**COUNCIL OF THE EUROPEAN UNION**

**Brussels, 23 October 2013 (OR. en)**

**14528/13**

**LIMITE**

**CYBER 21**

**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Friends of the Presidency Group on Cyber Issues (FoP) |
| Subject: | Debate on the implementation of the Council conclusions on the Joint Communication on the EU Cybersecurity Strategy |

**Introduction**

1. In line with paragraph 48 of the Council conclusions on the EU Cybersecurity Strategy adopted by the Council on 25 June 2013[1], the Presidency put forward four options[2] at the last FoP meeting on 15 July 2013 to foster discussion on the role that the Member States would like to attribute to the FoP for it to fulfil its task of reviewing and supporting the ongoing implementation of the Strategy. The Presidency underlined that the four options, namely an action plan (option 1), Trio Presidency programme (option 2), subject/field areas (option 3) and a purely supportive role (option 4) were ideas for discussion, but that the final solution might be a combination of these options or a totally different one.

1 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

2 DS 1563/13

2. During the initial debate at that FoP meeting the majority of Member States welcomed the Presidency initiative and indicated their provisional preference. While some of them favoured the Trio Presidency programme (option 2) with a clear list of priorities, others voted for a model closer to an action plan (option 1) or a combination of these two options.

   One delegation was of the view that a purely supportive role for the FoP (option 4) should be ruled out, as the FoP had to steer and drive the ongoing implementation of the Council conclusions.

   The Commission, supported by the EEAS, expressed the view that the Strategy was to be considered an action plan of which the implementation had already started, and invited the Member States to develop their individual national Action Plans.

   Despite the divergent opinions on the implementation options, a general agreement was reached that the strategic and holistic aspect of the FoP should be preserved, that duplication of other Working Parties' work should be avoided and that the ownership of their respective cyber-related items should be maintained. Furthermore FoP's work should not be overloaded by the creation of additional project groups or new highly demanding administrative mechanisms.

3. As Member States requested more time to study the options, the Presidency set 16 September 2013 as the deadline for written comments.

   Ten delegations and the Commission jointly with the EEAS sent their written comments and/or proposals. A table containing these written contributions is set out in Annex 1.

4. Judging from the positive tone of the initial debate and the written comments received, and taking into consideration the outcome of the informal meeting of JHA Ministers of July 2013, the Presidency is reassured that the FoP should actively contribute through proposals and recommendations towards the successful implementation of the EU Cybersecurity Strategy and the Council conclusions, thereby ensuring more effective cybersecurity in the EU.

5. The Presidency would therefore like to propose a way, which combines elements of the options previously proposed, but reflects the nuances of the various views expressed so far.

This way forward is based on the general assumption that the EU Cybersecurity Strategy already constitutes an action plan by itself, and that the FoP's role would be seen primarily in relation to its implementation, together with the Council conclusions of June 2013 that build upon it.

In the Presidency's view there is a need for a "road map" because the above documents call for action, some explicitly, some through the definition of target areas. Different in nature and reach, their implementation does require coordination among the various actors involved, strategically oriented debates, identification of synergies between the different strands, avoidance of overlaps or unnecessary administrative burdens and, even more importantly, a clear understanding of the main work strands and their prioritisation. As voiced by several Member States, in order to translate these actions into a real workable plan, it is necessary to know where to start.

According to the Presidency this could be achieved by drawing up a "road map" encompassing the following elements, illustrated in a table set out in Annex 2:

– a list of work strands on the basis of the Strategy and the Council conclusions and clustered in six fields - values and prosperity, cyber resilience, cybercrime, CSDP, industry & technology and international cyberspace cooperation. The priority work strands which should be addressed and require further attention should be established through strategic debate within the framework of the FoP. A draft non-exhaustive list of potential work strands in no particular order is set out in the second column of the table given in Annex 2. *The FoP would provide a forum for strategic debate and dialogue to the relevant key actors.*

– a list of actions predefined by the Strategy and the Council conclusions, clustered by work strands. Within its horizontal and cross-cutting framework, the FoP should identify on an ad hoc basis which actions in the priority work strand list are still to be implemented, and thus would benefit the most from synergies. A draft non-exhaustive list of potential actions not currently covered by or under the responsibility of any Working Party will be set out in the third column of Annex 2 once the MSs identify the priority work strands for the respective fields. *The FoP would ensure horizontal consistency and follow-up.*

