



EUROPEAN PARLIAMENT

2009 - 2014

---

*Committee on Foreign Affairs*

---

**2012/2096(INI)**

22.6.2012

# **DRAFT REPORT**

on Cyber Security and Defence  
(2012/2096(INI))

Committee on Foreign Affairs

Rapporteur: Tunne Kelam

**CONTENTS**

	<b>Page</b>
MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION .....	3

## MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

### on Cyber Security and Defence

(2012/2096(INI))

*The European Parliament,*

- having regard to the report on implementation of the European Security Strategy endorsed by the European Council on 11 and 12 December 2008,
- having regard to the Council of Europe Cybercrime Convention, Budapest of 23 November 2004,
- having regard to the Council conclusions on Critical Information Infrastructure Protection of 27 May 2011 and the previous Council's conclusions on cyber security,
- having regard to the Commission's 'Digital Agenda for Europe' of 19 May 2010 (COM(2010)0245),
- 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<sup>1</sup>,
- having regard to the recent Commission Communication on the creation of a European Cybercrime Centre as a priority of the Internal Security Strategy (COM(2012)0140),
- having regard to its resolution of 10 March 2010 on the implementation of the European Security Strategy and the Common Security and Defence Policy<sup>2</sup>,
- having regard to its resolution of 11 May 2011 on the development of the common security and defence policy following the entry into force of the Lisbon Treaty<sup>3</sup>,
- having regard to its resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security<sup>4</sup>,
- having regard to the conclusions of the Chicago Summit of 20 May 2012,
- having regard to Title V of the EU Treaty,
- having regard to Rule 48 of its Rules of Procedure,
- having regard to the report of the Committee on Foreign Affairs (A7-0000/2012),

A. whereas in today's globalised world, the EU and its Member States have become crucially reliant on safe cyber space;

---

<sup>1</sup> OJ L 345, 23.12.2008, p. 75.

<sup>2</sup> Texts adopted, P7\_TA(2010)0061.

<sup>3</sup> Texts adopted, P7\_TA(2011)0228.

<sup>4</sup> Texts adopted, P7\_TA(2012)0237.

- B. whereas cyber challenges and threats are growing at a dramatic pace and constitute a major threat to the security, stability and competitiveness of the nation states as well as of the private sector; whereas such threats should not therefore be considered future issues; whereas cyber challenges and threats are increasingly of a politically motivated nature; whereas the vast majority of cyber incidents remain primitive;
- C. whereas there are numerous obstacles of a political, legislative and organisational nature in the EU and its Member States; whereas there is a lack of common standards and common measures in the sensitive and vulnerable area of cyber security;
- D. whereas sharing and coordination within the EU institutions and with and between Member States is still insufficient;
- E. whereas clear and harmonised definitions of ‘cyber security’ and ‘cyber defence’ are lacking at EU and international levels; whereas the understanding of cyber security and other key terminology varies considerably among different countries;
- F. whereas the EU has not yet developed coherent policies of its own regarding critical information and infrastructure protection;
- G. whereas the EU has proposed various initiatives to tackle cybercrime, including the establishment of a new Cybercrime Centre;
- H. whereas building trust and confidence between the private sector and law enforcement authorities is of utmost importance in the fight against cybercrime;
- I. whereas trust and mutual confidence in the relations among state and non-state actors is a prerequisite for reliable cyber security;
- J. whereas a large number of cyber incidents in the private sector remain unreported due to the sensitive nature of the information and possible damage to the image of the companies involved;
- K. whereas the European Network and Information Security Agency (ENISA) is being engaged as a facilitator for Member States to support the exchange of good practices in the area of cyber security by recommending how to develop, implement and maintain a cyber security strategy; and has a supportive role in National Cyber Security Strategies, National Contingency Plans, organising Pan-European and International exercises on Critical Information Infrastructure Protection (CIIP), and development of scenarios for national exercises;
- L. whereas only 10 EU Member States had, as of June 2012, officially adopted a National Cyber Security Strategy;
- M. whereas cyber defence is one of the top priorities of the EDA, which has set up, under the Capabilities Development Plan, a project team on cyber security with the majority of Member States working to collect experiences and propose recommendations;
- N. whereas investments in cyber security and defence research and development are crucial

for advancing and for maintaining a high level of cyber security and defence; whereas defence expenditure on research and development has decreased instead of reaching agreed 2% of overall defence expenditure;

