Council of the European Union

Brussels, 7 December 2018
(OR. en)

15244/18

LIMITE

CYBER 310	POLMIL 226
COPEN 435	RELEX 1064
COPS 473	TELECOM 455
COSI 312	DAPIX 372
DATAPROTECT 265	CATS 93
IND 393	CSC 362
JAI 1255	CSCI 167
JAIEX 165	IA 410

NOTE

From:	Presidency
To:	Delegations
Subject:	Draft Council conclusions on cybersecurity capability and cyber capacity building in the EU

Delegations will find in Annex draft Council conclusions on cybersecurity capability and cyber capacity building in the EU which will be discussed at the meeting of the HWP on Cyber Issues of 12 December 2018. The draft has been prepared in cooperation with the incoming Romanian Presidency.

ANNEX

Draft Council conclusions on cybersecurity capability and cyber capacity building in the EU

The Council of the European Union,

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

RECALLING its Conclusions on external cyber capacity building[2];

REITERATING that a high level of security of network and information systems can be provided by enhancing the cybersecurity capabilities and capacities of the Member States, and the consequent strengthening of their cyber resilience;

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

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 artificial intelligence, blockchain and quantum computing;

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;

UNDERLINING that cyber exercises are effective tools to assess and further improve the level of preparedness of the economy and society against natural disasters, technology failures, cyber-attacks and emergencies;

---

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

REITERATING that cyberspace has no boarders so cross-border and cross-sector perspective and cooperation have to be an unwavering principle of cyber capacity building activities and initiatives.

STRESSING the importance of cooperation of the public and private sector (in particular through Public-Private Partnerships and collaboration);

NOTING that cybersecurity research is still very fragmented as well as segregated from other research areas, and face a lack of cooperation between industrial, civilian and defence communities;

WELCOMES the objectives 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;

COMMENDS the (ongoing) work of the NIS Cooperation Group on cyber capacity building;

CALLS on the Member States to move beyond their national cybersecurity strategies supplementing them with sector-specific strategies taking into account the particular requirements of the underlying critical infrastructures;

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;

CALLS on the Member States to mainstream cybersecurity and digital literacy in curricula at all levels of education (primary, secondary, tertiary, lifelong learning);

CALLS on the Member States to carry out cybersecurity awareness programmes for the public and end users, trainings targeting public sector employees as well as obligatory specialized cybersecurity training for specific posts in the public sector;

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 skills effectively and practically;

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

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

CALLS on the Commission to carry out a EU wide cybersecurity awareness programmes 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;

CALLS upon the EU and its Member States to share 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;

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;

CALLS upon the EU and its Member States to support the integration of the results of cybersecurity research in the market;

CALLS upon the EU and its Member States to take cybersecurity into consideration in calls for ICT procurement and research.