– a list of key actors, clustered by work strand and action. The comprehensive and high-level framework of the FoP should be used to foster Member State cooperation and dialogue on strategic partnerships, including outside the EU. A draft list of potential actors is set out in the fourth column of Annex 2. *The FoP would serve as a platform for promoting cooperation and exchange.*

**Concluding remarks**

At its meeting on 30 October 2013, the FoP is invited to:

– discuss the way forward as proposed by the Presidency;

– if possible, to approve the way forward, so that forthcoming meetings can, in line with its Term of Reference[3] and subject to renewal of the FoP's mandate, be devoted to examination of a draft list of work strands and selection of the priority ones for which a strategic supervision is necessary and on that basis define potential actions for their implementation.

---

[3] 15686/12 POLGEN 183 JAI 750 TELECOM 198 PROCIV 170 CSC 72 CIS 6 RELEX 988 JAIEX 91 RECH 398 COMPET 659 IND 181 COTER 107.

| MS | Comments | Option 1 Action plan | Option 2 Trio Presidency programme | Option 3 Subject/fields area | Option 4 A purely supportive role |
|---|---|---|---|---|---|
| AT | Austria is for option 1 or 2, with a slight preference for Option 1.<br>We favour an action plan as described in the definition of the document (DS 1563/13) but emphasizing that we don't want a duplication of working groups by project groups of the FOP<br>Motivation:<br>Option 1 ensures a broad coordination structure performing an opportunity for Member States to get involved in the decision process if they want to. Because of the visibility of the implementation activities the option offers also a good possibility to participate in the various working groups.<br>Moreover, option 1 strengthens the character of the FoP group being the coordinative body of the EU regarding Cyber Security. | x | | | |
| | | | x | | |
| BE | Belgium would like to thank the Presidency for its options paper on the implementation of the EU Cybersecurity Strategy (doc DS01563). Belgium believes that an Action Plan or a document of a similar nature (option 1) would be the best way forward in order to follow on the implementation of the EU Cybersecurity Strategy. The listing of actions contained in the Strategy itself (cfr. Boxes) is not sufficient in the sense that there should be some kind of prioritization and a timeframe. | x | | | |
| CZ | CZ would like to express thanks to the Presidency for the proposal, welcomes the proposed document outlining several options and would like to present several comments on the possible follow-up. | x | | | |
| | | | | | x |

