Council of the
European Union

Brussels, 20 March 2019
(OR. en)

7737/19

CYBER 101	**RELEX 287**
COPEN 118	**TELECOM 141**
COPS 92	**DAPIX 109**
COSI 52	**CATS 43**
DATAPROTECT 98	**CSC 111**
IND 102	**CSCI 47**
JAI 313	**IA 106**
JAIEX 44	**EJUSTICE 44**
POLMIL 31	

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	19 March 2019
To:	Delegations
No. prev. doc.:	6866/19
Subject:	Council conclusions on cybersecurity capacity and capabilities building in the EU

Delegations will find in the annex the Council conclusions on cybersecurity capacity and capabilities building in the EU adopted by the General Affairs Council held on 19 March 2019.

ANNEX

Council conclusions on cybersecurity capacity and capabilities 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 of the Member States and the EU institutions, agencies and bodies, and by the subsequent strengthening of their cyber resilience;

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

6. COMMENDING the establishment of the CSIRTs Network by the Member States with the active support of the Commission and ENISA as well as the strengthened cooperation at strategic level through the NIS Cooperation Group, composed of the Member States, the Commission and ENISA;

---

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 on EU External Cyber Capacity Building Guidelines of 26 June 2018)

7. EMPHASISING the key role of the NIS Cooperation Group in providing the necessary guidance to align as much as possible the approach in the transposition of the NIS Directive[4] across the EU as well as in tackling relevant cybersecurity issues;

8. ACKNOWLEDGING the existing support being provided by the Commission to the Member States for capacity-building CSIRTs through the Connecting Europe Facility;

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

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

11. COMMENDING the progress achieved in the implementation of the NIS Directive by the Member States;

12. NOTING that cybersecurity is a complex, interdependent and continuously changing domain requiring the adaptation of the political and legal framework to new technological trends and emerging technologies such as artificial intelligence, blockchain and quantum computing;

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016).

13. EMPHASISING that cybersecurity related training and education programmes as well as information and awareness raising on security threats for end users are key to decreasing cybersecurity risks;

14. UNDERLINING that cyber exercises are effective tools for assessing and further improving the level of preparedness of the EU and its Member States for countering large scale cybersecurity incidents and crises;

15. REITERATING that cyberspace has no borders, which means that cross-border and cross-sector perspectives and cooperation are an unwavering principle of cyber capacity-building activities and initiatives;

16. STRESSING the importance of cooperation between the public sector, the private sector and academia, in particular through collaborative projects;

17. STRESSING the importance of civil-military cooperation, working towards common goals in the cyber field to ensure a coherent and effective response to cyber threats;

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

19. WELCOMES the ongoing discussion in the Council on 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 Centres;

20. ENCOURAGES active participation in the ongoing work of the NIS Cooperation Group, in particular with regard to cyber capacity-building;

21. ENCOURAGES the ongoing work of the NIS Cooperation Group on EU coordinated response to large-scale cybersecurity incidents and crises;

22. INVITES the Member States to build on their national cybersecurity strategies and mainstream cybersecurity, taking into account sector-specific requirements;

23. INVITES the Member States to perform continuous monitoring, evaluation/assessment of the impact of measures taken to strengthen cyber resilience and enhance cyber capabilities and capacities at national level;

24. INVITES 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 established and future job profiles;

25. INVITES the Member States to carry out cybersecurity awareness and cyber hygiene initiatives for the public and end users, targeting public sector employees;

26. ENCOURAGES the Member States to conduct cybersecurity exercises at national level as well as to conduct and/or participate in cybersecurity exercises at EU level in order to test and train for strategic and technological aspects, as well as to develop the necessary skills effectively and on a practical level;

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

28. CALLS on the Commission and ENISA to continue their support in 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;

29. INVITES the Member States to continue to help law enforcement authorities develop specific competences in coordination with the competent European authorities in order to effectively fight cybercrime at EU level;

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

31. CALLS on the Commission and ENISA to carry out cybersecurity awareness programmes and training targeting employees of the EU institutions, agencies and bodies;

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

33. INVITES the EU and its Member States to support cybersecurity research and to promote cybersecurity as an issue in other fields of study, bringing various branches of cybersecurity-related research and development together into an integrated whole, and to foster excellence in cybersecurity research;

34. INVITES the EU and its Member States to develop cybersecurity research reflecting societal needs and integrating the research results into the market;

35. CALLS upon the EU and its Member States to take cybersecurity into consideration in calls for ICT procurement, as appropriate.