**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 5 March 2013

7062/13

**POLGEN 31
JAI 178
TELECOM 38
PROCIV 33
CSC 24
CIS 7
RELEX 185
JAIEX 18
RECH 55
COMPET 125
IND 57
COTER 29
ENFOPOL 66
DROIPEN 26
CYBER 4**

OUTCOME OF PROCEEDINGS

of:	Friends of Presidency (FoP) Group on Cyber issues
on:	25 February 2013
Subject :	Summary of discussions

1. Adoption of the agenda

The agenda was adopted as set out in doc. CM 1626/13 with the addition of that the issue of cyber attachés under AOB.

2. Joint Communication on the Cyber Security Strategy of the European Union. Presentation, handling and discussion

The COM (DG Connect and DG Home) and the EEAS gave presentations on their respective elements of the strategy. DG Connect explained both the principles and values guiding EU activities and the strategic priorities.

DG Home also focused on the fight against cybercrime and mentioned other current EU cyber initiatives in this field (European Cybercrime Centre, the fight against child sexual abuse online, the EU-US working group on cyber security and cybercrime, and the EU network of national centres of excellence for cybercrime training, research and education which has existed since 2010). The EEAS underlined the aspects relating to the EU external policy, inter alia: internet freedom and human rights, international security, capacity building assistance, promoting the Budapest Convention on cybercrime, accountability and stability of the internet and relations with partners and international organisations.

A large number of Member States took the floor and comments were in general supportive of the strategy, along the lines that the five strategic priorities were well identified and underlining the correct balance of the cyber security strategy.

A number of Member States questioned the funding of the strategy, with the COM responding that there was a reference in footnote 32 of the strategy to this subject and that in the main, the budget for the actions points would come from existing budgets.

Some delegations also felt that the EU-NATO communication in cyber issues could be improved. BE noted that the use of the solidarity clause in cyber security should be analysed after discussions in the other working parties dealing with this matter.
The UK stated that the action points in the strategy should be prioritised via Council conclusions and implementation of the actions points should only start after that.

The Presidency explained its intention to produce Council conclusions by the end of its term and informed the FOP that a number of working parties in the Council had been invited to discuss the strategy within their own remit and submit their views by 28 March. Member States may also wish to coordinate their contributions on a national basis and send them to cyber@consilium.europa.eu by the same date. Using this input, the Presidency intended to circulate a first draft of the Council conclusions to the FOP group by April 15 with a view to a discussion at the next FOP meeting scheduled for the last week of April.

The Presidency also clarified that the proposed Directive on Network and Information Security would be dealt with solely by the Telecommunications working party.

3. Overall report on the various strands of on-going work and on future activities and priorities.

The Presidency referred to the terms of reference of the FoP on cyber issues (doc. 15686/12) which stated that the Group was expected to meet at the beginning of each new Presidency to take stock of the state of play in the field and identify the key issues of relevance to its work. The Presidency mentioned as one of these key issues the recent successful conclusion of the negotiations on a new mandate for ENISA. To enter into force, the text still needed to be formally approved by the Parliament, whose vote in plenary was expected to take place before the summer, and by the Council after that.

The meeting agreed that the FOP was an appropriate strategic forum for the EEAS to report on its negotiations on cyber issues with third countries, without interfering with the mandates of other working parties.
SE highlighted that the FoP could be a very efficient instrument for strengthening overall performance in bilateral and multilateral international fora. FR underlined that the FoP should be briefed on these issues in advance of the bilateral/multilateral dialogues.

4. Any other business

The meeting agreed on the Presidency proposal that each Member State nominates a cyber attaché based in Brussels, who would be able to take part in the FOP meetings at attaché level. The delegations were invited to send the nominations to cyber@consilium.europa.eu.