COUNCIL OF
THE EUROPEAN UNION

Brussels, 13 December 2012

17414/12

**POLGEN 212
JAI 885
TELECOM 251
PROCIV 213
CSC 88
RELEX 1126
JAIEX 123
RECH 458
COMPET 762
IND 228
COTER 122**

OUTCOME OF PROCEEDINGS

of:	Friends of Presidency (FoP) Group on Cyber issues
on:	3 December 2012
Subject :	Summary of discussions

1. Adoption of the agenda

The agenda as set out in doc. CM 5559/12 was adopted.

2. Presentation of the FoP Group and scope of activities

The Presidency presented the FoP Group and the scope of its activities, as set out in doc. 15686/12. The Chair highlighted that the Group had been created to ensure horizontal coordination of cyber policy issues in the Council and examine any relevant horizontal issues, without prejudice to the existing mandate of other Working Parties.

SE welcomed the activation of the Group and underlined its complementary role rather than replacing the activities of other groups.

3. Presentation of the state of play of the Proposal of the European Strategy for Cyber Security

The COM focused on the main reasons for further EU action on cyber security and explained the main aspects of the draft European Strategy for Cyber Security which are the following:

- principles and values guiding EU activities;
- strengthen security and resilience of network and information systems;
- prevent and fight cybercrime, and
- address cyber defence and develop an external EU cyber security policy.

The COM also described the roadmap for the European Strategy for Cyber Security: After consultation of the stakeholders, the target adoption date for the Communication on the European Strategy for Cyber Security, and the accompanying legislative proposal (most probably a directive) on network and information security, would be the end of January 2013. The follow-up discussions would then take place in the Council (where the FoP on Cyber Issues may play a steering role in the discussion on the Communication on the European Strategy for Cyber Security), followed by an implementation report and an annual conference on Cyber security.

SE called for a global and broader approach to the strategy that should focus on cyber and not be limited to cyber security. UK and NL supported the SE intervention.

4. International activities in Cyber issues

The EEAS presented a non paper about the international activities on cyber issues and made specific reference to the idea of having cyber attaches to the Permanent Representations. Some delegations supported this idea as a means for the capitals to better coordinate and be more effectively updated on cyber issues (not for taking decisions). A number of delegations also suggested having more participation or information with regards to bilateral talks on cyber issues (EU-China, EU-India, etc) and mentioned the role that the FoP could play in developing an EU position for these international cyber foras. Delegations also felt that the EU-NATO communication in cyber issues could be improved.

EE announced that it was organising a Cyber Security Conference in Brussels on 13 January 2013.

UK highlighted the importance of capacity building, sharing best practices and a good reliable trust and mentioned a recent UK initiative that will invest 2 million GBP a year in a Centre that will focus on capacity building of administrations in order to manage the challenges of cyber security.

The Presidency concluded that the FoP Group took note of the issue of having cyber attaches in Brussels and underlined that the FoP could assist the EU in international cyber matters.

5. Information from Agencies (EDA, ENISA and EUROPOL) on recent and future relevant developments on Cyber issues

The EDA representative presented the following military aspects of cyber:

- critical functions increasingly dependent on cyber domain;
- military is increasingly dependent on civilian (critical) infrastructures and services;
- constant growth and increasingly complex and interconnected networks (NEC) and
- rapid development of new threats and vulnerabilities.

He highlighted that the FoP may play an important role in some EU cyber defence aspects of the "Pooling & Sharing Opportunities" and mentioned EDA as a focal point and facilitator for MS for collaborative European military capability development and Research for Cyber Defence.

The ENISA representative explained several of its cyber-related activities in relation to protecting critical information infrastructure, participation in cyber exercises and the lessons learned. ENISA is also preparing a "good practice guide" which will describe, among others, good practices, standards and policies; the elements of a good Cyber Security Strategy and challenges in developing and maintaining a Strategy. He underlined the importance of the existing national cyber security strategies in the MS. He also underlined how ENISA assists operational communities and explained the role of the agency in security and data breach notifications.

The EUROPOL representative focused on the European Cybercrime Centre, the collection of information from the relevant actors and its integration by the agency. He referred to the importance of training on capacity building not only for law enforcement bodies, but also for prosecutors and stressed the relevance of the coordination with other agencies, MS, Interpol and the private sector.

6. Handling a cyber incident and the need for cross border cooperation. Presentation by the Director Cyber Security in the Netherlands

The Director of Cyber Security in the Netherlands described a real cyber attack which highlighted, among others, the detection, escalation and wide reaching effects of an incident as well as the interdepartmental crisis handling, the cross border effects and the follow through practices. Some important lessons learned were identified from the incident, notably that the international CERT-community is an important structure on operational level and the PKI (Public Key infrastructure) has become a critical infrastructure in itself.

The COM pointed out the importance of developing cyber risk management and the EEAS underlined the need for contingency plans and how this kind of incidents may reach the threshold of becoming an incident which requires a national crisis management.

7. Any other business

The COM (DG Home) informed the group about the launch of the Global Alliance against Child Sexual Abuse Online and the conference which would take place on 5 December by the EU Commissioner for Home Affairs together with the US Attorney General. The initiative aims to unite decision-makers all around the world to better identify and assist victims and to prosecute the perpetrators. Participants at the launch include Ministers and high-level officials from 27 EU Member States, who are also joined by 21 countries outside the EU.
The countries of the Alliance are committing themselves to a number of policy targets and goals. Thanks to increased international cooperation, the fight against child sexual abuse online should become therefore more effective.

The meeting concluded with a brief description of the programme of the incoming EU Presidency which intends to identify in an early stage the number, dates and likely content of forthcoming meetings in the IE Presidency.

It was underlined that those MS which had not yet done so, should designate the national focal point(s) on cyber policy issues, as set out in doc. 15686/12, and communicate their contact details to cyber@consilium.europa.eu.