EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2011/2284(INI)

22.3.2012

OPINION

of the Committee on Civil Liberties, Justice and Home Affairs

for the Committee on Industry, Research and Energy

on Critical Information Infrastructure Protection. Achievements and next steps: towards global cyber-security
(2011/2284(INI))

Rapporteur: Ágnes Hankiss

PA_NonLeg

SUGGESTIONS

The Committee on Civil Liberties, Justice and Home Affairs calls on the Committee on Industry, Research and Energy, as the committee responsible, to incorporate the following suggestions in its motion for a resolution:

1. Considers that the protection of critical information infrastructure requires an interdisciplinary approach that needs to include the important aspects of civil liberties, justice and home affairs such as internal security, personal data protection and the right to confidentiality and private life, thus enhancing security while respecting fundamental rights;

2. Recalls that the protection of critical information infrastructure is included in the EU Internal Security Strategy in the context of raising levels of security for citizens and businesses in cyberspace;

3. Urges that the identification of European Critical Infrastructure be completed and continuously updated under the supervision of the Commission, in accordance with Council Directive 2008/114/EC[1] (on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection); stresses also the need to create the Critical Infrastructure Warning Information Network at European level as soon as possible; insists that, in view of the strong dependency of public institutions, businesses and private households on Information and Communication Technologies (ICT), Council Directive 2008/114/EC should be reviewed in order to also recognise ICT as a critical sector;

4. Calls on the Member States to develop a national strategy and ensure a solid policy-making and regulatory environment, comprehensive risk management procedures and appropriate preparatory measures and mechanisms; urges Member States that have not founded their national CERT (Computer Emergency Response Team) to found it in due course, with the assistance of the European Network and Information Security Agency (ENISA) if needed;

5. Takes the view that any large-scale database handling sensitive personal data, such as those of the EU, Member State governments and financial and healthcare institutions, should be considered to be part of the critical information infrastructure and that the protection of such data should be ensured according to the highest possible standards;

6. Calls on the Commission and the Member States to take the necessary measures in order to protect critical infrastructure from cyber attacks and provide for means to cut off access to critical infrastructure if a direct cyber attack severely threatens its proper functioning;

7. Emphasises the importance of pan-European exercises in preparation for large-scale network security incidents, and the definition of a single set of standards for threat assessment;

[1] OJ L 345, 23.12.2008, p. 75.

8. Considers that ENISA can fulfil a key role at European level in the protection of critical information infrastructures by providing technical expertise to Member States and European Union institutions and bodies, as well as reports and analyses concerning information system security at European and global level;

9. Believes that international cooperation beyond the EU is indispensable, as the nature of cyber-threats is global, requiring global responses that comply with the provisions of international law; stresses also that any international agreement involving the exchange of sensitive data should take into consideration the security of data transfer and storage;

10. Emphasises that the Commission's upcoming 'Internet Security Strategy' should take the work on CIIP as a central point of reference and aim for a holistic and systematic approach towards cyber security by including both proactive measures, such as the introduction of minimum standards for security measures or the teaching of individual users, businesses and public institutions, and reactive measures, such as criminal-law, civil-law and administrative sanctions;

11. Believes that coordination within the EU should be strengthened and enhanced first and foremost between civilian and military actors and also the judicial and other competent authorities in preventing, combating and penalising attacks against information systems, including the police and other law enforcement authorities from the Member States, as well as specialised agencies at European level, such as Eurojust, Europol and ENISA;

12. Emphasises the importance of strong cooperation between the public and the private sectors, as the different strengths of the sectors should contribute, through mutual complementation, to the efforts made to protect the infrastructure and thus the lives and privacy of European citizens; calls on the Commission to establish the European Public-Private Partnership for Resilience, which would be integrated with the work of ENISA and the European Government CERTs Group;

13. Points out that the vast number of ongoing activities performed by various international and EU institutions, bodies and agencies as well as Member States requires coordination in order to avoid duplication, for which purpose it is worth considering designating an official responsible for coordination, possibly through the appointment of an EU cyber-security coordinator;

14. Considers that the efforts to protect Critical Information Infrastructures will not only enhance the overall security of citizens but will also improve citizens' perception of security and their trust in measures adopted by government to protect them;

15. Emphasises the importance of establishing and ensuring durable integration of European research to maintain and enhance European excellence in the area of Critical Information Infrastructure Protection;

16. Emphasises the importance of an active research roadmap in the area of cyber-security;

17. Advocates promoting cyber-security education (PhD student internships, university courses, workshops, training for students, etc.) and specialised training exercises in Critical Information Infrastructure Protection;

18. Advocates a close relationship and interaction between national private sectors and ENISA to interface the National/Governmental CERTs with the development of the European Information Sharing and Alert System (EISAS);

19. Emphasises the importance of a common European Cyber Security Strategy and of articulating a timeline for its definition in terms of actions and resources needed;

20. Underlines the importance of a structured dialogue between the main players and legislators in the EU and the USA involved in CIIP for a common understanding and common interpretations and positions regarding legal and governance frameworks.

RESULT OF FINAL VOTE IN COMMITTEE

Date adopted	21.3.2012
Result of final vote	+: 45 –: 0 0: 2
Members present for the final vote	Roberta Angelilli, Edit Bauer, Arkadiusz Tomasz Bratkowski, Philip Claeys, Carlos Coelho, Rosario Crocetta, Frank Engel, Cornelia Ernst, Tanja Fajon, Kinga Göncz, Nathalie Griesbeck, Sylvie Guillaume, Anna Hedh, Salvatore Iacolino, Lívia Járóka, Teresa Jiménez-Becerril Barrio, Juan Fernando López Aguilar, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu, Anthea McIntyre, Jan Mulder, Antigoni Papadopoulou, Judith Sargentini, Csaba Sógor, Renate Sommer, Rui Tavares, Kyriacos Triantaphyllides, Wim van de Camp, Renate Weber, Josef Weidenholzer, Cecilia Wikström
Substitute(s) present for the final vote	Vilija Blinkevičiūtė, Andrew Henry William Brons, Michael Cashman, Anna Maria Corazza Bildt, Ana Gomes, Nadja Hirsch, Stanimir Ilchev, Iliana Malinova Iotova, Franziska Keller, Wolfgang Kreissl-Dörfler, Mariya Nedelcheva, Hubert Pirker, Zuzana Roithová, Kārlis Šadurskis
Substitute(s) under Rule 187(2) present for the final vote	Luis de Grandes Pascual