Council of the European Union

Brussels, 7 November 2017
(OR. en)

13943/17

CYBER 168
TELECOM 263
ENFOPOL 506
JAI 996
MI 771
COSI 258
JAIEX 90
RELEX 933
IND 285
CSDP/PSDC 597
COPS 333
POLMIL 124

'I/A' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
No. prev. doc.:	12762/5/16 REV 5
No. Cion doc.:	12211/17, 12210/17
Subject:	Draft Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - adoption

1. At the meeting of the Horizontal Working Party on Cyber Issues ("HWP Cyber") of 26 September 2017 the Commission presented its cybersecurity package, comprising inter alia a Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[1]. It addresses the EU ability to protect against cyber threats by envisaging measures aimed at building greater resilience, deterrence and defence to boost EU's cybersecurity as well as at providing incentives and support to Member States to further develop and maintain their more and better cybersecurity capacity.

[1] doc. 12211/17.

2. The discussions that followed the Commission's presentation clearly indicated the importance of thinking strategically ahead on the issues outlined in that Joint Communication, the need of a political commitment to achieve the goals and endorsement of the initiatives stipulated therein.

3. At the HWP Cyber meeting of 6 October 2017 the Presidency presented the first draft of the Council Conclusions[2] which built upon the initial Member States' comments and input. The discussion allowed to structure and focus the messages while taking due account of all the ongoing processes, including the one on NIS Directive transposition in the national laws.

4. Three additional rounds of discussions took place at the HWP Cyber meeting of 13 and 30 October as well as 6 November, which together with the written contributions provided by delegations allowed to complete the negotiations at the working party level and to prepare the final compromise text[3].

5. On this basis, COREPER is requested to invite the Council to approve the draft Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, as set out in the Annex.

---

[2] doc. 12762/17.
[3] doc. 12762/5/17 REV5.

ANNEX

Draft Council conclusions on the Joint Communication to the EP and the Council: Resilience, Deterrence and defence: Building strong cybersecurity for the EU

The Council of the European Union,

1. RECOGNISING the importance of cybersecurity for the prosperity, growth and security of the EU and integrity of our free and democratic societies and their underpinning processes in the digital age, both by protecting rule of law and human rights and fundamental freedoms of every individual;

2. UNDERLINING the need to address cybersecurity with a coherent approach at national, EU and global level, as cyber threats can have an impact on our democracy, prosperity, stability and security;

3. NOTES that a high level of cyber resilience across the EU is also important for achieving trust in the Digital Single Market and further development of a digital Europe ;

4. REITERATING that the EU will continuously promote an open, global, free, peaceful and secure cyberspace, where human rights and fundamental freedoms, in particular the right to freedom of expression, access to information, data protection, privacy and security, as well as the core EU values and principles, are both within the EU and globally, fully applied and respected and EMPHASISING the crucial importance of ensuring an appropriate balance between the human rights and fundamental freedoms and meeting the requirements of the EU's internal security policy[4],

5. RECOGNISING that international law, including the UN Charter in its entirety, international humanitarian law and human rights law apply in cyberspace and thereby UNDERLINING the need to continue the efforts to ensure that international law is upheld in cyberspace;

[4] 12650/17.

6. RECALLING its Conclusions on the EU Cyber security Strategy[5], on Internet governance[6] Strengthening EU Cyber Resilience[7], on Cyber Diplomacy[8] and on a Framework for Joint EU Diplomatic Response to Malicious Cyber Activities[9], on improving criminal justice in cyberspace[10]; on Security and Defence in the context of the EU Global Strategy[11], the Joint Framework on countering hybrid threats[12], and on the mid-term review of the renewed European Union Internal Security Strategy 2015-2020[13];

7. RECOGNISING that the framework provided by the Council of Europe Convention on Cybercrime (the Budapest Convention), provides a solid basis among a diverse group of countries to use an effective legal standard for the different national legislation and for international cooperation addressing cybercrime;

8. RECOGNISING the need for a renewed emphasis on the implementation of the 2014 EU Cyber Defence Policy Framework and to update it to further integrate cyber security and defence into Common Security and Defence Policy (CSDP) and to the wider security and defence agenda;

9. RECOGNISING that a globally competitive European industry is an important element to achieve a high level of cybersecurity nationally and across EU;

10. RECALLING that according to article 4.2 of the TEU, national security is the sole responsibility of each Member State.

