COUNCIL OF
THE EUROPEAN UNION

EN

Council conclusions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security"

3093rd TRANSPORT, TELECOMMUNICATIONS and ENERGY Council meeting
– telecommunication items only –

Brussels, 27 May 2011

The Council adopted the following conclusions:

"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 Communication of 30 March 2009 on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and 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]

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

P R E S S

Rue de la Loi 175 B – 1048 BRUSSELS Tel.: +32 (0)2 281 8239 / 6319 Fax: +32 (0)2 281 8026
press.office@consilium.europa.eu http://www.consilium.europa.eu/Newsroom

4. The Presidency Conclusions on CIIP of the Tallinn Ministerial Conference of 27-28 April 2009;[5]

5. The relevant provisions on information and network security of the new electronic communications regulatory framework; [6]

6. The Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security;[7]

7. The Commission Communication 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 ; [8]

8. The Council Conclusions of 31 May 2010 on the Digital Agenda for Europe;[9]

9. The Commission Communication of 22 November 2010 on "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe"; [10]

10. The Presidency Statement on CIIP of the Balatonfüred Ministerial Conference of 14-15 April 2011[11].

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 and also underlines the need to make IT systems and networks resilient and secure to all possible disruptions, whether accidental or intentional ;

2. That 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 and widespread use of ICT to contribute to economic growth as well as to a better quality of life;

3. That efforts in this regard should not only help boost growth and jobs, but also enable the Union to protect effectively its vital interests;

4. The increasing risks resulting from new and more sophisticated threats to ICT networks and services and the Internet in particular, which can be addressed, among others, by the development of new and more sophisticated self-protecting systems based on effective research and innovation, but also make effective protection more pressing than ever;

---

5 http://www.riso.ee/tallinnciip/ http://www.riso.ee/tallinnciip/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

6 OJ 18.12.2009, L 337 p. 11-68.

7 Doc 15841/09.

8 Doc 9981/10.

9 Doc 10130/10.

10 Doc 16797/10.

11 http://www.eu2011.hu/document/presidency-statement-en-ministerial-conference-critical-information-infrastructure-protecti

5. The major damage that vulnerabilities of or disruption to information and communication technology systems, infrastructures and services could cause to the European economy, taking into account that substantial disruption in one Member State also affects other Member States and the EU as a whole;

6. In consequence, the need, as a common objective for Europe, to stimulate and support the development of a high level of preparedness, security and resilience capabilities and to up-grade technical competences to allow Europe to face the challenge of networks and information infrastructure protection;

7. The need of taking up existing and further developing generally 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;

8. The need to stimulate trust and security among all involved stakeholders which constitutes a condition for fostering improved cooperation in the protection of vital infrastructures and for making every European digital, as pursued in the Digital Agenda for Europe;

9. The need of a collaborative approach to network and information security, involving all stakeholders, considering the broad use of ICT and the Internet by all kinds of users and for all kinds of purposes, in order to raise users' awareness and increase consciousness in use;

10. The need for public and private stakeholders to work together and to take responsibility in developing their own capabilities and preparedness to prevent, detect and respond to security challenges with potential impact on the availability of electronic communications networks and services;

11. The need to make the objective of preventing any disruption not only a national and European challenge but also an international and global one, considering the interconnectedness of information and communication technology systems, infrastructures and services.

IV. UNDERLINES

1. The strategic importance of the European ICT and NIS industry with regard to sustainable protection of European Critical Information Infrastructures;

2. With regard to national capabilities, 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;

3. With regard to European cooperation, the need to foster cooperation between Member States by developing 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, if appropriate, or on Internet stability and resilience as well as promoting, together with the private sector, a strong IT security industry;

4. The significant progress made by the European Forum of Member States (EFMS) in fostering discussion and exchanges between the Member States and the Member States and the Union on good policy practices related to security and resilience of ICT infrastructures;

5. The importance of multi-stakeholder efforts, for instance related to the European Public-Private Partnership for Resilience (EP3R), an evolving Europe-wide collaboration framework for the resilience of ICT infrastructures;

6. The important role of the European Network and Information Security Agency (ENISA) in relation to the activities performed by Member States and public and private stakeholders in the Union in the field of network and information security, in particular to the establishment of well functioning National/Governmental CERTs;

7. The success of the first pan- European cyber exercise of 4 November 2010 demonstrating the shared will for cross-border collaboration between Member States;

8. The benefits that are arising for network and information security from a national, European and global culture of risk analysis and management at all levels and by all stakeholders focused to promote coordinated actions to prevent, detect, mitigate and respond to all kinds of disruptions;

9. The opportunities opened to economic competitiveness through harnessing the power of new knowledge on network and information security systems, and especially on applications security by design and on novel self-protecting systems;

10. The benefits that could be drawn from further promoting, with the support of ENISA, a coherent and cooperative approach on network and information security in the Member States, in the EU Institutions and in the private sector.

