EUROPEAN PARLIAMENT 2009 - 2014

Plenary sitting

A7-0335/2012

17.10.2012

REPORT

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

Committee on Foreign Affairs

Rapporteur: Tunne Kelam

CONTENTS

Page

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[1],

– 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[2],

– 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[3],

– having regard to its resolution of 22 May 2012 on the European Union's Internal Security Strategy [4],

– having regard to its resolution of 27 September 2011 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology[4],

– having regard to its resolution of 12 June 2012 on critical information infrastructure

[1] OJ L 345, 23.12.2008, p. 75.
[2] Texts adopted, P7_TA(2010)0061.
[3] Texts adopted, P7_TA(2011)0228.
[4] Texts adopted, P7_TA(2012)0207.
[4] Texts adopted, P7_TA(2012)0406.

protection – achievements and next steps: towards global cyber-security[1],

– having regard to the resolution of the UN Human Rights Council of 5 July 2012 entitled 'The promotion, protection and enjoyment of human rights on the Internet'[2], which recognises the importance of human rights protection and the free flow of information online,

– 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 (A7-0335/2012),

A. whereas in today's globalised world, the EU and its Member States have become crucially reliant on safe cyber space, on a secure use of information and digital technologies and on resilient and reliable information services and associated infrastructures;

B. whereas information and communication technologies are also used as tools of repression; whereas the context in which they are used determines to a great extent the impact these technologies can have as a force either for positive developments or for repression;

C. whereas cyber challenges, threats and attacks are growing at a dramatic pace and constitute a major threat to the security, defence, 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 a majority of highly visible and disruptive cyber incidents are now of a politically motivated nature; whereas the vast majority of cyber incidents remain primitive, threats to critical assets become increasingly sophisticated and warrant in-depth protection;

D. whereas cyberspace, with its nearly two 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 to 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;

E. whereas there are numerous obstacles of a political, legislative and organisational nature in the EU and its Member States to the development of a comprehensive and unified approach to cyber defence and cyber security; whereas there is a lack of common definition, standards and common measures in the sensitive and vulnerable area of cyber security;

[1] Texts adopted, P7_TA(2012)0237.
[2] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx.

F. whereas sharing and coordination within the EU institutions and with and between Member States, as well as with outside partners is still insufficient;

G. 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;

H. whereas the EU has not yet developed coherent policies of its own regarding critical information infrastructure protection which requires a multidisciplinary approach thus enhancing security while respecting fundamental rights;

I. whereas the EU has proposed various initiatives to tackle civilian level cybercrime, including the establishment of a new European Cybercrime Centre**,** yet lacks any concrete plan at the level of security and defence;

J. whereas building trust and confidence between the private sector and law enforcement authorities, defence and other competent institutions is of utmost importance in the fight against cybercrime;

K. whereas trust and mutual confidence in the relations between state and non-state actors is a prerequisite for reliable cyber security;

L. whereas the majority of cyber incidents in both the public and private sectors remain unreported due to the sensitive nature of the information and possible damage to the image of the companies involved;

M. whereas a large number of cyber incidents occur due to lack of resilience and robustness of private and public network infrastructure, poorly protected or secured databases and other flaws in the critical information infrastructure; whereas only few Member States consider the protection of their network and information systems and associated data as part of their respective duty of care which explains the lack of investment in state-of-the-art security technology, training and the development of appropriate guidelines, whereas a large number of Member States depend on security technology from third countries and should increase their efforts to reduce this dependency;

N. whereas the majority of perpetrators of high level cyber attacks that threaten national or international security and defence are never identified and prosecuted; whereas there is no internationally agreed form of response to a state-backed cyber attack against another state, nor an understanding of whether this could be considered a casus belli;

O. 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;

P. whereas only 10 EU Member States had, as of June 2012, officially adopted a National

Cyber Security Strategy;

Q. 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;

R. 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 the agreed 2 % of overall defence expenditure;

S. whereas raising awareness and educating citizens on cyber security should constitute the basis of any comprehensive cyber security strategy;

T. whereas a clear balance has to be established between security measures and citizens' rights in accordance with the TFEU, such as the right to privacy, data protection and freedom of expression; with neither being sacrificed in the name of the other;

U. whereas there is an increasing need to better respect and protect individuals' rights to privacy as stipulated in the EU Charter and Article 16 TFEU; whereas the need to secure and defend cyberspace at a national level for institutions and defence bodies, while important, should never be used as an excuse to in any way limit rights and freedoms in cyber and informational space;

V. whereas the global and borderless nature of the internet requires new forms of international cooperation and governance with multiple stakeholders;

