Thursday 12 September 2013

4. Requests the Commission to support Member States in reducing the gender pay gap by at least five percentage points annually with the aim of eliminating the gender pay gap by 2020;

5. Recognises that a multi-level, multifaceted approach calls for the Commission to support Member States in promoting good practices and implementing policies to address the gender pay gap;

6. Urges the Commission to revise Directive 2006/54/EC without delay and to propose amendments to it in accordance with Article 32 of the Directive and on the basis of Article 157 TFEU, following the detailed recommendations set out in the annex to the Parliament's resolution of 24 May 2012;

7. Instructs its President to forward this resolution to the Council, the Commission and the governments of the Member States.

P7_TA(2013)0376

EU cybersecurity strategy: an open, safe and secure cyberspace

European Parliament resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP))

(2016/C 093/16)

The European Parliament,

— having regard to the Joint Communication of 7 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)0001),

— having regard to the Commission proposal of 7 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 the 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 Commission Communication of 27 September 2012 entitled 'Unleashing the Potential of Cloud Computing in Europe' (COM(2012)0529),

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

— having regard to Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA ([1]),

— 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]),

---

([1]) OJ L 218, 14.8.2013, p. 8.
([2]) OJ L 345, 23.12.2008, p. 75.

— having regard to Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA ([1]),

— having regard to the Stockholm Programme ([2]) in the area of freedom, security and justice, the Commission communications entitled 'Delivering an area of freedom, security and justice for Europe's citizens — Action Plan Implementing the Stockholm Programme' (COM(2010)0171) and 'The EU Internal Security Strategy in Action: Five steps towards a more secure Europe' (COM(2010)0673), and its resolution of 22 May 2012 on the European Union's Internal Security Strategy ([3]),

— having regard to the Joint Proposal of the Commission and the High Representative for a Council Decision on the arrangements for the implementation by the Union of the Solidarity Clause (JOIN(2012)0039),

— having regard to Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment ([4]),

— having regard to its resolution of 12 June 2012 on critical information infrastructure protection — achievements and next steps: towards global cyber-security ([5]) and to the Council conclusions of 27 May 2011 on the Commission communication entitled 'Critical Information Infrastructure Protection — Achievements and next steps: towards global cyber-security' (COM(2011)0163),

— having regard to its resolution of 11 December 2012 on completing the digital single market ([6]),

— having regard to its resolution of 22 November 2012 on cyber security and defence ([7]),

— having regard to its position of 16 April 2013 at first reading 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)0521) ([8]),

— having regard to its resolution of 11 December 2012 on a digital freedom strategy in EU foreign policy ([9]),

— having regard to the Council of Europe Convention on Cybercrime of 23 November 2001,

— having regard to the Union's international obligations, notably under the General Agreement on Trade in Services (GATS),

— having regard to Article 16 of the Treaty on the Functioning of the European Union (TFEU) and to the Charter of Fundamental Rights of the European Union, in particular Articles 6, 8 and 11 thereof,

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

— having regard to Rule 110(2) of its Rules of Procedure,

A. whereas growing cyber-challenges, in the form of increasingly sophisticated threats and attacks, constitute a major threat to the 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 will therefore be a constantly evolving challenge;

([1]) OJ L 335, 17.12.2011, p. 1.
([2]) OJ C 115, 4.5.2010, p. 1.
([3]) Texts adopted, P7_TA(2012)0207.
([4]) OJ L 149, 2.6.2001, p. 1.
([5]) Texts adopted, P7_TA(2012)0237.
([6]) Texts adopted, P7_TA(2012)0468.
([7]) Texts adopted, P7_TA(2012)0457.
([8]) Texts adopted, P7_TA(2013)0103.
([9]) Texts adopted, P7_TA(2012)0470.

