P7_TA(2012)0237

Critical information infrastructure protection: towards global cyber-security

European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security (2011/2284(INI))

The European Parliament,

– having regard to its resolution of 5 May 2010 entitled 'A new Digital Agenda for Europe: 2015.eu'[1],

– having regard to its resolution of 15 June 2010 entitled 'Internet governance: the next steps'[2],

– having regard to its resolution of 6 July 2011 entitled 'European broadband investing in digitally driven growth'[3],

– having regard to Rule 48 of its Rules of Procedure,

– having regard to the report of the Committee on Industry, Research and Energy and the opinion of the Committee on Civil Liberties, Justice and Home Affairs (A7-0167/2012),

A. whereas information and communication technologies (ICTs) are able to deploy their full capacity for advancing the economy and society only if users have trust and confidence in their security and resilience, and if existing legislation on matters such as data privacy and intellectual property rights is enforced effectively in the internet environment;

B. whereas impact of the internet and ICT on various aspects of citizens' lives is increasing rapidly, and whereas they are crucial drivers for social interaction, cultural enrichment and economic growth;

C. whereas ICT and internet security is a comprehensive concept with a global impact on economic, social, technological and military aspects, demanding a clear definition and differentiation of responsibilities as well as a robust international cooperation mechanism;

D. whereas the aim of the EU Digital Agenda flagship is to boost Europe's competitiveness, based on strengthening ICT, and to create conditions for high and robust growth and technology-based jobs;

E. whereas the private sector remains the primary investor in, and owner and manager of, information security products, services, applications and infrastructure, with billions of euros invested over the last decade; whereas this involvement should be strengthened by appropriate policy strategies for promoting the resilience of public, private or public-privately owned or operated infrastructures;

F. whereas developing a high level of security and resilience in ICT networks, services and

---

1 OJ C 81 E, 15.3.2011, p.45.
2 OJ C 236 E, 12.8.2011, p. 33.
3 Texts adopted, P7_TA(2011)0322.

technologies should increase the competitiveness of the EU economy, both by improving cyber risk assessment and management and by providing the EU economy at large with more robust information infrastructures to support innovation and growth, creating new opportunities for enterprises to become more productive;

G. whereas available law enforcement data for cybercrimes (covering cyber-attacks, but also other types of online crime) suggest major increases in various European countries; whereas, however, statistically representative data concerning cyber attacks from both law enforcement and the CERT (computer emergency response team) community remains scarce and will need to be better aggregated in future, which will enable stronger responses from law enforcement across the EU and better informed legislative responses to ever-evolving cyber threats;

H. whereas a proper level of information security is critical for robust expansion of internet based services;

I. whereas recent cyber-incidents, disruptions and attacks against the information infrastructure of EU institutions**,** industry and Member States demonstrate the need to establish a robust, innovative and effective system of critical information infrastructure protection (CIIP), based on full international cooperation and minimum resilience standards among the Member States;

J. whereas the rapid development of new avenues of ICT such as cloud computing require a strong focus on security in order to make it possible to fully reap the benefits of the technological achievements;

K. whereas the European Parliament has repeatedly insisted on applying high standards for data privacy and data protection, net neutrality and intellectual property rights protection;

Measures to reinforce CIIP at national and Union level

1. Welcomes the Member States' implementation of the European Programme for CIIP, including the setting-up of the Critical Infrastructure Warning Information Network (CIWIN);

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

3. Acknowledges that the Commission is considering revising Council Directive 2008/114/EC[1] and calls for evidence to be provided of the effectiveness and impact of the directive before further steps are taken; calls for consideration to be given to expanding its scope, notably by including the ICT sector and financial services; calls, furthermore, for consideration to be given to areas such as health, food and water supply systems, nuclear research and industry (where these are not covered by specific provisions); takes the view that these sectors should also benefit from the cross-sectoral approach adopted in CIWIN (consisting of cooperation, an alert system and the exchange of best practices);

