Council of the
European Union

Brussels, 22 December 2015
(OR. en)

15059/15

CYBER 126
POLMIL 107
TELECOM 230
RELEX 1018
JAIEX 97
COPS 392
IND 206
COSI 185

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	1 December 2015
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 CM 4657/1/15 REV 1, with the addition of one information point by the French delegation under AOB.

2. Information from the Presidency, Commission and EEAS

The Presidency debriefed on the outcome of the seminar on 'Communication Satellites for European Defence and Security: Challenges and Opportunities', which took place in Betzdorf (LU) on 25 November 2015. The participants expressed their views on the challenges and opportunities that satellite communications in the military and the security domains were facing. The debates focused mainly on the importance of pooling and sharing of existing systems, along with the deployment of new generation resources.

The Commission (DG GROW) gave a general presentation of its study on the identification of the requirements for Satellite Communication (SATCOM) to support EU Security Policies and Infrastructures and its main findings relating to the growing security needs of users, the specific security and defence risks and the uncertain evolution of the SATCOM supply.

The Presidency also presented ENISA's main recommendations from its 2015 Report on National and International Cyber Security Exercises, which would help to improve the quality of future cybersecurity exercises. The recommendations included the possible establishment of a Common dataset maintained by ENISA to serve as a common ground for best-practice exchange on cybersecurity exercise development. ENISA would also develop and maintain a European cyber exercise calendar.

The Commission (DG HOME) gave an update on the EU Internet Forum, which was expected to be launched on 3 December 2015. It will tackle the abuse of the internet for terrorist purposes. Follow-up meetings would be organised in the course of 2016 on a number of topics.

The EEAS reported that:

– the EU-China Cyber Task Force would meet on 3 December 2015 in Brussels, with the participation of nine Member States. The agenda would focus on international security, internet governance, an overview of legislation on both sides and the economics of cybersecurity; and that

– the EU-US Cyber dialogue would take place on 7 December 2015 in Washington DC, to discuss issues related to international security, cyber norms, human rights online, capacity building and sectorial cooperation. On the following day a stakeholder meeting was planned.

The EEAS also gave an update on preparations for the World Summit on the Information Society +10 ('WSIS+10') meeting in New York on 15-16 December 2015. The final draft of the outcome document circulated by the co-facilitators was still under discussion.

3. Internal Security Strategy Implementation - Item 4 'Gaps in the Fight against Cybercrime and Practical Responses'

The Presidency recalled that this issue was discussed at the last two cyber attachés meetings, and a summary of those discussions, together with the main conclusions (namely the need of an appropriate legal framework, enhanced cooperation and appropriate law enforcement authority (LEA) capacity), were set out in 14151/15. The Presidency explained that the paper would be provided as input to COSI and CATS as the Presidency view on the matter.

The European Cybercrime Centre (EC3) presented its paper jointly drafted with Eurojust (14812/15) identifying, on the basis of their operational and practical experience, the common challenges in combating cybercrime. Those challenges were clustered in six big groups - loss of data (especially data retention given the lack of common legal framework); loss of location (especially in the context of the use of cloud services); legal framework; public-private-partnership-related aspects; international cooperation and lack of expertise. The representative of EC3 also underlined the need to strengthen the rule of law and to clarify what LEA were allowed to conduct online as well as enhancing the accessibility of information in the framework of a MLA procedure. The final version of the paper would be presented as a result of one of the EMPACT projects on cybercrime (EU policy cycle for organised and serious international crime).

A number of delegations stressed the importance of this issue and referred to some of the problems raised by the Presidency, namely the need to tackle the issue of data retention for the LEA, which often plays as the success or failure factor for their investigations. Some delegations also underlined that the EU should take into account global developments - especially in the Council of Europe and the work done by its Cybercrime Convention Committee (T-CY) as well as that the legal framework should allow the operational level to adapt to the changing technologies. They also pointed out the need to improve both international cooperation, given transnational access to data, and partnership with the private sector. One delegation suggested also involving other relevant Council preparatory bodies, such as the Judicial Cooperation in Criminal Matters (COPEN) Working Party.

The Commission welcomed the work done by the current Presidency, as well as the priorities put forward by the upcoming Presidency, and stressed the importance of finding a legal framework which would ease the establishment of PPP.

4. Internal Security Strategy Implementation - thematic discussion on item 5 ' Research & Development Contribution against Cybercrime'

The Commission (DG HOME) briefed the Group on the former European Union's Research and Innovation funding programme for 2007-2013 (FP7) and on the current programme (Horizon 2020) and its main security research objectives, namely: reinforcing support for the EU's internal and external security, improving the competitiveness of the EU industry, addressing security gaps and preventing threats to security, maintaining a mission-oriented approach, integrating end-users' needs and enhancing the societal dimension.

It also reported on the cybercrime projects in FP7 and the goals of the Commission's call on Fight against crime and terrorism (2014-2015) to avoid incidents and to mitigate its potential consequences. The call was divided in four sub-sectors: forensics, law enforcement capabilities, urban security and ethical/societal dimension. Information was also provided on the Commission's intention to publish another call in 2016 on prevention, detection, response and mitigation of the combination of physical and cyber threats to EU critical infrastructure.

5. Responsible disclosure - way ahead

The Presidency informed the delegations that ENISA, following FoP's request and within its legal framework and mandate, had started gathering information from Member States on how they deal with the issue of responsible disclosure at national level. ENISA would prepare the result for next year.

The Presidency also reported on the main findings and recommendations of the study prepared by ENISA on 'Good Practice Guide on Vulnerability Disclosure ('From challenges to recommendations') as set out in 14721/15.

One delegation underlined the related risks that should be taken into account and recalled that unauthorised access to computer systems was a crime under its domestic law. Another delegation gave an update on progress made so far in introducing this policy on national level.