| | | | | | |
|---|---|---|---|---|---|
| | CZ would like to point out that the final version of the Council Conclusions, as approved on 25 June, appears under document number 12109/13. That is important, as the Paragraph 48 of that version reads slightly differently (emphasis added):<br>CALLS UPON the Commission and High Representative to produce a progress report on the Cybersecurity Strategy to be presented at the High Level Conference to be held in February 2014; and PROPOSES to hold regular meetings of the competent Council preparatory bodies, (in particular the FoP on Cyber Issues) to assist in setting EU cyber priorities and strategic objectives as part of a comprehensive policy framework and review and support ongoing implementation of the Strategy,<br>The Council Conclusions recognize, in Paragraph 47, the responsibility of the Commission and the High Representative for design of the European activities in this area.<br>While CZ broadly welcomes the main thrust of the Joint Communication, it considers the plans presented by it to be a primary responsibility of its authors. It is difficult, in this setting, to consider Member States responsible for implementation of the Joint Communication made by the Commission and the High Representative.<br>In its Conclusions, the Council proposed to assist in setting EU cyber priorities and strategic objectives. This offer of assistance should not be transformed into parallel driving effort. Therefore, the options proposed should reflect the nature of Council participation.<br>The Czech Republic welcomes the Option 1 of the Presidency document – to put forward an action plan or a document of a similar operational nature which should identify the priority areas. The action plan should specify the priorities and give clear deadlines, so that the Member States would clearly know, what they are bound to do.<br>Further, CZ prefers to focus on discussions among Member States aimed at formulating priorities and strategic objectives on the basis of Member States' common needs and challenges. In addition, Option 4 proposed by the Presidency could dovetail nicely with such activities. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| ES | Spain is in favor of option 2 of doc. DS 1563/13, having always in mind that the mandate of the group of Friends of the Presidency for Cyber Issues is to be a holistic and horizontal forum providing input on horizontal aspects of cyber issues. Duplication of work already done by other groups and overloading the work of the FoP should be avoided. | | x | | |
| FI | Finland warmly welcomes the Presidency's paper (DS 1563/13) on the implementation of the Council Conclusions on EU's Cyber Security Strategy. The implementation of this important set of measures should be proceed without undue delays. Efficient implementation of the Conclusions would require some prioritization of actions, clear identification of responsible parties to take specific actions through, and setting of timeframes for the actions to be implemented.<br>Finland's view is that actors and responsible parties for the implementation of the Strategy at the EU-level are already in place, i.e. there is no need for new significant administrative arrangements or bodies to be found. Council's Friend's of the Presidency on Cyber Issues group is a natural forum for coordination and follow-up of the implementation. The overall sphere of the Strategy and the Conclusions being very broad, we feel that no 'one way fits for all' –approach can be followed with the implementation in various sectors. Same methods for taking the Conclusions forward might not be suitable for different policy fields, like cyber resilience, cybercrime, CDSP or international cooperation.<br>For these reasons, Finland believes that of the four options presented in the Presidency's paper (DS1563/13), the option number 3 might be the most suitable approach. It would allow sector-specific measures to be implemented in a way most appropriate regarding the sector in question. It would also help coordinating the implementation within the FoP-group in a structured way, when coordination and follow-up could be done, first, sector by sector and, as a second step, bringing all sectors together.<br>Our view of the other presented options is that the option number 1 would be administratively very heavy, and therefore not to be supported. Option number 2 could be workable, but it might place a heavy burden on the Trio-Presidency, and leave other Members States with poor ownership of the implementation process. Option number 4 might as well be acceptable for us, but we doubt whether it would | | | x | |

| | | | | | |
|---|---|---|---|---|---|
| | be effective. | | | | |
| DE | The Federal Government of Germany wishes to expressly thank the Lithuanian Presidency for putting forward the options for implementation. The document circulated by the Presidency on 10th of July underlines the shared responsibility of COM, EEAS and the Member States through the respective Council working groups to implement the Cybersecurity Strategy of the COM and the EEAS. Thus, the importance of consistency between the implementing stakeholders cannot be underestimated.<br>The Cyber-FoP should play a central role in implementing the Cybersecurity strategy and the corresponding Council conclusions. Option 2 supports a good balance between coordinating power and flexibility for Member States as well as Commission respecting the different responsibilities. The proposed working plan seems most adequate to coordinate the implementation by focussing on identifying (and aligning) priorities and allocating resources. Another possibility would be combining elements of options 1 and 2 with the 2nd sentence of option 3.<br>Additionally, in the light of increasing importance of digital issues within the EU, in EU-external relations and in global settings, highlighted by the European Council on the "Digital Agenda" in late October, an extension of the FoP mandate beyond the initial one year should be considered.<br>It is worth noting in this context, that the FoP's terms of reference (ANNEX I to council document 15686/12) define a two-fold responsibility of the group: it shall explicitly address Cybersecurity issues including discussions on the implementation of the cyber security strategy of the Commission and EEAS; same time the FoP shall act as a comprehensive cross-cutting forum to, inter alia, coordinate EU-positions towards third countries and in international fora.<br>Additionally, we could ask the Council secretariat to set up a "Cyber Foresight Timeline" for Working groups and Councils where cybersecurity/cyber issues are scheduled to be discussed. | x | | | |
| | | x | | | |
| NL | • Creating an open, free and secure cyberspace for the EU, on the basis of common European values, and active propagation of these values outside the EU, is of importance to the Netherlands. We will work on this together with the international partners and organisations, the private sector and civil society. | x | | | |