---

5 12109/13 and doc. 6225/13 (Joint Communication to European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (COM JOIN (2013) 1 final).

6 16200/14 and doc. 6460/14 (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Internet Policy and Governance Europe's role in shaping the future of Internet Governance (COM(2014) 72 final)

7 14540/16 and doc. 11013/16 (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (COM 2016(410) final).

8 6122/15.

9 9916/17.

10 10007/16.

11 9178/17.

12 7688/16 (Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats: A European Union Response).

13 12650/17.

HEREBY

11. WELCOMES the Joint Communication to the European Parliament and the Council, entitled: Resilience, Deterrence and defence: Building strong cybersecurity for the EU for putting forward an ambitious goal of enhancing cybersecurity within the EU. It also contributes to the EU's strategic autonomy as referred to in its Conclusions on the Global Strategy on the European Union's Foreign and Security Policy[14] by aiming to build a digital Europe that will be more secure, trust-enabling, conscious of its strengths, competitive, open to the world, respectful of EU's shared values on open, free, peaceful and secure global internet – and therefore reaching a higher level of resilience to prevent, deter, detect and respond to cyber threats and be able to respond jointly to cyber threats across the EU, and

12. INVITES the Member States, the EU institutions, agencies and bodies to work together, respecting each other's' areas of competence and the principle of subsidiarity and proportionality, in response to the strategic objectives set out in these Conclusions, and

13. UNDERLINES the need for the EU, its Member States and the private sector to ensure sufficient financing respecting the available resources to support building cyber resilience and cybersecurity research and development efforts across the EU, as well as to strengthen cooperation to prevent, deter, detect and respond to cyber threats and to be able to respond jointly to large-scale cyber incidents and malicious cyber activities across the EU;

---

14 13202/16.

Chapter I

ENSURING AN EFFECTIVE EU CYBER RESILIENCE AND TRUST IN DIGITAL SINGLE MARKET

14. UNDERLINES that each Member State bears the primary responsibility for enhancing its own cybersecurity and ensuring its response to cyber incidents and crises while the EU can provide a strong added value in supporting the cooperation between the Member States. In this context, STRESSES the need for all Member States to make the necessary resources available for national authorities responsible for cybersecurity in order to ensure prevention, detection and response to cyber incidents and crises across EU;

15. UNDERLINES the need, where possible, to make use of existing mechanisms, structures and organisations at the EU level;

16. COMMENDS:

- the progress achieved in the transposition of the NIS Directive by the Member States and STRESSES the need for achieving a full and effective implementation by May 2018 as stipulated in that Directive[15];
- the work done within the NIS Cooperation Group in enhancing the strategic cooperation and exchange of information between the Member States;
- the work done within the CSIRTs Network, especially in strengthening the operational cooperation of Member States, building trust and confidence in sharing information in handling large-scale cybersecurity incidents and, based on national conclusions from Member States, in providing elements for a European-level shared situational awareness;
- the work done within the contractual Public-Private Partnership on cybersecurity (cPPP).

[15] Without prejudice to the competence of the Member States for the transposition of the NIS Directive, especially with respect to the operators of essential services.

