Council of the
European Union

Brussels, 14 March 2016
(OR. en)

6908/16

CYBER 22
POLMIL 25
TELECOM 27
RELEX 172
JAIEX 19
COPS 73
IND 46
JAI 196
COSI 38

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	1 March 2016
To:	Friends of the Presidency Group on Cyber Issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda was adopted as set out in CM 1560/1/16 REV 1, with the addition under AOB of a presentation from the General Secretariat of the Council on the new delegates portal.

2. Information from the Presidency, the European Commission and the EEAS

The Presidency presented its programme for the Friends of the Presidency Group (FoP) on Cyber Issues for its six-month term and the ministerial meeting which will take place in Amsterdam on 12 May 2016 (morning session combined with the high-level cyber security meeting on 12 and 13 May). The aim of the ministerial meeting is to create additional political energy in the cyber security field, identify open issues in current EU policies and practices, and explore opportunities to create and strengthen partnerships with the private sector.

The Presidency provided a debriefing on the outcome of the discussions on both cybercrime and cyber security at the informal meeting of the JHA Ministers in Amsterdam on 25 and 26 January 2016, and on the consultation meetings for the Tallinn Manual 2.0, which took place in The Hague from 2 to 5 February 2016. The latter resulted in constructive discussions and substantive input for the authors of the manual.

The Commission (DG HOME) gave an update on the EU Internet Forum, which was launched on 3 December 2015 to counter terrorist content and hate speech online. It intends to prepare a set of potential measures and further engagement with internet companies in the coming months, as well as possible workshops, in particular with smaller companies, which are also particularly targeted by this phenomenon.

It also debriefed the latest activities of the Public Safety Working Group (PSWG) of the ICANN Governmental Advisory Committee (GAC), which held a meeting in Brussels on 28 January 2016. At that meeting, the progress of related policy issues was discussed, as well as possible next steps and action items for ICANN's upcoming 55th meeting, which will be held in Marrakech from 5 to 10 March 2016. The Commission representative also stressed the importance that the GAC attaches to this working group.

The Commission (DG CONNECT) gave a general presentation of its preliminary plans and dates for the implementation of the CSIRT network and the Cooperation Group (both of which are provided for in the proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, which may be adopted in May this year).

The EEAS reported that it will attend the ASEAN Regional Forum's (ARF) cyber confidence-building workshop in Kuala Lumpur on 2 and 3 March 2016, which will be supported by the NL Presidency, and pointed out the importance of the ARF for cyber stability in that region.

It also provided an update on the possible EU cyber dialogues expected for 2016 (Republic of Korea, Japan and Brazil) and on the follow-up to the OSCE Informal Working Group on cyber CBMs held in Vienna on 12 February 2016.

The new Head of the European Cyber Crime Centre (EC3) presented some of the main challenges ahead, in particular the further development of capacity-building, the fight against online terrorist radicalisation, cybercrime-as-a-service, high-level ransomware activities and crimes related to child sexual exploitation.

He also reported on the three Europol cybercrime-related focal points ('Cyborg', 'Twins' and 'Terminal'), on his intention to continue working and cooperating closely with CERT-EU, and on the recent coordinated European action against money muling, supported by Europol, Eurojust and the European Banking Federation (EBF), in which nearly 700 money mules were identified across Europe and 81individuals were arrested.

3. Monitoring of the implementation of the EU cyber security strategy: reshaped road map

The Presidency presented its proposal for a new approach to the road map as set out in doc. 5776/1/16 REV 1 which takes into account all the relevant EU instruments shaping cyber policy (the renewed Internal Security Strategy, the Digital Single Market Strategy, the Cyber Defence Policy Framework, the Council conclusions on cyber diplomacy, and the EU cyber security strategy) as well as all the new proposed thematic measures and those taken from the previous version of the road map.

Six delegations expressed their overall support of the more simplified structure and the use of the above-mentioned EU cyber instruments to develop the road map. Some Member States suggested to reflect in the road map the Commission's upcoming initiatives in the cyber field. Another delegation defined the road map as a living document and asked for it to be updated with possible actions related to international cyber events. Another delegation requested a more detailed description of the actions to better understand what they meant and were aimed at.

The Presidency pointed out that contact would be made with the Commission to further develop the road map and explained that the current wording of the actions was simply a proposal or suggestion for delegations. It concluded by setting a deadline of 11 March 2016 for written comments on both the new structure of the road map and the content of the actions contained in it. A revised version of the road map, with more developed and precise actions, would subsequently be presented at the next cyber attachés meeting on 8 April 2016, with a view to holding a final discussion at the next FoP meeting on 27 May 2016.

4. Internal security strategy implementation

The Presidency briefed the Group on the state of play and future developments of the Global Forum on Cyber Expertise (GFCE), which was launched in April 2015. It provides a global platform for countries, international organisations and private companies to exchange best practices, lessons learned and expertise on cyber capacity building.

In this context, the Presidency informed the Group about a number of GFCE initiatives to develop best practices in cyber security awareness in certain African countries, in particular its assistance to Senegal to promote cyber awareness.

It also underlined that the FoP would continue to be used as a platform for informing Member States about GFCE initiatives, mainly as regards capacity building.

One Member State informed the Group about a joint initiative with two others to organise an expert meeting on responsible disclosure on 22 and 23 March 2016.

Another delegation reported on the recent formal launch by a number of GFCE members of a critical information infrastructure protection (CIIP) initiative which aims to support the development of CIIP capabilities, especially in developing countries.

The three Member States which have not yet ratified the Budapest Convention on Cybercrime gave an update on their ratification status.

5. Cyber diplomacy: developing a joint EU diplomatic response to coercive cyber operations

The Presidency presented its non-paper set out in doc. 5797/2/16 REV 2 on developing a joint EU diplomatic response to coercive cyber operations, which includes a possible comprehensive cyber diplomacy toolbox. It stated that it deemed it a timely and appropriate discussion.

Overall, delegations welcomed the non-paper and considered it a good starting point for further discussions. They generally felt that discussions should firstly focus on reaching an agreement on the content of the paper, and that Council conclusions could subsequently be a possible second stage. Suggestions were made by some delegations concerning the need for strategic autonomy of digital security and the convenience deterrence effect of the joint EU diplomatic response, among other things.

There were also a number of points of reflection and concern for some Member States, although some delegations felt that they could be overcome and encouraged the Group to continue discussing the issue at further meetings.

These points concerned: situational awareness and the fact that it could be a possible precondition to undertaking the measures provided in the above toolbox; the possible issue of national and EU competences in this specific matter; difficulties in the proper attribution of perpetrators; the need for a proper alignment with the same measures provided in the NIS Directive, which is still to be adopted; the identification of the required measures and time at which they should be activated, and their possible relationship with and/or applicability to the solidarity clause, hybrid threats and CSDP measures; the legal basis; the possible involvement of other working groups and the possible role of NATO.

The Presidency concluded by setting a deadline of 11 March 2016 for written comments on the non-paper and informed the Group that no Council conclusions on the above toolbox were planned at this stage, but that the possibility of 'technical only' conclusions might be explored, to state the EU's need for this kind of mechanism.

6. AOB

The General Secretariat of the Council presented the new delegates portal.