COUNCIL OF THE EUROPEAN UNION

Brussels, 12 June 2014 (OR. en)

10594/14

CYBER 36
TELECOM 129
RELEX 483
IND 178

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	23 May 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 2819/1/14 REV 1 was adopted with the addition of an information point under AOB.

2. Information from the Presidency, Commission and EEAS

This item was taken together with item No 5.

3. EU Values & Human Rights in Cyberspace

– Guidelines on Freedom of Expression Online and Offline

EEAS presented the Guidelines on Freedom of Expression (doc. 9647/14) adopted on 3 May 2014 by the Foreign Affairs Council and based on the EU Strategic Framework and Action Plan on Human Rights and Democracy of 2012. Their main aim was to promote human rights in the EU's external relations and to provide political guidance in that regard to MS and EU missions abroad when interacting with third countries or taking part in international fora on related issues. EEAS underlined that the guidelines were not legally binding by nature and were meant as an operational instrument, i.e. providing tools to tackle the challenges of new technologies, e.g. dangers of unwarranted interference. Furthermore, during their preparation the guidelines were submitted to broad open public consultation and there was a lot input from civil society. Finally, to support efforts to promote the rule of law, human rights and best practice in cyberspace they were published on EU delegations' websites and translated into many languages. Delegations welcomed the document and underlined its great value as an operational instrument to be used on the ground by their offices and missions abroad.

– EU Fundamental Rights and Cyberspace

FRA briefly presented the methodology and key findings of three recently conducted surveys. The first, on access to data protection remedies in MS, based on a comparative legal analysis and social research, found that most data protection violations arose from the Internet (social networks, online shopping, etc.) and that victims were not aware of the available tools, in particular the protection that judicial authorities could offer, with the result that judicial procedures were rarely used and little case-law existed. Also, great variations between MS were observed in terms of how data violations were remedied and of courts' ability to impose sanctions. The second survey, on violence against women, revealed that cyber stalking (offensive communication by email, sms or other offensive or threatening messages by the same person) and sexual harassment through ICTs were not sufficiently addressed by public discourse and underreported by the victims, primarily young women; this showed the need for quick and effective recourse to assistance, especially for social media. The third survey, on cyber hate against the Jewish population, found that the Internet increased both the perception and the reality of anti-Semitism. Joint action at EU level was therefore needed to prevent misuse of the Internet and to enhance the legal basis for the prosecution of hate crimes, which could be also done through ratification of the additional protocol to the Budapest Convention.

Delegations stressed the need to improve reporting by using all the available mechanisms and channels as well as the role that law enforcement authorities could play in addressing these crimes. COM pointed out that some of the reporting channels existing under the current legislation and the MS' capacity to fight cybercrime would be the subject of the 7th evaluation round.

FRA concluded that it would work closely with COM to see how best to use the findings of their surveys as well as the available funding (DAPHNE, structural funds) to ensure human rights protection.

4. International Cyber Space Cooperation

– **NetMundial outcome and conclusions**

COM debriefed delegations on the outcome of the multi-stakeholders meeting that took place on 23-24 April in Sao Paulo, Brazil, stressing that for the first time the final statement had been adopted by a "rough consensus", through a transparent, bottom-up process and with content close to the COM Communication on Internet Governance and Policy and the COREPER Lines to take. Although not all parties involved were entirely satisfied with the end result, as some controversial issues were left out, it could be considered as satisfactory and as a good basis for further work. COM further explained that current discussions were centred primarily on the globalisation of the IANA functions, capacity building, jurisdictional problems and the review of the Sao Paulo process (use of the lessons learned) and referred to some of the relevant upcoming global events (IGF, ITU Plenipotentiary Conference). COM underlined the importance of the EU being seen as a key player in these processes and the need for a coordinated voice when it came to the issue of Internet governance, which, together with the development of the Internet economy and Internet society, would be addressed at the ministerial lunch on 6 June in Luxembourg.

Some of the delegations that took part in the Brazil meeting also shared their views and experience, emphasizing the success in terms of procedure - the multi-stakeholder model had been proven to work, but also in terms of substance - the content of the statement adopted, which would serve as a useful reference. They also acknowledged the need for improvement of coordination at EU level.

One delegation expressed its readiness to continue the discussions on Internet governance in FoP together with COM and EEAS provided that FoP could provide the impetus for a clear international EU strategy. COM expressed their willingness to maintain the dialogue with FoP and have a holistic approach at EU level as well as a coordinated voice externally, keeping the successful part of the international engagement and the momentum created as well as protecting the multi-stakeholder model and an open, secure and single Internet.

– **European Cyber Diplomacy** - follow up

The Presidency briefly presented the paper as set out in doc. 9967/14, prepared on the basis of the initial EEAS food for thought paper and MS comments. EEAS welcomed the paper, underlining the usefulness of strategic discussions and streamlining MS positions on the various trends mentioned therein and made some general comments on the text. A number of delegations took the floor, supporting the text as a basis for further discussions in general, but indicating at the same time areas for further clarification or improvement. COM entered a reservation on the text, explaining the need to study the document in detail. The Presidency set 2 June as the deadline for written comments.