Thursday 12 September 2013

B. whereas cyberspace and cyber-safety should be one of the strategic pillars of the security and defence policies of the EU and of each Member State; whereas it is crucial to ensure that cyberspace remains open to the free flow of ideas and information and to free expression;

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

D. whereas the strategic priorities outlined in the Joint Communication on a cyber-security strategy for the European Union include achieving cyber-resilience, reducing cybercrime, developing a cyber-defence policy and cyber-capabilities related to the Common Security and Defence Policy (CSDP), and establishing a coherent international cyberspace policy for the EU;

E. 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;

F. whereas cyber-security across the Union, as in the rest of the world, is only as strong as its weakest link, and disruptions in one sector or Member State have an impact on another sector or Member State, creating spill-over effects with implications for the Union economy as a whole;

G. whereas, as of April 2013, only 13 Members States have officially adopted national cyber-security strategies; whereas fundamental differences remain between the Member States in terms of their preparedness, security, strategic culture and capacity to develop and implement national cyber-security strategies, and whereas an assessment should be made of these differences;

H. whereas different security cultures and the lack of a legal framework lead to fragmentation, and are of primary concern, in the digital single market; whereas the lack of a harmonised approach to cyber-security entails serious risks to economic prosperity and to the security of transactions, and whereas concerted efforts and closer cooperation are therefore required between governments, the private sector, and law enforcement and intelligence agencies;

I. whereas cybercrime is an increasingly expensive international problem, currently costing — according to the United Nations Office on Drugs and Crime — the global economy almost EUR 295 billion each year;

J. whereas international organised crime, taking advantage of technological advances, is continuing to shift its operational terrain into cyberspace, where cybercrime is radically altering the traditional structure of organised crime groups; whereas this has led to organised crime being less localised and more likely to exploit territoriality and differing national legal jurisdictions on a global level;

K. whereas the investigation of cybercrime by competent authorities is still hindered by several obstacles, among them the use, in cyberspace transactions, of 'virtual currencies' that can be used for money laundering, the issues of territoriality and jurisdictional boundaries, insufficient intelligence-sharing capabilities, a lack of trained staff, and inconsistent cooperation with other stakeholders;

L. whereas technology is the foundation for the development of cyberspace, and continuous adaptation to technological changes is essential if the resilience and safety of EU cyberspace is to be improved; whereas measures must be taken to ensure that legislation keeps up to date with new technological developments, enabling the effective identification and prosecution of cyber-criminals and the protection of victims of cybercrime; whereas the Cybersecurity Strategy of the

EU must include measures focused on awareness, education, the development of Computer Emergency and Response Teams (CERTs), the development of an internal market for cyber-security products and services, and the promotion of investment in research, development and innovation;

1. Welcomes the Joint Communication for a cyber-security 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 cyberspace, has for political, economic, and societal transactions, not only within the Union but also in in relation to other actors around the world;

3. Stresses that it is necessary to develop a strategic communication policy on EU cyber-security, cyber-crisis situations, strategy reviews, public-private collaboration and alerts, and recommendations to the public;

4. Recalls that a high level of network and information security is required not only in order to maintain services that are essential to the smooth functioning of society and the economy, but also to safeguard the physical integrity of citizens by enhancing the efficiency, effectiveness and secure functioning of critical infrastructures; stresses that, while the security of networks and information must be addressed, improving physical security is also an important issue; emphasises that infrastructure should be resilient to both intentional and unintentional disruptions; stresses that, in this respect, the cyber-security strategy should put greater emphasis on the common causes of unintentional system failures;

5. Reiterates its call on the Member States to adopt national cyber-security strategies that cover technical, coordination, human resources and financial allocation aspects, and that include distinct rules on the benefits for and responsibilities of the private sector, in order to guarantee their participation, without undue delay, and to provide for comprehensive risk management procedures as well as to safeguard the regulatory environment;

6. Notes that only combined leadership and political ownership on the part of the Union institutions and the Member States will permit a high level of network and information security across the Union, and thus contribute to the secure and smooth functioning of the single market;

7. Stresses that the Union's cyber-security policy should provide a secure and reliable digital environment based on, and designed to guarantee, the protection and preservation of freedoms and respect for fundamental rights online, as laid down in the EU Charter and Article 16 TFEU, in particular the rights to privacy and data protection; believes that specific attention should be paid to the protection of children online;

8. Calls on the Member States and the Commission to take all the action needed to come forward with training programmes aimed at promoting and improving awareness, skills and education among European citizens, in particular with regard to personal security, as a part of a digital literacy curriculum from an early age; welcomes the initiative to organise a European Cyber Security Month, with the support of ENISA and in cooperation with public authorities and the private sector, in order to raise awareness of the challenges involved in protecting network and information systems;

