Council of the European Union

Brussels, 8 February 2017
(OR. en)

6056/17

CYBER 15
COPEN 35
JAI 97
POLMIL 8
TELECOM 33
RELEX 107
JAIEX 8
COPS 38
IND 30
COSI 23

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	20 January 2017
To:	Horizontal Working Party on Cyber Issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda as set in doc. CM 1011/1/17 REV 1 was adopted with the addition of an information provided by the Commission under item 2, a presentation by ENISA under item 4, an update by the EE delegation under AOB and the cancellation of item 8.

2. Information from the Presidency, Commission, EEAS and EU Agencies

The Presidency stressed that the single market and security were among the priorities for their semester and in the cyber field the focus would be on cyber detection and awareness raising. The Presidency also announced the dates of the next two meetings - 17 February (attaches) and 22 March (capitals), specifying that they would hold joint sessions where necessary.

The Commission (**DG Connect**) provided an extensive update on internet governance issues, referring more specifically to the last Internet Governance Forum, at which the EU was very well represented, the WSIS+10 working group on enhanced cooperation, which had been revived, the ITU Working Group on international telecommunications regulations, the G7 and G20 discussion on internet and jurisdiction and ICANN after the transfer of the IANA functions. In this regard, the Commission (**DG Home**) added some information on the last meeting of the Public Safety Working Group within ICANN, at which LEA access to domain names data, the security of top level domain names and the development of WHOIS were discussed.

The Commission (**DG Connect**) announced that a public consultation on the ENISA mandate review had been launched on 18 January 2017 as set out in the Commission's 2017 work programme, with the ambition being to present a proposal by the end of the year. In parallel, talks with the Management Board of ENISA were ongoing to identify the new challenges and priorities on the horizon.

The Commission (**DG Home**) provided a brief overview of the recent ECJ Tele2 judgment (data retention), explaining that it was currently assessing its impact, which might have serious implications for national legislation and would thus require more reflection on its side with the support of Europol and Eurojust. In that connection, the Presidency announced its plan to devote the breakfast session of the informal meeting of the Justice and Home Affairs Ministers to that issue. The Council Legal Service stated that it also was analysing the Tele2 judgment and was preparing a note, in view of its importance.

EEAS reported on the EU-US Cyber Dialogue recently held in Brussels, during which many general and specific elements of their cooperation were discussed, together with exchanges of information on some cyber-relevant events. The US presented their new response plan and expressed a willingness to work more intensively on capacity-building. In addition, EEAS announced that the EU-Japan cyber-dialogue would take place on 25 January in Brussels, while the dialogue with China and India would take most probably take place in spring. With regard to the second set of confidence-building measures adopted by the OSCE, it was explained that current focus was on implementation, although discussions on a potential new set was not to be excluded. EEAS stated that work was proceeding on the diplomatic toolbox and that it was looking at possible adoption in the coming months.

INTCEN provided some information in brief on the EU cyber fusion cell, newly created last year, which aimed at improving the flow of information and operational capabilities, and in this context mentioned some recent examples of cyber threats that had been observed. Delegations welcomed the initiative of the new body as well as the Presidency initiative to address emerging cyber threats by providing examples and expressed interest in continuing this practice in the future.

Europol/EC3 reported on the current state of play on engagement with the regional internet registries and the topics addressed, explaining the aim of improving current practices to ensure the accuracy of the information in the WHOIS database.

3. E-evidence

The Commission (DG Home) briefly reminded delegations that after the June Council conclusions, which provided the mandate for their work, progress was reported to the last Council in December; however no policy options for possible future solutions were included there. The Commission (DG Home) underlined that work was continuing and two events had already taken place in January: a round table with civil society and industry, where user notification was raised as issue for further discussion, and an expert meeting with Member States on connecting factors, during which a large amount of feedback was provided. The next round of feedback would be expected for the June Council, when policy options would be also presented. Meanwhile a number of additional round tables and other events were expected to take place, an outline of which was set out in doc. WK 518/2017.

Delegations were also presented with the main findings of the **evidence project** running in the last two and a half years under a consortium of different partners from law enforcement and academia, which had prepared a roadmap to be delivered to the Commission. The roadmap looked at harmonising the ways e-evidence was exchanged to ensure consistency both on the background and legal layers. As a result of the project some recommendations had also been formulated, relating inter alia to the need to enhance legislation and technical standards, professionalise digital forensics and improve trust, as well as some technical suggestions for new standards and extending some of the existing platforms for the purpose of exchanging e-evidence.

