Council of the European Union

Brussels, 17 June 2016
(OR. en)

9924/16

CYBER 64
POLMIL 58
TELECOM 114
RELEX 488
JAIEX 58
COPS 181
IND 132
JAI 539
COSI 97

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	27 May 2016
To:	Friends of the Presidency Group on Cyber Issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda was adopted as set out in doc. 2681/2/16 REV 2.

2. Information from the Presidency, Commission and EEAS

The Presidency informed about the outcome of the High Level Event on cybersecurity held on 12-13 May 2016, in Amsterdam (doc. 8861/16). It underlined the need to establish strong cooperation between the public and private sector, to find a comprehensive approach on standardisation in the EU to fight fragmentation and to work towards an increased digital literacy and cybersecurity awareness. During the event a vulnerability disclosure manifesto was signed by more than 28 private companies and organisations by which they undertook the obligation to put in place such policies and rules as well as to encourage other companies to do so. The outcome report would be presented to the June Council (JHA).

The Presidency also updated on the state-of-play of the two sets of draft Council Conclusions on cyber judicial network and on improving criminal justice in cyberspace, both expected to be adopted by the June Council (JHA).

The Commission provided an update on the contractual Public-private partnership on cybersecurity for which the accompanying Communication would be finalised in June. Member States demonstrated interested in the concrete way they would be involved in the governance structure of that partnership, the funds that would be available for training or awareness raising and the content of the accompanying Communication.

In addition, the recently published Communication on Priorities for ICT Standardisation for the Digital Single Market was presented. The Commission representative explained that its main aim was to address the numerous interoperability challenges regarding standards as well as specific key priority areas outlined during the consultation phase such as the Internet of Things, cloud computing, big data, data operability, cybersecurity. The need of support from the Council in this regards was explicitly mentioned.

EEAS informed that the EU-South Korea cyber dialogue was scheduled to take place in 16 June and its agenda was discussed in COASI whereas the one with Japan would take place early September. It also stated that a new cybersecurity capacity building project was expected to kick off very soon. With regard to cyber defence the group was informed that the last Implementation Report on the Cyber Defence Framework Policy would be presented and discussed in PMG on 30 May together with a feasibility study on how to proceed further in that area.

ENISA updated on the cyber exercises calendar launched on 2015 and the respective report on national cyber exercises. Furthermore it informed that ENISA's 2016 work programme required some adjustments of the tasks to accommodate the NIS Directive implementation, in particular the creation of the SCIRT network and Cooperation group. ENISA also reported about the work done in relation to certification followed up in two workshops held in January and March this year. With regard to civil - military collaboration, ENISA had taken steps towards EDA to explore the support that it could provide and to set an agenda for that.

Finally EC3/Europol made a presentation of the Cybersecurity ecosystems concept, explaining that one of the main objectives was to connect initiatives and partners in key sectors to make sure they work together and to provide an overview of what was existing to avoid overlaps but also to allow easier steps and multiplication of efforts especially in the area of capacity building. The concept provided also for main and sub-ecosystems to be created in order to map existing partnerships or other form of cooperation and to assist the building of future programmes.

3. Implementation of the EU Cybersecurity strategy

The Presidency explained its intention to continue exploring the area of capacity building, trying to approach the issue in a strategic manner. It briefly presented the way ahead as outlined in doc. DS 1283/16. Delegations once again expressed their general support and made concrete suggestions both in terms of procedure and substance. Some of them requested a clarification of the scope of this exercise and reminded about the need to avoid duplication. The incoming Presidency was invited to continue the work started in that area.

4. Public-private partnerships - exchange of good practices

The Presidency briefly summarised the discussions that have taken place on ISACs and Vulnerability disclosure topics during the previous cyber attaches meetings and presented a proposal for the way forward (doc. DS 1282/16) which was supported by the delegations that took the floor.

5. Cyber resilience of the EU Institutions networks

A representative of CERT-EU updated the group on the latest development both in terms of human capacity, but also of services and capability. He informed about some changes in the advisory system as of 2015 and about a recently singed technical agreement. A brief overview of the major recent threats and cybersecurity trends was presented.

Likewise a representative of the Commission and of the General Secretariat of the Council explained what measures they have taken and what kind/number of cybersecurity incidents they have faced. Some insight was provided by the Commission also on its new governance structure and recent campaigns.

Delegations welcomed the update. The coordination between EU institutions and CERT-EU role were further discussed.

6. Cyber crises cooperation and management

A representative of the GSC explained the mechanism for activation of the IPCR (Political Crisis Response arrangements) in the occurrence of a crisis and whenever a cooperation/coordination at EU level was needed. He compared its activation - predominantly by decision of the Presidency (but could be also done upon request of Member State) with the invoking of the solidarity clause (Article 222 TFEU) which was only a prerogative of Member States. He further explained some of the main tools IPCR was centred around (a web platform and Integrated Situation Awareness and Analyses).

Under the same point ENISA presented its 2015 report on cyber crises cooperation and management (doc. 8865/16) and underlined the importance of the establishment of clear rules and procedures for cyber crisis cooperation, good preparation inter alia by cyber exercises and training and finally an appropriate follow-up.

ENISA also presented the 2015 Threat landscape (doc. 8866/16) drawn on the basis of publicly available information to fulfil the respective business needs. The necessity of developing proper statistic and control models was underlined together with work to better defragment EU cyber environment.

Delegations welcomed the discussion on this topic and suggested to consider in the future some additional aspects such as the civil-military cooperation, especially in view of hybrid threats.

7. FOP Mandate Renewal

An initial discussion on the FOP mandate renewal took place during the meeting. Delegations were invited to reflect on the questions set out in doc. DS 1265/16 and to provide their written views by the end of June. On that basis the incoming SK Presidency would consider and propose, if necessary, changes in the terms of reference to ensure that the renewed structure corresponded to the current needs.

A number of delegations shared their preliminary views stressing the need to continue the mandate of the group preserving its strategic, horizontal and cross-cutting nature. Some even suggested to look for a long-term solution. In terms of substance they indicated the value of carrying on the information exchanges and discussions on cybersecurity, cyber defence and cyber diplomacy matters, to take part in decision-making, consult and coordinate positions, whenever necessary taking due account of the new Cooperation group and the SCIRT network as part of the NIS Directive implementation.

8. Incoming SK Presidency priorities and work programme for FOP on Cyber Issues

The incoming SK Presidency briefly presented their preliminary programme and priorities for the FOP detailed in doc. DS 1287/16.

9. AOB

No items were raised under this point.