17. WELCOMES the confirmation in the Joint Communication that strong and trusted encryption is highly important for properly ensuring human rights and fundamental freedoms in EU and for public trust in the Digital Single Market, while taking into account the need of law enforcement authorities to access data necessary for their investigations and the confirmation that secure digital identification and communication both play a key role in ensuring effective cybersecurity in EU;

18. WELCOMES the plan within the Joint Communication to increase the ambition in conducting the pan-European cybersecurity exercises on a regular basis, building upon experiences from the Cyber Europe exercises, combining response across different levels, as this will be an important element in advancing preparedness of Member States and EU institutions in responding to large-scale cyber incidents;

19. CALLS upon EU and its Member States to conduct regular strategic cybersecurity exercises in different Council formations, building upon the experience gained during the EU CYBRID 2017 and

20. Without prejudice to the outcome of the legislative process:

- WELCOMES the proposal for a strong and permanent mandate for ENISA with a primary objective to support and develop closer cooperation between Member States, to increase their capacities and to increase confidence in a digital Europe;

- REAFFIRMS that the future ENISA should rely on the experience and expertise within the Member States and EU and to support the consistent development and implementation of existing and upcoming EU cybersecurity policies and regulations, while ensuring that all competences of ENISA should be developed to complement those of the Member States;

- REAFFIRMS the goal of growing the confidence in a digital Europe by increasing trust and confidence in digital solutions and innovations, including the Internet of Things, e-commerce and e-governance, especially in terms of a world-class European cybersecurity certification framework [16]. This is a key requirement for enhancing trust and security in digital products and services, protecting critical infrastructures, governmental, citizens' and business data and instrumental for adopting a security-by-design approach for products, services and processes in the Digital Single Market;

- STRESSES that legislative work to strengthen cybersecurity certification on the EU level will have to meet the needs of the market and the users, build upon experiences of certification capacities and processes existing in the EU (for example the SOG-IS framework) and would have to provide a framework able to swiftly adapt to the state-of-the-art of future digital developments;

- STRESSES that in enhancing cybersecurity certification in the EU, the whole spectrum of security requirements should be covered, up to the highest ones, where resistance against attackers' capabilities has to be demonstrated. Key success factors would be ensuring a reliable, transparent and independent process for security certification to promote the availability of trusted and secure devices, software and services within the Single Market and beyond; recognising European industry, governments and evaluation specialists' respective expertise through European and global standards [17]; respecting Member States' role in the certification process in particular as regards to evaluation at higher security levels and especially in relation to essential security needs and skills assessment. Such certification framework should also ensure that any EU-wide certification scheme is proportionate to the level of assurance needed for the use of ICT products, services and/or systems involved, and it enables cross-border trading for businesses of all scales to develop and sell new products, both within the EU and outside the EU markets.

---

16 Through global standards developed in accordance with the spirit of WTO – TBT Code of Good Practice.

17 Through European and global standards developed in accordance with the spirit of WTO – TBT Code of Good Practice.

21. WELCOMES the intention to set up a Network of Cybersecurity Competence Centres to stimulate the development and deployment of cybersecurity technologies and to offer an additional impetus to innovation for the EU industry on the global scene in the development of next-generation and breakthrough technologies, such as artificial intelligence, quantum computing, blockchain and secure digital identities;

22. STRESSES the need for the Network of Cybersecurity Competence Centres to be inclusive towards all Member States and their existing centres of excellence and competence and pay special attention to complementarity and with this in mind;

23. NOTES the planned European Cybersecurity and Research Centre, which should, as its key role, focus on ensuring complementarity and avoiding duplication within the Network of Cybersecurity Competence Centres and with other EU agencies; STRESSES that the Network of Cybersecurity Competence Centres should address a spectrum of issues from research to industry and therefore should contribute inter alia to achieving the objective of European strategic autonomy;

24. With a view to the proposed Network of Cybersecurity Competence Centres, REAFFIRMS the need for the EU, through its Member States, to develop a European capacity for evaluating the strength of cryptography used in products and services available for citizens, businesses and governments within the Digital Single Market while recognizing that policies for cryptography are a key aspect of national security and thus lay within the competence of Member States;

25. INVITES all the relevant stakeholders to increase the investments in cybersecurity applications of new technologies in order to contribute to ensuring cybersecurity across all sectors of the European economy;