4. Encryption - follow-up and future steps

The Commission (DG Home) presented to delegations its initial work plan on encryption, as set out in doc. WK 528/17 following the tasking by the December Council, and briefly explained its thinking on how to involve Member States in this process. It underlined the importance of a proper balance between strong encryption and the ability of LEAs to carry out their functions. The Commission also stated its ambition to come up with a position considering all possible options and ongoing (including outside the EU) discussions by the end of 2017. The process will have an information-gathering phase, which will be structured in two streams: technical (including Europol and ENISA) and legal (including Eurojust and FRA). Although this process would be kept separate from that dealing with e-evidence, the appropriate links would be made where necessary. At the end of the first stage, on the basis of the information collected, the Commission would move to a second phase of policy analysis, during which possible policy options were expected to be identified, which would be presented to the Council.

Delegations welcomed the information provided by the Commission and underlined the strong commitment of ministers to dealing with this issue at the EU level. Member States stressed the need also to consider legislative measures as a possibility, to differentiate between online and offline encryption and to deal with the matter in a transparent and horizontal way, involving both home and justice ministers. The Commission provided some additional explanations, following requests from some delegations, of how Member States would be involved in the process to be organised on encryption. With a view to that, the Presidency invited delegations to send their comments in writing by 3 February 2017.

Europol/EC3 explained how encryption functions on a technical level, explaining the difference between the two main types of encryption as well as informing on the challenges it poses to LEAs in conducting their criminal investigations and outlining some of the possible legal and technical solutions. It underlined their role as a centre of excellence that could serve Member States by providing different services, regarding in particular its decryption platform. Europol/EC3 also briefly updated on the state of play on the joint working group set up together with ENISA, which was expected to draft a position paper on encryption.
ENISA also shared their experience and work related to the use of cryptography.

5. The Carrier-Grade NAT technology - use and challenges

Europol/EC3 presented the challenges faced by LEAs as result of the use of Carrier Grade NAT technology (doc. 5127/17), explaining the link with the delays in the transition from ipv4 to ipv6 and the exhaustion of available IP addresses. Some examples of how recent investigations had been affected by the CG NAT Technology and suggestions for possible solutions were also provided. Europol/EC3 briefly referred to the upcoming meeting this month to discuss this issue and share examples and good practices as well as to launch a network of LEA specialists on Carrier Grade NAT to represent the voice of LEAs in reaching out the policy and decision-making level.

Delegations welcomed the presentation and agreed on the need to address this matter in a coordinated way at EU level. No conclusive position was reached on which channel it could be best used to tackle it. Some Member States expressed the view that a voluntary scheme could be an approach to follow and saw in this regard some role for the EU Internet Forum; others pointed out the limitations of this approach. In addition, some delegations shared their national experiences.

The Presidency invited written comments by 3 February 2017 in order to continue the discussion.

6. Prevention and cyber awareness

The Presidency presented the questionnaire on cyber awareness set out in doc. CM 1124/17, aimed at collecting information to build a comprehensive picture of the current situation, including any gaps that might exist, in order to define ways to address them and the matter further in general.

Europol/EC3 stated that many of their awareness activities were organised within the EMPACT policy cycle, specifying that last year operations were followed by prevention campaigns and media impact assessments (e.g. mobile malware prevention campaign, 'don't be a criminal' campaign, etc.). In one of the projects on "no more ransoms" a novel approach was used, going beyond prevention and involving the industry as a partner. The prevention and awareness-raising activities would continue in the course of 2017. Some of them would specifically focus on combating payment card fraud.

ENISA presented their activities in that area, in particular the European Cybersecurity Month, coordinated with the US cybersecurity month, and explained that the aim was coordinated action, education and sharing of good practices, taking a thematic approach and trying to involve as many actors as possible. ENISA reported that in 2016 there were 14 Member States engaged in that initiative, but the aim was to increase their number still further. During the discussion, the importance of applying a proper matrix for measuring the social impact and scope of impact were underlined. Some delegations shared their national experiences, emphasising that prevention was key and that it would be useful to see where and how EU could add value. Europol explained the translation efforts that had been undertaken from their side with respect to the prevention campaign materials they have produced so far.

The Presidency restated its intention to take stock of national activities in the area, in order to identify gaps and reflect on the best approach to addressing them, either by holistic programmes or rules at EU level, depending on the answers that delegations provided.

7. Detection Capabilities - scoping the problems

The Presidency gave a brief introduction of the topic, explaining that the aim was to look into the possibilities for minimising the general detection time of cyber incidents and encouraged Member States to share their national initiatives and ideas on how further to address this issue.

The Commission's Joint Research Centre presented some figures on the matter: a typical cyber accident scenario and possible techniques for its detection. It explained that a number of research activities were ongoing in this field, as detection was closely linked to prevention and awareness, which were extremely important in the interconnected environment of today.

8. Accreditation technologies - the way ahead

This agenda item was cancelled.

9. AOB

The EE delegation presented their idea, as incoming Presidency, of organising a strategic cyber exercise to test the different instruments that the EU and MS have in their disposal, They also announced the launch of the Tallinn Manual 2.0 next month in Washington DC, Tallinn and The Hague, on which delegations would be provided with further details.