| | | | | |
|---|---|---|---|---|
| | • For strategic oversight, the Netherlands finds that the 'Friends of Presidency Group on Cyber Issues' has an important role. This group can guarantee a comprehensive approach to the strategy. The Netherlands attaches great importance to a strong, comprehensive approach of the Member States to the broad area of cybersecurity. Also because the Netherlands has published a National Cyber Security Strategy in which the Netherlands already works on comprehensive policy and implementation of cyber activities, during the last few years. The Netherlands will present an update of the national strategy shortly.<br>• The existing responsibilities will remain in the respective policy areas. Therefore, the FoP will act with respect for the ongoing activities.<br>• With regard to the execution of the strategy, the NL prefers to create an action or working plan or programme by the FoP, for example on the basis of a draft by the Commission and the EEAS. This plan would make it possible for the FoP to measure progress with regard to the implementation of the strategy in a comprehensive manner. Preferably, the FoP can (over the coming semester) give more insight into the priorities, specific responsibilities and ongoing implementation on the basis of such a plan, in which the actions, timeframes and responsible parties are covered.<br>• <u>The Netherlands therefore proposes a combination of the first two options in the paper</u>.<br>• We do not propose to form new project groups however. The respective working groups will cover most parts probably.<br>• The trio presidency would on the basis of such a plan or programme, be able to play a proactive role to ensure the implementation of this programme with the support of the FoP. The FoP would then have an advisory role towards the trio presidency, the Commission and EEAs, and the other MS, both in the preparation phase and in evaluation.<br>• The work of the FoP should be focused, result oriented and avoid overlap. | | | |
| UK | I. The United Kingdom would like to thank the Lithuanian Presidency for circulating their paper DS 1563/13 (10 July 2013) on "Options for implementation of the Council Conclusions on the Joint Communication on Cyber Security | x | | |

| | | | | | |
|---|---|---|---|---|---|
| | Strategy of the European Union".<br>II. The UK believes that a 3 year mandate for the Friends of the Presidency is a sensible way forward to allow more time to take forward the main work strands.<br>III. The UK are in favour of a combination of Options 1 and 2, i.e. a work plan which highlights priorities (Option 1) and agree that it is essential to develop a Work Programme of corresponding activity (i.e. what is going on and where – Option 2) for the Friends of the Presidency to progress.<br>The UK would be prepared to assist in the development of the work plan. | | | | |
| BG | The Republic of Bulgaria expresses its satisfaction with the Options for implementation of the Cyber Security Strategy of the European Union, proposed by the Lithuanian Presidency.<br>No doubt, the Friends of Presidency Group on Cyber Issues has a serious role to play in the implementation of the Strategy.<br>Taking into account the fact that the Cyber Security Strategy of the European Union itself has elements of an action plan (responsibilities, terms) and of a working programme (priorities, activities), and taking into account the need of setting up project groups and drafting working documents if Options 1 or 2 are accepted, we believe that the Friends of the Presidency could play a supportive role (Option 4) and this will contribute to a sufficient extent to the implementation of the Cyber Security Strategy of the European Union. | | | | x |

