Council of the
European Union

Brussels, 11 July 2016
(OR. en)

10964/16

CYBER 82

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	DS 1265/16
Subject:	Questionnaire on the Friends of the Presidency Group on Cyber Issues' Mandate Renewal - Compilation of Member States answers

Delegations will find in Annex a compilation of the answers provided in reply to the Questionnaire on the Friends of Presidency Group on Cyber Issues mandate renewal in view of its expiration in November this year.

ANNEX

CZECH REPUBLIC

With reference to the questionnaire distributed to Member States in May 2016, the Czech Republic wishes to provide the following comments concerning the renewal of the mandate of the Friends of Presidency Group on Cyber Issues (FoP).

Main FoP strengths:

- The cross cutting nature of cyber agenda is rather well addressed by FoP with its horizontal focus, offering on one hand information by various EU bodies and on the other relevant insights by the Member States' representatives (be it at attaché or capitals level).
- We also perceive as positive various non-papers and policy proposals drafted by the group, the cyber diplomacy toolbox being an example.
- We are satisfied with the current frequency of FoP meetings, which offer enough space for discussing cyber issues and keeping up-to-date with developments in other EU entities, while providing cyber attachés with time to work on other agendas.

Areas needing improvement:

- It might be beneficial for each meeting to be focused on one specific issue (beyond the regular information provided by EU bodies), which would, if needed, enable the MS to bring relevant experts for the given meeting. In that regard, reducing the number of agenda items could benefit the quality of discussions.
- Setting a group work plan for each presidency period as well as indicating the time scope for the meetings (especially at the capital level) could be useful.
- While the level of representation in the group should in the event be left to the Member States, indication by PRES of meetings where senior official/capital level representation is desirable to facilitate the decision making.

- To enable better preparation of Member States for the meetings, an earlier distribution of documents, at least five working days prior to the session, together with an annotated agenda is highly recommended.

- In addition, certain topics could be given more space on the FoP agenda. The floor could be opened for briefings on regional initiatives' progress or important PPP projects serving as Lessons Learned.

- Recent work of the group has shown the need for better and closer coordination with other Council structures on some of the topics. We would therefore suggest to include a possibility of organising ad hoc joint sessions with relevant working groups/committees.

- A mechanism should also be sought to enable the FoP to submit proposals to the EU bodies while not being a regular working group within the procedural hierarchy of the Council.

- We should however avoid overlaps with other coordination and cooperation platforms within the EU, namely with the Cooperation Group established by the NIS directive. We trust the Member States will have sufficient access to information on NIS implementation and progress achieved in that group and the FoP will not have to spare much effort and time on this issue (unlike indicated in SK PRES priorities for cyber).

DENMARK

We would welcome the idea of not distinguishing between capital and attachés formats. In that regard we would also like to suggest the meetings to take place with a lower frequency. Maybe 3-4 per presidency.

SPAIN

a) What is your opinion on the functioning of the FoP until now (coordinating role, composition, reporting lines within the Council, reporting lines at Member State level, visibility within the Council structure, relationship with other working groups / EU agencies / other stakeholders?

The Lisbon Treaty made the FoP on cyber issues group possible as it assigned coordination competences with the General Affairs Council. In December 2012 the group was created to ensure horizontal coordination of cyber policy issues in the Council and to examine any relevant horizontal issues, without prejudice to the existing mandate of other Working Parties.

Spain, as other Member States do, confirms the need to continue the mandate of the group preserving its strategic, horizontal and cross-cutting nature.

In general, our opinion on the functioning of the FoP until now is positive.

b) What are the main strengths of the group that should be maintained? Can you please provide specific examples?

- The role of the FoP on cyber issues is not to "produce" as this could mean to interfere in the work of other groups and their competences. The FoP should not duplicate the work of other groups. Its tasks are different. The FoP is the transveral forum on cyber issues and can be the best place to exchange information. Also, the transversal character of the FoP can be useful when misunderstandings are blocking an issue in other groups, for example. The Presidency can include on the agenda, with prior notice, an exchange of opinions, so that the different parties can explain their positions. Each national delegate has to prepare the instructions for the meetings of both FoP and cyber attachés with the comments of several national agencies, given the specific transversal character of the group.

