COUNCIL OF THE EUROPEAN UNION

Brussels, 25 July 2013 (OR. en)

12777/13

CYBER 17
POLGEN 150
JAI 673
ENFOPOL 256
TELECOM 216
PROCIV 94
CSC 79
RELEX 711
JAIEX 63
RECH 377
COMPET 599
IND 225
COTER 110
POLMIL 48

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	15 July 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 3581/13 was adopted with the addition of an information point by the Presidency under AOB.

2. Information from the Presidency, Commission and EEAS

The Presidency briefly informed about the upcoming informal Council meeting to be held in Vilnius on 18-19 July 2013 stating that a discussion paper has been produced and disseminated in order to facilitate the deliberations on the JHA contribution to improved cybersecurity. Delegations were further notified that the EDPS (doc. 11408/13) and the Committee of the Regions recently published their opinions on the European Cybersecurity Strategy and that a Resolution of the European Parliament on the same matter was expected to be endorsed in plenary in September this year.

The COM (DG Home) informed that as outcome of the video conference held earlier this month in the framework of the EU-US Working Group on Cybersecurity and Cybercrime 5 key priorities were identified, namely: the practical challenges to transborder cybercrime investigations (to be discussed at the September meeting), the exchange of tools and training material and best practices for cybercrime law enforcement, the common approach in international organisations and fora, where calls for new cybercrime instruments were made, the law enforcement orientation debate on the consequences of the transition from IPv4 to IPv6 and the follow-up and expansion of participating countries (currently 50) in the Global Alliance against Child Sexual Abuse online. In regard to the latter, COM was collecting reports from the participants in order to prepare and publish a threat report in the fall.

EEAS provided some details regarding the upcoming Conference on cyberspace to be held in Seoul, 17-18 October 2013, as a follow-up of the London (2011) and Budapest (2012) ones, which will focus on economic growth and development, social and cultural benefits, cybersecurity, international security, cybercrime and capacity building. EEAS would provide support to this process and would take part in some of the meetings. The preparatory meeting was held on 6 June in Budapest. HU and UK delegations added to these explanation that the Conference was meant to be a high level political event with global reach both geographically and content wise (i.e. "cyberspace") with active involvement of the private sector and international organisations. The conference was expected to produce a stock-taking document and a summary of the proceeding. Several delegations stressed the need for participating MS to have the same EU message and underlined the importance of human rights and freedoms being applicable online and being guaranteed by proper check and balances.

EEAS also briefly mentioned that the issue of the US NIS surveillance was currently steered by COREPER with the involvement of the relevant authorities, that the EU-China meeting was expected later this year and that the EU-India one was postponed to the fall.

3. State of play & Ongoing implementation of the Council Conclusions on the Joint Communication on Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace

Presidency presented doc. DS 1563/13 underlining that the 4 options stated therein were ideas for discussion but that the final solution might be a combination of these options or a totally different one.

The majority of delegations that took the floor welcomed the Presidency initiative to include this issue in the FoP agenda. They called for avoidance of both the duplication of the work of other Council bodies and the establishment of project groups which would overload the work of the FoP. They stressed the need to preserve the strategic and holistic aspect of the FoP, without falling into operational activities. Some delegations expressed a preference for the Trio Presidency program (option 2) and proposed to create a list of the cyber security priorities that should be addressed where others voted for a model closer to an action plan (option 1) or a combination of these options. One delegation was of the view that a purely supportive role of the FoP (option 4) should be ruled out as the FoP must steer and drive the ongoing implementation of the Council conclusions. Following the request for more time to study these options the Presidency set 16 September 2013 as deadline for written comments.
The COM stated that the EU Cybersecurity Strategy had already the elements to be considered an action plan and provided some examples in support of the fact that its implementation has already been started. MS were invited to develop their individual national Action Plans.
EEAS welcomed the discussion and underlined the need to look at the FoP mandate, i.e. strategic horizontal approach on cross-cutting issues and agreed that the implementation had already been started and it was proceeding.

4. CSDP aspects of the EU Cyber Security Strategy

The FR delegation presented their non-paper outlined in doc. DS 1564/13, describing the main ideas grouped in 6 points, namely: cyber security of CSDP-related networks, the cyber dimension, CSDP exercises, training in the field of cyberdefence, military cyberdefence and EU-NATO cooperation. In general, delegations and EEAS welcomed the ideas expressed therein, specifying that they would be useful for the preparation of the European Council in December and therefore should be further addressed in the relevant working parties. Several delegations were of the opinion that EU-NATO cooperation should not be kept as a separate item, but should rather be streamlined and reflected in all the security efforts. A number of delegations raised the concern that proper definitions of "cybersecurity", "cyberdefence", "cyber resilience", etc. were lacking at EU level and neither the EU Cybersecurity Strategy, nor the proposed NIS Directive were providing a remedy to that situation. In addition one delegation suggested to add the "cyber diplomacy" to the list of issues addressed in the FR non-paper.

5. Exchange of best practices

ENISA presented their good practice of assisting MS in the preparation of a National Cyber Security Strategy (NCSS), explaining ENISA's role in the process and the NCSS related activities in 2012 that led to the publication of a Good Practice Guide and other soft law instruments. It was stressed that a complementarity approach was used in order to make the most of MS expertise and to ensure that the deliverables were a collective achievement. ENISA's representative listed the main recommendations to MS while establishing a NCSS and outlined as future steps the preparation of a training kit on how to develop and implement a NCSS. Currently 15 MS have a NCSS.

EUROPOL presented several practical examples of successful cooperation in combating cybercrime, underlining three key principles bringing the relevant partners together, coordinating the efforts and information sharing.

Presidency invited delegations to share their best practices at the next meeting and asked those who volunteer to do so to announce this by 16 September 2013.

6. AOB

The Presidency repeated the request to delegations to nominate a cyber attaché and to communicate the name and contact details to cyber@consilium.europa.eu.

Delegations were informed that the Working Party on General Matters, including Evaluation (GENVAL) was currently examining "cybercrime" as a possible topic for the 7th round of mutual evaluation and were advised to coordinate their national position.

As items for the next meeting to be held on 11 October 2013 the Chair indicated the renewal of the FoP mandate, exchange of best practices and discussion of the Council Conclusions on the European Cybersecurity Strategy implementation.