COUNCIL OF THE EUROPEAN UNION

Brussels, 25 November 2013 (OR. en)

16446/13

CYBER 32
POLGEN 227
JAI 1026
ENFOPOL 366
TELECOM 318
PROCIV 136
CSC 153
RELEX 1043
JAIEX 95
RECH 548
COMPET 842
IND 337
COTER 145
POLMIL 60

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	30 October 2013
To:	Friends of Presidency (FoP) Group on cyber issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda as set out in doc. CM 4361/1/13 was adopted with the addition under AOB of four information items by the FR, NL and AT delegations respectively.

2. Information from the Presidency, Commission & EEAS

The Presidency briefly reported on the latest relevant cyber issues, notably the adoption of a Directive on attacks against information systems and the issue by the High Representative/Head of the EDA of their final report on the Common Security and Defence Policy (CSDP) in preparation for the December 2013 European Council on Security and Defence. The Presidency also presented a table (DS 1868/13) reflecting cyber-related initiatives in the various Council working parties.

The COM (DG CONNECT) reported on the state of play of the current discussions in the Working Party on Telecommunications on the proposal for a Directive concerning measures to ensure a high common level of network and information security (NIS) across the Union. There had already been a kick-off meeting of the NIS platform at which three working groups were set up, on risk management, information sharing and research priorities.

The COM (DG HOME) reported that they are working on the implementation of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography and for which the deadline was 18 December 2013. A meeting was planned in the US in the autumn of 2014 to discuss achievements of the Global Alliance against child sexual abuse online; as a next step, the possibility of private-sector participation and the terms of such participation was being explored. On the EU-US Working Group on Cybersecurity and Cybercrime, the COM intended to organise quarterly videoconferences to take stock of the activities related to the priorities identified by the Group.

ENISA briefed delegations on the main activities of the European Cyber Security Month (ECSM), held in October, which proved a very successful experience.

The EEAS reported that cyberdefence would be part of the EU's package of CSDP issues to be discussed at the forthcoming European Council in December 2013. On the Conference on cyberspace held in Seoul on 17 and 18 October 2013, there were two main and parallel trends to note: the growing divide on internet governance issues and the need to raise investment for Cyber Capacity Building. When it came to an open, free and secure cyberspace, it was noted that a number of countries were not taking this approach and that the EU therefore needed to keep promoting it. The next conference would be held in The Hague in the spring of 2015.

The EEAS also reported on the EU-China Cyber Task-Force, the last meeting of which was held on 21 October 2013 in Brussels. It was chaired by the EEAS and the COM and 7 MS participated. There was a constructive exchange of views on cyber-related issues and China reported on their recent cyber developments. The EEAS intended to issue a note on this meeting.

3. Report on the activities of the FoP: proposal for renewal of mandate

Presidency presented the report on the activities carried out by the Friends of the Presidency Group on Cyber Issues for the period from December 2012 to October 2013, as set out in doc. 13970/13, and the proposal therein to COREPER of an extension of the mandate by one year under the existing Terms of Reference.

A number of delegations expressed their wish for an extension of the mandate to 3 years to fully anchor the Group in the Council's working landscape and to provide continuity and a longer work span while at the same time maintaining its horizontal, strategic and cross-cutting nature.

There was also a general agreement on increasing the minimum number of meetings to two per Presidency, and the possibility for the Group to have ad-hoc meetings of cyber attachés. One delegation, supported by a number of MS, also stated the need for a minimum level of attendance of senior officials at all Group meetings.

The Presidency concluded that it would revise the activity report and the current terms of reference of the FoP to reflect these proposals, invite COREPER to renew the FoP's mandate to 3 years and endorse the Group's amended terms of reference.

4. State of play & ongoing implementation of the Council Conclusions on the Joint Communication on Cyber Security Strategy of the European Union

The majority of delegations that took the floor welcomed the Presidency initiative to continue the discussions on this issue in the FoP agenda as set out in doc. 14528/13.

