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.