6. Contractual PPP on cybersecurity - state of play and challenges

The Commission (DG Connect) gave a presentation on the state of play on the future setup of the contractual Private-Public Partnership on cybersecurity (cPPP) as envisaged in the Digital Single Market Strategy, which was aimed at stimulating the competitiveness and innovation capacities of the digital security and privacy industry in Europe and ensuring a sustained supply of innovative cybersecurity products and services in Europe. The cPPP would focus on gathering industrial and public resources to deliver innovation against a jointly agreed strategic research and innovation roadmap; maximising available funds through better coordination with Member States; concentrating on a few technical priorities defined jointly with industry; seeking synergies to develop common, sector-neutral technological building blocks with maximum replication potential; and obtaining economies of scale through engagement with users/demand-side industries and bringing together a critical mass of innovation capacities.

A paper prepared by the Commission (14152/15) had been distributed, providing background information regarding the establishment of this initiative, the relevant legal requirements stipulated in the Horizon 2020 Regulation and several questions relating to Member States' involvement in the cPPP structure.

One delegation expressed its wish to be involved in the governance and contribute to the work and suggested also inviting non-EU countries to contribute and participate, since otherwise there would be the risk of developing EU products not suited for the rest of the world.

Delegations were invited to participate at an appropriate level (including in terms of expertise) in the preparatory workshop that the COM would organise in January 2016 which was aimed at the following three goals. First, Member States and industry sector representatives would be informed about the prerequisites needed to conclude a cPPP. Second, milestones for the industry should be agreed on how to set up a legal entity and to develop the proposal. Thirdly, an understanding should be reached on the desired structure and governance model of cPPP as well as on Member States' role in this structure, membership criteria for the legal entity representing the industry.

7. Network and information security of the EU institutions - update on recent developments

The Head of CERT-EU presented some statistics on alerts and incident response coordination, its detecting tools, the results of a survey conducted and challenges and objectives ahead. CERT-EU also informed delegations that it had set up a web page (http://cert.europa.eu/).

The Commission's Chief Information Security Officer (CISO) briefed the meeting on the current landscape on Network and Information Security of the Commission and its recent development.

The Network Defence Coordinator of the General Secretariat of the Council of the European Union (GSC) explained the Defence Capability (NDC) projects and the current status of the inter-institutional Cyber Security Framework Contract initiated by GSC with the aim at improving the technical interoperability and operational cooperation and providing cybersecurity services and systems to support all EU entities.

8. Cyber Hygiene Project

The LV and EE delegations gave updates on the Cyber Hygiene Project progress. EE recalled the main elements of this initiative, launched in the spring of this year, when six Member States and EEAS signed a pledge to mitigate the human-related risks in cyberspace and undertook to implement behavioural guidelines by introducing an e-learning platform for all categories — users, managers and specialists — in a strategic attempt to change the cybersecurity culture.

LV added that it was currently integrating that initiative in its Ministry of Defence. The UK mentioned in this context its 'Cyber essentials scheme', a government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. It also underlined the role of ENISA as the EU Agency responsible for cybersecurity.

9. Debriefing by the Luxembourg Presidency on the implementation of their priorities and work programme for FoP

The Presidency recalled the concept paper which it had distributed at the beginning of its Presidency term (DS 1416/15) and in which its priorities for FoP were set out, along with a calendar of cyber-related meetings and events during its presidential semester. In this context, it pointed out that a higher number of joint meetings with other Working Parties at attaché level would be desirable.

The Presidency noted the increased number of implemented actions (marked in green) of the EU cybersecurity strategy implementation roadmap (6183/4/15), indicating some misgivings regarding the limited achievements in the field of international development cooperation, due to the complexity of the matter.

10. Priorities and work programme for FoP of the incoming NL Presidency

The incoming NL Presidency presented its main priorities for the FoP for the next six months and reported its intention to distribute its work plan at the first cyber attaché meeting. The work plan built on the preparatory work done with SK and MT from the upcoming Trio and would build on the achievements of the LU Presidency.

The incoming NL Presidency would continue with a strategic horizontal approach and would work on cyberdiplomacy-related aspects, including possible EU positions in international fora and capacity-building; in close contact with the Telecom Working Party it would follow the development of the Digital Single Market, in particular the cPPP standards. It would also continue to follow the implementation of the common cyber-defence policy and work towards the implementation of the Cyber-Security Strategy and its roadmap. Last but not least it would carry on the work started by the LU Presidency on the gaps in the fight against cybercrime in the framework of the EU Renewed Internal Security Strategy and would explore the EU response to cyber-incidents. The NL Presidency would go on with the discussions of responsible disclosure, taking into account the sensitivity of the issue and building on ENISA's results and findings. Together with the future SK Presidency, it would start looking into the renewal of FOP mandate.

The preliminary calendar of meetings would include two FoP meetings on 1 March 2016 and 27 May 2016 respectively, and three cyber-attaché meetings on 26 February 2016, 8 April 2016 and 20 May 2016. The NL Presidency intends to organise a conference on cybercrime-related matters on 3 or 4 March 2016 and on PPP - on 3 or 4 May 2016 (both dates to be confirmed).

11. AOB

The French delegation briefed the meeting on its Digital Security Strategy, updated in October 2015, which was a highly inclusive document bringing together different sectors (e.g. justice, education, internal security, etc.) and spanning five strategic objectives namely: ensuring the defence and security of critical infrastructures and essential operators; fighting cybercrime and protecting the privacy of the citizens; building a culture of cybersecurity, including initial training and continuing education; developing an environment favourable to digital technology businesses, industrial policy and a digital strategic autonomy in Europe; and promoting the overall stability of cyberspace.