26. STRESSES the importance of credible, trusted and coordinated provision of cybersecurity services for the EU Institutions and CALLS on the COMMISSION and other EU Institutions to further develop CERT-EU according to those aims and to ensure adequate resources for that as well;

27. WELCOMES the call to acknowledge the important role of third party security researchers in discovering vulnerabilities in existing products and services and CALLS upon Member States to share best practices for coordinated vulnerability disclosure;

28. STRESSES everyone's responsibility in cybersecurity and INVITES the EU and its Member States to promote digital skills and media literacy helping users to protect their digital information online and raise their awareness on the risks when placing personal data on the Internet;

29. WELCOMES the emphasis put within the Joint Communication on education, cyber hygiene and awareness in Member States and EU;

30. CALLS ON THE COMMISSION to provide rapidly an impact assessment on and propose by mid-2018 the relevant legal instruments for the implementation of the initiative establishing a Network of Cybersecurity Competence Centres and a European Cybersecurity Research and Competence Centre;

31. INVITES the Member States:

- to prioritise cyber-awareness in information campaigns and stimulate cybersecurity as part of academic, education and vocational training programmes. Particular focus should be put on youth education and digital skills fostering, to create future-proof professionals ready for the challenges in security, economy and services;

- to advance efforts in opening specialised high-level cybersecurity programmes in order to fill the current gap in cybersecurity professionals in EU;

- to create an effective cooperation network of education points of contact (POCs) under the umbrella of ENISA. The PoCs network should aim to enhance coordination and exchange of best practices among Member States on cybersecurity education and awareness, as well as training, exercise and capacity building;

- to consider applying the rules of the NIS Directive also to public administrations that participate in critical societal or economic activities, if not already covered by national legislation and if deemed appropriate, and to provide cybersecurity-related training also in public administrations given the role they play in our society and economy.

Chapter II

BUILDING EU CAPACITY TO PREVENT, DETER, DETECT AND RESPOND TO MALICIOUS CYBER ACTIVITIES

32. STRESSES that a particularly serious cyber incident or crisis could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause[18] and/or the Mutual Assistance Clause[19];

33. WELCOMES the adoption of the "Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities" which contributes to conflict prevention, cooperation and stability in cyberspace by setting out measures within the CFSP including restrictive measures, which can be used to prevent and respond to malicious cyber activities and CALLS upon the EEAS and Member States to regularly exercise on that Framework;

[18] Article 222 TEU
[19] Article 42.7 TEU

34. STRESSES the need for an efficient EU-level response to large-scale cyber incidents and crises, while respecting the competences of Member States, and the need for cybersecurity to be mainstreamed into existing crisis management mechanisms at the EU level[20]. In order to achieve that, CALLS for the EU level response to large-scale cyber incidents to be exercised regularly - from diplomatic-strategic to technical responses - based on and refining as necessary, the relevant frameworks and procedures[21];

35. STRESSES the importance of well integrated response and information exchange mechanisms between different communities which are critical for ensuring cybersecurity in Europe, including between relevant EU bodies and authorities of Member States. Such mechanisms will have to be tested and verified as part of EU level cybersecurity exercises and formalised by respective agreements if necessary;

36. NOTES the possibility to examine, should the Commission present a proposal for the establishment of a Cybersecurity Emergency Response Fund alongside the existing efforts of Member States and respecting the available resources (especially within the EU Multiannual Financial Framework) to help Member States to respond to and mitigate large scale cyber incidents, provided that the Member State had put in place a prudent system of cybersecurity prior to the incident, including full implementation of the NIS Directive and mature risk management and supervisory frameworks at the national level;

37. RECOGNISES the growing linkages between cybersecurity and defence and CALLS to step up cooperation on cyber defence, including by encouraging cooperation between civilian and military incident response communities and to continue strengthening the cyber security of CSDP missions and operations;

---

[20] C/2017/6100 final

[21] 9916/17 and C/2017/6100 final.