9. Considers that education on cyber-security increases European society's awareness of cyber-threats, thereby encouraging responsible use of cyberspace, and helps boost the supply pool of cyber-skills; recognises the key role of Europol and its new European Cybercrime Centre (EC3), and of ENISA and Eurojust, in providing training activities at EU level in the use of international judicial cooperation tools and law enforcement relating to different aspects of cybercrime;

10. Reiterates the need to provide technical advice and legal information, as well as to establish programmes on the prevention and combating of cybercrime; encourages the training of cyber-engineers specialised in protecting critical infrastructure and information systems, as well as of operators of transport control systems and traffic management centres; underlines the dire need to introduce regular cyber-security training schemes for public sector staff at all levels;

Thursday 12 September 2013

11. Reiterates its call for caution in applying restrictions on the ability of citizens to make use of communication and information technology tools, and stresses that the Member States should aim never to endanger citizens' rights and freedoms when developing responses to cyber threats and attacks, and should have adequate legislative means to distinguish between civilian- and military-level cyber-incidents;

12. Considers that regulatory involvement in the cyber-security field should be risk-oriented, focused on critical infrastructure the proper functioning of which is of major public interest, and should build on the existing, market-based efforts of the industry to ensure network resilience; underlines the crucial role of cooperation at the operational level in fostering a more efficient exchange of cyber-threat information between public authorities and the private sector — at both Union and national level, as well as with strategic partners of the Union — with the aim of ensuring the security of networks and information, by generating mutual trust, value and commitment, and exchanging expertise; considers that public-private partnerships should be based on network and technological neutrality, and should focus on efforts to address problems that have high public impact; calls on the Commission to encourage all the market operators involved to be more vigilant, and more cooperative, in order to protect other operators from damage to their services;

13. Recognises that the detection and notification of cyber-security incidents is vital in promoting cyber-resilience in the Union; believes that proportionate and necessary disclosure requirements should be in place to allow for the notification of incidents involving significant security breaches to the competent national authorities and thereby enable improved monitoring of cybercrime incidents and facilitate efforts to raise awareness at all levels;

14. Encourages the Commission and other actors to introduce cyber-security and cyber-resilience policies that include economic incentives to promote high levels of cyber-security and cyber-resilience;

Cyber-resilience

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

16. Considers that requirements for small and medium-sized enterprises should follow a proportionate and risk-based approach;

17. 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; calls on the Commission and the High Representative to take this risk into account in their joint integrated threat and risk assessment reports to be issued as from 2015;

18. Stresses that in order to guarantee the integrity, availability and confidentiality of critical services in particular, the identification and categorisation of critical infrastructure must be up to date, and the necessary minimum security requirements for their network and information systems must be set;

19. 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;

20. Calls on the Member States and the Union to set in place adequate frameworks for rapid, two-way information exchange systems that will ensure anonymity for the private sector and keep the public sector constantly updated, and, where necessary, to provide assistance to the private sector;

21. Welcomes the Commission's notion to create a risk-management culture with regard to cyber-security, and urges the Member States and Union institutions rapidly to include cyber-crisis management in their crisis management plans and risk analyses; calls, furthermore, on Member State governments and on the Commission to encourage private sector actors to include cyber-crisis management in their management plans and risk analyses, and to train their staff in cyber-security;

22. Calls on all Member States and on the Union institutions to establish a network of well-functioning Computer Emergency and Response Teams (CERTs) operational on a 24/7 basis; points out that national CERTs should be part of an effective network in which relevant information is exchanged in keeping with requisite standards of trust and confidentiality; notes that umbrella initiatives bringing together CERTs and other relevant security bodies can serve as useful tools in the development of trust in a cross-border and cross-sector context; recognises the importance of efficient and effective cooperation between CERTs and law enforcement agencies in the fight against cybercrime;

23. Supports ENISA in exercising its duties with regard to network and information security, in particular by providing guidance and by advising Member States, as well as by supporting the exchange of best practices and the development of an environment of trust;

