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

2011/2284(INI) - 31/03/2011 - Non-legislative basic document

PURPOSE: to take stock of the results achieved since the adoption of the Critical Information Infrastructure Protection (CIIP) action plan and describe the next steps planned for each action.

BACKGROUND: the Commission adopted on 30 March 2009 a communication on Critical Information Infrastructure Protection (the 'CIIP action plan') to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures. The aim was to stimulate and support the development of a high level of preparedness, security and resilience capabilities both at national and European level. The action plan is built on five pillars: preparedness and prevention, detection and response, mitigation and recovery, international cooperation and criteria for European Critical Infrastructures in the field of ICT.

At the same time the Digital Agenda for Europe, adopted in May 2010, emphasises the need for all stakeholders to join their forces in a holistic effort to ensure the security and resilience of ICT infrastructures, by focusing on prevention, preparedness and awareness, as well as developing effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyber-attacks and cyber-crime.

Complementing this, the Commission tabled a proposal for a new mandate to strengthen and modernise the European Network and Information Security Agency (ENISA) in order to boost trust and network security.

This Communication takes stock of the results achieved since the adoption of the CIIP action plan in 2009. It describes the next steps planned for each action at both European and international level. It also focuses on the global dimension of the challenges and the importance of boosting cooperation among Member States and the private sector at national, European and international level, in order to address global interdependencies.

CONTENT: the Communication begins by identifying the potential threats which may disrupt access to information networks. In order to gain a more comprehensive understanding of these various threats, it can be useful to regroup them along the following categories:

– **exploitation purposes**, such as "advanced persistent threats" for economic and political espionage purposes (e.g. GhostNet), identity theft, the recent attacks against the Emissions Trading System etc;

– **disruption purposes**, such as Distributed Denial of Service attacks or spamming generated via botnets (e.g. the Conficker network of 7 million machines) ;

– **destruction purposes**, which is a scenario that has not yet materialised but, cannot be ruled out for the years to come.

In order to counter these threats, the Commission highlights some of the actions it has taken:

1) Preparedness and prevention:

- the establishment of the European Forum of Member States (EFMS) made significant progress in fostering discussion and exchanges related to security and resilience of ICT infrastructures;

- the European Public-Private Partnership for Resilience (EP3R) aims at fostering the cooperation between the public and the private sectors on strategic EU security and resilience policy issues;

- the creation of a network of well-functioning National/Governmental CERTs in all Member States by 2012, which will be the backbone of the European Information Sharing and Alert System (EISAS) for citizens and SMEs.

2) Detection and response: ENISA devised a high-level roadmap for the development of a European Information Sharing and Alert System (EISAS) by 2013.

3) Mitigation and recovery: so far only 12 Member States that have organised exercises for large-scale network security incident response and disaster recovery. The first pan-European exercise on large-scale network security incidents (Cyber Europe 2010) took place on 4 November 2010 with the involvement of all Member States, plus Switzerland, Norway and Iceland.

Future pan-European cyber exercises would undoubtedly benefit from a common framework.

4) International cooperation: the Commission will discuss and promote the principles with relevant stakeholders, in particular the private sector (via EP3R), bilaterally with key international partners, in particular the US, as well as multilaterally. It will do so, within its competences, in fora such as G8, OECD, NATO, etc.

5) Criteria for European Critical Infrastructures in the ICT sector: the technical discussion in EFMS led to a first draft of the ICT sector-specific criteria for identifying European Critical Infrastructures, with a focus on fixed and mobile communications and the Internet. The technical discussion will continue and benefit from the consultations on the draft criteria, at national and European (via EP3R) level, with the private sector. The Commission will also discuss with Member States the ICT sector- specific elements to be considered for the review of the Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection in 2012.

Next steps: in the face of global challenges, the Commission will:

- **promote principles for the resilience and stability of the Internet**: international principles for the resilience and stability of the Internet should be developed with other countries, with international organisations and, where appropriate, with global private- sector organisations – by using existing fora and processes, such as those related to Internet Governance. These principles should serve as a tool for all stakeholders to frame their activities, relating to the stability and resilience of the Internet;

- build strategic international partnerships: strategic partnerships should be built on ongoing efforts in critical areas, like **cyber-incident management**, including exercises and cooperation among CERTs. The engagement of the private sector, which operates on a global scale, is of paramount importance. The EU-U.S. Working Group on Cyber-security and Cyber-crime is an important step in this direction. The Working Group will focus on cyber incident management, public-private partnerships, awareness raising and cyber-crime. On the European side, key factors for success would be good coordination between all EU institutions, relevant agencies (in particular ENISA and Europol) and Member States.

- **develop trust in the cloud**: it is essential to strengthen discussions on the best governance strategies for emerging technologies with a global impact, such as cloud computing.

Member States are called upon to:

- enhance EU preparedness by establishing a network of well functioning National/Governmental CERTs by 2012. This activity will also advance the development of a European Information Sharing and Alert System (EISAS) to the wider public by 2013;

- **establish a European cyber-incident contingency plan by 2012** and regular pan-European cyber exercises. Future pan-European cyber exercises should be based on a European cyber incident contingency plan that builds upon and interlinks with national contingency plans. Such a plan should provide the baseline mechanisms and procedure for communications between Member States and, last but not least, support the scoping and organisation of future pan-European exercises. ENISA will work with Member States on the development of such a European cyber incident contingency plan by 2012;

- ensure European coordinated efforts in international fora and discussions on **enhancing security and resilience of Internet.** Member States should cooperate together and with the Commission on promoting the development of an approach based on principles or norms to the issue of the global stability and resilience of the Internet.

It should be noted than an Annex to the Communication gives a detailed overview of achievements of the CIIP action plan as well as the next steps.