The multidisciplinary nature of the subject is mirrored in a complex institutional construction at the EU and national level. This means that the coordination before each meeting is also complex. As pointed out at the beginning, there is a always a need to know well in advance the points included on the agenda, and the necessary documentation has to be sent well in advance too.

Additionally, it is also important in order to avoid duplication that the new NIS Directive is taken into account, so that future activities of the FoP have in mind the tasks of the groups established by the NIS Directive, in particular, the Cooperation Group.

- One of the objectives of the FoP, as stated in its mandate, is to assist in setting EU cyber priorities and strategic objectives as part of a comprehensive policy framework. Therefore, the Presidency or the Member States can propose “strategic” debates on transversal issues, which are not dealt with in the different other sectorial groups. It is very important that this kind of debate should be prepared and announced in advance. As an example, already mentioned by Spain in previous consultations with the representatives of the FoP, at the meeting of the FoP of 22 September 2015, the Presidency tried to start a debate on the preparation of the WSIS 2015, in order to help the ongoing debate in UN in New York on the non paper for the WSIS 2015. This was not a bad idea per se, but the Presidency could have prepared the debate so that the delegations could have asked their national agencies for instructions. Actually, several delegations stated that they could not intervene without instructions. Once more, we should not forget that the FoP cyber issues is tranversal, the prior national coordination in the different Member States is essential.

c) *What aspects could be improved in order to support its efficient functioning? Can you please provide concrete suggestions?*

- The meetings of both the FoP on cyber issues and the cyber attachés group usually include on the agenda information on activities, past and future, presented by the Commission, the EEAS, ENISA, EDA, EUROPOL, etc.

  The delegations of the Member States at the FoP/cyber attaches need to take into account for each meeting of both groups all the opinions and comments of the different national agencies which have competences on cyber issues. It is very useful that Commission, EEAS, etc distribute a document with the information on the activities (at least a list of the meetings, etc.). This information is of utmost importance as the delegates of the group cannot be specialists in all the activities, given the transversal nature of the FoP on cyber issues. Therefore, in order to be able to understand and follow the information presented, delegates need to have a kind of guide of what is presented. Some Presidencies and some agencies have already distributed this kind of information and it has always been very helpful.

- One of the tasks of the FoP on cyber issues is to follow up the implementation of the EU Cybersecurity Strategy. One of the problems we have been facing is that the Member States do not send regularly information on the implementation of the Roadmap. The FoP EUMSS (EU Maritime Security Strategy) has started to ask periodically the Member States to send a table, designed by the Presidency/Commission and EEAS, with the information on the implementation of the said EUMSS. The information does not have to be exhaustive but more on best practices, lessons learned, actions with transversal character, etc. This could be an example for the FoP on cyber issues.

- The Member States should be encouraged to present best practices and national experiencies in the field of cybersecurity. This has been already done by some delegations and has been really enriching.

- All national agencies with competences on cyber issues should be familiar with the work of the FoP on cyber issues, not only in theory but also more "vitally". They should be encouraged to send representatives to attend at least one time the FoP or cyber attachés meetings, in order to present best practices or simply to get in touch with these two transversal groups

d) Should certain topics be given more place/attention on FOP's agenda? If yes, which ones?

At this point, we do not see specific points to be given more attention on FoP's agenda.

e) Are you happy with the current frequency of meetings? Should FOP be convened more/less often, on the basis of what criteria and in which format?

The current system is acceptable (capitals and attaché meetings).

f) On the basis of the above answers, would you change anything in the current mandate ?

The current mandate is acceptable.

g) Any other suggestions or comments ?

FINLAND

Finland would like to thank the Presidency for initiating discussion on the mandate of cyber FOP - well ahead of November – and for the questions that will help guide our deliberations.

a) What are the main strengths of the group that should be maintained? Can you please provide specific examples.

