Basic information

2013/2606(RSP) RSP - Resolutions on topical subjects	Procedure completed
Resolution on a cybersecurity strategy of the European Union: an open, safe and secure cyberspace **Subject** 3.30.07 Cybersecurity, cyberspace policy	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
IMCO Internal Market and Consumer Protection	SCHWAB Andreas (PPE) HARBOUR Malcolm (ECR)	20/03/2013 20/03/2013
	Shadow rapporteur GARCÉS RAMÓN Vicente Miguel (S&D) MANDERS Antonius (ALDE) ENGSTRÖM Christian (Verts/ALE) SALVINI Matteo (EFD)	

Council of the European Union

Council configuration	Meetings	Date
General Affairs	3251	2013-06-25

European Commission

Commission DG	Commissioner
Communications Networks, Content and Technology	KROES Neelie

Key events

Date	Event	Reference	Summary
25/06/2013	Resolution/conclusions adopted by Council		Summary
09/07/2013	Vote in committee		
10/09/2013	Debate in Parliament		
12/09/2013	Decision by Parliament	T7-0376/2013	Summary

12/09/2013	Results of vote in Parliament		
12/09/2013	End of procedure in Parliament		

Technical information	
Procedure reference	2013/2606(RSP)
Procedure type	RSP - Resolutions on topical subjects
Procedure subtype	Resolution on statement
Legal basis	Rules of Procedure EP 136-p2
Other legal basis	Rules of Procedure EP 165
Stage reached in procedure	Procedure completed
Committee dossier	IMCO/7/12435

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Motion for a resolution		B7-0386/2013	06/09/2013	
Text adopted by Parliament, single reading		T7-0376/2013	12/09/2013	Summary

European Commission

Document type	Reference	Date	Summary
Commission response to text adopted in plenary	SP(2013)816	19/12/2013	

Resolution on a cybersecurity strategy of the European Union: an open, safe and secure cyberspace

2013/2606(RSP) - 25/06/2013

On 7 February 2013, the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy issued a Joint Communication to the European Parliament and the Council on “the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace".

On this basis, the Council adopted a series of conclusions as follows:

Comprehensive approach: the Council regarded it essential and urgent to develop further and implement a comprehensive approach for EU cyberspace policy that:

- protects and promotes enjoyment of human rights and is grounded in the EU’s fundamental values of democracy, human rights and the rule of law,

- advances European prosperity and the social and economic benefits of cyberspace including the Internet,
- promotes effective and improved cyber security across the EU and beyond,
- advances the efforts to bridge the global digital divide and promotes international cooperation in cybersecurity,
- reflects the roles and rights of individual citizens, the private sector, and civil society in cyber issues.

In this context, the Council invited the Member States, the Commission and the High Representative to work together, respecting each others' areas of competence and the principle of subsidiarity, in response to the strategic objectives:

(1) Values: the Council invited Member States to take all reasonable steps to ensure that all EU citizens are able to access and enjoy the benefits of the Internet.

(2) Prosperity: legislation in support of cybersecurity should foster innovation and growth according to the Council. The digital economy is a major driver of growth, innovation and employment, and cybersecurity is key to protecting the digital economy. The Council also stated the importance at national level of CIIP (Critical Information Infrastructure Protection).

(3) Cyber resilience: Member States are invited to take steps to ensure they reach an efficient national level of cybersecurity, by developing and implementing the proper policies, organisational and operational capacities in order to protect information systems in cyberspace, in particular those considered to be critical. The Council called for a series of measures such as: (i) support awareness-raising on the nature of the threats and the fundamentals of good digital practices, at all levels; (ii) support the owners and providers of ICT systems in protecting their own systems; (iii) foster pan-European cybersecurity cooperation, in particular by enhancing pan-European cybersecurity exercises; (iv) strengthen and expand cooperation between Member States and EU users, building on existing structures; (v) take into account cybersecurity issues in light of ongoing work on the solidarity clause.

(4) Cybercrime: the Council invited the Commission to support Member States, at their request, to identify gaps and strengthen their capability to investigate and combat cybercrime. It suggested the use of the future Internal Security Fund (ISF), within its budget limit, to support relevant authorities fighting cybercrime as well as the use of the Instrument for Stability (IfS) to develop the fight against cybercrime as well as cybercriminal organisations. It also suggested continuing to facilitate cross-community cooperation, in particular by supporting Europol.

Other proposals have been made as regards the fight against cybercrime through the cooperation with third countries and the Common Security and Defence Policy.