24. Stresses the need for the industry to implement appropriate cyber-security performance requirements across the whole value chain for ICT products used in transport networks and information systems, to carry out appropriate risk management, to adopt security standards and solutions, and to develop best practices and information-sharing with a view to ensuring cyber-secure transportation systems;

Industrial and technological resources

25. Is of the opinion that ensuring a high level of network and information security plays a central role in raising the competitiveness of both suppliers and users of security solutions in the Union; considers that while the IT security industry in the Union has important untapped potential, private, public and business users are often uninformed about the costs and benefits of investing in cyber-security and, thus, remain vulnerable to harmful cyber-threats; stresses that the implementation of CERTs is a relevant factor in this regard;

26. Believes that a strong supply of, and demand for, cyber-security solutions requires adequate investment in academic resources, research and development (R&D), and knowledge- and capacity-building on the part of the national authorities involved in ICT matters, in order to foster innovations and create sufficient awareness about network and information security risks, leading towards a concerted European security industry;

27. Calls on the Union institutions and the 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;

28. Encourages the Member States 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

29. Considers that criminal activities in cyberspace can be as harmful to the well-being of societies as offences in the physical world, and that these forms of crime often reinforce one other, as can be observed, for example, in the sexual exploitation of children and in organised crime and money laundering;

30. Notes that there is in some cases a link between legitimate and illicit business activities; stresses the importance of the link, facilitated by the internet, between the funding of terrorism and serious organised crime; stresses that the public must be made aware of the seriousness of becoming involved in cybercrime, and of the possibility that what at first sight may seem to be a 'socially acceptable' crime — such as the illegal downloading of films — often generates large sums of money for international crime syndicates;

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

32. 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;

33. Strongly welcomes the establishment of the EC3, and encourages the future development of this agency and of its vital role in coordinating timely and efficient cross-border exchange of information and expertise in support of efforts to prevent, detect and investigate cybercrime;

34. Calls on the Member States to ensure that citizens can easily access information on cyber-threats and how to fight them; believes that such guidance should include information on how users can protect their privacy on the internet, how to detect and report cases of grooming, how to install software and firewalls, how to manage passwords and how to detect false identification (phishing), luring (pharming) and other attacks;

35. Insists that the Member States that have not yet ratified the Council of Europe's Budapest Convention on Cybercrime should do so without undue delay; welcomes the reflections of the Council of Europe on the need to update the Convention in light of technological developments to ensure its continuing efficacy in addressing cybercrime, and calls on the Commission and the Member States to participate in this debate; encourages efforts to promote the ratification of the Convention among other countries, and calls on the Commission to promote it in an active manner outside the Union;

Cyber-defence

36. Stresses that cyber-challenges, -threats and -attacks put Member States' defence and national security interests at risk, and that civilian and military approaches to the task of protecting critical infrastructure should maximise the benefit to both through efforts to achieve synergies;

37. Calls, therefore, on the Member States to intensify their cooperation with the European Defence Agency (EDA) with a view to developing proposals and initiatives for cyber-defence capabilities, building on recent initiatives and projects; underlines the need to increase R&D, including by pooling and sharing resources;

38. Reiterates that a comprehensive EU cyber-security strategy should take into account the added value of existing agencies and bodies, as well as the good practices gleaned from those Member States that have already introduced national cyber-security strategies of their own;

39. 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; calls on them to pool together a European cyber-defence force;

40. Underlines the good practical cooperation with NATO in the field of cyber-security, and the need to step up this cooperation, in particular through closer coordination in the areas of planning, technology, training and equipment;

41. Calls for efforts on the part of the Union to enter into an exchange with international partners, including NATO, identify areas of cooperation, avoid duplication and complement activities, wherever possible;

International policy

42. Believes that international cooperation and dialogue play an essential role in creating trust and transparency, and in promoting a high level of networking and information exchange at global level; calls, therefore, on the Commission and the European External Action Service to set up a cyber-diplomacy team, whose responsibilities would include the promotion of dialogue with like-minded countries and organisations; calls for more active participation on the part of the EU in the wide range of international high-level conferences on cyber-security;

43. Considers that a balance needs to be struck between the competing goals of cross-border transfers of data, data protection and cyber-security, in line with the Union's international obligations, notably under the GATS;