W. whereas governments increasingly rely on private players for the security of their critical infrastructure;

X. whereas the European External Action Service (EEAS) has not yet proactively included a cyber security aspect in its relations with third countries;

Y. 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;

Z. 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 and attacks against government, administrative, military and international bodies are a rapidly growing menace and occurrence in both the EU and globally, and that there are significant reasons for concern that state and non-state actors, especially terrorist and criminal organisations, are able to attack critical information and communication structures and infrastructures of EU institutions and members, with the potential to cause significant harm, including kinetic effects;

2. Underlines, therefore, the need for a global and coordinated approach to these challenges

at the EU level through the development of 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 should 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; stresses the crucial importance of coordination and creating synergies at the Union level to help combine different initiatives, programmes and activities, both military and civilian; emphasises that such a strategy should ensure flexibility and be updated on a regular basis to adapt it to the rapidly changing nature of cyberspace;

3. Urges 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); takes, furthermore, the view that although cyber attacks endangering national security still need to be defined by common terminology, they could be covered by the Mutual Defence Clause (Article 42.7 TEU), without prejudice to the principle of proportionality;

4. Emphasises that CSDP must ensure that forces on EU military operations and civilian missions are protected against cyber attacks. Underlines that cyber defence should be made an active capability of CSDP;

5. Stresses that all EU cyber security policies should be based on and designed to ensure maximum protection and preservation of digital freedoms and respect for human rights online; believes the Internet and ICTs should be included in the EU's foreign and security policies in order to advance this effort;

6. Calls on the Commission and Council to unequivocally recognise digital freedoms as fundamental rights and as indispensable prerequisites for enjoying universal human rights; stresses that Member States should aim never to endanger their citizens' rights and freedoms when developing their responses to cyber threats and attacks and should have adequate legislative differences between civilian and military level cyber incidents; calls for caution in applying restrictions on the ability of citizens to make use of communication and information technology tools;

7. Calls on the Council and the Commission, together with the Member States, to elaborate a White Paper on Cyber Defence establishing clear definitions and criteria separating levels of cyber attacks in the civilian and military spheres, according to their motivation and effects, as well as levels of reaction, including the investigation, detection and prosecution of perpetrators;

8. Sees a clear need to update the European Security Strategy with a view to identifying and finding means of pursuing and prosecuting individual, network-related and state-supported cyber attackers;

EU level

9. Stresses the importance of horizontal cooperation and coordination on cyber security within and between EU institutions and agencies;

10. Stresses that new technologies challenge the way in which governments perform traditional core tasks; reaffirms that defence and security policies ultimately lie in the hands of government, including adequate democratic oversight; takes note of the increasingly important role of private actors in executing security and defence tasks often without transparency, accountability or democratic oversight mechanisms;

11. Stresses that governments need to abide by the basic principles of international public and humanitarian law, such as respect for state sovereignty and human rights, when using new technologies in the scope of security and defence policies; points to the valuable experience of EU Member States, such as Estonia, in defining and designing cyber security policies as well as cyber defence;

12. 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; places particular emphasis on the need to strengthen critical information infrastructure;

13. Stresses, likewise, the need to provide information on vulnerabilities, alerts and warnings of fresh threats to information systems;

14. 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;

15. 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;

16. 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 training on cyber security to all their staff; suggests conducting cyber exercises once a year similarly to emergency exercises;

17. 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; welcomes the fact that, by May 2012, all EU Member States have set up national CERTs; urges the further development of national CERTs and an EU-CERT capable of being deployed within 24 hours if needed; stresses the need to look into the feasibility of public-private partnerships in this field;

18. 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; stresses also the need to create the Critical Infrastructure Warning Information Network at European level as soon as possible;

19. Emphasises the importance of pan-European exercises in preparation for large-scale network security incidents, and the definition of a single set of standards for threat

assessment;

20. Calls on the Commission to explore the necessity and feasibility of an EU Cyber Coordination post;

21. Considers that, given the high level of skill required both to adequately defend cyber systems and infrastructures and to attack them, the possibility of developing a 'white hat' strategy between the Commission, Council and Member States should be considered;, notes that the potential for 'brain drain' in these cases is high and that, notably, minors convicted of such attacks have a high potential for both rehabilitation and integration in defence agencies and bodies;

European Defence Agency (EDA)

22. Welcomes the recent initiatives and projects relating to cyber defence, especially on gathering and mapping relevant cyber security and defence data, challenges and needs and urges Member States to cooperate more, also at military level, with the EDA on cyber defence;

23. 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;

