Council of the
European Union

Brussels, 18 January 2019
(OR. en)

15244/3/18
REV 3

LIMITE

CYBER 310
COPEN 435
COPS 473
COSI 312
DATAPROTECT 265
IND 393
JAI 1255
JAIEX 165

POLMIL 226
RELEX 1064
TELECOM 455
DAPIX 372
CATS 93
CSC 362
CSCI 167
IA 410

NOTE

From: Presidency

To: Delegations

Subject: Draft Council conclusions on cybersecurity capacity and capabilities building in the EU

Delegations will find in Annex a revised text of the draft Council conclusions on cybersecurity capacity and capabilities building in the EU prepared on the basis of the discussions at the Horizontal Working Party on Cyber Issues of 19 December 2018 and 9 January 2019 and on the basis of the comments received from Member States.

The revised text will be discussed at the meeting of the Horizontal Working Party on Cyber Issues of 23 January 2019.

Deletions are marked with strikethrough and additions with bold and underlined.

ANNEX

Draft Council conclusions on cybersecurity capacity and capabilities~~y and cyber capacity~~ building in the EU

The Council of the European Union,

1. RECALLING its Conclusions on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[1];

2. RECALLING its Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises[2];

3. RECALLING its Conclusions on external cyber capacity building[3];

4. REITERATING that a high level of security of network and information systems can be provided by enhancing the cybersecurity **capacity and** capabilities~~ and capacities~~ of the Member States **and EU institutions, agencies and bodies**, and the consequent strengthening of their cyber resilience;

5. WELCOMES the progress achieved by Member States in strengthening Computer Security Incident Response Teams (CSIRTs);

6. ACKNOWLEDGING the existing support being provided by the Commission to the Member States´~~ for~~ for capacity building ~~of Member State Computer Security Incident Response Teams (~~CSIRTs~~)~~ through the Connecting Europe Facility;

[1] 14435/17 (Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU of 20 November 2017)

[2] 10086/18 (Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises of 26 June 2018)

[3] 10496/18 (Council conclusions EU External Cyber Capacity Building Guidelines of 26 June 2018)

7. ACKNOWLEDGING the support provided to law enforcement authorities for capacity building in fighting cybercrime through the Internal Security Fund and CEPOL;

8. WELCOMES the update of the EU Cyber Defence Policy Framework to further support the development of cyber defence capabilities of EU Member States;

9. COMMENDING the progress achieved in the implementation of the NIS Directive by the Member States, but noting at the same time the differences in the national transposition laws as well as in the culture, governance and organizational structures which require a tailored-made approach in cyber capacity building reflecting MS needs**;**

10. COMMENDING the establishment of a trusted Network of CSIRTs by Member States with the active support of the Commission and ENISA;

11. NOTING that cybersecurity is a complex, interdependent and continuously changing domain that requires ~~constant~~ adapting of the political and legal framework to the new technological trends and emerging technologies such **as** artificial intelligence, blockchain and quantum computing;

12. EMPHASIZING that cybersecurity related training and education programmes as well as information and awareness raising about security threats for end users are key to decrease the cybersecurity risks ~~for businesses and society~~;

13. UNDERLINING that cyber exercises are effective tools to assess and further improve the level of preparedness of the **EU** ~~economy and society against natural disasters, technology failures, cyber-attacks and emergencies~~ **for countering large scale cybersecurity-related challenges and threats;**

14. REITERATING that cyberspace has no bo~~a~~rders so cross-border and cross-sector perspective and cooperation have to be an unwavering principle of cyber capacity building activities and initiatives;

15. STRESSING the importance of cooperation of the public **sector,** ~~and~~ private sector **and academia** ~~(in particular through Public-Private Partnerships and collaboration)~~, **in particular through collaborative projects**;

16. **STRESSING the importance of civil-military cooperation in the cyber field to ensure a coherent response to cyber threats;**

