Council of the
European Union

Brussels, 15 November 2016
(OR. en)

14540/16

CYBER 130
COMPET 597
IND 245
RECH 320
TELECOM 241

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	15 November 2016
To:	Delegations
No. prev. doc.:	13967/1/16 REV 1
Subject:	Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - Council conclusions (15 November 2016)

Delegations will find in the annex the Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, adopted by the General Affairs Council at its 3499th meeting held in Brussels on 15-16 November 2016.

ANNEX

Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING:

- its conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace[1];
- the EU Cyber Defence Policy Framework[2];
- its conclusions on Cyber Diplomacy[3];
- the Commission Communication entitled "A Digital Single Market Strategy for Europe"[4];
- its conclusions on Countering Hybrid Threats[5];
- its conclusions on the e-Government Action Plan 2016-2020[6];
- the Commission Communication on Strengthening Europe´s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity System[7];
- its conclusions on the Global Strategy on the European Union's Foreign Policy and Security Policy[8];

1 doc. 12109/13.
2 doc. 15585/14.
3 doc. 6122/15.
4 COM (2015) 192 final, 6 May 2015.
5 doc. 7857/16.
6 doc.12080/16.
7 COM (2016) 410 final, 5 July 2016.
8 doc. 13202/16.

NOTING:

- the outcome of the High Level Conference on Cyber Security held in May 2016 in Amsterdam;

- the outcomes of the series of Global Conferences on Cyber Space from 2011 (London), 2012 (Budapest), 2013 (Seoul) and 2015 (the Hague).

RECOGNISES THAT:

1. Member States, the Commission and the other EU entities in accordance with the principle of subsidiarity, have been closely collaborating on advancing Europe´s cybersecurity and cyber resilience at EU and national levels, especially since the adoption of the EU Cybersecurity Strategy and that further intensive and joint collaboration is indispensable to protect the EU against cyber threats while maintaining a comprehensive and coherent approach to cybersecurity;

2. cyber threats and vulnerabilities continue to evolve and intensify which will require continued and closer cooperation, especially in handling large-scale cross-border cybersecurity incidents;

3. cybersecurity is a key enabler for the proper functioning of the Digital Single Market as cybersecurity incidents can cause not only severe disruptions in the modern society and major economic damage to European businesses, but as such can also undermine the trust of citizens and enterprises in the digital society and bring reluctance in using digital technologies;

4. the recently adopted NIS Directive[9], which establishes new cooperation mechanisms and the EU Cybersecurity Strategy - to be renewed in due time, and the role of ENISA Regulation - to be soon reviewed, form the core elements of an EU cyber resilience framework, in which cybersecurity of Member States and those of EU entities should be effectively addressed;

5. adequate cybersecurity skills through education and training, related both to preventing cybersecurity incidents and to dealing with and mitigating their impacts, are some of the key aspects in achieving cybersecurity resilience, while fostering the collaboration among Member States, Commission, EEAS, ENISA, Europol, Eurojust, EDA as well as NATO, where applicable;

6. both strategic and operational cooperation and information exchange across the sectors in Member States and across borders in the EU is critical to maintain cybersecurity and to prevent and mitigate the impact of cybersecurity incidents. Such cooperation helps not only to increase preparedness and resilience but also to better understand interdependencies, e.g. through the implementation of the European Programme for Critical Infrastructure Protection;

7. assessment of the volume of shared risks and of large-scale cybersecurity incidents impact is determined by the degree of cross-border and cross-sectorial interdependence, both in public and private sectors;

8. it is important to ensure an appropriate funding capacity to support SMEs and start-ups in the area of cybersecurity, in particular their access to finance and investment, especially in their early development phases;

9. the added value of establishing a contractual PPP on cybersecurity under *Horizon 2020,* is to stimulate the competitiveness and innovation of Europe´s cybersecurity industry;

[9] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

10. dynamic technologic developments in the digital domain translated into a large scale of various ICT products, services and solutions trigger not only new societal and economic but also new security challenges, especially in relation to data, which should be further reflected and promoted within the Digital Single Market;

11. the cyber theft of trade secrets is a potentially damaging to the ability of European industry to innovate and compete and its impact deserves further consideration;

12. Member States share the common goal of contributing to Europe's strategic autonomy, as outlined in the Council Conclusions on the Global Strategy on the European Union's Foreign Policy and Security Policy, also in cyberspace;

STRESSES THAT:

13. each Member State remains responsible for taking the necessary measures to ensure the protection of the essential interests of its security in full respect of the Treaties;

14. Member States, as a matter of priority, should be transposing the NIS Directive into their national legislative frameworks reflecting effectively the cooperation within the newly established Cooperation Group and the CSIRT Network which would have positive effect on strengthening cyber resilience and cybersecurity and on handling large-scale incidents;

