Council of the
European Union

Brussels, 25 July 2016
(OR. en)

11475/16

CYBER 92
POLMIL 89
TELECOM 140
RELEX 674
JAIEX 77
COPS 252
IND 168
COSI 124

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	22 July 2016
To:	Friends of the Presidency Group on Cyber Issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda, as set out in doc. 3419/1/16 REV 1, was adopted with the addition of one information point under AOB by the Bulgarian delegation.

2. Information from the Presidency, Commission and EEAS

The Presidency presented its overall work programme and priorities, specifying that for cyber issues the focus would be on achieving a coordinated EU approach in cyberspace while ensuring synergies between the various cyber-related policies and working towards a fully functioning digital single market. In addition to the concrete topics to be dealt with by the group, the Presidency also shared its provisional calendar of meetings and cyber-related events.

It provided information on the outcome of the informal meeting of the JHA Ministers held on 7 and 8 July and on the Conference on Cyber Defence held on 20 and 21 July in Bratislava. The topics discussed at these events would be examined further during the Presidency semester.

On its side, the Commission provided an update on the recent developments in the field of internet governance, referring to the latest meeting of ICANN held on 27 June in Helsinki, and to the meeting of the Public Safety Working Group within ICANN's GAC, at which discussions were held on issues related to, *inter alia*, the accuracy of domain name and IP address registration information, the functioning of WHOIS and the registrar accreditation agreements. A brief update was also provided on the two main objectives of the EU Internet Forum – terrorist use of the internet and developing counter narratives – and its upcoming ministerial-level meeting in December was announced.

Finally, the EEAS informed the group that, at the June meeting of PSC, the initiative for a diplomatic toolbox to be used in the event of coercive cyber-attacks had received support. The first deliverable was expected to be ready by the beginning of 2017, and delegations would be regularly updated on its progress. With respect to the cyber-dialogues, the EEAS referred to the one held with South Korea in June as well as to the upcoming dialogues with the US, China, India and Japan, to be held in the autumn. As regards the international agenda, the EEAS drew delegations' attention to the new edition of the UN Group of Governmental Experts in the ICT field, in which six Member States were taking part and which was expected to hold its first meeting in August, as well as to the latest developments in relation to the IANA transition process. A brief update was also provided in the area of cyber-defence, where the latest report on the implementation of the Cyber Defence Policy Framework had recently been presented to PMG, and EDA's feasibility study was discussed.

3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

COM presented its Communication as set out in doc. 11013/16, establishing a link between its objectives, the recently adopted NIS Directive and the contractual PPP on cyber-security launched a few days earlier. Delegations were provided with an explanation of the rationale behind the various measures enumerated in the Communication, which are aimed at supporting the growth of the European cyber-security industry while taking into account the rapidly changing landscape. COM underlined its commitment to creating a blueprint for cooperation, particularly in the event of a major cyber-attack, and an information hub to maximise the use of the various resources available.

In this regard, delegations were informed that the ENISA mandate would need to be revised in the near future as well as that in the area of training and education more synergies were needed to allow for the creation of a cyber-security training platform. Other issues addressed in the communication include inter-sector interdependencies and cyber-security certification and labelling.

Delegations welcomed the presentation of the Communication, which some of them were still scrutinising. They requested additional explanations and information regarding some of the specific measures envisaged therein. They appreciated COM's strategic thinking ahead and expressed general readiness for a political commitment, but underlined the importance of first concentrating efforts on the implementation of the NIS Directive and the measures set out therein. In that regard, the Presidency drew delegations' attention to the list of key messages set out in doc. DS 1373/16, which could serve as the basis for the future Council conclusions containing the political endorsement of the communication. Member States welcomed the idea in general and made some concrete proposals, regarding both the scope and the way of approaching the issues. Following a request from delegations, the Presidency set 20 August as the deadline for written comments, to enable it to present a first draft of these Council conclusions at the meeting of the group in September.

