Procedure file

Basic information

INI - Own-initiative procedure	2012/2096(INI)	Procedure completed
Cyber security and defence		

Subject
3.30.06 Information and communication technologies, digital technologies
3.30.07 Cybersecurity, cyberspace policy
6.10.02 Common security and defence policy (CSDP); WEU, NATO

Key players

European Parliament	Committee responsible	Rapporteur	Appointed
	AFET Foreign Affairs		06/03/2012
		PPE KELAM Tunne	
		Shadow rapporteur	
		S&D YÁÑEZ-BARNUEVO GARCÍA Luis	
		ALDE NICOLAI Norica	
		Verts/ALE TARAND Indrek	
		ECR VAN ORDEN Geoffrey	
		EFD TERHO Sampo	

European Commission	Commission DG	Commissioner
	Communications Networks, Content and Technology	KROES Neelie

Key events

24/05/2012	Committee referral announced in Parliament		
10/10/2012	Vote in committee		
17/10/2012	Committee report tabled for plenary	A7-0335/2012	Summary
21/11/2012	Debate in Parliament		
22/11/2012	Results of vote in Parliament		
22/11/2012	Decision by Parliament	T7-0457/2012	Summary
22/11/2012	End of procedure in Parliament		

Technical information

Procedure reference	2012/2096(INI)

Procedure type	INI - Own-initiative procedure
Procedure subtype	Initiative
Legal basis	Rules of Procedure EP 54
Other legal basis	Rules of Procedure EP 159
Stage reached in procedure	Procedure completed
Committee dossier	AFET/7/09320

Documentation gateway

Committee draft report		PE489.358	22/06/2012	EP	
Amendments tabled in committee		PE494.798	11/09/2012	EP	
Committee report tabled for plenary, single reading		A7-0335/2012	17/10/2012	EP	Summary
Text adopted by Parliament, single reading		T7-0457/2012	22/11/2012	EP	Summary
Commission response to text adopted in plenary		SP(2013)110	02/04/2013	EC	

Cyber security and defence

The Committee on Foreign Affairs adopted an own-initiative report by Tunne KELAM (EPP, EE) on cyber security and defence. The main recommendations contained in the report are the following:

Actions and coordination in the European Union (EU): given that cyber threats and attacks against government, administrative, military and international bodies are a rapidly growing menace and occurrence in both the EU and globally, the report underlines, therefore, the need for a global and coordinated approach to the question of cyber security which should:

·   establish a common definition of cyber security and defence and of what constitutes a defence-related cyber attack;

·   a common operating vision and;

·   take into account the added value of the existing agencies and bodies; as well as good practices from those Member States which already have national cyber security strategies.

The report calls on the Commission and the High Representative of the Union for Foreign Affairs and Security Policy to consider the possibility of a serious cyber attack against a Member State in their forthcoming proposal on the arrangements for the implementation of the Solidarity Clause (Article 222 TFEU).

The Council and the Commission are urged to unequivocally recognise digital freedoms as fundamental rights and as indispensable prerequisites for enjoying universal human rights, and together with the Member States, to elaborate a White Paper on Cyber Defence.

EU level: the Members stress the importance of horizontal cooperation and coordination on cyber security within and between EU institutionsand agencies.

The EU institutions are called on to: i) develop their cyber security strategies and contingency plans with regard to their own systems in the shortest time possible; ii) include in their risk analysis and crisis management plans, the issue of cyber crisis management.

The report also underlines the importance of:

·   the efficient development of the EU Computer Emergency Response Team (EU-CERT) and of national CERTs as well as the development of national contingency plans in the event that action needs to be taken;

·   to create as soon as possible at European level the Critical Infrastructure Warning Information Network;

·   of pan-European exercises in preparation for large-scale network security incidents;

·   and the definition of a single set of standards for threat assessment.

The report underlines the importance for Member States of close cooperation with the European Defence Agency (EDA) on developing their national cyber defence capabilities. It encourages the EDA to deepen its cooperation with NATO, national and international centres of excellence, the European Cybercrime Centre at Europol contributing to faster reactions in the event of cyber attacks.

The Member States, for their part, are urged to:

·   develop and complete their respective national cyber security and defence strategies without further delay and ensure a solid policy-making and regulatory environment, comprehensive risk management procedures and appropriate preparatory measures and mechanisms;

·   create designated cyber security and cyber defence units within their military structure, with a view to cooperating with similar bodies in other EU Member States;

·   introduce specialised courts at regional level geared to ensuring that attacks on information systems are punished more effectively;

- develop national contingency plans and to include cyber crisis management in crisis management plans and risk analysis;

- make research and development one of the core pillars of cyber security and defenceand to encourage the training of engineers specialised in protecting information systems.