- We believe there continues to be a need for cyber FOP that has a strategic and horizontal approach to cyber issues.

b) What aspects could be improved in order to support its efficient functioning? Can you please provide concrete suggestions?

- Annotated agendas would be highly useful.
- Timely distribution of background documents would be very useful and would increase effective functioning of esp. capital FOP meetings.
- We would consider it useful to have cyber diplomacy related issues discussed at PSC few times a year. This, we believe, would also bring visibility to highly topical cyber diplomacy issues.

c) Should certain topics be given more place/attention on FOP's agenda? If yes, which ones?

- We would like to see capital FOP to focus more on cyber diplomacy related issues and not to duplicate discussions taking place in other council formats.

d) Are you happy with the current frequency of meetings? Should FOP be convened more/less often, on the basis of what criteria and in which format?

- Current frequency of meetings is good. We would not like to see number of capital level meetings increased.
- We consider it useful to have separate attaché and capital level meetings with capital FOP concentrating on strategic policy level discussions.
- It would be worth exploring how to better take advantage of the attaché level meetings for information sharing (incl. in writing).
- We consider it very necessary not to duplicate the work – i.e. by giving same briefings in both attaché and capital FOP meetings.
- Annotated agendas would be highly useful.
- We would like to see annotated agenda for capital FOP be formulated so that the most important items for discussion are dealt with first; information points only after the policy discussions.
- We would also support organizing whole day meetings at capital FOP but would suggest that enough advance information would be given when whole day meetings are expected to take place.
- We would also welcome the annotated agendas and the background documents to be sent well in advance so as to allow for necessary governmental co-ordination in capitals.

e) On the basis of the above answers, would you change anything in the current mandate ?

HUNGARY

What is your opinion on the functioning of the FoP until now (coordinating role, composition, reporting lines within the Council, reporting lines at Member State level, visibility within the Council structure, relationship with other working groups / EU agencies / other stakeholders?

The Friends of Presidency group is functioning well, it fulfils its role as a coordinating body. We prefer not to distinguish between attaché and capital formats of the meetings: as pointed out by SK as incoming PRES in their document presented at the last FoP meeting, this should be the decision of the MS whom they want to delegate for a specific meeting. The visibility of the FoP within the Council structure needs to be improved. It is important to clearly define which Council formation is responsible for specific topics. The relationship with EU agencies involved in cyber issues is good, as these organisations are also frequent guests in the FoP presenting their activities. FoP visibility towards other Council working parties is probably subject to each MS internally communicating the work done by the FoP.

a) What are the main strengths of the group that should be maintained? Can you please provide specific examples.

We think the FoP is an important format for taking stock of all the activities going on in the EU Council, the Commission, the different agencies and EEAS connected to cyber issues. But it also is a good forum to share Member States' best practices and activities connected to cyber security. We think it is very useful to receive the presentations from the different EU institutions and agencies about their activities in this field.

FoP is an important coordinating body for taking stock of the progress of the EU cybersecurity strategy, and to discuss issues on cyber diplomacy. The value of the FoP also lies in networking with counterparts from other MSs. Since most of the participants of the FoP have a coordinating role for cyber issues in their home countries they are the persons who will probably be able to help if experts for a specific field from a certain country are needed.

b) What aspects could be improved in order to support its efficient functioning? Can you please provide concrete suggestions?

Since this is a horizontal working group comprising several fields of cyber issues, the participants regularly deal with specific issues where they are not experts. It is for this very reason that capitals need to have more time to prepare for FoP meetings – which means that documents to be discussed in a working group meeting should be sent out well in advance (5-7 working days at least), in order to have the possibility to coordinate the national positions internally in advance.

As it was suggested by some delegations at the last FoP an annotated agenda of the meetings would be more than welcome, thus facilitating the preparation for the meetings.
A clear definition would be required what the responsibilities of the cyber attachés and capital format meetings are. Is the attaché meeting a preparatory body of the capital meeting?

c) Should certain topics be given more place/attention on FOP's agenda? If yes, which ones?

