Council of the
European Union

Brussels, 17 April 2018
(OR. en)

7667/18

COSI 60
CYBER 54
TELECOM 78
JAI 271
DAPIX 82
RELEX 286
ENFOPOL 151

NOTE

From:	Presidency
To:	Delegations
Subject:	EU Coordinated response to Large Scale Cybersecurity Incidents and Crises - the way ahead (continuation) - discussion

Delegations will find in Annex a discussion paper on the EU Coordinated response to large-scale cybersecurity incidents and crises.

ANNEX

EU Coordinated response to Large Scale Cybersecurity Incidents and Crises

I. Introduction

On 13 September 2017 as part of the cybersecurity package, the Commission adopted a Recommendation on a coordinated response to large-scale cybersecurity incidents and crises[1] ("the Blueprint"). The 2017 Council Conclusions on Building strong cybersecurity for the EU[2] stressed the *need for an efficient EU-level response to large-scale cyber incidents and crises,* for *mainstreaming cybersecurity into existing crisis management mechanisms at EU level* and *of information exchange between the different communities critical for ensuring cybersecurity in Europe, including the relevant EU bodies and Member States authorities*.

A detailed presentation of the Blueprint was made at the HWP Cyber meeting of 19 January 2018. On that basis at the HWP Cyber meeting of 5 March, the Presidency explored delegations' views on the way ahead. It suggested the preparation of a dedicated set of Council Conclusions to support the coordinated EU response to large scale cybersecurity incidents and crises, taking into account the Commission's recommendation. This approach was welcomed by delegations and motivated the elaboration of the present paper as basis for the preparation of the first draft text of these Conclusions.

During the Cybersecurity Challenges Conference hosted by the Presidency on 26 March 2018 in Sofia the challenges of providing an effective collective response to large-scale cyber attacks at all those different levels were explored. The outcome of those discussions highlighted the need to operationalise the various crises management mechanisms co-existing at EU level and bring up-to-date the national ones. They also underlined the importance of sharing a common "language" and understanding when it comes to establishing a common response in this complex domain. With the support of ENISA, the Presidency started the development of a common taxonomy in the framework of the NIS Cooperation Group aiming its finalisation within its semester.

1 OJ L 239, 19.9.2017, p.36.
2 14435/17.

II. Objectives and design of the Council Conclusions

The Council Conclusions would aim at providing a clear view on how the various existing EU crisis mechanisms would operate in the context of large-cybersecurity incidents and crises, and at facilitating the MS understanding of how they relate to each other and to the national response mechanisms as well as how they can support them. The conclusions would also seek to clarify the existing links among the different processes, actors and communities or to establish links where such are missing at all the different levels (technical, operational, political/strategic).

The Conclusions would not redesign the existing processes, procedures and mechanisms, but raise awareness on their applicability in the event of cyber incidents and crises. Therefore procedures and mechanisms would not be reproduced in the body of the Conclusions but would be either referenced or attached to them for the sake of comprehensiveness.

Furthermore, the Conclusions would not seek to change the roles, responsibilities and competences of the actors involved, but to supply them with a tool that could assist their actions - notably in terms of information flows and escalation mechanisms - and clarifying how those actions fit in the overall crisis response approach. This is of a crucial importance given the possible diversification of the response, i.e. technical, law enforcement or judiciary, diplomatic, political, etc. at either EU or national level.

Also, cyber incidents have the potential of leading to a cross-sectorial crisis, i.e. impacting simultaneously the functioning of different sectors, infrastructures or services. Thus, the Conclusions would also draw attention to the need for good coordination of the activities in the cyber domain with parallel actions in other affected sectors, and the possible escalation to an IPCR activation if required.

Moreover, the Conclusions would seek to encompass the full crisis management cycle, i.e. looking at not only response but also at preparedness, mitigation and recovery aspects. Special attention would be paid to promoting and sharing the analysis of lessons of large cybersecurity incidents, crises, and exercises throughout the community of relevant actors involved.

In conclusion, the Presidency would strive towards developing Conclusions that are operational in nature and would invite delegations to make every effort to contribute with concrete and concise language in support of this objective.

III. Next steps

Delegations are invited to express their views on the objectives and design of the Council Conclusions as outline above. On the basis of input received, the Presidency would elaborate the first draft of the Conclusions to present it for discussion at the next meeting of the HWP Cyber.

Delegations are encouraged to send their suggestions or positions also in writing by 27 April 2018 to the following email address: cyber@consilium.europa.eu.