---

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

4. Emphasises the importance of establishing and ensuring durable integration of European research to maintain and enhance European excellence in the area of CIIP;

5. Calls, in view of the inter-connected and highly interdependent, sensitive, strategic and vulnerable nature of national and European critical information infrastructures, for the regular updating of minimum resilience standards for preparedness and reaction against disruptions, incidents, destruction attempts or attacks, such as those resulting from insufficiently robust infrastructure or insufficiently secured end-terminals;

6. Emphasises the importance of information security standards and protocols and welcomes the 2011 mandating of CEN, Cenelec and ETSI to establish security standards;

7. Expects owners and operators of critical information infrastructure to enable and, if necessary, assist users to utilise appropriate means for protecting themselves from malicious attacks and/or disruptions, through both human and automated supervision, where needed;

8. Supports cooperation between public and private stakeholders at Union level, and encourages their efforts to develop and implement standards for security and resilience for civilian (whether public, private or public-private) national and European critical information infrastructure;

9. 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;

10. Calls on the Commission, in cooperation with the Member States, to assess the implementation of the CIIP action plan; urges the Member States to establish well-functioning national/governmental CERTs, develop national cyber security strategies, organise regular national and pan-European cyber incident exercises, develop national cyber incident contingency plans and contribute to the development of a European cyber incident contingency plan by the end of 2012;

11. Recommends that operator security plans or equivalent measures be put in place for all European critical information infrastructures, and that security liaison officers be appointed;

12. Welcomes the current review of Council Framework Decision 2005/222/JHA[1] on attacks against information systems; notes the need to coordinate EU efforts in countering large-scale cyber-attacks by including ENISA, Member State CERTs and the future European CERT‘s competences;

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

Further EU activities for robust internet security

14. Urges ENISA to coordinate and implement annual EU Internet Security Awareness Months, so that issues relating to cyber-security become a special focus for the Member States and

---

[1] OJ L 69, 16.3.2005, p. 67.

EU citizens;

15. Supports ENISA, in line with the Digital Agenda goals, in exercising its duties with regard to network information security, and in particular by providing guidance and advising Member States on how to meet baseline capabilities for their CERTs, as well as supporting the exchange of best practices by developing an environment of trust; calls on the agency to consult relevant stakeholders with a view to defining similar cyber-security measures for owners and operators of private networks and infrastructure, as well as to assist the Commission and Member States in contributing to the development and uptake of information security certification schemes, norms of behaviour and cooperation practices among national and European CERTs and owners and operators of infrastructure as and where needed through the definition of technologically neutral common minimum requirements;

16. Welcomes the current proposal for review of ENISA‘s mandate, in particular its extension, and for the expansion of the tasks of the agency; believes that, along with its assistance to Member States by providing expertise and analysis, ENISA should be entitled to manage a number of executive tasks at EU level, and, in cooperation with US counterparts, tasks related to the prevention and detection of network and information security incidents and enhancing cooperation among the Member States; points out that, under the ENISA Regulation, the agency might also be assigned additional responsibilities related to the response to internet attacks, to the extent that it clearly adds value to existing national response mechanisms;

17. Welcomes the results of the 2010 and 2011 pan-European cyber security exercises conducted across the Union and monitored by ENISA, whose goal was to assist Member States in designing, maintaining and testing a pan-European contingency plan; calls on ENISA to keep such exercises on its agenda and progressively involve relevant private operators as appropriate in order to increase Europe‘s overall internet security capacities; looks forward to a further international expansion with like-minded partners;

18. Calls on the Member States to set up national cyber incident contingency plans and to include key elements such as relevant contact points, provisions of assistance, containment and repair in the event of cyber disruptions or attacks with regional, national or cross-border relevance; notes that the Member States should also put in place appropriate coordinating mechanisms and structures at national level, which would help to ensure better coordination among competent national authorities and make their actions more coherent;