- O. whereas raising awareness and educating citizens on cyber security should constitute the basis of any comprehensive cyber security strategy;
- P. whereas a clear balance has to be established between security measures and citizens' rights;
- Q. whereas cyberspace, with its nearly 2 billion globally interconnected users, has become one of the most potent and efficient means of advancing democratic ideas and organising people as they seek to realise their aspirations for freedom and fight against dictatorships; whereas the use of cyberspace by undemocratic and authoritarian regimes poses an increasing threat to individuals' rights to freedom of expression and association; whereas it is therefore crucial to ensure that cyberspace will remain open to the free flow of ideas, information and expression;
- R. whereas there is an increasing need to better respect and protect individuals' rights to privacy;
- S. whereas global cyber challenges and threats call for an international collective response;
- T. whereas the European External Action Service (EEAS) has not yet proactively included a cyber security aspect in its relations with third countries;
- U. whereas the Instrument for Stability is so far the only EU programme which is designed to respond to urgent crises or global/transregional security challenges, including cyber security threats;
- V. whereas responding jointly – through the EU-US working group on cyber security and cybercrime – to cyber security threats is one of the priority issues in EU-US relations;

#### **Actions and coordination in the EU**

1. Notes that cyber threats are a rapidly growing menace both in the EU and globally, and that there is increasing concern about the potential for organised criminal, terrorist or politically motivated attacks against the critical information systems and infrastructures of the Member States and the EU institutions;
2. Underlines therefore the need for a global and coordinated approach to these challenges at the EU level with the development of a comprehensive EU cyber security strategy which should provide a common definition of cyber security and defence, a common operating vision and take into account the added value of the existing agencies and bodies; stresses the crucial importance of coordination and creating synergies at the level of the Union to help combine different initiatives, programmes and activities; emphasises that such a strategy should ensure flexibility and be updated on regular basis to adapt to the rapidly changing nature of cyberspace;

3. Urges the Commission to investigate the possibility of evoking the solidarity clause, pursuant to the Treaty on the Functioning of the EU (Title VII, Article 222), in the event of a serious cyber attack against a Member State;

#### **EU level**

4. Stresses the importance of horizontal cooperation and coordination on cyber security within and between EU institutions;
5. Recognises the need for an assessment of the overall level of cyber attacks against EU information systems and infrastructure; highlights, in this context, the need for continuous assessment of the degree of preparedness of EU institutions to tackle potential cyber attacks;
6. Notes that recent cyber attacks against European information networks and governmental information systems have caused considerable economic and security damage, the extent of which has not been adequately assessed;
7. Calls on all the EU institutions to develop their cyber security strategies and contingency plans with regard to their own systems in the shortest time possible;
8. Calls on all EU institutions to include in their risk analysis and crisis management plans the issue of cyber crisis management; calls, furthermore, on all EU institutions to provide awareness-raising trainings on cyber security to all of its staff; suggests conducting cyber exercises once a year similarly to emergency exercises;
9. Underlines the importance of the efficient development of the EU Computer Emergency Response Team (CERT) and CERTs as well as the development of national contingency plans in the event that action needs to be taken; welcomes the fact that, by May 2012, all EU Member States had set up national CERTs; urges the further development of national CERTs and EU CERT capable of being deployed within 24 hours if needed; stresses the need to look into the feasibility of a public-private partnership in this field;
10. Recognises that 'Cyber Europe 2010', the first pan-European exercise on critical information infrastructure protection, which was carried out with the involvement of various Member States and led by ENISA, proved to be a helpful action and an example of good practices;
11. Calls on the Commission to explore the necessity and feasibility of an EU Cyber Coordination post;

#### **European Defence Agency (EDA)**

12. Welcomes the recent initiatives and projects relating to cyber defence, especially on gathering and mapping relevant cyber security and defence data, challenges and needs;
13. Underlines the importance for Member States of close cooperation with the EDA on developing their national cyber defence capabilities; believes that building synergies, pooling and sharing at European level are crucial for effective cyber defence at European

and national level;

14. Encourages the EDA to deepen its cooperation with NATO, national and international centres of excellence, and especially with the Cooperative Cyber Defence Centre of Excellence (CCDCOE), and to concentrate on capacity building, training as well as on exchange of information and practices;
15. Observes with concern that only one Member State achieved the level of 2 % expenditure on defence research and development by 2010, and that five Member States spent nothing on R&D in 2010; urges the EDA, together with Member States, to pool resources and to effectively invest in collaborative research and development, with particular regard to cyber security and defence;