Cyber is a fast moving field, there will always be issues needing special attention. Some flexibility in the agenda is necessary to be able to deal with the most pressing issues. Cyber diplomacy is certainly a topic which should be kept on the agenda. Regular updates about the work done in international fora (e.g. London process, GFCE, UN GGE, etc.) would be welcome.

d) Are you happy with the current frequency of meetings? Should FOP be convened more/less often, on the basis of what criteria and in which format?

Approximately one meeting per month on average should be sufficient, however, the issues should determine the number of meetings. Should certain topics require the FoP’s immediate attention more frequent meetings would be acceptable but there may be times when the workload would not necessitate holding meetings in every month.

e) On the basis of the above answers, would you change anything in the current mandate?

In our opinion the mandate of the FoP is broadly well defined, however some fine tuning might be necessary based on the experience of the past four years and the upcoming discussions in the FoP. The mandate should be renewed for a longer period of time, up to five years. It should provide enough flexibility for the FoP to be able to deal with topical issues that come up unexpectedly.

Any other suggestions or comments?

We would like to receive regular updates within the FoP about the work done by the newly formed NIS Coordination Group.

In case of capital format meetings (should this distinction remain) we would generally prefer not to have meetings on Fridays or Mondays.

ITALY

We appreciate the unique horizontal dimension of the group on all matters related to Cyber issues in the EU context. At the moment though, this 'basket' gets the information *ex post* from all the relevant experts working on the matter (JHA, defense, diplomacy, infrastructure, digital internal market, TLC etc..) We have also noticed that, as it has become clear during some recent bilateral meetings in Brussels, these actors share the developments in their various fields of competence only sporadically and with some delay.

· The EU institutions are working in a fragmented and uncoordinated manner. This shows a lack for coherence in the activities and its increasingly critical repercussion in security issues.

· Therefore, while **we are in favour of the renewal of the mandate of FoP Cyber** and appreciate its increasing added value, we would like to see it evolving from a place of *ex post* synthesis and information gathering into an horizontal forum of timely consultation, ahead of and during key moments. To this end we would like to suggest some inputs:

o A timely involvement of the group in all the EU cyber initiatives, while they are still ongoing and not, as it happens at the moment, only once the individual processes in the specialists areas are concluded.

o A longer mandate, more flexible in terms of number of meetings, with a reduction of the 'capital format' meetings.

o A clear and early decision on the key points on the Group's agenda with a medium term perspective (yearly) and with a strategic vision of the objectives.

o Distribution of all relevant documents well in advance, allowing for a proper and effective consultation time in MS Capitals.

LITHUANIA

What is your opinion on the functioning of the FoP until now (coordinating role, composition, reporting lines within the Council, reporting lines at Member State level, visibility within the Council structure, relationship with other working groups / EU agencies / other stakeholders?

a) What are the main strengths of the group that should be maintained? Can you please provide specific examples?

- FoP is instrumental in information exchange and horizontal coordination, as well as exchange of views;
- See merit in keeping distinction between FoP Capitals and Cyber Attaché meetings.

b) What aspects could be improved in order to support its efficient functioning? Can you please provide concrete suggestions?

- Better long-term planning - need to develop a work programme for 1,5 - 2 years, which could be updated every 6 months accompanied by Presidency programme/agenda of the next six months meetings;
- Better preparation for the FoP Capitals - earlier dissemination of the meeting agenda (1 month before the meeting) as well as timely distribution of the supporting material (at least 2 weeks before the meeting) would be helpful.
- Making the group more operational - FoP could more often discuss topical/urgent cyber issues, using the opportunity that most countries have Brussels based Cyber Attaches.
- Ensuring consistency and continuity - it might be worth considering preparing meeting minutes to ensure continuity of the work.

c) Should certain topics be given more place/attention on FOP's agenda? If yes, which ones?

- In principle, all EU cyber domain work strands should be given an adequate attention; In addition, we would support more policy coordination/exchange of views before EU Cyber Dialogues, EU dialogues and cooperation initiatives on cyber security issues with NATO, as well as before Cyber related discussion in other international organisations (UN, OSCE);

d) Are you happy with the current frequency of meetings? Should FOP be convened more/less often, on the basis of what criteria and in which format?