A number of MS reiterated the need to avoid duplication of the work of other Council bodies, stressed the need to preserve the strategic, holistic and horizontal aspect of the FoP, without entering into operational activities and called for strategic topics to be discussed, including international cyber policy with a coordinated EU position, capacity building, (high-level) internet governance, management and response of cyber issues, cyber resilience, and input of topics for the next abovementioned cyber space conference in The Hague.

The Presidency initiative to set up the road map described in doc. 14528/13 was also welcomed as it would enable to monitor EU Cybersecurity Strategy and may facilitate the implementation of a bigger number of measures by both the COM and MS. However, different opinions were expressed as to what detail it should contain (i.e. whether to identify who should do what and when).

The Presidency, pending possible written comments to be sent by 15 November 2013, proposed to continue the road map as set out in the concluding remarks in doc. 14528/13. Forthcoming FoP meetings could thus be devoted to the examination of a draft list of measures and the selection of priority measures for which strategic supervision was necessary and, on that basis, define potential measures for their implementation.

5. IE-EE-LT Non-paper on Cyber Security issues

The EE delegation presented their non-paper as outlined in DS 1757/13, describing their main ideas on Cyber Security in view of the adoption of the Cyber Security Strategy of the European Union and the upcoming European Council addressing defence issues. They grouped those ideas into 8 points, namely: filling a policy vacuum, public-private partnership, innovation and technology development, cyber defence in the area of CSDP, institutional capacity building and policy coordination in the EU, crisis management procedures, cyber-related training and education and co-operation with NATO. The non-paper encouraged MS, EU institutions and all relevant stakeholders to strengthen their efforts in the area of cyber security to define concrete proposals and move them forward by means of three strands of work: enhancing cooperation between all actors in the EU, mainstreaming cyber-security and defence in EU crisis management as well as enhancing EU-NATO cooperation in the field of cyber defence.

In general, delegations and the EDA welcomed the ideas expressed in the non-paper, specifying that they would be adequately covered in the implementation of the EU Cyber Security Strategy and the Council conclusions on the Strategy. Some delegations intervened to express their views on the scope of EU-NATO cooperation and the importance of cyber exercises, training and partnership with the private sector.

6. EU Policy Cycle on organised and serious international crime between 2014 and 2017 (EU crime priority "cybercrime")

The EC3 Europol Head of Strategy gave a presentation on this topic and explained the different steps and relevant actors intervening in the structure of the EU priority "fight against cybercrime" which has been split into the following three strands of crime: card payment fraud, child sexual exploitation online and cyber attacks.

7. The EU Integrated Political Crisis Response (IPCR) arrangements

A representative from the General Secretariat of the Council presented this topic, explaining the rationale for integrated crisis arrangements at the EU political level, the decision-making process in this respect and the key supporting elements, highlighting that one of the latter is the permanently available Council-owned web platform, with overall management by the GSC, working together with the Commission, EEAS and MS experts.

The web platform had already been activated three times so far and delegations were provided with examples of potential situations or scenarios where IPCR arrangements could be used.

8. Cyber attachés

The list of cyber attachés was circulated in the meeting room for updating and checking by delegations. By the end of the meeting, 22 MS nominated cyber attachés.

9. AOB

FR reported on their initial ideas for the support, promotion and defence of European industries and services in the fields of information technology and communication (ICT) and cyber security.

NL informed delegations on the updated National Cyber Security Strategy and the Third Cyber Security Assessment. Both documents would follow.

AT reported on the Sino-European Cyber Dialogue, which was an initiative of European and Chinese Academic Institutions to conduct a dialogue as a confidence-building measure in the area of Cyber Security. On the European side, the dialogue was being led by the Austrian Institute of Foreign Affairs and the Geneva Centre for Security Policy. The Dialogue aimed to bring together Chinese and European governmental and non-governmental experts for 1.5 days. The first meeting had been held in July 2013 in Vienna and the next meeting would be in Geneva in March 2014 .