Council of the
European Union

Brussels, 30 September 2014
(OR. en)

13750/14

CYBER 47
TELECOM 167
RELEX 789
IND 268

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	22 September 2014
To:	Friends of the Presidency Group on Cyber Issues
Subject:	Summary of discussions

1. Adoption of the agenda

The agenda as set out in doc. CM 4047/14 was adopted with the addition of information points by the NL, DE, EE and ES delegation.

2. Information from the Presidency, COM and EEAS

The Presidency opened the meeting with a brief presentation on the "cyber week" in Israel (14-17 September), explaining Israel's interest in launching a dialogue with the EU. It also drew delegations' attention to the TECHITALY 2014 event on Horizon 2020 which would take place on 25 September in Brussels and where a panel would be dedicated to cybersecurity, protection of critical infrastructure and research & industrial needs. In addition, the Presidency presented the main points of the informal Telecom Ministerial meeting that would be held in Milan on 3 October, where Internet Governance would be discussed at length.

The Presidency congratulated LU on the recent ratification of the Budapest Convention and acknowledged the positive developments in the remaining four MS (PL, EL, SE and IE).

COM (DG Connect) explained that the European Cybersecurity month (ECSM) was a core element of the EU Cyber Security Strategy and ENISA provided some details on the more than 100 events planned, which could also be found on a specially dedicated website (cybersecuritymonth.eu). The ECSM would be opened with a High Level Event on 1 October, attended by Commissioner Neelie Kroes.

COM (DG Connect) further reported on the Financial Times' Cybersecurity Summit that had taken place in London on 3 September and the Internet Governance Forum (IGF), held in Istanbul on 2-5 September 2014, explaining that Internet Governance was rising on the political agenda. Some of the main issues of consideration in this regard were the renewal/extension of the IGF mandate, the transition of IANA functions, the accountability of ICANN and the upcoming quadrennial meeting of ITU plenipotentiaries. COM informed the meeting that the High-Level Group on Internet Governance would meet in Brussels on 30 September to discuss some of these issues in order to secure a clear EU position. Delegations were also informed that the TELECOM WG would draw up Council Conclusions on the Commission's Communication on Internet governance and policy.

COM (DG Connect) also stated that a lot of effort was being put into adopting a general approach on the NIS Directive in the Council by the end of this month and starting trilogues with the EP in October. However, discussions in the TELECOM WG were continuing on the outstanding issues (scope, operational cooperation) but it was expected that the step-by-step approach taken would produce the desired result.

COM (DG Home) notified delegations that at the EU-US Ministerial Meeting on Global Alliance taking place in Washington DC on 29-30 September, the Secretariat of the Alliance would be handed over from EU to the US side. Also, following the adoption of the Implementation Decision on ISF- Police Funding (C(2014) 5651 final) which allocated € 5 million for cyber-related issues, the Commission was planning to publish a call for projects in October.

COM (DG Home) explained that it had launched public consultations with regard to the review of the Internal Security Strategy. The final text was expected in spring 2015 and the Presidency also intended to submit draft conclusions on the renewal of the ISS to the Council on 4-5 December. This issue would also be at the centre of the High level Conference that would take place in Brussels on 29 September.

Finally **COM (DG Home)** reported that:

– a Conference dedicated to the tools and techniques against Child Sexual Exploitation had taken place on 16 September in Hanover and that an agreement with Europol had been reached to host the tools depository;
– the contact group on the Directive on attacks against information systems would meet this week to discuss the main issues related to the Directive's implementation which should be completed by 4 September 2015;
– the plenary meeting of the NIS platform would take place in Brussels on 25 November, where the deliverables of its working groups would be discussed.

In its brief to the group, **EC3** mentioned that it was preparing quarterly reports on cybercrime, that it was currently carrying out a mapping exercise of existing trainings and it was working on the finalisation of iOCTA, the summary of which would be presented to the upcoming Police Chiefs Convention on 24-25 September. EC3 also underlined the launch of J-CAT (focus on operations), in which 11 MS were participating, and explained the idea of formalising J-CAT in 2015 and embedding it in EC3. EC3 also advised delegations on its current work on preparing a legislative package based on its operational experience.

