Council of the
European Union

Brussels, 3 May 2017
(OR. en)

8586/17

CYBER 63
COPEN 120
JAI 374
POLMIL 40
TELECOM 94
RELEX 351
JAIEX 37
COPS 139
IND 93
COSI 84

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	22 March 2017
To:	Horizontal Working Party on Cyber Issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda as set out in doc. CM 1551/1/17 REV 1 was adopted with no additional points under AOB.

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

The Presidency announced the dates of the next meetings (19 April and 12 May) and of an interactive workshop planned for 24 May. It also reported on the outcome of the informal meeting of the Justice Ministers and on the GENVAL and CATS meetings, respectively.

The Commission (DG Connect) provided an update on the state of play of the 2016 Communication on Cyber Resilience implementation, referring more specifically to the work on certification and labelling, and stressing the need for further development of the roadmap. It also announced the upcoming third workshop with Member States, ENISA and industry on 24 April on this matter. A brief report was provided on the Cooperation Group kick-off meeting and on the state of play of the contractual public-private partnership on cybersecurity.

The Commission (DG Home) debriefed on the Council of Europe Cloud Evidence Working Group meeting (31/1-1/2/2017) in Strasbourg and announced the adoption of a non-binding guidance note on 1 March. It stressed that due to the limited scope of the note, a common EU position on e-evidence might help the ongoing discussions within the Council of Europe. The Commission (DG Home) also provided an update on the last EU Internet Forum (9-10 March 2017) and mentioned two recent key deliverables - a database of hashes allowing automated removal or non-reposting of terrorist material and an online narrative by civil society partners. It also announced that the next High Level Experts meeting of the Forum would be held in June and the third ministerial meeting would be in December.

The EEAS referred to a recent discussion within the UNODC on the new legal instrument for cybercrime, recalling the EU position that existing law also applies in cyberspace and highlighting the need to focus on developing and applying voluntary peace-time rules. It stressed the good work carried out by the EU in applying the existing law and the recent launch of the Tallinn Manual 2.0. The EEAS also underlined the OSCE's work in relation to the confidence-building measures (CBMs) and of UN GGE on norms of state behaviour. The HU delegation provided some details on OSCE as it currently holds the chairmanship of the working group on CBMs within the OSCE.

EUROJUST provided a brief update on the state of play of the European Judicial Cybercrime Network, the preparation of its work programme, and announced an upcoming meeting at which the Council, the Commission and Europol would be invited to provide an update on ongoing activities, with the purpose of discussing, among other things, how the network can contribute.

ENISA reported on the CSIRT network kick-off meeting (23-24 February) in Malta, specifying that the next meeting was scheduled to take place in Estonia at the end of May.

3. Carrier Grade NAT - exchange of good practices

Europol/EC3 underlined the need to focus on IPv6 transition, as many investigations were hampered and difficulties were experienced in attributing crimes due to the use of CGN to cope with the exhaustion of IP addresses under the current IPv4. The matter was further illustrated by a recent case of child sexual exploitation. The Belgian model - an agreed voluntary code of conduct with ISPs - providing in particular limitation of the number of end-users behind one IP address when CGN was used, was presented as a good practice. In addition, Member States were informed about the creation of a network of CGN specialists on 31 January in Europol to exchange good practices, build expertise, collect cases, and engage with service providers.

Several delegations expressed the view that CGN was closely linked to the data retention matter and underlined the need to look at it while discussing the way forward after the TELE2 ECJ Judgement. Some stressed the importance of promoting the transition to IPv6 and suggested using the EU Internet Forum to address the CGN issue. The Commission acknowledged the need for incentives for companies to transit to IPv6 and not maintain CGN.

4. Common challenges to LEA and judiciary in combatting cybercrime

The Commission informed the meeting about the state of play of the Encryption expert process after tasking by the December JHA Council. It explained that technical and legal work streams were being established. At present, efforts were being directed at defining the scope of information needed. A number of workshops were planned to get input from Member States' experts and academia. Pragmatic options were expected to be presented in the second half of 2017. The group will be kept regularly informed.

Europol and Eurojust jointly presented an updated version of the common challenges in combating cybercrime which were initially presented at the end of 2015 (doc. 7021/17). They clustered them in six big groups encompassing a number of new issues to be addressed together with data retention, encryption, CGN, cloud based storage, and the lack of expedited tools for the sharing of evidence. The need to have a level playing field in terms of sharing information was stressed, and innovation and cooperation were underlined as the two main vectors for the way ahead together with changes in legislation, further sharing of best practices to allow smart choices, and practical approaches to practical problems.

5. Cyber Threat Landscape - emerging trends

Europol referred to some of the emerging trends identified in the recently published SOCTA. It specified that currently technology was a driver for crime which also explains SOCTA's subtitle ("crime in the age of technology"). The main cyber-related areas of focus mentioned were cyber-dependent crime, child sexual exploitation and transnational payment fraud; it was also underlined that the big number of devices in circulation led to a vast attack surface and numerous attack vectors. It also stressed the high rate of juvenile delinquency.

Eurojust underlined the need for an integrated approach, focusing on all the four pillars in tackling cybercrime: detect, disrupt, deter and prevent.

ENISA referred to their 2017 report on emerging threats, stressing the high level of complexity and demonetisation. It underlined the difficulty of analysing the cost of cybercrime, the ease of committing a cybercrime on any of the attack vectors, and the problem of attribution. In this regard, ENISA stressed the need to better define the roles and responsibilities of the various stakeholders, specifying that the only way of tackling cybercrime, given its global nature, was fast and secure collaboration.