44. Calls on the VP/HR to mainstream the cyber-security dimension into the EU's external actions, especially in relation to third countries, in order to intensify cooperation, and the exchange of experiences and information, on how to deal with cyber-security;

45. Calls for efforts by the Union to enter into an exchange with international partners with a view to identifying areas of cooperation, avoiding duplication and complementing activities, where possible; calls on the VP/HR and the Commission to be proactive in international organisations and to coordinate the positions of the Member States on how to promote solutions and policies in the cyber-field in an effective way;

46. Is of the opinion that efforts should be made to ensure that existing international legal instruments, in particular the Council of Europe's Convention on Cybercrime, are enforced in cyber-space; considers, therefore, that there is no need at present for the creation of new legal instruments at international level; welcomes, however, international cooperation to develop norms of behaviour for cyberspace, supporting the rule of law in cyberspace; considers that the updating of existing legal instruments to reflect advancements in technology should be considered; holds the view that jurisdictional issues require a thorough discussion on the subject of judicial cooperation and prosecution in transnational criminal cases;

47. Considers that, in particular, the EU-US Working Group on Cybersecurity and Cybercrime should serve as an instrument for the EU and the US to exchange, wherever appropriate, best practices on cyber-security policies; notes, in this context, that areas linked to cyber-security, such as services depending on the secure functioning of network and information systems, will be included in the upcoming negotiations of the Transatlantic Trade and Investment Partnership (TTIP), to be concluded in a manner that safeguards the EU's sovereignty and the independence of its institutions;

48. Notes that cyber-security skills, and the capacity to prevent, detect, and effectively counter threats and malicious attacks, are not evenly developed around the globe; emphasises that efforts to increase cyber-resilience and fight cyber-threats must not be confined to like-minded partners, but should also address regions with less developed capacities, technical infrastructure and legal frameworks; believes that coordination of CERTs is crucial in this matter; calls on the Commission to facilitate — and, if necessary, assist in — efforts on the part of third countries to build cyber-security capabilities of their own, using appropriate means;

Implementation

49. Calls for regular evaluations of the effectiveness of national cyber-security strategies at the highest political level, with a view to ensuring the adaptation to new global threats and to guaranteeing the same level of cyber-security in different Member States;

50. Asks 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 for the assessments thereof; invites the Member States to agree on a similar delivery plan for national activities under this strategy;

Thursday 12 September 2013

51. Asks for regular reports — from the Commission, the Member States, Europol and the newly established EC3, Eurojust and ENISA — assessing the progress made on the objectives set out in the cyber-security strategy, including key performance indicators measuring the progress of implementation;

o

o o

52. Instructs its President to forward this resolution to the Council, the Commission, the governments and parliaments of the Member States, Europol, Eurojust and the Council of Europe.

P7_TA(2013)0377

Digital agenda for growth, mobility and employment

European Parliament resolution of 12 September 2013 on the Digital Agenda for Growth, Mobility and Employment: time to move up a gear (2013/2593(RSP))

(2016/C 093/17)

The European Parliament,

— having regard to the Commission Communication of 18 December 2012 entitled 'The Digital Agenda for Europe — Driving European growth digitally' (COM(2012)0784),

— having regard to the questions to the Commission and to the Council on 'the Digital Agenda for Growth, Mobility and Employment: time to move up a gear' (O-000085 — B7-0219/2013 and O-000086 — B7-0220/2013),

— having regard to Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union ([1]),

— having regard to Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multiannual radio spectrum policy programme ([2]),

— having regard to the ongoing negotiations on the Connecting Europe Facility and in particular to the amended proposal for a regulation of the European Parliament and of the Council on guidelines for trans-European telecommunications networks and repealing Decision No 1336/97/EC (COM(2013)0329),

— having regard to its resolution of 5 May 2010 on 'a new Digital Agenda for Europe: 2015.eu' ([3]),

— having regard to the Commission Communication of 27 September 2012 entitled 'Unleashing the potential of cloud computing in Europe' (COM(2012)0529),

— having regard to the proposal of 25 January 2012 for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011),

---

([1]) OJ L 172, 30.6.2012, p. 10.
([2]) OJ L 81, 21.3.2012, p. 7.
([3]) OJ C 81 E, 15.3.2011, p. 45.