EUROPEAN PARLIAMENT 2009 - 2014

Plenary sitting

6.5.2013 B7-0000/2013

MOTION FOR A RESOLUTION

to wind up the debate on the statement by the Commission

pursuant to Rule 110(2) of the Rules of Procedure

on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
(2013/2606(RSP))

Malcolm Harbour, Andreas Schwab
on behalf of the Committee on the Internal Market and Consumer Protection

B7-0000/2013

European Parliament resolution on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
(2013/2606(RSP))

The European Parliament,

– having regard to the Joint Communication of 07 February 2013 by the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy entitled "Cybersecurity Strategy for the European Union: An Open, Safe and Secure Cyberspace" (JOIN(2013)1),

– having regard to the proposal of 07 February 2013 for a Directive concerning measures to ensure a high common level of network and information security across the Union (COM (2013)0048),

– having regard to Commission Communications of 19 May 2010 entitled "A Digital Agenda for Europe" (COM (2010)0245) and of 18 December 2012 entitled "The Digital Agenda for Europe - Driving European growth digitally" (COM(2012)0784),

– having regard to the European Union Internal Security Strategy entitled "Towards a European Security Model" (COM(2010)0673) as adopted by the Council on 25 and 26 February 2010, and its resolution[1] of 22 May 2012 thereon,

– having regard to Commission Communication of 28 March 2013 entitled "Tackling crime in our digital age: Establishing a European Cybercrime centre" (COM(2012)0140 final) and to the Council Conclusions of 7 June 2012 thereon,

– having regard to the proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA of 30 September 2010 and the ongoing negotiations thereon,

– having regard to Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[2],

– having regard to its resolution[3] of 12 June 2012 and the Council conclusions of 27 May 2011 on the Commission communication on critical information infrastructure protection entitled "Achievements and next steps: towards global cybersecurity",

– having regard to its resolution of 11 December 2012 on Completing the Digital Single Market[4],

[1] Text adopted, P7_TA(2012)0207
[2] OJ L 345, 23.12.2008, p. 75.
[3] Text adopted, P7_TA(2012)0237
[4] Text adopted, P7_TA(2012)0468

– having regard to its resolution of 22 November 2012 on Cybersecurity and Defence[1],

– having regard to its legislative resolution of 16 April 2013 on the proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (COM(2010)521) establishing its position in the first reading[2],

– having regard to its resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy[3],

– having regard to the Convention on Cybercrime of 27 November 2004 by the Council of Europe,

– having regard to the ongoing negotiations on Transatlantic Trade and Investment Partnership (TTIP) between the European Union and the United States of America;

– having regard to Rule 110 of its Rules of Procedure,

A. whereas growing cyber challenges, increasingly sophisticated threats and attacks constitute a major threat to national security, stability and economic prosperity of the Member States as well as of the private sector and the wider community; whereas the protection of our society and economy therefore will be a constantly evolving challenge;

B. whereas e-commerce and online services are a vital force of the internet and are crucial to the aims of the EU 2020 strategy, benefitting both citizens and private sector; whereas, the Union must fully realise the potential and opportunities that the internet, presents to the further development of the single market;

C. whereas the strategic priorities outlined in the Joint Communication on a cybersecurity strategy for the European Union include achieving cyber resilience, reducing cybercrime, developing cyberdefence policy and capabilities related to Common Security and Defence Policy (CSDP);

D. whereas network and information systems across the Union are highly interconnected; whereas, given the global nature of the internet, many network and information security incidents transcend national borders and have the potential to undermine the functioning of the internal market and the confidence of consumers in the digital single market;

E. whereas cybersecurity across the Union is only as strong as its weakest link and disruptions in one sector or Member State impact another sector or Member State creating spill over effect on the Union economy as a whole;

F. whereas, as of April 2013, only 13 Members States have officially adopted national cybersecurity strategies; whereas there remain fundamental differences between the Member States in terms of maturity, complexity of and capacities to implement their national cybersecurity strategies;

[1] Text adopted, P7_TA(2012)0457
[2] Text adopted, P7_TA(2013)0103
[3] Text adopted, P7_TA(2012)0470

G. whereas this fragmentation and lack of legal certainty are primary concerns in the digital single market; whereas the lack of a harmonized approach to cybersecurity calls for concerted efforts and closer cooperation;

1. Welcomes the Joint Communication for a cybersecurity strategy of the European Union and the proposal for a directive concerning measures to ensure a high level of network and information security across the Union;

2. Stresses the paramount and increasing importance that the internet and the cyberspace has for political, economic, and societal transactions within the Union but also in relation to other actors around the world;