15. the enhancement of the network and information security of the EU entities should be considered as part of the priority for reinforcing cybersecurity across the EU;

16. cyber capacity building and confidence building measures are necessary to prevent and limit the risk of cybersecurity incidents and to create trust and confidence in the digital single market;

17. applying tools of diplomatic, legal and technical nature and enhancing cooperation at EU and national levels are needed to successfully respond to cybersecurity incidents, including coercive cyber operations, and fight against cybercrime;

18. the EU needs to fully adapt the security and privacy by design approaches to develop, supply and deploy effective, high-quality, affordable and interoperable cybersecurity products and services as well as to take action for achieving a more integrated and global market for them;

19. fostering cybersecurity dialogue with industry could help to identify gaps in cybersecurity certification and validation mechanisms as well as in labelling schemes which should take into account internationally accepted standards and principles;

20. coherence is necessary between the respective actions and EU policies, financial instruments and programmes for an effective operationalizing of Europe´s cyber resilience systems.

21. the contractual PPP on cybersecurity should remain open to newcomers, the conditions for joining it should remain transparent and information on these conditions should continue to be easily accessible.

CALLS ON THE COMMISSION TO:

22. meet the targets specified in the Communication on Strengthening Europe´s Cyber Resilience, in particular by:

a) submitting a cooperation blueprint to respond to large-scale cyber incidents at EU level for consideration by the NIS Directive bodies and other relevant stakeholders, especially ENISA in the first half of 2017 while taking into account the blueprint's complementary function;

b) finalizing the evaluation of ENISA, the latest by end 2017, whilst proposing any aspects related to the renewal of the ENISA´s mandate (including its extension to cover the tasks as envisaged by the NIS Directive) as soon as possible;

c) establishing in close cooperation with Member States, EEAS, Europol, Eurojust, ENISA, EDA and other relevant EU entities a cybersecurity training platform;

d) examining the necessary legal and organisational conditions in order to allow Member States to conduct regular vulnerability checks of publicly accessible network infrastructure;

e) exploring the opportunity to create a cybersecurity certification and labelling scheme, while reflecting the existing effective security schemes, if relevant, with a view to proposing measures, including legislative ones, to address these challenges by 2017;

f) raising awareness in the cybersecurity community about the existing funding mechanisms and fostering the use of EU tools and instruments for support innovative SMEs;

g) exploring ways for facilitating the access to finance and investment (e.g. through a dedicated Cybersecurity Investment Platform) for SMEs and start-ups, especially in their early development phase;

h) where relevant, evaluate the current functioning of the European ISACs and work towards proposals to further strengthen these structures, together with the Member States and, where appropriate, existing national ISACs;

i) promoting a security-by-design approach in major infrastructure investments that have a digital component and are co-financed by the EU funds;

23. consult Member States prior to establishing any new mechanisms and structures (for example such as an "information hub" or a high-level advisory group) or prior to introducing new instruments (e.g. cooperation blueprint), both related to cybersecurity, their complementary role, objectives and given tasks;

24. report annually to the Council in writing on the progress made.

INVITES THE MEMBER STATES TO:

25. fully operationalise the cybersecurity cooperation mechanisms and to enhance cross-border cooperation in relation to readiness for preventing, handling and/or mitigating the impact of large-scale cybersecurity incidents in conformity with the principles and provisions agreed within the NIS Directive;

26. actively participate in the contractual PPP on cybersecurity for strengthening the competitiveness, research and innovation of Europe's industry;

27. cooperate with the Commission on the creation of an open European framework, while taking into account the development of a global framework for certification of cybersecurity products and services, in line with the international standards and based on experts involvement that would cover a wide range of ICT systems and solutions at any security level and which would be applicable in all Member States with the aim of building a genuine and secure Digital Single Market making Europe a leader in global standardization;

28. cooperate with the Commission and other relevant parties on the attainment of the strategic objectives set out in these Conclusions.

INVITES THE RELEVANT STAKEHOLDERS TO:

29. adopt the best practices in the field of cybersecurity, support the awareness raising, up-skilling and improve training in the area of cybersecurity;

30. consider increasing investment in market of high-quality cybersecurity products and services while deepening cooperation with public authorities, including national CERTs, if relevant;

31. make the best use of the contractual PPP on cybersecurity and the European ISACs, in order to foster industrial cooperation, especially in the fields of research and innovation, standardization, certification, labelling, joint investment and industrial consolidation;

32. contribute proactively to the attainment of the strategic objectives set out in these Conclusions in order to strengthen the resilience of the European industry;

33. focus on increasing uptake of cybersecurity solutions in all sectors and by the full range of users.