- Do not envisage more than 2-3 FoP Capitals meetings a year; Cyber Attaches could meet more often depending on the work programme, to prepare Capitals meeting as well as if there is an urgent need.

e) On the basis of the above answers, would you change anything in the current mandate ?

- Do not envisage any major changes to the mandate, above mentioned proposals are more linked to a working methods and do not necessarily require the change of legal basis.

Any other suggestions or comments?

- FoP Capitals meetings whenever possible should be organised back to back with NIS Cooperation group in order to reduce the travel expenses and time as well as to keep number of meetings at optimal level.

FRANCE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Paris, le 30 juin 2016

NOTE DES AUTORITÉS FRANÇAISES

Objet : Evolution du mandat du groupe des amis de la Présidence cyber (GAP Cyber).
Ref. : Document DS 01265/16

Les autorités françaises remercient la Présidence d'avoir lancé une réflexion sur l'évolution du mandat du groupe des amis de la Présidence sur les questions inhérentes au cyberespace (GAP Cyber). En effet, le mandat actuel vient à échéance en novembre 2016.

Les autorités françaises considèrent que depuis sa création, le GAP Cyber a montré son utilité à de multiples occasions, notamment dans le cadre :

- de la rédaction de projets de conclusions (cyberdiplomatie, cadre politique européen en matière de cyberdéfense) ;
- d'échanges approfondis sur certains enjeux tels que le cadre européen de la réponse diplomatique de l'UE en cas d'attaque cyber, l'industrie européenne de cybersécurité, la cybersécurité des institutions de l'UE.

Le GAP a toutefois montré certaines insuffisances telles que :

- l'absence de mandat clair attribué au GAP format attachés ;
- la diversité des sujets placés à son agenda sans réelle feuille de route consolidée.

Ces éléments ainsi que la création prochaine d'un groupe de coopération dédié à la cybersécurité, établi par la directive européenne sur la sécurité des réseaux et systèmes d'information (directive NIS), invitent par conséquent à un réexamen et à une clarification des missions et du mode de fonctionnement du GAP Cyber.

Dans le sillage des travaux amorcés par le GAP Cyber ainsi que du 7e cycle d'évaluation GENVAL sur la cybercriminalité, qui recouvre une large diversité de problématiques, les autorités françaises estiment qu'une réflexion devrait par ailleurs être menée sur l'utilité de constituer une enceinte idoine pour utilement contribuer au traitement de la cybercriminalité dans son ensemble, dont sa dimension de coopération internationale. En effet, la cybercriminalité, à la différence du terrorisme et des questions migratoires, ne bénéficie pas d'enceinte dédiée, actuellement.

2

Les autorités françaises souhaitent formuler à titre préliminaire les suggestions suivantes :

En termes d'organisation

- Les deux formats « Capitales » et « Attachés » devraient être préservés.
- Le format « Capitales » devrait se réunir trois fois par an. Les réunions du GAP attachés pourraient se tenir au moins trois fois par an, voire davantage selon les besoins.
- Il est également nécessaire d'assurer la continuité et la visibilité à moyen terme des programmes de travail des trios de Présidences pour le GAP Cyber.

En termes de complémentarité avec les enceintes existantes, les deux formats du GAP devraient s'inscrire en complémentarité des groupes de travail formels du Conseil. En tant que de besoin, en fonction des sujets examinés, des réunions conjointes du GAP Cyber format « attachés » et des groupes pertinents du Conseil pourraient être organisées.

En particulier, concernant le groupe de coopération sur la cybersécurité établi par la directive NIS :

- Le GAP Cyber devrait constituer, pour le futur groupe de coopération, un débouché au sein du Conseil de l'UE pour des travaux réalisés / propositions formulées dans le cadre du groupe de coopération susceptible d'être adoptés sous forme de conclusions du Conseil.
- Par symétrie, le GAP Cyber devrait pouvoir inviter le groupe de coopération à se pencher sur certaines thématiques intéressant son domaine de compétence conformément au mandat octroyé par la directive NIS au groupe de coopération.
- Par extension, le GAP Cyber ne devrait pas tenter de dupliquer les initiatives du groupe de coopération ou initier des travaux qui pourraient être plus efficacement traités dans le cadre du groupe de coopération.

