**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 18 December 2013
(OR. en)

17814/13

CYBER 40
POLGEN 265
JAI 1146
ENFOPOL 416
TELECOM 352
PROCIV 150
CSC 188
RELEX 1175
JAIEX 119
RECH 605
COMPET 924
IND 374
COTER 164
POLMIL 66

REPORT

From:	General Secretariat of the Council
On:	3 December 2013
To:	Delegations
Subject:	Summary of discussions

1. **Adoption of the agenda**

The agenda was adopted as set out in CM 5398/13 with the addition of information points by the SE and CZ delegations.

2. **Information from the Presidency, Commission & EEAS**

The Presidency gave information about the renewal of the mandate for 3 years and the endorsement of the amended Terms of Reference as set out in 15111/13.

The Presidency also stated that the next round of mutual evaluations dealt with by the GENVAL Working Group would be on cyber crime, for the purpose of which a first draft of the questionnaire (doc. 16369/13) was presented and discussed on 27 November 2013.

DG CNECT reported on the progress in negotiations on the NIS Directive, and expressed optimism (not shared by one MS) that trilogues could be started in early 2014 with the aim of reaching an agreement before the end of this parliamentary term. DG CNECT also announced that the High-Level Conference on the Cyber Security Strategy implementation would take place in late February 2014. DG CNECT explained that discussions relating to the project committee on Horizon 2020 had almost been completed and that the December European Council on cyber defence would deal with some civilian aspects of cyber security.

DG HOME added that the High-Level Conference would coincide with the publication of the Strategy implementation report. MS would need to state their progress as COM would provide information only on those actions it had carried out itself as part of the Strategy. DG HOME also stated that negotiations on the MFF (home affairs) had almost been concluded and that two thirds of the allocated funding would be managed by MS, with one third managed by COM. Furthermore, DG HOME announced that the first year of EC3 would be celebrated with a event on 20 January 2014 and stated that the Eurobarometer on cybersecurity had been released in November 2013.

EEAS presented two UN and one UNESCO cyber-related initiatives (described in doc. 17030/13), highlighting the attempts to introduce a new global legal instrument on cyber issues which the EU was opposed to and was, thus, promoting the Budapest Convention. In addition, EEAS suggested that MS attending such international fora should be accompanied by diplomats from their foreign affairs ministries.

3. **Implementation of the Council Conclusions on the Joint Communication on the Cybersecurity Strategy of the European Union: Cyber-policy development in the field of industry & technology**

The Presidency briefly stated that the implementation of the Council conclusions on the Joint Communication on the EU Cybersecurity Strategy had been discussed at the last two FoP meetings and delegations had expressed their general support for the Presidency initiative to set up the road map as outlined in doc. 14528/13. One MS had provided written comments asking that a methodology and a work programme be determined for the FoP.

The Presidency suggested first examining the field of industry & technology as a follow-up to one of the main topics of the last European Council conclusions (doc. EUCO 169/13), the digital economy, innovations and services.

– **Big data and cloud computing**

DG CNECT gave a presentation on cloud computing, explaining the next steps in this field following the last European Council conclusions, i.e. promoting high standards, single market, European cloud partnership and national digital coordinators. DG CNECT also gave information about the state of play and the progress made in respect of the Strategy on "Unleashing the Potential of Cloud Computing in Europe", which is designed to speed up and increase the use of cloud computing across different sectors of the economy. The relevance of the European Cloud Partnership Steering Board and of the Cloud for Europe project, which had started in June 2013, was underlined.

After explaining what made the cloud critical for big data, DG CNECT listed the main links between the last European Council conclusions and big data – digital innovation, technologies building on big data, the digital single market and the improvement of public services, and described the reasons why big data was so important, in particular as it was currently fuelling the growth of the knowledge economy.

A number of delegations thanked DG CNECT for the presentation and underlined its value for the FoP, highlighting the need for the EU to be competitive and for the public to be informed about what big data and the cloud were, as well as the importance of performing a cyber mapping in Brussels in order to know what was being done to ensure consistency between the European Council conclusions and the Cybersecurity Strategy.

– **FR non-paper on the support, promotion and defence of European industries and services in the fields of ICT and cybersecurity**

The FR delegation presented their non-paper as in doc. DS 1975/13, stating the importance of grasping the momentum and starting the discussion in this field, as there was a high dependence on companies outside EU and the European Council in February 2014 would also address these issues. The intention of the non-paper was to provide food for thought and launch ideas. FR expressed its satisfaction with the COM report on R&D.

EDA stated that the December European Council was of great importance for them, as it looked into the security of value and supply chains. Four MS took the floor to support and welcome the FR document. A number of issues, along with a sound education system, were stated as relevant to improve competitiveness – establishment of the digital single market, global standards, businesses functioning in a open environment and encryption capacity. Some doubts were expressed whether Horizon 2020 could meet these broad needs.

COM also welcomed the FR non-paper and the subsequent discussion, and expressed its willingness to give a presentation mapping the state of play of Horizon 2020 at the next FoP in preparation for the upcoming European Councils in 2014.

– **Orientation debate**

As there were no interventions by delegations on doc. 16742/13, the Presidency set 23 December 2013 as a deadline for written comments, and concluded that the road map as set out in doc. 14528/13 for the implementation of the EU Cybersecurity Strategy and the Council conclusions was agreed.

4. **New Emergency Response Team service for the Spanish private sector and strategic operators**

The ES delegation outlined the latest cybersecurity initiatives in Spain, notably the National Security Strategy, which defined the main cyber security actions, the Digital Agenda, which reflects the Government's strategy for the economy and digital society development for the 2013-2015 period, and the National Cybersecurity Strategy, currently under finalisation with the involvement of four ministries.

The ES delegation also presented the Cybersecurity Coordination Office, which was the point of contact in the Ministry of Interior for issues related to cybersecurity, and explained that the CERT for Security and Industry which was created within the Ministry in order to provide an adequate response to cyber incidents had greatly facilitated liaisons with the specialised law enforcement units.

5. **Presentation by the incoming EL Presidency of their programme for FoP**

The EL delegation stated their intention to continue both the work started by the LT Presidency on the Strategy implementation by focussing their efforts on operational cooperation among MS, and the discussion of cyber-relevant topics such as Internet governance and exchange between MS of their experiences, technology used and methodology followed to solve problems. It was underlined that the FoP would be regularly updated on developments regarding the NIS Directive. The EL delegation also announced that an event on Cyber issues would be held in Athens on 6 and 7 March 2014. The FoP meetings were planned to take place on 24 February, 26 March and 14 May 2013.

DE suggested that Cyber resilience be discussed in cyber attaches format.

6. AOB

The SE delegation presented their ideas on the future of the Internet (doc. DS 1976/13) and called for substantial discussion in the FoP on the related international strategic challenges. The SE delegation saw an urgent need for increased coordination among MS in close cooperation with the EEAS and COM. Therefore, the SE delegation proposed that EEAS prepare a food-for-thought paper identifying how to address these challenges together. That proposal and the SE non-paper were supported by five MS, one recommending that the issue be dealt with at the next FoP meeting, and the EEAS agreed to proceed that way.

The CZ delegation presented information about the recently created cybersecurity platform composed of national CERTS from AT, CZ HU, PL and SK, which meets at NIS directors level. Its initial meeting was held in Prague in 2013. The platform intends to share information and experience among its members, to promote mutual consultations for the EU and NATO and other fora, and to plan a joint cyber exercise. CZ was currently chairing the platform and next year this will be taken over by AT.

––––––––––––––––