38. STRESSES the need to possibly take a full advantage of the proposed defence initiatives to accelerate the development of adequate cyber capabilities in Europe and RECOGNISES the opportunities in possibly developing cyber defence projects through PESCO, if deemed necessary by PESCO participating Member States and RECOGNISES the role played by the European Defence Technological and Industrial Base (EDTIB) and the wider civilian cyber security industry base in providing means for Member States to safeguard their cyber-related security and defence interests;

39. NOTES the proposal by the Commission to put in place a cyber defence training and education platform by the end of 2018 and STRESSES that the platform should upscale the training and education opportunities within the Member States and should ensure complementarity with other EU efforts and initiatives, notably with ESDC and EDA;

40. CALLS upon the EU and its Member States to be responsive to the threat of ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors;

41. RECOGNISES the need to address crimes in cyberspace, including those in the Darkweb, child sexual exploitation online as well as fraud and counterfeiting of non-cash means of payment, notably by aiming at creating an improved intelligence picture, conducting joint investigations and sharing operational support;

42. WELCOMES the work by EU and its Member States in addressing the challenges posed by systems that allow criminals and terrorists to communicate in ways that competent authorities cannot access, STRESSES that this work has to keep in mind that strong and trusted encryption is of high importance to cybersecurity and for the trust in the Digital Single Market and ensuring the respect of human rights and fundamental freedoms;

43. UNDERLINES the importance of providing the law enforcement with tools that enable to detect, investigate and prosecute cybercrime, so that crimes committed in the cyberspace would not go unnoticed or unpunished and WELCOMES the contribution of the European Judicial Cybercrime Network in the fight against crime through judicial authorities cooperation;

44. STRESSES the importance of ensuring a coordinated EU position to efficiently shape the European and global internet governance decisions within the multi-stakeholder community, such as ensuring swiftly accessible and accurate WHOIS databases of IP-addresses and domain names, so that law enforcement capabilities and public interests are safeguarded;

45. STRESSES the importance of uptaking the IPv6 Internet protocol which is vital for the development of Internet of Things at scale as well as for improving attribution of crimes in cyberspace;

46. ENCOURAGES the ongoing work on cross-border access to electronic evidence, addressing data retention and on the challenges for criminal proceedings posed by systems that allow criminals and terrorists to communicate in ways that competent authorities cannot access bearing in mind the need to respect human rights and fundamental freedoms and data protection ;

47. CALLS on the Commission:

- to present by December 2017 a progress report on the implementation of the practical measures for improving the cross-border access to electronic evidence;
- to present in early 2018 a legislative proposal to improve the cross-border access to electronic evidence;

48. INVITES Europol, ENISA and Eurojust:

- to continue strengthening their cooperation in the fight against cybercrime, both among themselves and with other relevant stakeholders, including the CSIRTs community, Interpol, the private sector and academia ensuring synergies and complementarities, in accordance with their respective mandates and competences.

- to contribute jointly with Member States a coordinated approach for EU law enforcement response to large-scale cyber-incidents and crises to complement the procedures outlined in the relevant frameworks[22];

49. INVITES the EU and its Member States to continue working:

- to remove obstacles to investigation of crime and to effective criminal justice in cyberspace as well as to enhance international cooperation and coordination in the fight against crime in cyberspace;

- to address the challenges posed by anonymising technologies while keeping in mind that strong and trusted encryption is of high importance to cybersecurity and for the trust in the Digital Single Market;

- to shape internet governance decisions, which impact law enforcement capability to fight crime in cyberspace

[22] 9916/17 and C/2017/6100 final.