19. Suggests that the Commission propose binding measures via the EU cyber incident contingency plan for better coordination at EU level of the technical and steering functions of the national and governmental CERTs;

20. Calls on the Commission and the Member States to take the necessary measures in order to protect critical infrastructure from cyber attacks and to provide ways of hermetically cutting off access to a critical infrastructure if a direct cyber attack poses a severe threat to its proper functioning;

21. Looks forward for the full implementation of CERT-EU, which will be a key factor in the prevention, detection, response and recovery from intentional and malicious cyber-attacks targeting the EU institutions;

22. Recommends that the Commission propose binding measures designed to impose minimum standards on security and resilience and improve coordination among national CERTs;

23. Calls on the Member States and the EU institutions to assure the existence of well-functioning CERTs, featuring minimum security and resilience capabilities based on agreed best practices; points out that national CERTs should be part of an effective network in which relevant information is exchanged in accordance with the necessary standards of confidentiality; calls for the establishment of a 24/7 continuity of CIIP service for each Member State, as well as the setting-up of a common European emergency protocol to be applicable between the national contact points;

24. Emphasises that building trust and promoting cooperation between Member States is crucial for protecting data and national networks and infrastructures; calls on the Commission to suggest a common procedure for identification and designation of a common approach to tackle cross-border ICT threats, with the Member States being expected to provide the Commission with generic information concerning the risks and threats to, and the vulnerabilities of, their critical information infrastructure;

25. Welcomes the Commission's initiative of developing a European Information Sharing and Alert System by 2013;

26. Welcomes the various stakeholder consultations on internet security and CIIP initiated by the Commission, such as the European Public-Private Partnership for Resilience; acknowledges the already significant involvement and commitment of ICT vendors in such efforts, encourages the Commission to make further efforts to encourage academia and ICT users' associations to play a more active role and to foster constructive, multi-stakeholder dialogue on cyber-security issues; supports further development of the Digital Assembly as a framework for CIIP governance;

27. Welcomes the work accomplished so far by the European Forum of Member States in terms of setting sector-specific criteria to identify European critical infrastructures with a focus on fixed and mobile communications, as well as discussing the EU principles and guidelines for the resilience and stability of the internet; looks forward to continued consensus-building among the Member States, and in this context encourages the Forum to complement the current approach focused on physical assets with efforts to also encompass logical infrastructure assets which, as virtualisation and cloud technologies develop, will become increasingly relevant to the effectiveness of CIIP;

28. Suggests that the Commission launch a public pan-European education initiative, geared towards educating and raising awareness among both private and business end-users about potential threats on the internet and fixed and mobile ICT devices at every level of the utility chain and towards promoting safer individual online behaviours; recalls, in this regard, the risks associated with outdated IT equipment and software;

29. Calls on the Member States, with support from the Commission, to strengthen the information security training and education programmes aimed at the national law enforcement and judicial authorities and the relevant EU agencies;

30. Supports the creation of an EU curriculum for academic experts in the field of information security, as this would have a positive impact on the expertise and preparedness of the EU with regard to the constantly evolving cyberspace and the threats to it;

31. Advocates promoting cyber-security education (PhD student internships, university courses, workshops, training for students, etc.) and specialised training exercises in CIIP;

32. Calls on the Commission to propose, by the end of 2012, a comprehensive internet security strategy for the Union, based on clear terminology; takes the view that the internet security strategy should aim at creating a cyberspace (supported by a secure and resilient infrastructure and open standards) which is conducive to innovation and prosperity through the free flow of information, while ensuring robust protection of privacy and other civil liberties; maintains that the strategy should detail the principles, goals, methods, instruments and policies (both internal and external) necessary in order to streamline national and EU efforts, and to establish minimum resilience standards among the Member States to ensure a safe, continuous, robust and resilient service, whether in connection with critical infrastructure or general internet use;