CERT-EU provided some incident information demonstrating the dynamic nature of the landscape and specified that the current focus was on targeted attacks.

INTCEN explained that it was working closely with CERT-EU and that it was providing regular updates to Member States on cyber-attacks.

Delegations welcomed the presentations and voiced their wish for regular updates, especially from CERT-EU and INTCEN in relation to incidents involving EU institutions. In addition, some requested the provision of more focused information on the Eastern partners and Western Balkans at one of the forthcoming meetings. An appeal for a more coordinated capacity-building effort in that region was also made.

6. EU Cyber Security Strategy review - state-of-play and future steps

The Commission (**DG Connect**) explained that the review was a result of the changed geopolitical landscape since the adoption of the EU Cyber security strategy in 2013, referring inter alia to the increasing use of cybercrime as a tool, the cyber-enabled interference in democratic processes, and the cybersecurity considerations linked to the Internet of Things. The review process would be used to engage Member States' reflections on a number of questions related to the main treats, potential gaps, priorities, and the role of the EU agencies, questions which would be addressed in a roundtable with VP Ansip. The revision of the ENISA mandate together with certification would be fed into the Strategy and would form part of it. The Commission underlined its intention to use the group for more detailed and deeper discussions on these questions.

The Commission (**DG Home**) stressed the need to use an integrated approach in which all agencies and the private sector could contribute in order to strengthen the deterrent effect. In that regard, it stressed that Internet Governance should also be taken into consideration in this process.

EEAS stated that a lot had already been achieved in the policy field, underlining the importance of addressing the challenges and looking at the future of Internet in the new setting of an increased number of users and constant shortages of expertise and skills. It also underlined the need to look at regulatory policy and threats beyond the EU.

Delegations welcomed the information provided, in particular the intention to set up an inclusive and integrated process for the review of the Strategy. Some delegations voiced the need to adopt a global and horizontal approach and suggested in this regard that the Council put forward some strategic guidelines for the preparation of the Strategy. Others addressed the importance of achieving digital strategic autonomy, mainstreaming cybersecurity and avoiding fragmentation and regionalisation of the Internet.

Member States also referred to some specific matters such as the Internet of Things, Artificial Intelligence and Quantum computing. In reply to requests from delegations for clarification on the timeline, the Commission explained that their aim to deliver the new strategy, together with a proposal for an updated ENISA mandate, on 1 September.

The Presidency announced that the discussion on this matter would continue at the next meeting.

7. United Nations Intergovernmental Expert Group on Cybercrime meeting, 10-13 April 2017, Vienna

The EEAS and t**he Commission (DG Home)** presented the draft lines to be taken (doc. 7130/17) in the context of the meeting of the intergovernmental expert group meeting in Vienna and outlined the official EU position in this regard.

Delegations supported the draft line to be taken. Some of them underlined the importance of proactive diplomacy towards third countries, especially those not yet parties to the Budapest convention, and stressed the importance of the convention as a reference legal framework on cybercrime internationally.

The Presidency invited delegations to send their written comments on the draft line by 29 March 2017.

8. Digital Object Architecture - cyber risks

The UK delegation presented the cyber risks related to the digital object architecture outlined in doc. WK 2981/2017, noting that it was considered by certain parties in the ITU as a solution to the Internet of Things and as a replacement for DNS. It stressed that its resilience had not been tested in a non-safe environment and a great number of powers were vested in its administrators. In this regard, the UK delegation invited delegations to liaise with their ITU representative with a view to the upcoming meeting on 24 April to support the position expressed in the paper presented.

9. Joint EU Diplomatic Response to Cyber Operations (Cyber Toolbox)

The EEAS outlined the key features of the cyber toolbox as set out in doc. WK 2569/2017. The latter was presented to the PSC on 14 March 2017 and its significance in relation to cyber resilience and hybrid threats was underlined; a mandate was given to the HWP on Cyber Issues to develop it further.

Delegations welcomed the paper, specifying the need to take the necessary time to discuss it in detail. They provided views on both the substance and the process. In terms of process, many defined attribution as a key element to be addressed and stressed the importance of cooperation, in particular with NATO and OSCE. As a way forward, a large number of delegations voiced a preference for the development of Council conclusions accompanying the toolbox itself.

The Presidency set 3 April as the deadline for written comments both on the content of the cyber toolbox paper, and also on the way ahead.

10. Prevention and cyber awareness

The Presidency presented the main findings set out in doc. 6142/17 of the questionnaire on prevention and cyber awareness (doc. CM 1124/17) distributed to delegations in January. Twenty replies had been received, all indicating that Member States conducted such campaigns. However, there should be a greater focus in the future on vulnerable social groups as well as on better cooperation at a pan-European level, together with exchanges of experience and the allocation of more resources.

Delegations welcomed the report, underlining the need to further improve cooperation with ENISA in this regard and to promote the participation and organisation of prevention and awareness-raising events. Europol referred to the upcoming meeting of the prevention forum on 6 April where best practices would be exchanged and discussed.

The adoption of dedicated legislation or of Council conclusions on the matter were not considered as options for the way ahead. Given the upcoming review of the EU Cybersecurity Strategy, the Presidency favoured the inclusion of prevention and cyber awareness in the future Strategy.

The Czech delegation presented their National Cyber Awareness Campaign.

11. AOB

No points were raised under this item of the agenda.