Council of the European Union

Brussels, 26 June 2018
(OR. en)

10086/18

CYBER 139
COPEN 209
COPS 210
COSI 148
DATAPROTECT 128
JAI 637
JAIEX 66
POLMIL 82
TELECOM 188
DAPIX 187

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	26 June 2018
To:	Delegations
No. prev. doc.:	10085/18
Subject:	EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises - Council conclusions (26 June 2018)

Delegations will find in the annex the Council conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises, adopted by the General Affairs Council at its 3629th meeting held on 26 June 2018.

ANNEX

COUNCIL CONCLUSIONS ON EU COORDINATED RESPONSE TO LARGE-SCALE CYBERSECURITY INCIDENTS AND CRISES

The Council of the European Union,

1. RECOGNISING the need for an efficient EU level response to large scale cybersecurity incidents and crises as stressed in its 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[1].

2. RECALLING its conclusions of 19 June 2017[2] on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox") and the corresponding implementing guidelines of 11 October 2017 as well as the Integrated Political Crisis Response arrangements adopted in 2013[3].

3. TAKING INTO CONSIDERATION the Commission Recommendation of 13 September 2017[4] on a Coordinated Response to Large-scale Cybersecurity Incidents and Crises and the core objectives and guiding principles set out therein.

4. NOTING the discussions held at the Cybersecurity Challenges Conference in Sofia on 26 March 2018.

5. RECOGNISING the competences of the Member States and their responsibility for national security in the domain of cybersecurity.

---

1 14435/17.
2 9916/17.
3 10708/13.
4 C(2017) 6100 final.

6. WELCOMING the adoption of the CSIRTs Network Standard Operating Procedures (SOPs) and the on-going work within the NIS Cooperation Group on a common taxonomy for cybersecurity incidents.

7. RECOGNISING the on-going work on the Law Enforcement Emergency Response Protocol, that describes a mechanism for early detection and identification of cybersecurity incidents and crises, eventually leading to an investigation under the normal applicable operating procedures, complementing and aligning a response by the law enforcement community with existing EU crisis response mechanisms.

8. TAKING INTO CONSIDERATION the Memorandum of Understanding to establish a framework for cooperation signed by ENISA, EC3, CERT-EU and the EDA which will further strengthen their cooperation within their respective mandates, in particular on matters of information exchange, cyber exercises as well as technical cooperation.

9. UNDERLINING the need to make use of the existing crisis management mechanisms, processes and procedures at national and European level.

10. RECALLING the importance of an effective implementation of the Directive on Security of Network and Information systems[5] and the development of capabilities of national CSIRTs competent authorities and Single Points of Contacts as regards responding to and handling of cybersecurity incidents.

11. RECALLING that activities at EU level with regard to large-scale cybersecurity incidents and crises take place in accordance with the principles of subsidiarity and proportionality.

[5] 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).

12. RECOGNISING the importance of shared situational awareness based on national conclusions from Member States, coordinated public communication and effective response during large-scale cybersecurity incidents and crises at EU level through existing mechanisms.

13. ACKNOWLEDGING the EU - NATO cooperation on cybersecurity and defence in full respect of the principles of inclusiveness, reciprocity and decision-making autonomy of the EU, including information sharing between CERT-EU and NATO Computer Incident Response Capability (NCIRC).

Fostering the preparedness and crisis prevention

14. REAFFIRMS the need to prevent cybersecurity incidents and crises by continuing to bolster the EU and its Member States capabilities to address cyber threats.

15. CALLS upon the Member States to ensure that their national crisis management mechanisms adequately address cybersecurity incidents and crises as well as use, and where necessary provide**,** appropriate procedures for cooperation at EU level at the technical, operational and political level.

16. STRESSES the importance for the EU and its Member States to regularly exercise their response to large-scale cybersecurity incidents and crises, including in the CYBER Europe exercises organised by ENISA.

Increasing the situational awareness

17. CALLS upon the EU and its Member States to cooperate and, based on national conclusions from Member States, contribute to EU situational awareness at all levels (technical, operational, political) both before and during large-scale cybersecurity incidents and crises through quick and effective sharing of situational information, where appropriate as well as with key strategic partners.

Ensuring the effective response

18. RECOGNISES that a response to large-scale cybersecurity incidents and crises could take many forms and might require a coordinated approach at EU level, ranging from identifying technical measures to operational measures as well as political measures, depending on the type of incident or crises.

19. CALLS upon the Member States to swiftly identify, develop and implement further means of operational cooperation, including in the CSIRTs Network SOPs, in relation to early warnings, mutual assistance and principles and modalities for coordination when Member States respond to cross-border risks and incidents and to report on the progress made.

20. NOTES the initiative by a group of Member States within the Permanent Structured Cooperation (PESCO) to deepen voluntary cooperation in cyber field through enhancing cyber information sharing and creating Cyber Rapid Response Teams for mutual assistance in response to major cybersecurity incidents.

21. RECOGNISES that cybersecurity incidents have the potential of leading to cross-sectorial or cross-border crises, impacting simultaneously the functioning of different infrastructures or services, CALLS upon the Member States to identify and put in place appropriate procedures and concrete measures for timely information sharing and situational awareness at operational level amongst competent authorities, such as the national Single Point of Contacts under the NIS Directive.

Streamlining the public communication

22. RECOGNISES that public communication could mitigate negative effects of large-scale cybersecurity incidents and crises as well as could serve as a clear signal of likely consequences of a diplomatic response to influence the behaviour of potential aggressors.

23. CALLS upon the EU institutions, agencies and bodies and Member States to ensure effective and, where necessary and possible, coordinated communication towards the public through existing mechanisms.

Building on the lessons learned and post incident analysis

24. CALLS upon the EU and its Members States, based on their national conclusions, to promote and share the analysis of operational and strategic aspects of lessons of large-scale cybersecurity incidents, crises, and exercises throughout the community of relevant actors involved.

Developing a European Cybersecurity Crisis Cooperation Framework

25. CALLS upon the EU and its Member States to jointly work towards the development of European Cybersecurity Crisis Cooperation, putting in place the practical operationalisation and documentation of all the relevant actors, processes and procedures within the context of existing EU crises management mechanisms, in particular the Integrated Political Crisis Response arrangements.

26. CALLS upon the EU and its Member States to undertake necessary steps to remove obstacles and/or fill in gaps identified both in terms of information flows and in terms of interoperability of the existing procedures, processes and mechanisms where necessary.