3. Reminds that the need for a high level of network and information security is not only required for maintaining virtual services that are essential for the well-functioning of society and economy, but also for safeguarding the physical integrity of citizens through the secure functioning of critical infrastructures;

4. Reiterates its call on Member States to adopt cybersecurity strategies without undue delay; notes that only a combined leadership and political ownership on the part of the Union institutions and Member States will lead to a high level of network and information security across the Union, and thus contribute to the secure and smooth functioning of the single market;

5. Stresses that the Union cybersecurity policy should be based on and designed to ensure the protection and preservation of freedoms and respect for fundamental rights online;

6. Underlines the crucial role of cooperation between the public authorities and the private sector, both at Union and national level, with the aim of generating mutual trust and exchanging expertise;

Cyber resilience

7. Notes that sectors and Member States have different levels of capabilities and skills which hinders the development of trusted cooperation and undermines the functioning of the single market;

8. Underscores that for guaranteeing integrity, availability and confidentiality particularly of critical services, the identification and categorization of critical infrastructure must be up to date and necessary minimum security requirements for their network and information systems must be set;

9. Recognises that the proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union foresees such minimum security requirements for providers of information society services and operators of critical infrastructures;

10. Calls on Member States and the Union institutions to establish a network of well-functioning Computer Emergency and Response Teams (CERTs);

11. Supports ENISA in exercising its duties with regard to network and information security;

Industrial and technological resources

12. Is of the opinion that ensuring a high level of network and information security plays a central role in raising the competitiveness of both the suppliers of security solutions and the users in the Union; considers that on the one hand the IT security industry in the Union has important untapped potential, while on the other hand private, public and business users are often uninformed about the costs and benefits of investing in cyber security and thus remain vulnerable towards harmful cyber threats;

13. Deems that a strong supply and demand require adequate investments in research and development to foster innovations and sufficient awareness about the network and information security risks;

14. Calls on the Union institutions and the Member States to take the necessary measures towards the establishment of a "Single Market for Cybersecurity", where users and suppliers benefit best from innovations, synergies and combined expertise;

15. Encourages Member States to consider investing jointly in the European cybersecurity industry similar to what has been done in other sectors such as in aviation;

Cybercrime

16. Considers that criminal activities in the cyberspace can be as harmful to the well-being of societies as offences in the physical world and often reinforce each other as can be observed with regard to, inter alia, the sexual exploitation of children and organized crime;

17. Agrees with the Commission that the same norms and principles that uphold offline also apply online and that therefore the fight against cybercrime needs to be stepped up in up to date legislation and operational capabilities;

18. Is of the view that joint efforts and expertise beyond the individual Member States at Union level are particularly important and that therefore Eurojust and the European Cybercrime Centre within Europol need to be provided with adequate resources and capabilities to properly function as hubs for expertise, cooperation and information-sharing;

19. Calls on Member States who have not yet ratified the Council of Europe Convention on Cybercrime to do so without undue delay,

Cyberdefence

20. Underlines that cyber challenges, threats and attacks put Member States' defence and national security interests at risk and that civilian and military approaches for the protection of respective critical infrastructure should maximize their benefits from synergies;

21. Calls for efforts of the Union to enter into an exchange with international partners,

including NATO, to identify areas of cooperation, to avoid duplication, and to complement activities, where possible;

International policy

22. Believes that international cooperation and dialogue play an essential role in creating trust and promoting a high level of network and information at a global level;

23. Is of the opinion that efforts should be made to ensure that the existing international legal instruments are enforced in the cyberspace; considers therefore that currently there is no need for the creation of new legal instruments at international level;

24. Considers that, in particular, the EU-US Working Group on Cybersecurity and Cybercrime should serve as an instrument to prepare the ground for an alignment of the cybersecurity policies between the EU and the US, wherever appropriate; notes in this context that areas linked to cybersecurity, such as e-commerce, consumer protection online, including data protection, and other services depending on the secure functioning of network and information systems are expected to be an important element of the upcoming negotiations of Transatlantic Trade and Investment Partnership (TTIP);

25. Notes that cybersecurity skills and the capacity to fight threats and malicious attacks are not evenly developed around the globe; emphasizes that efforts to increase cyber resilience and fight cyber threats must not be confined to like-minded partners, but should also address the regions with less developed capacities, technical infrastructure and legal frameworks;

Implementation

26. Calls for regular evaluations of the effectiveness of national cybersecurity strategies at the highest political level to ensure adaptation to new global threats and broader developments;

27. Asks for regular reports by the Commission and Member States assessing the progress that has been made on the objectives set out in the cybersecurity strategy, including key performance indicators measuring the progress of implementation;

28. Instructs its President to forward this resolution to the Council and Commission.