### **Member States**

16. Calls on all Member States to develop and complete their respective national cyber security and defence strategies with no further delay; calls on ENISA to assist the Member States; expresses its support to ENISA in developing a Good Practice Guide on good practices and recommendations on how to develop, implement and maintain a cyber security strategy;
17. Encourages Member States to create designated cyber security and cyber defence units within their military structure;
18. Calls on the Commission to continue to work on a coherent and efficient European approach to avoid redundant initiatives, encouraging and supporting Member States in their efforts to develop cooperation mechanisms and to enhance the exchange of information; is of the opinion that a minimum level of obligatory cooperation and sharing should be established between the Member States;
19. Urges the Member States to develop national contingency plans and to include cyber crisis management in crisis management plans and risk analysis; further underlines the importance of adequate training on essential cyber security for all staff in public entities; calls on ENISA and other relevant bodies to assist Member States in ensuring the pooling and sharing of resources as well as avoiding duplication;
20. Urges the Member States to make research and development one of the core pillars of cyber security and defence; calls on the Member States to live up their commitment to increase defence expenditure on research and development to at least 2 %, with particular regard to cyber security and defence;
21. Calls on the Commission and Member States to come forward with programmes to promote general safe use of internet and information systems; calls on the Member States to include education on cyber security in school curricula from the earliest possible age;

### **Public Private Cooperation**

22. 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; 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;

23. A permanent dialogue should be established with these partners on the best use and resilience of information systems and the sharing of responsibility required for the safe and proper functioning of these systems;
24. Is of the view that Member States, EU institutions and the private sector, in cooperation with ENISA, should take steps to increase the security and integrity of information systems, to prevent attacks and to minimise the impact of attacks; Supports the Commission in its efforts to come forward with minimum cyber security standards for companies;
25. Calls on the Commission and on the Member States' governments to encourage the private sector and civil society actors to include cyber crisis management in their crisis management plans and risk analysis; calls, furthermore, for the introduction of awareness-raising training on essential cyber security and cyber hygiene for all members of their staff;
26. Calls on the Commission, in cooperation with Member States and relevant agencies and bodies, 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;
27. Emphasises the need for the EU to facilitate the development of a competitive and innovative market for cyber security in the EU in order to better enable SMEs to operate in this field which will contribute to boosting economic growth and creating new jobs;

### **International cooperation**

28. Calls on the EEAS to take a proactive approach regarding cyber security and to mainstream the cyber security aspect in all of its actions, especially in relation to third countries; calls for the speeding up of cooperation and exchange of information on how to tackle cyber security issues with third countries;
29. Stresses that the completion of a comprehensive EU cyber security strategy is a precondition to establishing the sort of efficient international cooperation on cyber security that the cross-border nature of cyber threats necessitates;
30. Calls on those Member States which have not yet signed or ratified the Council of Europe Convention on Cybercrime (Budapest Convention) to do so without further delay; supports the Commission and the EEAS in their efforts to promote the Convention and its values among third countries;
31. Is aware of the need for an internationally agreed and coordinated response to cyber threats; calls, therefore, on the Commission, EEAS and Member States to take the lead in the efforts to achieve a broader international agreement on norms of behaviour in cyber space;

32. Proposes to set up a joint working group with BRICS countries in order to tackle cyber security matters, and especially to explore possibilities for a possible common response to growing cybercrime and cyber attacks;
33. Urges the EEAS and the Commission to take a proactive approach within the relevant international forums and organisations, notably the UN, the OSCE, the OECD and the World Bank, with the aim of applying existing international law and achieving consensus on norms for responsible state behaviour on cyber security and defence, and by coordinating the positions of the Member States with a view to promoting the EU's core values and policies in the field of cyber security and defence;
34. Calls on the Council and the Commission to insist, during its negotiations and cooperation with third countries, on minimum requirements for preventing and fighting cyber criminality and cyber attacks; and on minimum standards in information system security;
35. Calls on the Commission to facilitate and assist third countries, if needed, in their efforts to build their cyber security and cyber defence capabilities;

### **Cooperation with NATO**

36. Reiterates that, on the basis of their common values and strategic interests, the EU and NATO have a special responsibility and capacity to address the increasing cyber security challenges more efficiently and in close cooperation by looking for possible complementarities, without duplication and with respect for their respective responsibilities;
37. Underlines the need to pool and share on a practical level, considering the complementary nature of the EU and NATO approach to cyber security and defence; emphasises the need for closer coordination, especially concerning planning, technology, training and equipment with regard to cyber security and defence;
38. Building on the existing complementary activities in defence capability development, 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;

### **Cooperation with the United States**

39. 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;
40. Welcomes the creation, at the November 2010 EU-US Summit, of the EU-US Working Group on Cyber-Security and Cyber-Crime, and supports its efforts to include cyber security issues in the transatlantic policy dialogue;
41. Welcomes the joint establishment, by the Commission and the US Government, under the umbrella of the EU-US Working Group, of a common programme and roadmap towards joint/synchronised trans-continental cyber exercises in 2012/2013; takes note of the first

Cyber Atlantic exercise in 2011;

42. Instructs its President to forward this resolution to the Council, the Commission, the HR/VP, EDA, ENISA and NATO.