Council of the European Union

Brussels, 6 July 2015
(OR. en)

10362/15

CYBER 63
POLMIL 69
TELECOM 155
RELEX 525
JAIEX 52
COPS 198
IND 107

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	8 June 2015
To:	Friends of the Presidency Group on Cyber Issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda as set out in CM 2768/1/15 REV 1 was adopted with the addition of one information point under AOB by the LU delegation.

2. Information from the Presidency, Commission and EEAS

The Chair briefly presented the cyber-related events outlined in DS 1338/15. Some additional updates regarding the status of the draft NIS Directive, recent events (the Berlin Conference on Cyber Defence and the Hague Global Cyber Security Conference) and upcoming events in June (the Cloud Security Conference and the Digital Assembly in Riga) were also provided. The Chair recalled the recently launched Cyber Hygiene Project and invited MS and EU institutions to consider joining it.

COM (DG Connect) briefly presented the Digital Single Market Strategy adopted on 6 May 2015, focusing on the objectives and actions under each of its three pillars: better access, advanced digital networks and enhancing the digital economy. It also provided an update on recent developments in the area of Internet governance, specifically the Internet Governance Forum meeting held on 26 May 2015 in the US, the South Eastern European Dialogue on Internet Governance (3 June 2015) and the EuroDIG meeting (4-5 June 2015), both held in Sofia, and the approval by COREPER on 29 May of the draft Council conclusions[1] on the transfer of the stewardship of the Internet Assigned Numbers Authority (IANA) functions to the multi-stakeholder community, which is due to take place in autumn this year.

COM (DG Home) gave a general presentation of the European Agenda for Security, adopted on 28 April 2015, where cybercrime was listed as one of the three priorities, and explained that efforts were currently focused on its implementation, which will be a shared task of the EU institutions.

EEAS reported that the cyber dialogues with South Korea and India had been held on 29 April and 21 May 2015 respectively. Various issues with an external dimension had been discussed, such as the multi-stakeholder model, the cyber norms process and cyber capacity.

EEAS also underlined that COREPER had recently approved the lines to take[2] to guide the EU and its Member States in the preparation for the World Summit on the Information Society +10 ('WSIS+10') Review Process. The first meeting of co-facilitators would be held on 10-11 June 2015 in New York.

The Presidency took note of the position of one delegation regarding the need for a collective and proactive approach to ensure that actions taken by each actor at EU level were coherent. The Presidency also took note of the requests by several delegations to receive information in advance in writing, in order to improve internal coordination, and for annotated agendas of group meetings to be circulated.

---

1 9482/15

2 9334/15

3. EU's cyber security, role of FoP and use of the road map - sum-up of the strategic discussion

The Presidency recalled that the discussions on this topic had started at the FoP meeting in February 2015. It was concluded that, in order to avoid duplication of efforts, the group should focus on areas not covered by other groups and that the road map should be considered as the main tool for the organisation of its work. The road map should serve as a basis for measuring achievements and progress in terms of implementation, but also a tool for defining future priorities in the cyber field, which would contribute to the fulfilment of FoP's role and to providing future-orientated and forward-looking political guidance. In addition to exchanging information and sharing good practices, cyber diplomacy was highlighted as one of the areas the group would focus on.

The Presidency pointed out, that in the new revised version of the road map (6183/2/15 REV 2), it had used colours to depict the different nature of the various actions or the stage of implementation that they had reached. An extra column had been inserted to outline ideas for implementation or to propose ways of making progress on certain actions. Delegations were invited to consider these ideas and proposals and to express their views in writing in order to allow the cyber attachés to discuss the document in depth. One delegation suggested that the road map should be a permanent item on the group's agenda and that a list should be drawn up of the meetings and topics for discussion at/for which the cyber attachés had been invited.

Several delegations took the floor to express their support for the new layout of the road map and to point out issues that in their view the FoP's work could focus on, such as foreign and security policy issues, including cyber diplomacy, and the cyber security of EU institutions. They emphasised the need for more coordination and more time for internal preparation in the capitals.

The Presidency took note of the various suggestions made by delegations, specifically that the international agenda should be taken into account when priorities were established; that efforts should continue to be made to provide an overview of cyber developments; that the FoP's coordination role should be strengthened; and that it should have a long-term strategic approach and a clear role, especially in view of the new groups that were likely to be created, such as the one under the draft NIS Directive, in order to avoid duplication.

4. Responsible disclosure policy - introduction and orientation debate

The Presidency introduced the topic outlined in DS 1340/15 by presenting a national cyber attack case involving positive collaboration with the attacker, which had given the impetus to start discussions at national level on the possible application of the responsible disclosure policy. The NL delegation presented its practical experience in this regard. It briefly outlined some of the benefits of this policy, and some of the principles on which it was based. Given the positive national experience, NL had started a joint initiative with HU under the Global Forum for Cyber Expertise as part of its effort to share this good practice with other countries.

Delegations broadly welcomed the discussion on this new practice, pointing out some of the legal challenges they would face if it were to be applied under the current legal framework and stressing the need for a proper legal basis.

The Presidency explained that it would continue to explore the topic, with support from ENISA, and clarified that the joint NL-HU initiative launched within the framework of the Global Forum for Cyber Expertise was aimed at creating an inventory of the application of the policy.

5. International Security Developments in cyberspace and cyber norms

EEAS presented a revised version of its paper (DS 1111/1/15 REV 1) reflecting delegations' comments made at the March cyber attachés' meeting and pointed out that the aim of the paper was to raise awareness of international security issues and to stimulate a debate within the EU. The paper reflected the discussion in the UN GGE and briefly explained the process of confidence-building measures (CBMs) and the application of international law in cyberspace.

Several delegations took the floor to discuss the code of conduct on international security, which had also been presented at the March cyber attachés' meeting, raising the question of the possible need to establish an EU position on the matter given that international security in cyberspace was one of FoP's core objectives. Several delegations underlined the need to increase awareness on cyber norms and CBMs.

One delegation recalled that not all MS were members of the UN GGE and stressed the importance of having a debate at EU level or even a common position, which would facilitate national coordination.

In response the Presidency explained that it would wait for the UN GGE report in late June before considering how to proceed on this topic, and asked delegations to provide written comments.

6. Exchange of good practices: use of Internet for terrorist purposes

The FR delegation made a presentation raising questions related to the understanding of the concept of cyber terrorism, its modus operandi and applicable rules. It stressed the need to assess the capacity to commit crime over the Internet and to keep a proper security level in cyberspace.

COM (DG Home) explained that the Terrorism Working Party (TWP) was following up on a set of guidelines on radicalisation and that the Internet was one of its priority areas. For that purpose a questionnaire had been sent to delegations and a discussion would take place at the next TWP meeting on 15 June 2015. COM also announced the establishment of an IT forum bringing together industry and government to develop counter-terrorism narratives and to limit access to illegal content (including referrals and the possible takedown of such content through Europol's Internet Referral Unit, to be launched on 1 July 2015). COM also mentioned that it was providing funding for the establishment of a serious strategic advisory team and to support the running of the anti-radicalisation network.

7. AOB

The incoming LU Presidency briefly presented its priorities and tentative planning for the work of the group in the second half of 2015. It announced 22 September and 1 December 2015 as tentative dates for the FoP (capital level) meetings and invited delegations and other EU institutions to provide their input.