En termes de missions

- Le GAP Cyber « Capitales » devrait :

- permettre des échanges de niveau stratégique autour d'enjeux transverses ou spécifiques aux différents thèmes relevant de son mandat (ex : travaux préparatoires à une future révision de la stratégie européenne de cybersécurité) ;
- finaliser et transmettre pour adoption formelle à la formation concernée du Conseil les projets de conclusions/résolutions/non-papiers ayant trait aux thèmes relevant de son mandat.

- Le GAP Cyber « Attachés » devrait :

- se concentrer sur la rédaction des projets de conclusions/résolutions du Conseil, ou l'examen de non-papiers ;
- faciliter la préparation des réunions du GAP Cyber « Capitales » ;
- permettre des échanges de bonnes pratiques nationales sur les sujets relevant de son mandat ;
- permettre une revue régulière de la feuille de route de mise en œuvre de la stratégie européenne de cybersécurité.

En termes de contenu

- l'agenda des deux formats du GAP Cyber devrait être organisé autour de thématiques clairement définies incluant : cybercriminalité, cyberdiplomatie, cyberdéfense, cybersécurité, gouvernance de l'Internet. Les problématiques de coopération judiciaire devraient également être prises en compte ;

- l'identification de ces thématiques ne devrait néanmoins pas appeler la structuration du GAP Cyber en sous-groupes qui rendraient son fonctionnement beaucoup trop lourd et risquerait d'empiéter sur les groupes de travail thématiques du Conseil préexistants ;
- ces thématiques devraient en revanche permettre l'identification d'enjeux à plus long terme et permettre un suivi plus efficace des activités du GAP Cyber par les Etats membres.

4

ESTONIA AND LATVIA

a) What are the main strengths of the group that should be maintained? Can you please provide specific examples.

The key strengths of the current FoP are its horizontal nature, flexibility and ability to include EU agencies like Europol, ENISA, EEAS, EDA etc. Additionally, participation by both Brussels-based attaches and representatives from capital is a plus. By including topics discussed in both COREPERs and PSC and by giving an overview of what is happening within the EU institutions and bodies, it acts as a positive tool for Member States. Having a platform from which to link cyber-related developments leads to closer coordination and reduces fragmentation.

The FoP format has allowed the Council to tackle transversal questions quite effectively, such as capacity building or the diplomatic toolbox. Inviting the FoP / Cyber attaches to other WPs also ensures a consistent Council approach to cyber. Additionally, the presence of attaches that cover differing sets of Council working groups also allows for more diverse input from the defence, justice and home affairs and foreign affairs perspectives.

b) What aspects could be improved in order to support its efficient functioning? Can you please provide concrete suggestions?

Currently, FoP is dependent on the initiative of each Presidency. The topics aren't set out, which leaves an option for the Presidency only to discuss topics suitable for them. On a practical level, materials are usually presented rather late. To some extent, the current situation reflects the mature nature of the current EU cyber security strategy. Presidencies should be encouraged to provide a longer term (trio) plan for the FoP that is coordinated with all relevant EU institutions and bodies, that give the FoP-Cyber input on what discussions are relevant in the longer term to be able to influence future communications, legislation and projects.

c) Should certain topics be given more place/attention on FOP's agenda? If yes, which ones?

FoP could take on a greater role in broader international cyberspace policy (beyond merely cyber security): e.g. IANA transitioning, internet governance, NATO-EU, UN and OSCE[1] related issues. Questions relating specifically to the NIS directive should be handled via the NIS cooperation group, but the FoP should be informed of the progress and major issues under discussion in the Cooperation group and possibly the CSIRT network.

d) Are you happy with the current frequency of meetings? Should FOP be convened more/less often, on the basis of what criteria and in which format?