| | | | | | |
|---|---|---|---|---|---|
| FR | France would like to thank the Lithuanian Presidency for circulating its paper "Options for implementation of the Council Conclusions on the Joint Communication on Cyber Security Strategy of the European Union" (DS 1563/13; 10 July 2013).<br>France is in favor of extending to three years the mandate of the Friends of the Presidency and therefore fully anchoring the FoP in the Council's working landscape. Besides, all member states shall enhance their representation level (the FoP shall meet at least twice a semester in a "Capital-format").France is supportive of a combination of Options 1 and 2: an action plan should highlight priorities to support the strategy (Option 1) and the Trio Presidency should be given a proactive role to play in the implementation of this action plan (Option 2). However, France does not believe in the need for the implementation of project groups (Option 1).<br>France would also like the FoP to ensure the consistency and the complementarity of the implementation activities, as mentioned in Option 3. | | x | | |
| COM/EEAS | The Commission and EEAS fully support the idea that Member States, in particular in the context of the Friends of Presidency Group on Cyber Issues (FoP), should take an active role in the implementation of actions set out in the strategy, in particular as far as these actions have a national dimension. For these purposes, the FoP meetings should serve as a platform for strategic debates between Member States. The Commission and EEAS could only encourage Member States to enter into constructive discussions and coordinate their activities in the implementation of the EU Cybersecurity Strategy. The Commission and EEAS are fully committed to support Member States in this effort, which should ideally start without further delay, given that the time to report on progresses is approaching.<br>The Commission and EEAS welcome the clarification provided at the last meeting of the FoP group that the options presented in this document are to be considered as indicative and purely as a basis for reflection and discussion.<br>The Commission and EEAS are of the view that such a process should not add unnecessary bureaucracy, detracting from the main effort of implementing the Strategy. For one, the EU Cybersecurity Strategy already constitutes an action plan, clearly indicating the relevant actions. Indeed the Commission, EEAS and | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | the other actors listed in the Strategy – including the Member States – have already begun to implement a number of the actions listed. Drawing up either an action plan or a working programme would seem to create an unnecessary administrative burden, especially in view of the diversity of actors involved, without promising to add any clear value. Dedicating resources to this exercise could result in significant delays in the actual implementation of the actions envisaged under the EU Cybersecurity strategy and risks tying down the FoP in questions of procedure, taking room from the strategic dialogues and high-level approach that its mandate sets as its central task. Such dialogue could, for example, include topics such as strategic partnerships outside the EU, current efforts to revise the Budapest Convention on Cybercrime and to negotiate a protocol on transborder access to data, and norms of behaviour in cyberspace, including the London/Budapest/Seoul process.<br>Secondly, as participants will recall, a less cumbersome approach was also favoured by the Member States in the discussions on the Council Conclusions on the Strategy, where the topic of an action plan/work programme was debated at length and discarded in favour of a progress report. In line with the Council Conclusions adopted on 25 June 2013, the Commission and EEAS plan to present this progress report on the implementation of the Strategy in February 2014, one year after the adoption of the Strategy. The presentation of the progress report should coincide with the high-level conference announced in the EU Cybersecurity Strategy, where relevant stakeholders will discuss the state of play of cybersecurity in the EU. The preparation of this high-level event will be coordinated with FoP. | | | | |

**DRAFT ROADMAP**

| Field | Potential work strand | Cc[4] | St | Potential action (not covered by any WP) | Actors |
|---|---|---|---|---|---|
| **A. Values and prosperity** | 1. protection of personal data | X | X | | |
| | 2. promote, protect and enforce values in external policies | X | X | | MS, COM, EEAS |
| | 3. universal applicability of human rights and fundamental freedoms | X | X | | EU, MS |
| | 4. promotion of digital literacy | X | | | EU, MS |
| | 5. for all EU citizens to have access to and enjoy benefits of the | X | X | | MS |

[4] The Potential priority can be present in general similar way in both Council Conclusions and COM/HR Strategy but they may address it in a different manner

| | | | | | |
|---|---|---|---|---|---|
| | Internet | | | | |
| | 6. appropriate legislation | X | | | |
| | 7. cybersecurity as a key to protecting the digital economy | X | | | |
| | | | | | |
| **B. Achieving Cyber resilience** | 1. adoption of proposal for NIS Directive | X | X | | |
| | 2. ensure own efficient level of cybersecurity | X | X | | EU, MS and ENISA |
| | 3. high level of network and information security, and national cyber resilience capabilities of MS | X | X | | MS supported by ENISA |
| | 4. raise EU wide resilience of critical infrastructures | X | X | | |

| | | | | | |
|---|---|---|---|---|---|
| | 5. engagement with industry and academia | X | | | |
| | 6. raise awareness | X | X | | |
| | 7. foster pan-European cybersecurity exercises | X | X | | |
| | 8. effective cooperation & coordination between MS and between MS and EU users | X | | | MS |
| | 9. counter cyber risks and threats with a cross-border dimension | | X | | |
| | 10. further develop the European Public-Private Partnership for Resilience (EP3R) as a sound and valid platform at EU level | | X | | |
| | 11. solidarity clause & | X | X | | |

| | | | | | |
|---|---|---|---|---|---|
| | cybersecurity | | | | |
| | | | | | |
| **C. Cybercrime** | 1. use of EC3 as a means of strengthening cooperation | X | X | | MS |
| | 2. cooperation at EU level and between Europol, Eurojust and all relevant stakeholders | X | X | | Europol, Eurojust |
| | 3. develop adequate digital forensic tools and technologies in view of evolving cybercrime | | X | | |
| | 4. swift ratification of the Budapest Convention on cyber crime | X | X | | Concerned MS |
| | 5. training and up-skilling capabilities of | X | X | | COM, Europol, CEPOL, ENISA |