EEAS brought delegations up-to-date on some recent external bilateral developments, notably the EU-China Cyber Taskforce, whose next meeting would be held in Beijing on 21 November; the EU-Japan Cyber Dialogue - the meeting would take place in Tokyo on 6 October; the EU-US Cyber dialogue- the meeting was planned for 5 December in Brussels; and reported on the High Representative's Visit to Vietnam on 12 August in which cyber issues had been discussed, in particular the promotion of the Budapest Convention, and online abuse.

EEAS also informed delegations that a draft of the European Cyber Defence Policy Framework had been circulated before the summer. It built upon 5 priority areas: 1) the protection of communication networks supporting CSDP structures, missions and operations; 2) civil-military cooperation and synergies with wider EU cyber policies and other relevant EU institutions and agencies; 3) training, education, exercises and cyber defence awareness-raising; 4) support for the development of Member States' cyber defence capabilities and 5) enhancing cooperation with relevant international partners, notably with NATO and, as appropriate, with the private sector and academia. The aim would be to finalise the draft in the autumn and adopt it in November at the Foreign Affairs Council.

3. Cyber exercises

ENISA explained that Cyber Europe 2014 was a multilayer exercise with more than 400 professionals participating. The final high level strategic part would be carried out next week whereas the main phase dedicated to operational collaboration would take place before the end of the year. Once all phases were completed, ENISA would draw up a report. The Commission recalled the importance of Member States' participation. Delegations reported on two other exercises that had taken place - a strategic exercise in Lisbon and an annual technical cooperation exercise in Tallinn.

The GSC presented the preparations for the first ICPR exercise, specifying that the idea was to keep the exercise short and simple using a step-by-step approach, and a realistic scenario based on Cyber Europe 2014, but not embedded in it. The exercise would aim at assessing the suitability of the procedures and tools in place in order to facilitate decision-making in the Council.

EEAS informed the group about the ML 14 exercise which would have an aspect of Cyber event response, explaining that it would provide further details upon its completion.

4. Finalisation of the Cyber diplomacy non-paper and way forward

The Presidency presented the last version of the Cyber diplomacy paper (doc. 9967/3/14 REV 3) and expressed its aim to close the discussions on the text in today's meeting. Several delegations made additional comments which the Presidency addressed by proposing a redrafting of the text. These proposals were discussed and preliminarily agreed at the meeting.

A new revised version incorporating all these proposals would be issued after the meeting and be subject to a silence procedure expiring on Friday 26 September at 12.00.

As a follow-up, the Presidency explained that it would proceed by preparing draft Council Conclusions on Cyber diplomacy which would refer to the Conclusions that the Telecom WG would draw up on Internet Governance.

5. Big data and cloud computing - presentation by the Commission

The Commission presented its recent Communication entitled "Towards a thriving data-driven economy", set out in doc. 11603/14 +COR1, in which it aimed at providing a response to the need to deal with the big data phenomenon. COM acknowledged the difficulty of storing, analysing and extracting value from big data with traditional tools as well as the fact that Europe was lagging behind the US on this issue. The Communication described what needed to be done to turn EU into an efficient data ecosystem and the conditions necessary in order to smoothen the transition as well as the framework conditions (data protection, IPR, security, skills). The Presidency specified that this Communication would be presented to the Competitiveness Council this month.

Delegations were also informed about current efforts to develop improved algorithms to extract value from data, which were expected to accelerate research and innovation; the signature of a contractual public-private partnership on 13 October to seek the most appropriate fields for research and innovation investments; the creation of an incubator of small partnerships to enable SMEs to deal with difficult data protection markets; and the possibility of drawing up an Action Plan in the future.

Two delegations intervened in support of the Communication, one of them explaining that a similar initiative had been launched at national level with regard to cloud computing, while the other suggested holding discussions on this subject within this group and requested more information on the follow-up. The Presidency welcomed in general the idea of a dialogue, but underlined that its realisation would require additional preparation and coordination among the relevant stakeholders.

