Procedure file

Basic information

INI - Own-initiative procedure	2011/2284(INI)	Procedure completed
Critical information infrastructure protection. Achievements and next steps: towards global cyber-security Subject 3.30.06 Information and communication technologies, digital technologies 3.30.07 Cybersecurity, cyberspace policy 3.30.25 International information networks and society, internet		

Key players

European Parliament	Committee responsible	Rapporteur	Appointed
	ITRE Industry, Research and Energy		07/06/2011
		S&D KALFIN Ivailo	
		Shadow rapporteur	
		PPE VAN NISTELROOIJ Lambert	
		ALDE CREUTZMANN Jürgen	
		Verts/ALE ANDERSDOTTER Amelia	
		ECR TOŠENOVSKÝ Evžen	
		EFD TZAVELA Niki	
	Committee for opinion	Rapporteur for opinion	Appointed
	AFET Foreign Affairs	The committee decided not to give an opinion.	
	LIBE Civil Liberties, Justice and Home Affairs		23/11/2011
		PPE HANKISS Ágnes	
European Commission	Commission DG	Commissioner	
	Communications Networks, Content and Technology	KROES Neelie	

Key events

31/03/2011	Non-legislative basic document published	COM(2011)0163	Summary
17/11/2011	Committee referral announced in Parliament		
08/05/2012	Vote in committee		
16/05/2012	Committee report tabled for plenary	A7-0167/2012	Summary
11/06/2012	Debate in Parliament		

12/06/2012	Results of vote in Parliament		
12/06/2012	Decision by Parliament	T7-0237/2012	Summary
12/06/2012	End of procedure in Parliament		

Technical information

Procedure reference	2011/2284(INI)
Procedure type	INI - Own-initiative procedure
Procedure subtype	Initiative
Legal basis	Rules of Procedure EP 54
Stage reached in procedure	Procedure completed
Committee dossier	ITRE/7/06163

Documentation gateway

Non-legislative basic document		COM(2011)0163	31/03/2011	EC	Summary
Committee draft report		PE474.017	07/02/2012	EP	
Amendments tabled in committee		PE483.516	06/03/2012	EP	
Committee opinion	LIBE	PE480.619	22/03/2012	EP	
Committee report tabled for plenary, single reading		A7-0167/2012	16/05/2012	EP	Summary
Text adopted by Parliament, single reading		T7-0237/2012	12/06/2012	EP	Summary
Commission response to text adopted in plenary		SP(2012)626	30/10/2012	EC	

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

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.

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

The Committee on Industry, Research and Energy adopted the own-initiative report drafted by Ivailo KALFIN (S&D, BG) on critical information infrastructure protection achievements and next steps: towards global cyber-security.

Members recall 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 Members propose 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: Members welcome the Member States implementation of the European Programme for CIIP, including the setting-up of the Critical Infrastructure Warning Information Network (CIWIN). 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.

Members call 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; 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. 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 report 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 ;
- maintain the exercises carried out in 2010 and 2011 on its agenda and progressively involve relevant private operators.

The report 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.

At EU level, 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.

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 report 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 Commissions 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 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: Members call 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, they call 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;
- a legislative proposal for further criminalising cyber attacks (i.e. spear-phishing, online fraud, etc.).

III. International Cooperation: Members recall 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 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. They 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, Members urge 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 EUs core values, goals and policies in the field of internet security and resilience; 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. They encourage the Commission and ENISA to participate in the main stakeholder dialogues to define technical and legal norms in cyberspace at an international level.

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

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 Commissions 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 EUs 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.