4. Public-private partnerships - exchange of good practices

COM briefly reminded delegations that the contractual PPP on cyber-security (cPPP) was a specific action under the Digital Single Market Strategy, for which the legal basis is the Horizon 2020 Regulation. The preparatory work dated back to January, when a dedicated workshop was organised together with Member States and the cyber-security industry. This led to the creation of an industry cyber-security association which included, in addition to representatives of industry, NGOs and academia, Member States' local, regional and national administrations, and some EEA, EFTA and Horizon 2020 associated countries. The cPPP was officially launched at its formal signing on 5 July in Strasbourg, and was expected to become a COM partner on a number of issues related to cyber-security.

Delegations were also provided with some further details on the structure and practical organisation of the industry association (European Cyber Security Organisation) by its representative, who referred to the assembly meeting and board of directors' election which took place on 7 July in Brussels. He explained that the association has a complex governance structure which reflects the diversity of its members, who come from both the private and the public sector, and from different spheres within these sectors. Members were therefore assigned to different categories, each of which is represented on the board of directors, which is to meet in the autumn of this year. The association would pursue activities in six policy areas, and task forces had been established for that purpose. A high-level round table was planned for the beginning of 2017.

Delegations welcomed the presentation and requested additional information with regard to the possibilities and conditions of participation in the association's work and activities.

5. Implementation of the EU Cybersecurity Strategy

The NL delegation presented the updated version of its concept paper (doc. 8732/1/16 REV 1) dedicated to the issue of cyber-capacity building, and underlined the follow-up measures listed therein aimed at making further progress on this initiative.

COM (DG DEVCO) gave a very detailed presentation of its current projects and funding opportunities, showing the links with the development cooperation processes. COM explained that its focus was twofold: on the one hand, promoting reforms of the legal framework to ensure compliance with international human rights standards and the principles of the Budapest Convention, and on the other hand, supporting technological development and progress. In view of the challenges faced, a process of reflection had been launched to identify the necessary elements to improve effectiveness.

Delegations welcomed the continued examination of this topic. They were in favour of putting in place a more coherent approach in this area and avoiding duplication. In this regard they underlined the importance of looking at the definition of cyber-capacity building to be able to properly map the various EU and national initiatives and projects, building on the mapping done so far by the Global Forum for Cyber Expertise and the Oxford Internet Centre.

Under this point COM (DG CONNECT) gave an update on the state of play of the preparation of the formal launch of the SCIRT network and the cooperation group, as envisaged in the NIS Directive. Member States were informed that the next informal meetings of the SCIRT network were being prepared by ENISA, and that they would look at both cooperation/exchanges with law enforcement and priorities. The preparation of the next informal meeting of the cooperation group in the autumn, at which various aspects of the transposition process would be discussed, was also advancing. COM also clarified the formal requirements to be fulfilled and their deadlines set out in the Directive. Delegations would be kept updated on the advancement of these processes.

6. FOP mandate renewal

The Presidency summarised the answers and written comments provided by delegations, of which a compilation is set out in doc. 10964/16, and drew delegations' attention to several key points outlined in doc. DS 1375/16.

A number of delegations took the floor to express their general satisfaction with the horizontal scope of the group and to support the extension of its mandate, preserving this main feature. Many of those who took the floor spoke in favour of making a long-term commitment and eventually changing the group's status to a permanent working group, given the growing importance of the cyber issues and the need for an appropriate forum to look at all of the different elements related to cyberspace in their entirety.

In this regard, some delegations reiterated the necessity of avoiding duplication with the work done within other Council preparatory bodies and externally by the cooperation group and SCIRT network expected to be formally set up under the NIS Directive. In addition to the 'horizontal' dimension, delegations also looked at the vertical relations with COREPER and the competent Council formations for cyber-related issues.

Delegations deliberated on the implications of a possible change in the status of the group in terms of both its everyday operation (i.e. interpretation regime, reimbursement of experts' travel) and the scope and substance of its activities (i.e. involvement in legislative activities, definition of the specific topics/issues covered, etc.).

Following and on the basis of this initial exchange of views, the Presidency would prepare and present a first draft of new Terms of Reference, to be discussed at the next meeting of the group in September.

7. AOB

The Bulgarian delegation briefly presented the Cyber-Security Strategy recently adopted in Bulgaria, explaining its main pillars and objectives.