Council of the
European Union

Brussels, 20 October 2017
(OR. en)

13527/17

CYBER 158
COPEN 312
JAI 953
POLMIL 120
TELECOM 247
RELEX 888
JAIEX 82
COPS 322
IND 268
COSI 243

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	26 September 2017
To:	Horizontal Working Party on Cyber Issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda as set out in CM 4146/17 was adopted with the addition of information points by the DE and UK delegations.

2. Cybersecurity package - initial discussion with a view to a discussion on Council Conclusions

The Commission presented its cybersecurity package consisting of an impressive number of documents, including a proposal for a new ENISA mandate and a cybersecurity certification framework ('Cybersecurity Act'), a Joint Communication on Resilience, Deterrence and Defence and a Recommendation on coordinated response to large-scale cybersecurity incidents and crises.

In its presentation the Commission (DG Connect) stressed that the Joint Communication was a strategic document supplementing the 2013 EU Cybersecurity Strategy (which remains valid), with a special focus on three policy objectives: achieving cyber resilience, reducing cybercrime, and developing cyber defence. The Commission underlined that cyber threats had evolved significantly since the adoption of the 2013 Strategy; accordingly, there was a need to strengthen ENISA's role by giving the agency a permanent, wider mandate enabling it to engage in long-term planning and provide strategic analyses to Member States and other relevant stakeholders.

Regarding the proposed Cybersecurity Act, the Commission explained the rationale behind combining the two elements, underlining the important role ENISA was expected to play with regard to the proposed certification framework and emphasising the voluntary nature of the scheme. The Commission also briefly presented its recommendation on coordinated response to large-scale cybersecurity incidents and said that the aim was to test it in a cyber exercise next year. The Commission also outlined its Communication on the implementation of the NIS Directive, which contained analyses of the most relevant issues and practical suggestions to support Member States in that process.

The Commission (DG Home) highlighted the cybercrime-related initiatives outlined in the cybersecurity package, explaining the importance of integrating law enforcement into the general prevention and response framework, creating the right procedural framework, supporting investigative capacities and increasing accountability online. It briefly presented its proposal for a Directive on fraud and counterfeiting of non-cash means of payment, before touching on the ongoing work on cross-border access to e-evidence and the forthcoming legislative proposal, as well as the initiatives aimed at supporting Europol as a centre of expertise for cyber investigations and cyber forensics, improving the functioning of WHOIS database and tackling criminality on the dark web.

Lastly, the EEAS described the external dimension, stressing in particular the importance of developing cyber-defence capabilities, training and education, advancing the EU's defence technical and industrial base, strengthening EU/NATO cooperation on cyber issues, and providing assistance to third countries in building their cyber capabilities. The EEAS emphasised the importance of protecting human rights and the freedom of the internet, observing that existing international laws, norms and principles should be reaffirmed and further promoted in cyberspace. The importance of the Joint EU Diplomatic Response to Malicious Cyber Activities was highlighted in this connection.

Delegations welcomed the Commission's presentation and the opportunity to express their views on the package as a whole. Nearly all of them took the floor to express their general satisfaction with the impressive work done in preparation for the package. Member States stressed that it was important that the package addressed challenges related to IOT, ipv6 and cyber defence matters, including EU-NATO cooperation and a coordinated EU response to cyber incidents. They also requested clarification with regard to some of the proposed initiatives, including those relating to dual-use in cyber defence, the proposed cybersecurity research and competence centre and the functioning of the certification schemes vis-à-vis national schemes. Delegations also expressed some concerns, for example in relation to the scale of the tasks envisaged in the ENISA proposal, in particular the agency's operational capacity, the creation of a European certification framework and its relationship to national schemes and global standards, and the possible burden for SMEs. Finally, some delegations questioned the idea of combining the certification scheme and ENISA's mandate into a single legislative proposal and suggested that two separate proposals be drawn up. In response, the Commission tried to provide further explanations on how the two were interlinked, given the envisaged involvement of ENISA in the development and implementation of EU policy on ICT security certification. It agreed on the need for more detailed discussion, and reassured delegations that the creation of an EU certification framework would reduce fragmentation and have a positive impact on the internal market.

After the discussion, the Presidency invited Member States to provide written comments containing the key messages they would like to be included in the text of the Council conclusions it was planning to put on the table at the next meeting of the working party.

3. Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities

Delegations held a final round of discussions on the third revised version of the draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (8946/3/17 REV 3). A number of additional suggestions for improving and/or clarifying the text were made and a number of compromises for the modification of text were agreed during the meeting.

The Presidency explained that, on the basis of this outcome, a new revised version would be drafted and subject to silent procedure before the text was submitted for approval by the PSC.

4. Initial informal comments by ECSO members about the cyber package

Representatives of the ECSO shared their preliminary informal comments on the cybersecurity package presented by the Commission, specifying that these comments did not constitute the official position of the ECSO, which was expected to be adopted soon. They welcomed the initiative addressing in particular the issues of certification, implementation of the NIS Directive, public-private cooperation and the cyber expertise gap in view of establishing a successful EU cybersecurity policy.

Following the presentation, the Presidency invited the ECSO to provide its official position for the next meeting on 6 October 2017.

5. Defence Ministers' table-top exercise CYBRID 2017 – debrief and lessons identified

The EE delegation provided information on the outcome of the first strategic table-top cyber defence exercise organised by the Estonian Ministry of Defence and the European Defence Agency using a fictitious scenario - a major offensive cyber campaign against EU military structures in a hybrid warfare context. The exercise was considered a useful tool for testing policy and procedures in the area of cybersecurity, including those related to information sharing and EU-NATO cooperation. The Defence Ministers welcomed the exercise as well as the opportunity for discussion it afforded. The exercise was the first element of the EU Pace exercise scheduled to be held at a later date.

6. European Cybersecurity Month 2017

ENISA presented an overview of the initiatives and Member States' involvement in the 2017 edition of European Cyber Security Month - an EU awareness campaign promoting cybersecurity in Europe. It explained that this year the slogan would be 'Cybersecurity is a shared responsibility' and a dedicated website would be set up. ENISA announced that 24 Member States would take part and a number of cybersecurity events were also planned at EU level. It stressed that European Cyber Security Month was also part of the global efforts in this area, as similar initiatives would run in parallel in the US, Japan, Australia and Canada. In addition, ENISA mentioned the Commission initiative to train Member States' 'Cyber Ambassadors'.

7. Information from the Presidency, Commission and EEAS

The Presidency briefly presented the outcome of the Cybersecurity Conference recently held in Tallinn, entitled 'Digital Single Market, Common Digital Security 2017', and of the Cooperation Group meeting.

The Commission provided an overview of the state of play on encryption and electronic evidence following the two expert meetings organised on 15 and 18 September 2017 respectively.

The EEAS informed about the upcoming meeting of the EU-China Taskforce, to be held on 19 October 2017 in Beijing, to which the Member States had been invited to participate as observers.

8. AOB

The UK delegation invited delegations to the event they were organising on 23 October 2017 dedicated to the question of how to protect democratic elections from interference, including through ICT means, and in this context to discuss how to support the EP in its upcoming elections in 2019.

The DE delegation highlighted the need to protect human rights and promote international law in cyberspace and invited the other Member States to arrive at a common EU position with a view to the upcoming discussion in the First Committee of the UN, given the lack of consensus in this year's UN GGE.