Critical information infrastructure protection. Achievements and next steps: towards global cyber-security

2011/2284(INI) - 12/06/2012 - Text adopted by Parliament, single reading

The European Parliament adopted by 573 votes to 90, with 26 abstentions, a resolution on critical information infrastructure protection – achievements and next steps: towards global cyber-security.

Parliament states that 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. It recalls that the impact of the internet and ICT on various aspects of citizens' lives is increasing rapidly. They are crucial drivers for social interaction, cultural enrichment and economic growth. A proper level of information security is critical for robust expansion of internet based services.

It is for this reason that the resolution proposes a draft resolution proposing a framework for protection at three levels: national, European and international, which may summarised as follows:

I. Measures to reinforce CIIP at national and Union level: Parliament welcomes the Member States' implementation of the European Programme for CIIP, including the setting-up of the Critical Infrastructure Warning Information Network (CIWIN). The critical information infrastructure protection (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.

It calls for existing measures to be strengthened, such as:

- extending the scope of Council Directive 2008/114/EC, notably by including the ICT sector and financial services as well as health, food and water supply systems, nuclear research and industry (where these are not covered by specific provisions);
- enhancing European excellence in the area of CIIP;
- updating of minimum resilience standards for preparedness and reaction against disruptions, incidents, destruction attempts or attacks;
- supporting cooperation between public and private stakeholders at Union level, and encourage 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;
- emphasising the importance of pan-European exercises in preparation for large-scale network security incidents.

Moreover, Members call on the Commission, in cooperation with the Member States, to assess the implementation of the CIIP action plan. They urge 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**. They recommend that operator security plans or equivalent measures be put in place for all European critical information infrastructures, and that security liaison officers be appointed.

II. Further EU activities for robust internet security: the resolution 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 EU citizens. It 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**.

ENISA is called upon 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 (in particular in the framework of the revision of the ENISA Regulation);
- obtain additional responsibilities related to the response to internet attacks to the extent that it clearly adds value to existing national response mechanisms;
- maintain the exercises carried out in 2010 and 2011 on its agenda and progressively involve relevant private operators.

The resolution 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. There should be better coordination among competent national authorities to make their actions more coherent.

European response to cyber-attacks: Parliament states that available law enforcement data for cybercrimes (covering cyber-attacks, but also other types of online crime) suggest major increases in various European countries. 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.

The Commission is called upon to:

- 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;
- take, along with the Member States, 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;
- propose binding measures designed to **impose minimum standards on security and resilience** and improve coordination among national CERTs.

CERT: Members call 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. They point 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. Furthermore, they call 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.

Common procedure: the resolution 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. It welcomes the Commission' s initiative of developing a **European Information Sharing and Alert System by 2013**.

Members welcome the **various stakeholder consultations** on internet security and CIIP initiated by the Commission. They advocate promoting cyber-security education (PhD student internships, university courses, workshops, training for students, etc.) and specialised training exercises in CIIP. They suggest 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.

Comprehensive internet security strategy: Parliament calls on the Commission to propose, by the end of 2012, a **comprehensive internet security strategy** for the Union, based on clear terminology. This 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**. Members maintain 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. 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 should be introduced. The Commission should propose a robust mechanism to coordinate the implementation and regular updating of the internet security strategy. The Commission is urged to improve the availability of statistically representative data on the costs of **cyber attacks** in the EU.

This mechanism should be supported by sufficient **administrative, expert and financial resources**.

In addition, Parliament calls for:

- a proposal for 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;
- the improvement of the availability of statistically representative data on the costs of cyber attacks in the EU, the Member States and industry ;
- measures to 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.

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

III. International Cooperation: Parliament recalls that international cooperation is the core instrument for introducing effective cyber-security measures. However, at present, the EU is not actively involved on an ongoing basis in international cooperation processes and dialogues relating to cybersecurity. Members call 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. Members maintain that, at the same time, the EU should, on a permanent basis, include internet security issues in the scope of its external relations and that ongoing activities performed by various international and EU institutions, bodies and agencies as well as Member States require coordination in order to avoid duplication.

Welcoming the creation, at the November 2010 EU-US Summit, of the EU-US Working Group on Cyber-security and Cyber-crime and the common programme and a roadmap towards joint/synchronised transcontinental cyber-exercises in 2012/2013, Members suggest 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.

Lastly, Parliament 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. It notes that such forums include NATO, the UN, the Internet Corporation for Assigned Names and Numbers, the Internet Assigned Numbers Authority, the OSCE, the OECD and the World Bank. It encourages the Commission and ENISA to participate in the main stakeholder dialogues to define technical and legal norms in cyberspace at an international level.