Council of the European Union

Brussels, 5 July 2017
(OR. en)

10876/17

CYBER 105
COPEN 220
JAI 652
POLMIL 83
TELECOM 179
RELEX 593
JAIEX 50
COPS 229
IND 178
COSI 154

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	12 May 2017
To:	Horizontal Working Party on Cyber Issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda as set out in doc. CM 2622/1/17 REV 1 was adopted with the addition of information points by the HU and the EE delegations.

2. Information from the Presidency, Commission and EEAS

The Presidency announced that the Cyber Attacks & Defence - Hands on Workshop would be held on 24 May 2017 in Brussels, and that live demo cyber-attacks would be presented.

The Commission **(DG Home)** informed delegations about the outcome of the United Nations Intergovernmental Expert Group on Cybercrime meeting held in Vienna on 10-13 April 2017, where the EU maintained that no new legal international cyber instrument was needed. The Commission explained that the draft resolution submitted there was generally acceptable, however the good coordination and proactive engagement of Member States should continue with a view to the upcoming CCPCJ meetings on 22-26 May 2017 and in 2018, when the main topic would be cybercrime.

The Commission **(DG Home)** provided an update on the encryption reflection process, referring back to the work plan presented in January and explaining that workshops covering that specific theme would be organised in June, and with the assistance of Europol, ENISA, FRA and Eurojust to gather the necessary information. Once collected the Commission would analyse the information and present the results by the middle of this year.

EEAS announced that it was preparing the cyber dialogue with China, India and the US this year, however no concrete dates had been fixed.

3. EU Cyber Security Strategy review - state-of-play and future steps

The Commission (DG Connect) presented the outcome of the High-level meeting with VP Ansip, stressing that it was only the beginning of the consultation process with Member States envisaged as part of the Strategy review. The input provided by delegations would be taken into account and specific issues would be dealt with in more detail with the current and future presidencies. The Commission explained that a summary of the interventions and discussion would be prepared and provided to Member States. However, the most recurrent topics included: the need for improved cyber resilience, a more effective fight against cybercrime, further building of cyber capacity and awareness raising, the EU's participation in global cybersecurity, streamlining cybersecurity, cyber governance and the cooperation framework. To bring the discussion forward the Commission proposed to split these topics and to hold more detailed discussions on a single specific topic at each of the upcoming meetings of the HWP on Cyber Issues, starting with cyber resilience in June and cybercrime in early July.

Delegations welcomed Commission's presentation and the opportunity to share their views on the review of the Cyber Security Strategy. The FR delegation presented their non-paper, supported by a number of other Member States, in which they expressed their goals and views for shaping the future strategy, insisting on the need to adopt a pragmatic approach and for inclusive drafting and follow-up processes. A number of delegations then supported some of the ideas expressed in the non-paper, but also provided additional comments on the review process, insisting on the need to ensure the inclusiveness of the process and, on the substance, for better coverage of certain elements such as the Internet of things, the application of human rights in cyberspace, and the use of EU capabilities to address the cyber threat collectively.

In general, the Member States that took the floor stressed that the objective of the review process would be to secure a high-level, ambitious strategy that was more concise than the current one. With respect to the review process as such several Member States suggested that Council conclusions be prepared before the reviewed Cyber Security Strategy was presented by the Commission, so as to provide political guidelines. The Presidency said it would reflect further on how to proceed, particularly since some other Member States felt that such conclusions might have limited value at this stage of the review process. The Presidency underlined the inclusive working method adopted currently as well as the ambition and readiness of the incoming EE Presidency to prepare Council conclusions once the Commission presented the new Strategy in September.

3.1. Foreign and security policy cyber issues - exchange of views

The DE delegation provided an update on the recent work of the UNGGE which was currently under DE chairmanship, providing details on both organisational matters (number of meetings, members, etc.) and content (CBMs, capacity building, use of internet for terrorist purposes, application of EU and international law in cyberspace, states' non-binding rules and principles). The consensus report of the fifth UNGGE was expected to be presented to the UN Secretary General in June this year for guidance on how to proceed. The rest of the UNGGE members provided some additional information and explanations, specifying their commitment to promoting the peace and stability framework and EU values.