The Commission and Member States are urged to come forward with programmes to promote and raise awareness among both private and business users ingeneral safe use of the Internet. The Members propose that the Commission launch a public pan-European education initiative in this regard, calling on the Member States to include education on cyber security in school curricula from the earliest possible age;

Finally, the report:

- underlines the crucial role of meaningful and complementary cyber security cooperation between the public authorities and the private sector, both at EU and national level, with the aim of generating mutual trust;

- calls for the speeding up of cooperation and exchange of information on how to tackle cyber security issues with third countries;

- urges all relevant bodies in the EU dealing with cyber security and defence to deepen their practical cooperation with NATO with a view to exchanging experience and learning how to build resilience for EU systems;

- believes that the EU and the US should deepen their mutual cooperation to counter cyber attacks and cybercrime, since this was made a priority of the transatlantic relationship following the 2010 EU-US Summit in Lisbon.

Cyber security and defence

The European Parliament adopted 454 votes to 39 with 96 abstentions a resolution on cyber security and defence. Parliaments principal recommendations are as follows:

Actions and coordination in the European Union (EU): given that cyber threats and attacks against government, administrative, military and international bodies are a rapidly growing menace and occurrence in both the EU and globally, Parliament stresses the need to develop a comprehensive EU cyber security strategy which should provide :

- a common definition of cyber security and defence and of what constitutes a defence-related cyber attack;

- a common operating vision and;

- take into account the added value of the existing agencies and bodies, as well as good practices from those Member States which already have national cyber security strategies.

Parliament calls on the Commission and the High Representative of the Union for Foreign Affairs and Security Policy to consider the possibility of a serious cyber attack against a Member State in their forthcoming proposal on the arrangements for the implementation of the Solidarity Clause (Article 222 TFEU).

The Council and the Commission are urged to unequivocally recognise digital freedoms as fundamental rights and as indispensable prerequisites for enjoying universal human rights, and together with the Member States, to elaborate a White Paper on Cyber Defence.

EU level: Members stress the importance of horizontal cooperation and coordination on cyber security within and between EU institutions and agencies.

The EU institutions are called on to: i) develop their cyber security strategies and contingency plans with regard to their own systems in the shortest time possible; ii) include in their risk analysis and crisis management plans, the issue of cyber crisis management.

Parliament also underlines the importance of:

- the efficient development of the EU Computer Emergency Response Team (EU-CERT) and of national CERTs as well as the development of national contingency plans in the event that action needs to be taken;

- to create as soon as possible at European level the Critical Infrastructure Warning Information Network;

- pan-European exercises in preparation for large-scale network security incidents;

- the definition of a single set of standards for threat assessment.

Parliament underlines the importance for Member States of close cooperation with the European Defence Agency (EDA) on developing their national cyber defence capabilities. It encourages the EDA to deepen its cooperation with NATO, national and international centres of excellence, the European Cybercrime Centre at Europol contributing to faster reactions in the event of cyber attacks.

Member States, for their part, are urged to:

- develop and complete their respective national cyber security and defence strategies without further delay and ensure a solid policy-making and regulatory environment, comprehensive risk management procedures and appropriate preparatory measures and mechanisms;

- create designated cyber security and cyber defence units within their military structure, with a view to cooperating with similar bodies in other EU Member States;

- introduce specialised courts at regional level geared to ensuring that attacks on information systems are punished more effectively;

- develop national contingency plans and to include cyber crisis management in crisis management plans and risk analysis;

- make research and development one of the core pillars of cyber security and defenceand to encourage the training of engineers specialised in protecting information systems.

The Commission and Member States are urged to come forward with programmes to promote and raise awareness among both private and

business users ingeneral safe use of the Internet. Members propose that the Commission launch a public pan-European education initiative in this regard, calling on Member States to include education on cyber security in school curricula from the earliest possible age.

Public-Private Cooperation: Parliament underlines the crucial role of meaningful and complementary cyber security cooperation between the public authorities and the private sector, both at EU and national level, with the aim of generating mutual trust. It is aware that further enhancing the reliability and efficiency of the relevant public institutions will contribute to the building of trust and to the sharing of critical information.

Members call on private sector partners to consider security-by-design solutions when designing new products, devices, services and applications, and also call for minimum transparency standards and accountability mechanisms to be established with regard to cooperation with the private sector to prevent and combat cyber attacks. They urge the Commission to develop frameworks and instruments for a rapid information exchange system that would ensure anonymity when reporting cyber incidents for the private sector, enable public actors to be kept constantly up to date and provide assistance when needed.

International and NATO cooperation: lastly, Parliament:

· calls for the speeding up of cooperation and exchange of information on how to tackle cyber security issues with third countries;

· urges all relevant bodies in the EU dealing with cyber security and defence to deepen their practical cooperation with NATO with a view to exchanging experience and learning how to build resilience for EU systems;

· believes that the EU and the US should deepen their mutual cooperation to counter cyber attacks and cybercrime, since this was made a priority of the transatlantic relationship following the 2010 EU-US Summit in Lisbon.