24. 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 and especially with the Cooperative Cyber Defence Centre of Excellence (CCDCOE) and to concentrate on capacity building and training as well as on exchange of information and practices;

25. 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

26. Calls on all Member States 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; 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;

27. Encourages all Member States to 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;

28. Encourages the Member States to introduce specialised courts at regional level geared to ensuring that attacks on information systems are punished more effectively; stresses the need to encourage the adaptation of national laws so that they can be adjusted to developments in techniques and uses;

29. 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;

30. 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 and, in particular, of providing suitable training for members of judicial and security institutions within the training bodies; calls on ENISA and other relevant bodies to assist Member States in ensuring the pooling and sharing of resources, as well as avoiding duplication;

31. Urges the Member States to make research and development one of the core pillars of cyber security and defence and to encourage the training of engineers specialised in protecting information systems; 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;

32. Calls on the Commission and Member States to come forward with programmes to promote and raise awareness among both private and business users in general safe use of the Internet, information systems and communication technologies; suggests the Commission launch a public pan-European education initiative in this regard, calls on the Member States to include education on cyber security in school curricula from the earliest possible age;

Public-Private Cooperation

33. 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;

34. Calls on private sector partners to consider ‘security-by-design’ solutions when designing new products, devices, services and applications, and incentives for those designing new products, devices, services and applications with security-by-design as a central feature; calls for minimum transparency standards and accountability mechanisms to be established with regard to cooperation with the private sector to prevent and combat cyber attacks;

35. Highlights that the protection of critical information infrastructure is included in the EU Internal Security Strategy in the context of raising levels of security for citizens as well as

businesses in cyberspace;

36. Calls for the establishment of a permanent dialogue 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;

37. 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 and systems of certifications for companies as well as providing the right incentives to stimulate private sector efforts to improve security;

38. 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;

39. 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;

40. 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

41. Calls on the EEAS to take a proactive approach to 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;

42. 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;

43. 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;

44. 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 all fora, and especially at the United Nations, with efforts to achieve broader international cooperation and final agreement on defining a common understanding of norms of behaviour in cyber space and also to encourage cooperation with a view to developing

cyber weapons control agreements;

45. Encourages exchanges of knowledge in the field of cyber security with BRICS countries and other countries with emerging economies, with the aim of exploring possible common responses to growing cyber crime and cyber threats and attacks; at both civilian and military levels;

46. 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;

47. Calls on the Council and the Commission, as part of their dialogues, relations and cooperation agreements with third countries, particularly those providing for cooperation or exchange in the field of technology, to insist on minimum requirements for preventing and fighting cyber criminality and cyber attacks; and on minimum standards in information system security;

48. 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

49. 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;

50. 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;

51. 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

52. 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;

53. 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;

54. 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;

55. Underlines the need for both the US and the EU, as the biggest sources of both cyber space and users, to work together for the protection of their citizen's rights and freedoms to use this space; underlines that while national security is a paramount objective, cyber space should be secured but also protected;

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

RESULT OF FINAL VOTE IN COMMITTEE

Date adopted	10.10.2012
Result of final vote	+: 47 –: 3 0: 6
Members present for the final vote	Bastiaan Belder, Franziska Katharina Brantner, Elmar Brok, Jerzy Buzek, Tarja Cronberg, Arnaud Danjean, Mário David, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Liisa Jaakonsaari, Anneli Jäätteenmäki, Jelko Kacin, Ioannis Kasoulides, Tunne Kelam, Nicole Kiil-Nielsen, Evgeni Kirilov, Maria Eleni Koppa, Wolfgang Kreissl-Dörfler, Eduard Kukan, Vytautas Landsbergis, Krzysztof Lisek, Sabine Lösing, Mario Mauro, Francisco José Millán Mon, Alexander Mirsky, María Muñiz De Urquiza, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Justas Vincas Paleckis, Bernd Posselt, Cristian Dan Preda, Fiorello Provera, José Ignacio Salafranca Sánchez-Neyra, Jacek Saryusz-Wolski, Werner Schulz, Sophocles Sophocleous, Laurence J.A.J. Stassen, Kristian Vigenin, Sir Graham Watson, Karim Zéribi
Substitute(s) present for the final vote	Charalampos Angourakis, Elena Băsescu, Jean-Jacob Bicep, Véronique De Keyser, Diogo Feio, Elisabeth Jeggle, Indrek Tarand, Sampo Terho, László Tőkés, Traian Ungureanu, Luis Yáñez-Barnuevo García
Substitute(s) under Rule 187(2) present for the final vote	Joseph Cuschieri