17. NOTING that cybersecurity research **and innovation development in the EU are**~~is~~ still very fragmented as well as segregated from other research areas; ~~and face a lack of cooperation between industrial, civilian and defence communities;~~

18. ~~**WELCOMES the progress achieved by Member States in developing CSIRTs to deepen voluntary cooperation in cyber field through mutual assistance**~~NOTES **the progress achieved by a group of Member States in developing Cyber Rapid Response Teams to deepen voluntary cooperation in cyber field through mutual assistance;**

~~**19. WELCOMES the update of the EU Cyber Defence Policy Framework to further support the development of cyber defence capabilities of EU Member States;**~~

20. WELCOMES ~~the objectives~~ **the ongoing discussion in the Council** of the Commission´s Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centers;

21. **ENCOURAGES**~~COMMENDS~~ the ~~(~~ongoing~~)~~ work of the NIS Cooperation Group on cyber capacity building;

22. **ENCOURAGES**~~**COMMENDS**~~ **the ongoing work of the NIS Cooperation Group on EU coordinated response to large-scale cybersecurity incidents and crisis;**

23. **INVITES**~~CALLS on~~ the Member States to ~~move beyond~~ **built on** their national cybersecurity strategies **and mainstream cybersecurity, in a consistent manner in** ~~supplementing them with~~ sector-specific strategies ~~taking into account the particular requirements of the underlying critical infrastructures~~;

24. INVITES the Member States to perform continuous monitoring, evaluation/assessment of the impact of measures taken towards the strengthening of cyber resilience and enhancement of cyber capabilities and capacities at national level;

25. **INVITES**~~CALLS on~~ the Member States to mainstream cybersecurity and digital literacy in curricula at all levels of education (primary, secondary, tertiary, lifelong learning) **based, where relevant, on created job profiles**;

26. **INVITES**~~CALLS on~~ the Member States to carry out cybersecurity awareness **and cyber hygiene initiatives**~~programmes~~ for the public and end users, trainings targeting public sector employees; ~~as well as specialized cybersecurity training for specific posts in the public sector;~~

~~27.~~ ENCOURAGES the Member States to conduct cybersecurity exercises at national level as well as conduct and/or participate in cybersecurity exercises at EU level in order to test and train strategic and technological aspects as well as to develop ~~operational~~**necessary** skills effectively and practically;

28. INVITES the Member States to further develop cybersecurity technical and operational capabilities of their CSIRTs in incident prevention and incident response;

29. **CALLS on the Commission and ENISA to continue their support for developing the capacity and capability of the Network of CSIRTs by Member States to better cooperate, share information on incidents and respond effectively to large-scale cross-border incidents;**

30. **INVITES the Member States to continue to develop specific competencies in law enforcement authorities to effectively fight cybercrime**~~w~~ **at EU level with the support of the Commission;**

31. INVITES the Member States to increase investment in cyber capacity building;

32. CALLS on the Commission **and ENISA** to carry out ~~a~~ ~~EU wide~~ cybersecurity awareness programmes **and trainings** ~~for the public and end users, trainings~~ targeting employees of EU institutions, agencies and bodies employees; ~~as well as obligatory specialized cybersecurity training for specific posts within EU institutions, agencies and bodies;~~

33. CALLS upon the EU and its Member States to share **on a voluntary basis** information and ~~in particular~~ best practices in order to contribute to the identification and tackling of main cyber capacity building needs at national and EU level;

34. **INVITES** ~~CALLS upon~~ the EU and its Member States to support cybersecurity research and promote cybersecurity as a perspective in other fields of study conjoining various branches of cybersecurity related research and development into an integrated whole **and to foster excellence in cybersecurity research**;

35. **INVITES** ~~CALLS upon~~ the EU and its Member States ~~to support the integration of the results of cybersecurity research in the market~~ **to develop cybersecurity research initiatives following the societal needs and the integration of the research results in the market**;

36. **INVITES** ~~CALLS upon~~ the EU and its Member States to take cybersecurity**, where relevant,** into consideration in calls for ICT procurement ~~and research~~.