



Brussels, 19 October 2018

CM 4655/1/18
REV 1

CYBER
COPEN
COPS
COSI
DATAPROTECT
IND
JAI
JAIEX

POLMIL
RELEX
TELECOM
DAPIX
CATS
CSC
CSCI
IA

COMMUNICATION

NOTICE OF MEETING AND PROVISIONAL AGENDA

Contact:	cyber@consilium.europa.eu
Tel./Fax:	+32.2.281.7489/+32.2.281.36.02

Subject:	Meeting of the Horizontal Working Party on Cyber Issues (Cyber attachés)
Date:	23 October 2018
Time:	9.00
Venue:	COUNCIL EUROPA BUILDING Rue de la Loi 155, 1048 BRUSSELS

Please note the Council's Security Regulations outlined on page 3 and 4, including the need to register all the delegates who will participate in the classified item of the meeting - ***SECRET UE/EU SECRET*** - meaning that the presentation and following discussion will take place in a separate and secured meeting room.

1. Adoption of the agenda

2. **Activities of INTCEN within the framework of the Cyber Diplomacy Toolbox**
 - Presentation and exchange of views (*SECRET UE/EU SECRET*)*
3. **Information from the Presidency, Commission and the EEAS**
 - Presidency:
 - = Outcomes of Cybersecurity in the Energy Sector conference, 11 October 2018
 - = Outcomes of Cyber Workshop AT Presidency and ISACA, 22 October 2018
 - EEAS:
 - = International cyber developments
4. **EE - BG - AT Trio Programme implementation - EU Cybersecurity Institutional Map**
 - Presentation by ENISA and exchange of views
doc. WK 12596/2018
5. **WHOIS domain names database reform: way forward**
 - Information by COM on the current state of play
 - Discussion on the outcome of the silence procedure on the Draft EU Lines To Take on WHOIS policy reform
doc. 13241/18
6. **UNGA Resolutions on follow up to the UN GGE and on cybercrime**
 - Information by the Presidency and the EEAS and exchange of views
7. **UN Secretary General's High Level Panel on Digital Cooperation**
 - Information by the Executive Director of the UN SG High Level Panel and exchange of views
8. **Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities**
 - 8.1. "Common messages"
 - Discussion
doc. 12854/18 (*RESTREINT UE/EU RESTRICTED*)
 - 8.2. Attribution of malicious cyber activities
 - Discussion
 - 8.3. EU Restrictive measures
 - Follow-up discussion in view of the European Council Conclusions of 18 October 2018

* The presentation will take place in meeting room 70.4.

9. AOB

Note: This meeting will cover information classified *SECRET UE/EU SECRET*, please see **item 2** of the agenda. In accordance with the Council's security rules, all delegates present at the discussion of such items must have a **valid personnel security clearance for access to EU classified information at least up to SECRET UE/EU SECRET level**. Due to the high classification level, item 2 will take part in the secured meeting room (room 70.4).

Delegates should note that in accordance with the Council's Security Rules, only persons with a need-to-know may be admitted to meetings where classified information is to be discussed.

By **18 October 2018**, delegations are requested to forward to cyber@consilium.europa.eu the following details for each delegate taking part in the discussion of these items: **full surname(s), given name, nationality, date of birth** and name of the organisation/institution sending them to the meeting.

The contact point for information for security clearances in the **General Secretariat of the Council (GSC)** is the **GSC Safety and Security Directorate** (security.clearances@consilium.europa.eu, **phone: +32 2 281 3594/9341/7331/6453/8169/3658 - fax: +32 2 281 5081**).

Please ensure that your **National Security Authority** or other competent national authority or your **organisation's security officer** sends a copy of your personnel security clearance certificate to the GSC Safety and Security Directorate **using the above e-mail address/fax number prior to the meeting**.

No admission to the discussion of this item will be granted to delegates for whose clearances the GSC Safety and Security Directorate has no record or who cannot present a valid, original personnel security clearance certificate issued by their National Security Authorities or by other competent national authorities.

It is in the interest of the participants to ensure that their personnel security clearance has not expired.

Please note that certificates sent by the delegates themselves will not be accepted.

During the discussion of SECRET UE/EU SECRET items, all electronic devices must be left outside in the lockers provided in front of the meeting room.

NB: Council documents are available on Delegates Portal. Room attendants will provide copies on request at the earliest opportunity.