**Council of the
European Union**

**Brussels, 13 January 2017
(OR. en)**

5015/17

**CYBER 3
JAI 25
TELECOM 10
RELEX 28
COSI 7**

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	9 December 2016
To:	Horizontal Working Party on Cyber Issues
Subject:	Summary of discussions

1.   Adoption of the agenda

The agenda, as set out in doc. CM 5034/16, was adopted with the addition of one item under Any Other Business by the DE delegation.

2.   Information from the Presidency, Commission, EEAS and EU Agencies

The Presidency gave a briefing on the outcome of the latest JHA and TTE Councils as well as on the recently held EU-US ministerial meeting.

The Commission (DG Home) reported on the outcome of the latest plenary meeting of the Budapest Convention Committee within the Council of Europe with regard to discussions on the draft Guidance Note on Production Orders. It explained that due to some divergent views, further work would be necessary to finalise the guidance note. That might necessitate a meeting of the Cloud Evidence Working Group in January. In addition, the latter might also assess the need for an additional protocol to the Convention, as suggested by some of the parties thereto.

The Commission (DG Connect) gave an update on the implementation of the July Communication on Cyber Resilience, outlining in particular how it plans to organise the work on certification and what steps were envisaged for the coming year. It was specified that a Roadmap would be published early in 2017 for that purpose, to be followed by extensive public consultation with all the relevant stakeholders so as to identify the best form for an EU framework for the certification of cybersecurity products. Further work in relation to the review of the ENISA mandate was expected to take place in the course of 2017.

The EEAS explained that the EU-US cyber dialogue would take place on 16 December 2016 in Brussels, where various topics related to cybersecurity and cybercrime would be discussed. Several other events such as an EU-NATO round table and a Microsoft-Carnegie event would be held prior to that. Cyber dialogues with Japan and China were expected to take place in the first quarter of 2017. The EEAS also informed the meeting that the second set of Confidence-Building Measures had been endorsed in the framework of OSCE and that the six-monthly report on the implementation of the Cyber Defence Policy Framework (doc.14904/16) had been adopted recently by the PSC and would now become an annual report.

Eurojust gave a briefing on the kick-off meeting of the European Judicial Cybercrime Network held on 24 November in The Hague, at which there had been a large attendance from the Member States, some associated countries and EU institutions and agencies. The agenda had included both issues of substance and some of an organisational nature. Currently the network intended to dedicate some time and effort to developing its work programme, which would be issued in the first quarter of 2017.

Europol/EC3 provided an overview of its activities in 2016, explaining its approach to countering cybercrime and how it was reflected in its internal structure, products and services provided to Member States. Some of the supported key operations over the past year were also mentioned.

ENISA reported on the structure and outcome of the recently concluded fourth annual pan-European cyber exercise, which had aimed at testing business continuity and crisis management. ENISA also updated delegations on the work done in relation to the CSIRT network and on the concrete deliverables expected soon.

3. **NIS Directive bodies - state-of-play and challenges**

The Commission briefly presented doc. 14948/16 outlining the timeline of the Cooperation Group and CSIRT network setup, which should be completed in February 2017, and stipulating what steps would need to be undertaken in that regard, including the adoption of implementing acts. During the discussion, delegations requested additional information regarding the process and raised issues related to the implementation of the NIS Directive.

4. **Research activities in the area of cyber**

The European Parliamentary Research Service explained that their mission was to respond to individual MEP enquiries, and to prepare studies and in-house analyses to support the activities of the EP. Among those, there was a series of research publications dedicated to engagement with the US in different sectors such as energy, defence and research. The preliminary findings of the one on cybersecurity focused on evaluating the benefits of greater EU-US cooperation and the costs of the lack of such. The US was chosen due to the shared threat environment and shared objectives.

5. **Presidency priorities for the Horizontal Working Party on Cyber Issues**

The incoming Maltese Presidency presented the priorities of its work programme, naming as key areas the security of EU citizens, the Digital Single Market and diplomacy as the first line of defence. It further explained its ambition to promote cyber awareness across the EU, for which purpose it would circulate a questionnaire to Member States. In addition to continuing the work started under the SK Presidency, in particular on encryption and capacity- building, it would focus on early detection capabilities within the EU and would discuss the cyber diplomacy toolkit. The Maltese Presidency also announced its meetings calendar and presented its team. Delegations welcomed the topics outlined, especially the focus on awareness-raising. The SK Presidency used the opportunity to summarise the main achievements during its semester.

6. **AOB**

The DE delegation informed delegations about a debriefing on the latest UN GGE meeting.