Council of the European Union

Brussels, 15 October 2015
(OR. en)

12918/15

CYBER 96
POLMIL 87
TELECOM 189
RELEX 805
JAIEX 73
COPS 307
IND 152

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	22 September 2015
To:	Friends of the Presidency Group on Cyber Issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda as set out in CM 3653/1/15 REV 1 was adopted with the addition of three information points under AOB by the UK, NL and LU delegations.

2. Information from the Presidency, Commission and EEAS

The Presidency invited Member States to attend the upcoming Conference on Mutual Legal Assistance (MLA) in the Digital Age to be held in Luxembourg on 15 October 2015. The Commission (DG Home) welcomed the conference, which could be helpful in finding out how to overcome one of the main obstacles that law enforcement authorities currently face in fighting cybercrime.

The Commission (DG Home) gave information about the first preparatory meeting held on 24 July 2015 in preparation for the official launch in December of the EU IT Forum to help counter terrorist propaganda and address concerns about new encryption technologies. On 22 October 2015, there would be another meeting to prepare this launch.

As regards the Directive on attacks against information systems, those Member States which had not yet done so were reminded to send notifications to the Commission on the implementation status of the Directive.

The Commission (DG Connect) gave an update on the upcoming European Cybersecurity Challenge (ECSC), which was to be held in Switzerland in October this year as an initiative by ENISA and the organisers of the national cyber security challenges. It stated that many European countries had set up national cyber security competitions for finding young cyber talents, encouraging them to pursue a career in cyber security, and that the ECSC leveraged these competitions in and added a pan-European layer to them: the top cyber talents from each country would come together and meet, network and collaborate. Finally they would compete against each other to determine the winner of the ECSC. There were participants from AT, DE, ES, RO, UK and CH as host. Detailed information on the ECSC can be found on the web link http://www.europeancybersecuritychallenge.eu

EEAS announced that the EU-US cyber dialogue would be held in Washington DC on 8 December 2015, the EU-China Task Force on 17 or 20 November 2015 and the EU-Japan Cyber dialogue in late November 2015 (the date had not been fixed yet). It also explained that a six-monthly progress report on the implementation of the Cyber defence policy framework had been agreed in the Politico-Military Group (PMG) and endorsed by the Political and Security Committee (PSC) in June 2015. The discussions had helped the cyber defence experts to review the actions needed in order to adjust them to the evolving priorities and needs related to cyberspace.

The ASEAN Regional Forum (ARF) Cyber Confidence Building Measures (CBMs) Workshop was being organised by the EU (with special support from NL and EEAS) and Malaysia. It would take place in March 2016. The EEAS hoped that this workshop would be able to build on previous engagements in ARF and offer more concrete and practical steps forward in the field of cyber CBMs within ARF.

Europol extended an invitation to the annual Europol-Interpol Conference in the Hague, 30 September to 2 October 2015.

ENISA briefly presented the findings of their freshly released Annual Incidents Report 2014.

3. International cyber issues

The first international cyber issue discussed under this item was related to the preparations for the World Summit on the Information Society +10 ("WSIS+10") meeting in New York in December 2015. A number of delegations took the floor to express the need for a constructive and common EU position on the WSIS+10 non-paper proposal given the short timeframe and urged to use as guidance the recently adopted Lines To Take (LTT) on the WSIS+10 Review Process (9334/15) thus avoiding any drafting initiative at the meeting.

The second part of the discussion under this item was devoted to the UN GGE Report issued during the summer, the Russian Resolution on developments in the field of ICT in the context of international security and the Chinese Code of Conduct. The delegations that took the floor welcomed the GGE report, expressed the view that the Russian Resolution was a good starting point but underlined the need to work on its current wording and upheld the multi-stakeholder model vs. the multilateral one. Some views were exchanged on the use of the notion "globalisation" versus "internationalisation" of Internet Governance.

Finally under this item the Commission (DG Home) presented the Public Safety Working Group of ICANN's Governmental Advisory Committee (GAC), which had been created to advise GAC on aspects of ICANN's policies and procedures that implicate the safety of the public when using the Internet. Two delegations announced that they intended to participate in the Working Group and would make sure that Law Enforcement Community provided its input.

4. Cybersecurity Strategy implementation: Cooperation with the private sector

The Presidency presented its paper on cooperation with private sector (11743/15), which outlined the outcome of discussion at the cyber attaché meeting held on 17 July 2015, compiled the subsequent written submissions and raised the potential involvement of the FoP in the set up of the contractual cybersecurity public-private partnership (PPP) as provided in the Digital Single Market Strategy and whose launch is planned for mid-2016.

The Commission (DG Connect) presented this PPP initiative, and informed delegations that it was going to use Horizon 2020 (H2020) as a legal basis and underlined the need to have a single EU market for EU solutions and services. Some delegations welcomed this initiative and asked what the Member States' role would be and how the new PPP would relate to the existing NIS platform. The Commission replied that MS would be closely involved in the process.

The Presidency concluded that this matter would be followed up.

5. Internal Security Strategy implementation

The Presidency announced its intention to start discussions on the way forward as regards the FoP contribution to the implementation of the renewed Internal Security Strategy, as set out in 10854/15, and that it would dedicate some more time to the actions provided for therein, in particular to the one related to the legal and operational obstacles for the Law Enforcement Community to fight cybercrime, which should be discussed at the next cyber attachés meeting.

6. AOB

The NL delegation presented a follow-up on responsible disclosure, which had already been discussed at the last FoP meeting on 8 June 2015. The Presidency would formally invite ENISA to gather information from Member States on how they dealt with this issue at national level.

The UK asked delegations to become involved in the Abu-Dhabi Seminar on Child Sexual Exploitation (CSE) and announced that it had invested in a UNICEF-related project to prevent CSE online and invited other MS to do so as well.

The LU delegation presented briefly their second Cybersecurity Strategy.

The Presidency announced that the next FoP at capitals' level will be held on 1 December 2015.