6. EU institutions' resilience

Representatives of the GSC, Commission, CERT-EU and ENISA described some of the concrete steps being taken by the EU institutions to enhance the resilience of their IT networks. With regard to the protection of Council networks, it was noted that since 2009 the GSC had put in place dedicated structures to enhance the protection of its IT systems with an annual budget of € 1.4 million and 10 full-time IT security specialists. Delegations were also informed that an alert mechanism had been set up in 2010 by the Council through which some MS provided useful feedback, and technical information was exchanged.

With respect to CERT-EU, the Group took note of doc. 12992/14 setting out the measures agreed among the EU institutions' Secretaries-General on CERT-EU's mandate, services and operational capacity following an independent review by four high-level IT security experts. It was underlined that CERT-EU had become a permanent structure within the institutions and as such had helped improve the overall level of IT security, including with the support of MS' CERTs. The new consolidated mandate for CERT-EU was expected by end of 2014.

The Group also examined a non-paper presented by eleven delegations on reinforcing the network and information security (NIS) of the EU institutions (doc. DS 1296/14), which aimed to identify priorities to be taken forward in implementing the EU's cybersecurity strategy at the level of EU institutions, in particular the establishment of a permanent and regular dialogue on NIS where all EU institutions work together with active support from ENISA and CERT-EU. The Group noted that CERT-EU had been established and continued to operate on a budget neutral basis through contributions in cash or in kind from its constituents.

The representatives of Commission, CERT-EU and the GSC welcomed the Presidency's initiative to discuss the issue and the interest shown by delegations in this matter. They noted that the larger institutions had already taken steps to improve their defence against attacks on the level of infrastructure, policies and cooperation. The Commission's representative also stressed the fact that this institution had recently appointed a Chief Information Security Officer, who was expected to consolidate this effort. The institutions' representatives also underscored the fact that cooperation among the EU institutions in that area was well developed, including at senior management level, not only through CERT-EU but also in the Inter-institutional Informatics Committee.

The Group noted the broad agreement on the need to further strengthen EU institutions' cybersecurity capabilities, especially in the smaller or weaker constituencies, and the general willingness to consider the various suggestions set out in the non-paper, in particular in the on-going work on updating CERT-EU's mandate and catalogue of services and defining CERT-EU's full operational capability target by mid-2015.

Several delegations raised concerns on potential budgetary implications of the implementation of the recommendations made in the non-paper, and expressed the necessity to remain within the limits of the current budgetary framework. Others drew attention to the need to make better use of ENISA's resources whereas a third group was open to hear what additional resources might be needed by the EU institutions on the basis of their risk profiles assessment.

The Presidency concluded that strategic political discussions on this issue would continue within the Group and that delegations would be updated on the progress made by the EU institutions in their work to increase the NIS of their systems and networks. It also welcomed the CERT-EU invitation to visit its premises and to receive more information on its activities.

7. AOB

Four information points were raised under this item:

a) the NL delegation reported on the preparations for the upcoming Conference on Cyberspace which they would host in 2015, specifying that it would take place in the Hague on 16-17 April and would highlight the on-going work and future inspiring initiatives. The agenda would cover inter alia cybercrime, freedom and privacy, cybersecurity, and capacity building. An interactive session on a fictitious scenario was also planned. The main objectives of the Conference would be to support the practical cooperation response to certain challenges, to promote capacity-building, responsible behaviour in cyberspace as well as human rights and privacy in the Internet. The deliverables would be provided by different project groups for which delegations would shortly receive an invitation. The organisers were expecting around 1300 participants from governments, the law enforcement and CERT community, academia and the private sector who would try to put principles into practice and present practical solutions to the problems. A fact sheet on the Conference would be distributed.

b) the DE delegation informed delegations about the Meridian process and invited them to the 2014 Meridian Conference which would be held in Tokyo on 12-14 November and which would focus on capacity development.

c) the EE delegation announced the recent adoption of a new cyber security strategy. It also asked the Commission how it planned to address the situation created by the recent annulment of the Data Retention Directive, which was also discussed by the June JHA Council and which forced several Member States to amend their legislation. In response, the Commission explained it would be for the new Commissioner to take a stand on this issue.

d) the ES delegation drew the Group's attention to the fact that the Maritime Security Strategy would also include a mention of cybersecurity.