33. 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 education of individual users, businesses and public institutions, and reactive measures, such as criminal-law, civil-law and administrative sanctions;

34. Urges the Commission to propose a robust mechanism to coordinate the implementation and regular updating of the internet security strategy; takes the view that this mechanism should be supported by sufficient administrative, expert and financial resources and that its remit should include facilitating the establishment of EU positions in relations with both internal and international stakeholders on internet security related issues;

35. Calls on the Commission to propose an EU framework for the notification of security breaches in critical sectors such as energy, transport, water and food supply, as well as in the ICT and financial services sectors, to ensure that relevant Member State authorities and users are notified of cyber incidents, attacks or disruptions;

36. Urges the Commission to improve the availability of statistically representative data on the costs of cyber attacks in the EU, the Member States and industry (in particular the financial services and ICT sectors) by enhancing the data-gathering capabilities of the planned European Cybercrime Centre (due to be set up by 2013), the CERTs and other Commission initiatives such as the European Information Sharing and Alert System, so as to ensure systematic reporting and sharing of data on cyber-attacks and other forms of cybercrime afflicting European industry and Member States, and to strengthen law enforcement;

37. 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);

38. Points out that the primary driving force behind the development and use of technologies designed to increase internet security is the ICT industry; recalls that EU policies must avoid impeding the growth of the European internet economy and include the necessary incentives in order to exploit the potential of business and public-private partnerships to the full; recommends the investigation of further incentives for the industry to develop more robust operator security plans in line with Directive 2008/114/EC;

39. Calls on the Commission to present a legislative proposal for further criminalising cyber attacks (i.e. spear-phishing, online fraud, etc.);

International Cooperation

40. Recalls that international cooperation is the core instrument for introducing effective cyber-security measures; recognises that, at present, the EU is not actively involved on an ongoing basis in international cooperation processes and dialogues relating to cyber-security; calls on the Commission and the European External Action Service (EEAS) to start a constructive dialogue with all like-minded countries with a view to developing a common understanding and policies with the aim of increasing the resilience of the internet and of critical infrastructure; maintains that, at the same time, the EU should, on a permanent basis, include internet security issues in the scope of its external relations, inter alia when designing various financing instruments or when committing to international agreements which involve the exchange and storage of sensitive data;

41. Takes note of the positive achievements of the 2001 Council of Europe Budapest Convention on cybercrime; points out, however, that while encouraging more countries to sign and ratify the Convention, the EEAS should also build bilateral and multilateral agreements on internet security and resilience with like-minded international partners;

42. 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;

43. Emphasises that a structured dialogue between the main CIIP players and legislators in the EU and the US is particularly important with a view to establishing a common understanding and common interpretations and positions regarding legal and governance frameworks;

44. Welcomes the creation, at the November 2010 EU-US Summit, of the EU-US Working Group on Cyber-security and Cyber-crime, and supports its efforts to include internet security issues in the transatlantic policy dialogue; welcomes the joint establishment, by the Commission and the US Government, under the umbrella of the EU-US Working Group, of a common programme and a roadmap towards joint/synchronised trans-continental cyber-exercises in 2012/2013;

45. Suggests establishing a structured dialogue between EU and US legislators in order to discuss internet-related issues as part of a search for common understanding, interpretation and positions;

46. Urges the EEAS and the Commission, on the basis of the work done by the European Forum of Member States, to secure an active position within the relevant international forums, inter alia by coordinating the positions of the Member States with a view to promoting the EU's core values, goals and policies in the field of internet security and resilience; notes that such forums include NATO, the UN (in particular through the International Telecommunication Union and the Internet Governance Forum), the Internet Corporation for Assigned Names and Numbers, the Internet Assigned Numbers Authority, the OSCE, the OECD and the World Bank;

47. Encourages the Commission and ENISA to participate in the main stakeholder dialogues to define technical and legal norms in cyberspace at an international level;

o

o o

48. Instructs its President to forward this resolution to the Council and the Commission.