At the same time, the Council called upon the Commission and High Representative to produce a progress report on the cybersecurity Strategy to be presented at the High Level Conference to be held in February 2014. It also proposed to hold regular meetings of the competent Council preparatory bodies, (in particular the FoP on Cyber Issues) to assist in setting EU cyber priorities and strategic objectives as part of a comprehensive policy framework.

Lastly, the Council invited the Commission to present the financing of the Strategy, taking into account the upcoming negotiations with the European Parliament.

Resolution on a cybersecurity strategy of the European Union: an open, safe and secure cyberspace

2013/2606(RSP) - 12/09/2013 - Text adopted by Parliament, single reading

The European Parliament adopted by 585 votes to 45 with 8 abstentions a resolution tabled by the Committee on the Internal Market and Consumer Protection and the Committee on Foreign Affairs on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, in response to the Joint Communication of 7 February 2013 by the Commission and the HR/VP on the subject.

It notes the growing cyber-challenges, in the form of increasingly sophisticated threats and attacks, as well as the need to ensure that cyberspace remains open to free expression and to online services. Members stress the need for a strategic communication policy on EU cyber-security, cyber-crisis situations, strategy reviews, public-private collaboration and alerts, and recommendations to the public.

Parliament reiterates its call on the Member States to **adopt national cyber-security strategies** that: (i) cover technical, coordination, human resources and financial allocation aspects, (ii) include distinct rules on the benefits for and responsibilities of the private sector, in order to guarantee their participation; (iii) provide for comprehensive risk management procedures as well as safeguard the regulatory environment. At the same time it stresses that **Member States should aim never to endanger citizens' rights and freedoms** when developing responses to cyber threats and attacks.

The resolution also emphasises the need for training programmes aimed at promoting awareness, among European citizens, in particular with regard to personal security, as a part of a digital literacy curriculum from an early age.

Cyber-resilience: Parliament insists on the development of cyber-resilience for critical infrastructures, and recalls that the forthcoming arrangements for the implementation of the Solidarity Clause (Article 222 TFEU) should take into consideration the risk of cyber-attack against a Member State. The Commission and the HR are asked to take this risk into account in their joint integrated threat and risk assessment reports to be issued as from 2015. Parliament welcomes the Commission's notion to create a risk-management culture with regard to cyber-security, and **urges Member States and Union institutions rapidly to include cyber-crisis management in their crisis management plans and risk analyses**. Private sector actors must also be encouraged to include cyber-crisis management in their management plans and risk analyses, and to train their staff in cyber-security.

Members stress the need to establish a network of well functioning Computer Emergency and Response Teams **(CERTs)** operational on a 24/7 basis. They also support ENISA in exercising its duties with regard to network and information security, in particular by providing guidance and by advising Member States.

Industrial and technological resources: Parliament calls on Union institutions and Member States to take the necessary measures to establish a 'single market for cyber-security' in which users and suppliers are able to make best use of the innovations, synergies and combined expertise on offer, and

which enables the entry of SMEs. Member States are asked to consider making **joint investments in the European cyber-security industry**, much in the same way as has been done in other industries, such as the aviation sector.

Cybercrime: recalling that cybercrime costs the global economy almost EUR 295 billion each year, Parliament takes the view that, given the borderless nature of cybercrime, joint efforts made, and expertise offered, at Union level, above the level of the individual Member States, are particularly important, and that Eurojust, Europol's EC3, CERTs, and universities and research centres must therefore be provided with **adequate resources** and capabilities to function properly as hubs for expertise, cooperation and information-sharing. Furthermore, citizens should be able easily to access information on cyber-threats and how to fight them.

Lastly, all Member States should ratify the Council of Europe's Budapest Convention on Cybercrime.

Cyber-defence: the resolution calls on Member States to **intensify their cooperation with the European Defence Agency** (EDA) with a view to developing proposals and initiatives for cyber-defence capabilities. It also calls on the VP/HR to **include cyber-crisis management in crisis management planning**, and stresses the need for the Member States, in cooperation with the EDA, to develop plans to protect CSDP missions and operations against cyber-attacks.

International policy: since international cooperation and dialogue play an essential role in creating trust and transparency, Parliament wants the Commission and EEAS to **set up a cyber-diplomacy team,** whose responsibilities would include the promotion of dialogue with like-minded countries and organisations. It calls on the VP/HR to **mainstream the cyber-security dimension into the EU's external actions,** especially in relation to third countries. In this connection, the **EU-US Working Group on Cybersecurity and Cybercrime** should serve as an instrument for the EU and the US to exchange best practices on cyber-security policies.

Implementation: Members ask the **Commission to draw up a clear roadmap determining the timelines for the objectives to be delivered at Union level** under the cyber-security strategy and invite Member States to agree on a similar delivery plan for national activities under this strategy.