– Discussion on CFSP and CSDP related cyber issues in the revised EU Cyber Security Strategy

The EEAS gave an overview of the various cyber initiatives being undertaken in the international sphere, in particular the efforts and resources invested in cyber capacity building in third countries, the cyber dialogues that had been launched, and the cooperation that was being developed with NATO in the cyber area. The EEAS stressed the achievements in the area of cyber defence and cyber diplomacy, observing that the norms for responsible state behaviour, CBMs and application of international law in cyberspace should be promoted further. The EEAS also underlined the need for even closer cooperation with strategic partners given the growing cyber threats and the many challenges stemming from the fast digitalisation, so as to improve the ability to protect cybersecurity collectively.

During the discussion delegations highlighted the importance of bringing a cybersecurity element into all EU policies in its international engagement (aid, development, etc.). Some Member States underlined the need to address the CFSP and CFDP aspects better in the new strategy, by promoting synergies between the various existing strategies. Delegations also mentioned some emerging cyber threats, stressing the need for coherence and a good understanding of their respective implications, and for a clear strategic vision for the EU in its external relations.

3.2. Prevention & awareness raising, education & training - exchange of views

The Presidency briefly presented the four questions set out in doc. WK 4977/17 that would serve as a basis for the discussion. A number of delegations presented their views on the issue, highlighting the need to develop more operational capacity at EU level (ENISA, Europol, etc.) while respecting the national sovereignty of Member States, and the importance of improving cyber resilience through awareness raising by sharing available materials and integrating awareness elements in the national prevention policies. Delegations stressed the lack of sufficient funding for cyber awareness campaigns as an obstacle, whilst pointing to the need for additional education and training on how to organise such campaigns more successfully. The Presidency set 31 May as the deadline for written comments.

4. Joint EU Diplomatic Response to Cyber Operations (Cyber toolbox)

4.1. Cyber toolbox - presentation of the revised text and initial views

The Presidency briefly presented the revised text on the cyber toolbox as set out in doc. 8946/17 stating that at this stage the work will be concentrated rather on the draft Council Conclusions and inviting delegations to submit written comments.

4.2. Draft Council Conclusions - examination of the revised text

The Presidency presented the revised text of the draft Council conclusions as set out in doc. 7923/1/17 REV 1 and invited delegations to examine it. Member States provided a number of additional comments and suggestions for improving the text, which were duly discussed, and those that were agreed were incorporated in the draft text. The Presidency explained that the draft Council conclusions as finalised during the meeting would be on the agenda for the PSC on 6 June with a view to their approval and subsequent submission to Coreper on 14 June for adoption by the FAC on 19 June 2017.

5. E-evidence

The Commission explained that since the start of the expert consultation process input had been collected from practitioners, industry, civil society and academia on both general and specific issues. The results would be summarised in a high-level paper to be presented to the JHA Council in June supported by a more detailed technical document. The first discussion of both papers would be held in CATS on 24 May and the Commission would give practical effect to solutions defined as valuable by Member States. As a practical measure, EUR 1 million had been made available for education and training aimed at improving direct cooperation with service providers and the US authorities.

The UK delegation provided some information on the draft agreement they were negotiating with the US on the possibility to serve a foreign LEA request for content data to a US service provider under certain conditions, including a high threshold for protection of privacy and judicial oversight. The process would be in two stages: firstly, amending the US ECPA and secondly, concluding an executive agreement that would set the standards for the requested data. Both the US administration and US service providers were supportive of this initiative and good progress had been made so far.

The ES delegation presented their non-paper on the challenges regarding the use of communication services over the Internet to hide cybercrime activities and threats to national security issues, as set out in doc. WK 5192/17. The ES delegation stressed the need for new legislative measures to address the issues outlined in the paper, more specifically over-the-top players, data access and data retention, and invited other delegations to pass on that paper to their capitals with a view to holding a more detailed discussion in one of the next meetings of the working party. Several Member States reacted to the paper, underlining some of the ongoing initiatives and discussions.

6. AOB

Under this point the HU delegation informed participants about the outcome of the first meeting of the OSCE informal group on cybersecurity held on 21 April 2017, where the work programme for this year was discussed.

The EE delegation said a presentation of the Tallinn Manual 2.0 and a discussion about it would be organised at the beginning of June. Some other events taking place in September were also announced (Cooperation Group meeting on 13 September and Cyber Conference on 14-15 September).