| | | | | | |
|---|---|---|---|---|---|
| | MS | | | | |
| | 6. use of funding (notably, ISF and IFS) | X | | | COM |
| | 7. fight against cybercrime in third countries where cybercriminal organisations operate from | X | | | COM, EEAS, MS |
| | 8. strong and effective legislation to tackle cybercrime | | X | | |
| | 9. fight against cybercrime in third countries where cybercriminal organisations operate from | X | | | |
| | | | | | |
| **D. CSDP** | 1. develop a cyber defence framework | X | X | | |

| | | | | | |
|---|---|---|---|---|---|
| | 2. enhance MS's cyber defence capabilities | X | X | | |
| | 3. develop cyberdefence capability concentrated on detection, response and recovery from sophisticated cyber threats | | X | | |
| | 4. use of European Security and Defence College | X | | | |
| | 5. utilise synergies with wider EU policies and between civilian and military approaches | X | X | | EU |
| | 6. use of pooling and sharing | X | | | MS, EDA |
| | 7. develop secure and resilient technologies | X | | | MS |
| | 8. research projects | X | | | MS, EDA |

| | | | | | |
|---|---|---|---|---|---|
| | 9. new cyber threats & early warning and response mechanisms | X | | | MS, COM, EEAS, ENISA, EC3, EDA |
| | 10. EU-NATO cooperation on cyber defence | X | X | | |
| | | | | | |
| **E. Industry & Technology** | 1. invest in research and development | X | | | |
| | 2. support and develop EU Information and Communication Technology (ICT) and ICT Security Sector, including owners and providers. | X | | | MS, COM |
| | 3. promote trustworthy European ICT and cybersecurity industries | X | X | | |
| | 4. boost internal market through R&D | X | X | | |

| | | | | | |
|---|---|---|---|---|---|
| | 5. strengthen efforts on R&D in the area of ICT and cybersecurity | X | X | | MS, COM, Enisa |
| | 6. leverage the Horizon 2020 framework programme for research and innovation | X | X | | COM |
| | 7. develop public-private, industrial and academia partnership | X | X | | MS, COM |
| | 8.encourage the private sector to ensure a high level of cybersecurity | | X | | |
| | 9. develop secure and resilient technologies for cybersecurity | X | X | | MS |
| | 10. support cybersecurity in small and medium-size businesses | X | | | MS, COM |

| | | | | | |
|---|---|---|---|---|---|
| | 11. adoption of common approaches among the MS | | X | | |
| | 12. security of the supply chain | | X | | |
| | 13. develop cooperation and information exchange on cybersecurity standards | X | X | | MS, COM, industry |
| | 14. promote the Digital Single Market | X | X | | COM |
| | | | | | |
| **F. International Cyberspace Cooperation** | 1. promote, protect and enforce values in external policies) | X | X | | |
| | 2. develop confidence building | X | X | | EU |
| | 3. Budapest Convention & national cybercrime legislation | X | X | | COM, EEAS |

| | | | | | |
|---|---|---|---|---|---|
| | to promote respect of fundamental rights in cyberspace | | | | |
| | 4. fight against cybercrime in third countries where cybercriminal organisations operate from | X | | | COM, EEAS |
| | 5. develop common EU messages on cyberspace issues | X | X | | COM, EEAS,MS |
| | 6. achieve a high level of data protection | | X | | |
| | 7. ICT capacity building | X | X | | |
| | 8. engage with key international partners and organisations | X | X | | MS, COM, EEAS |
| | 9. integrate and mainstream cyber | X | X | | MS, COM, EEAS |

| | | | | | |
|---|---|---|---|---|---|
| | issues into CFSP | | | | |
| | 10. coordinate global cyber issues and strengthen CIIP cooperation networks | X | X | | MS, COM, EEAS |
| | 11. define norms of behaviour in cyberspace that all stakeholders should adhere to | | X | | |
| | 12. capacity building on cybersecurity and resilient information infrastructures in third countries | X | X | | MS, COM, EEAS, private sector |