. **Regularly inform the European Parliament and the Council on initiatives taken at EU level relating to Network and Information Security**.

VIII. CALLS UPON THE ENISA TO

1. **Continue to actively support Member States in their effort to develop their national capabilities and to cooperate with each others;**
2. **Further develop its expertise on Network and Information Security and contribute to a better understanding of NIS emerging challenges for Europe.**

IX. INVITES STAKEHOLDERS TO

1. Initiate, promote and participate in actions aiming to strengthen network and information security and to foster the security and trust of users in electronic communications networks and services;
2. Share responsibility with public stakeholders on cyber-security challenges and help define ~~who is doing what~~ **individual responsibilities**, especially for ~~the~~ end user**s**;
3. Participate to Public-Private Partnerships with the aim to **contribute to the development of resilient and secure networks as well as a strong European IT security industry. These partnerships should also** reinforce multi-stakeholder dialogue and understanding of all challenges at stake;
4. Raise awareness among users on cyber-security risks and inform them on how they can best prevent and/or react to such risks;
5. **Support the Member States in their efforts to develop cyber-incident contingency plans and to organise** ~~Participate in national and/or~~ national**, cross border** and European cyber exercises, as appropriate;
6. Take all appropriate technical and organisational measures to safeguard the continuation, integrity and confidentiality of electronic communications networks and services;
7. Participate in the establishment and take up of European and international standards on **n**~~N~~etwork and **i**~~I~~nformation **s**~~S~~ecurity.