– **EU external representation** - information by the CLS

CLS gave a short presentation on the main principles of EU external representation, explaining that the issue was closely linked to that of competence, i.e. who could speak on behalf of EU, but was different from the question of what could constitute an EU position. Delegations were briefly informed of the main types of EU position depending on their legal effects and the respective procedures for taking them. Reference was made to several CLS opinions (doc. 8461/12; doc. 7225/13, doc. 12498/13and doc. 8515/13). Some delegations requested the information in writing. COM explained that there were a number of disagreements between the CLS and COM LS as well as the fact that there were two cases still pending.

5. Update on EU Cybersecurity Strategy implementation by COM

COM informed the meeting on the progress made on Horizon 2020, whose last Programme Committee was held in April; the organisation of the Cybersecurity exercise and the Cybersecurity championship, of which a full account would be provided upon their completion in the autumn; and the NIS platform, launched in June 2013, which had already produced its first set of recommendations. Discussions on how to take the platform work forward would be held during the next plenary meeting in the autumn, while an assessment would be carried out in 2015.

COM updated the meeting on the latest developments in the fight against cybercrime, explaining that all the actions envisaged by the Strategy had been implemented, namely:

– stronger legislation was already in place: the Directive on child sexual exploitation, whose transposition COM was currently assessing, as well as the Directive on cyber attacks, which should be transposed by September 2015 and whose implementation problems would be evaluated by the contact committee on 24 September;

– the Global Alliance already counted 54 members after Mexico had joined;

– the important role in cross-border cooperation played by EC3's support for international investigations. At the same time COM noted with concern that criminal behavior and patterns were evolving fast as result of existing loopholes and new technologies. The lack of reporting obligations for cybercrime, the difficulty of tracking down cyber criminals, the availability of crime as a service (use of malware and other) were mentioned as some of the main challenges. The need to foster new forms of cooperation as well as to improve capacity and provide training and additional resources to effectively tackle large-scale criminal groups was underlined. MS were encouraged to make good use of the funding available under the newly published Regulation on ISP-Police and were invited to take part in the upcoming event organised by the Council of Europe on safeguards and criminal justice (19-20 June).

EEAS also provided some update on the current status of some of the dialogues that had been launched or were in preparation with third countries (India, China, US, Japan, South Korea and Brazil) specifying the level of readiness of the respective terms of reference, timetables and means of reporting. It also informed delegations about the Paris meeting on capacity building held in March and about the presentation of the main areas of the draft cyber defense framework to PMG.

6. Roadmap development

A number of delegations took the floor to provide comments, corrections or suggestions on the revised text as set out in doc. 9298/1/14 REV 1. Some of them underlined the value of this document for their internal coordination back home and at EU level, while others saw it more as a tool for measuring implementation progress. COM also stressed the importance of coordination, but argued against adding additional layers of reporting, as this would only create more paper work without actual value for Strategy implementation.

One delegation proposed to consult the relevant EU agencies to verify whether their involvement in the actions was within their legal mandates and competence. That proposal was welcomed by the Presidency and would be put into practice when preparing the new revised version of the document.

Given the amount of new comments the Presidency requested a last round of written comments to be provided by 2 June 2014, reminding delegations that the road map was a living document and would be regularly updated, thus it would be useful to focus time and effort on implementation of the actions.

7. Presentation of the FoP programme of the incoming IT Presidency

The incoming Presidency briefly outlined their programme, starting with the "Digital Venice" event (7-8 July) that would bring together business and politics in five workshops, including one on trust and security whose focus would be the NIS Directive. The Venice declaration - a possible outcome of the event - would be tabled at the next TTE Council as well as at the first FoP on 23 July, which would also be devoted to unfinished business and possible action.

Other sets of events were planned for the last week of October in Rome, jointly with the IT Research and Innovation Council and ENISA. In the same framework, the IT Ministry of Defence would organise an exercise and would discuss the cyber defence framework. That set of events would be on the agenda for the two attachés meetings (end of September and mid-October). In the 3rd cyber attachés meeting in November some other issues, including cyber crime, would be addressed. Attention would also focus on the Global Alliance against sexual exploitation of children, as its second conference was expected to take place on 2 October 2014. The final capital-based meeting of FoP was planned to take place in the first week of December in order to wrap up their work and draw some conclusions and if possible make recommendations to the new COM. Some concerns were raised regarding the overlap of the first FoP meeting with the GGE meeting in New York as well as the large number of events in the autumn that might necessitate an additional FoP meeting.

8. AOB

The GSC briefly presented the work done so far in preparation for the 1st IPCR exercise based on ENISA's "Cyber Europe 2014" and aimed at testing and validating the respective procedures. Following the outcome of the kick-off meeting held on 22 May a short descriptive paper would be prepared and distributed in FoP IPCR. Delegations were invited to provide feedback by liaising with their respective colleagues.