The frequency should be dependent on the subjects discussed. Twice during the presidency for capitals meetings is enough, however when there is nothing on the agenda, there shouldn't be compulsory meetings. It might make sense to hold a limited number (1 per Presidency?) of clearly labelled "high-level" meetings and make the rest working level.

e) On the basis of the above answers, would you change anything in the current mandate ?

The mandate could be updated to maintain the horizontal clearing-house nature of the FoP but with an upgraded profile. A Cyber working group could serve as a bridge between cyber in different council formations and institutions (including EDA, EEAS; COM (DG-s HOME, CONNECT, GROW, etc). This group would report directly to COREPER (and possibly also PSC).

The mandate could include more explicit directions to institutions and other formats to report to the FoP. The mandate should maintain broad flexibility and freedom of initiative for the Presidency while also setting out concrete topics that the FoP should definitely deal with. The current mandate could (but does not absolutely need to) be expanded to include issues mentioned in (c).

Additionally, the current mandate could be made permanent or extended for a lengthier period (e.g. 5 years).

Any other suggestions or comments

[1] Update on the OSCE Informal Working Group on Cyber Security

THE NETHERLANDS

A. What are the main strengths of the group that should be maintained? Can you please provide specific examples.

• Broad participation from the Commission, EEAS and agencies such as ENISA. This enables the group to fulfil its role as comprehensive cross-cutting forum.
• The broad range of topics are discussed and should be maintained.
• The current structure in which a topic is discussed at the attaché level before it goes to the capital level works well. It helps focus the capital level discussion to the key strategic points.

B. What aspects could be improved in order to support its efficient functioning? Can you please provide concrete suggestions?

• The most productive discussions in the FOP were those that were accompanied by a cover note with only a handful of specific discussion questions instead of lengthy papers with no clear questions or conclusions. This is recommended for future discussions as well.
• To ensure follow-up of the discussions it is recommended that there are clear recommendations and/or task assigned to one or more actors (Commission, ENISA, Member States, etc).
• The make best use of the FOP as a cross-cutting forum the FOP should be involved earlier in the policy-making process where strategic input from the Member States on the course to take is most useful. The discussions on specific legislation can then be conducted in the relevant working groups.
• More innovative ways to stimulate discussions, for example through scenarios or exercise, could be explored.

C. Should certain topics be given more place/attention on FOP's agenda? If yes, which ones?

While the topics that are now discussed in the FOP cover a broad range that should be maintained, there are additional topics that deserve attention from the FOP:

• The positioning of the FOP vis-à-vis the NIS Directive's CSIRT network and Cooperation Group;
• Stronger emphasis on the future of the EU Cybersecurity Strategy and its Roadmap;
• Capacity-building in third countries
• Digital rights and freedoms
• Engaging the private sector and the internet community, for example through best practices such as ISACs and Coordinated Vulnerability Disclosure;
• Education and strengthening of the cybersecurity workforce;
• Best practices to advance cyber awareness and digital literacy;
• Contribute to the discussion on standardization and certification;
• Research and development;

The diversity of the topics discussed now (both from the Commission's side, EEAS, agencies and the Member States side) should be maintained.

D. Are you happy with the current frequency of meetings? Should FOP be convened more/less often, on the basis of what criteria and in which format?

Frequency of meetings is generally ok. The distinction between a high-level/capital meeting twice per presidency and attaché–level meeting is important, for two reasons:
1) Having senior level representatives from capital and Brussels-based attaches contributes to building trust and good relations between capitals as well as between attaches in Brussels;
2) Senior level officials sufficient have the kind of mandate needed for a good discussion with relevant conclusions.

E. On the basis of the above answers, would you change anything in the current mandate ?

The Netherlands supports a renewal of the mandate under the current terms of reference for another three years.

POLAND

What are the main strengths of the group that should be maintained? Can you please provide specific examples.