V. STRESSES

The importance of a rapid and appropriate modernisation of the ENISA to enable the Agency to better assume and focus on 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 and education, training and research programmes in the field of network and information security;

2. Create CERTs in Member States that have not yet developed such a capability;

3. Foster the cooperation between already established or still to be established National /Governmental CERTs and other internationally recognised CERTs in operation in Member States;

4. Promote a well functioning network of National/Governmental CERTs and other internationally recognised CERTs in operation in Member States by 2012, with the support of ENISA as appropriate;

5. Define a common understanding on how a European Information and Alert System (EISAS) could be implemented in view of establishing, with the support of ENISA as appropriate, their national Information Sharing and Alert Systems;

6. Consider the adoption of national cyber-security strategy where it does not exist;

7. Develop national cyber incident contingency plans in order to be prepared to act and, if appropriate, liaise with Member States in case of serious incidents;

8. Strengthen collaboration among Member States and contribute, on the basis of national crisis management experiences and results and in cooperation with ENISA to the development of European cyber incident cooperation mechanisms to be tested in the framework of the next CyberEurope exercise in 2012;

9. Organise national or cross-border cyber exercises to test preparedness to cope with network and information security disruptions, contribute, in the appropriate manner, to organising and participating in European cyber exercises under a relevant, manageable schedule and other capacity building activities in the Union;

10. Pursue 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;

11. On the basis of voluntary mutual assistance among Member States, assist each other in cross-border incidents;

12. Continue and coordinate their efforts in all relevant international fora and work together with the Union's institutions towards strengthening international cooperation in the field of global network and information security and towards establishing strategic international partnerships at bilateral and multilateral level, for example by participating, in close coordination with the Commission, in the activities of the EU-U.S. Working Group on Cyber-security and Cyber-crime;

13. Stimulate and support the cooperation with the private sector both at national and European level.

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. Promote, together with Member States and ENISA, the take up of existing and the further development of generally 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;

4. Closely cooperate with Member States and support their efforts resulting from these conclusions, as appropriate;

5. Support the efforts of Member States within EFMS and EP3R related to the work on the criteria for identifying European Critical Infrastructures in the ICT sector, notably for fixed and mobile communication and for the Internet;

6. Engage the private sector as much as possible in its activities aiming to promote global network and information security;

7. Foster an ambitious R&D programme on security of network and information systems and applications and effectively link it to the defensive plans regarding critical information infrastructure protection;

8. Support Member States in their efforts to explore the possibilities to develop European cyber incident cooperation mechanisms to be tested in the framework of the next CyberEurope exercise in 2012;

9. Monitor the development of the best governance strategies for emerging technologies with a global impact, including cloud computing;

10. Enhance EU preparedness by establishing a CERT for the Union's Institutions;

11. In close coordination with the Member States and together with relevant Union's bodies, work towards strengthening international cooperation in the field of network and information security with relevant international partners and within different relevant fora such as the EU-U.S. Working Group on Cyber-security and Cyber-crime;

12. 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 efforts to develop their national capabilities and to cooperate with each other;

2. Further develop its expertise on Network and Information Security and contribute to a better understanding of emerging challenges in Europe regarding NIS.

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 efforts with public stakeholders on network and information security challenges and help define individual responsibilities, especially for end users;

3. Develop and produce more secure and reliable ICT products, services and hardware and software solutions thus contributing to the protection of our economies who are largely dependent on ICT;

4. Participate in 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;

5. Raise awareness among users on network and information security risks and inform them on how they can best prevent and/or react to such risks;

6. Support the Member States in their efforts to develop national cyber-incident contingency plans and to organise cyber exercises, as appropriate;

7. Take all appropriate technical and organisational measures to safeguard the availability and security of electronic communications networks and services;

8. Participate in the establishment and take up of minimum requirements and generally internationally recognized standards on network and information security."