Chapter III

STRENGTHENING INTERNATIONAL COOPERATION FOR AN OPEN, FREE, PEACEFUL AND SECURE GLOBAL CYBERSPACE

50. RECOGNISES that ensuring cybersecurity is a global challenge, which requires effective global cooperation between all actors, and RECOGNISES that a special emphasis has to be given to uphold democratic values and the principles of open, free, peaceful and secure global cyberspace and with that in mind,

51. CALLS UPON the EU and its Member States to promote the establishment of a strategic framework for conflict prevention, cooperation and stability in cyberspace that is based on the application of existing international law, and in particular of the UN Charter in its entirety, the development and implementation of universal norms of responsible state behaviour, and regional confidence building measures between States;

52. RECOGNISES the role of the United Nations in further developing norms for responsible state behaviour in cyberspace and recalls that the outcomes of the United Nations Group of Governmental Experts discussions over the years have articulated a consensual set of norms and recommendations[20], which the General Assembly has repeatedly endorsed, and which States should take as a basis for responsible state behaviour in cyberspace;

53. RECOGNISES that those norms of responsible State behaviour include that States should not knowingly allow their territory to be used for internationally wrongful acts, should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts emanating from their territory and that States should take appropriate measures to protect their critical infrastructure from ICT threats;

54. RECOGNISES the shared cyber threats and risks faced by EU, NATO and their respective Member States and REITERATES the importance of continuing the EU-NATO cooperation on cybersecurity and defence in full respect of the principles of inclusiveness, reciprocity and decision-making autonomy of the EU and in accordance with its Conclusions of 6 December 2016 on the implementation of the Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization[23];

55. CALLS UPON the EU and its Member States to support and encourage the development of regional confidence building measures, which are an essential element to increase cooperation and transparency and reduce the risk of conflict. Implementing cyber security confidence building measures in the OSCE and other regional settings will increase predictability of state behaviour and further contribute to stabilising cyberspace;

56. REAFFIRMS that the EU will continue to uphold its core values in protecting human rights and fundamental freedoms building on the EU's Human Rights Guidelines on online freedom. EU also emphasises the importance of all stakeholders' involvement into the governance of the Internet, including academia, civil society and private sector;

57. CALLS UPON the EU and its Member States to promote cyber capacity building in third countries, with a special priority to the EU's neighbouring and developing countries experiencing fast growing connectivity, in addressing cybercrime and building cyber resilience, in accordance with the EU core values. For advancing EU efforts in this field, an EU Cyber Capacity Building Network and EU Cyber Capacity Building Guidelines should be developed which should be complementary to existing mechanisms and structures;

[23] 15283/16.

58. EMPHASISES the progress achieved in the EU-NATO cooperation in cyber defence and security, and its development in training, education and concepts while avoiding unnecessary duplication of efforts where requirements overlap, as well as fostering interoperability through cyber defence requirements, and standards and CALLS to continue cooperation on cyber defence exercises (staff level) and share good practices regarding crisis management, while avoiding unnecessary duplication of efforts, where requirements overlap, in full respect of the EU Exercise Policy and the principles of inclusiveness, reciprocity and decision-making autonomy of EU;

59. RECOGNISES that the Council of Europe Convention on Cybercrime, the Budapest Convention, offers an effective legal standard to inform national legislation on cybercrime. CALLS for all countries to design appropriate national legal frameworks and pursue cooperation within this existing international framework offered by the Budapest Convention;

60. RECALLS the achievements in conducting bilateral EU cyber dialogues and calls for further efforts to facilitate cooperation with third countries in cybersecurity;

61. RECALLS that EU has a robust and legally binding export control mechanism based on the decisions and best practices developed in the international non-proliferation regimes and NOTES the ongoing discussion in the Council to find the best ways to further improve the functioning of these controls and INVITES the Member States to continue to address, in the relevant international export control regime*s* (e.g. Wassenaar Arrangement), the critical cyber security applications of novel technologies, in order to ensure effective control of critical cyber security technologies of tomorrow.

62. As a follow-up to the European Council Conclusions of 19 October 2017[24] these Conclusions will be implemented by the means of an Action Plan to be adopted by the Council before the end of 2017. The action plan as a living document would be regularly reviewed and updated by the Council.

---

[24] EUCO 14/17.