Main strength of the group lies in its horizontal character and bringing up all the topics related to cyber affairs. This is extremely helpful in coordinating all the relevant activities related to "cyber" in the Council. This element should be kept. However we should not loose our focus here – the main goal should be to discuss issues related to cybersecurity of European Union. Any extension to other topics, for example different UN agenda, not related to European cyber issues, could be harmful in keeping the effectiveness of the group.

What aspects could be improved in order to support its efficient functioning? Can you please provide concrete suggestions?

We should (re)consider giving more prerogatives to the group as far as taking part in the legislative process in concerned. FoP has been focusing on "soft" aspects of coordinating cyber but due to increasing role of cybersecurity topics on the EU agenda it would be useful to look at the options of engaging the group more formally in the decision making process.

In day-to-day work due to huge amount of documents being discussed at the meetings it would be highly beneficial if they could be sent out through the Secretariat and not only uploaded to the Extranet/Delegates Portal. Especially as this is often done last minute. FoP Group should be kept aware of other cyber initiatives run by other than EU organizations such as OECD or UN, as long as they are related to European or crucial for European cyber security issues.

Are you happy with the current frequency of meetings? Should FOP be convened more/less often, on the basis of what criteria and in which format?

The final answer to that question depends on the scope of the mandate and the assignment FoP will be given. If the group is to be strengthened and given some formal prerogatives in the decision making process then more involvement of the Brussels based counsellors seems to be the right way forward (as in other working parties).

On the basis of the above answers, would you change anything in the current mandate?

The new mandate should not exclude involvement in the legislative processes taking place in the EU as cybersecurity is of cross sectoral nature and its elements are often covered within many different legislative initiatives taken. In terms of topics covered: we should not stretch it too much and stay focused on the crucial element of the level of cybersecurity in the EU.

Any other suggestions or comments ?

We highly appreciate the FoP work done over the last years. The role of the Group is unquestionable. Future attributing of more task, including legislative related ones, would be the next good step in strengthening our joint efforts for safer cyberspace.

ROMANIA

a) What is your opinion on the functioning of the FoP until now (coordinating role, composition, reporting lines within the Council, reporting lines at Member State level, visibility within the Council structure, relationship with other working groups / EU agencies / other stakeholders?

The FoP has a very important coordinating role, managing to harmonize different points of view that were raised during the NIS Directive discussions.

b) What are the main strengths of the group that should be maintained? Can you please provide specific examples.

The main strengths of the group come from the various backgrounds of the members, providing added value to the debates. It is a great format for specific matters of discussions.

c) Should certain topics be given more place/attention on FOP's agenda? If yes, which ones?

One of the topics that should have more room in the FoP agenda is the status of the Cyber Security Road Map implementation, with more info regarding who did what. It would be great if MS that implemented a certain measure could offer expertise to those who need it.

d) Are you happy with the current frequency of meetings? Should FOP be convened more/less often, on the basis of what criteria and in which format?

Currently, the number of meetings is sufficient, but if the situation requires it, there should be a way to increase the frequency of FoPs.

e) On the basis of the above answers, would you change anything in the current mandate?
The PRES SK provided a generous mandate for the FoP and it is a good way ahead.

UNITED KINGDOM

a) What are the main strengths of the group that should be maintained? Can you please provide specific examples.

The group effectively brings together cyber concerns from across the EU and is able to turn its attention to any issue as required. We would support maintaining this freedom so the group can consider topics as diverse as, for example, cyber-crime, NIS implementation and cyber diplomacy,

b) What aspects could be improved in order to support its efficient functioning? Can you please provide concrete suggestions?

c) Should certain topics be given more place/attention on FOP's agenda? If yes, which ones?

The agenda should have the flexibility to address the most important cyber topics as necessary.

d) Are you happy with the current frequency of meetings? Should FOP be convened more/less often, on the basis of what criteria and in which format?

We are happy with the current frequency of the meetings. We find the alternating capital and attaches format to be a useful way of managing the balance between working level and more strategic topics.

e) On the basis of the above answers, would you change anything in the current mandate ?

We see the group as a useful forum which can apply itself to the full range of cyber issues, and would support renewal of the mandate in the current format.