



Council of the European Union  
General Secretariat

030274/EU XXVII. GP  
Eingelangt am 08/09/20

Brussels, 8 September 2020

CM 3442/20

CYBER  
COPEN  
COPS  
COSI  
DATAPROTECT  
IND  
JAI  
JAIEX  
POLMIL  
RELEX  
TELECOM

### COMMUNICATION

#### **NOTICE OF MEETING AND PROVISIONAL AGENDA**

---

Contact:	cyber@consilium.europa.eu
Tel./Fax:	+32.2.281.8570 / 7040
Subject:	Horizontal Working Party on cyber issues
Date:	11 September 2020
Time:	14.45
Venue:	COUNCIL JUSTUS LIPSIUS BUILDING Rue de la Loi 175, 1048 BRUSSELS

---

Please note the Council's Security Regulations outlined on page 2 and 3, including the need to register all the delegates (1 per Member State) who will participate in the classified item of the meeting - **CONFIDENTIEL UE/EU CONFIDENTIAL** - meaning that the presentation and following discussion will take place in a secured meeting room.

**Delegations are informed that the discussion of items 1 to 4 of the agenda will take place via videoconference and will start at 10.00h.**

**The discussions of agenda items 5 to 8 will take place in meeting room 35.4 and will start at 14.45h.**

Part 1: Videoconference starting at 10.00h

- 1. Adoption of the agenda**
- 2. Information points**
  - a) NIS Cooperation Group on 22-23 September 2020: Joint Cyber Unit, Evaluation NIS Directive (state of play): Presentation by the Presidency
  - b) Cybersecurity Conference on 9 November 2020: Presentation by the Presidency
  - c) Agency for Innovation in Cybersecurity: Presentation by Germany
- 3. Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**
  - a) Technical meeting on 8-9 September 2020: Debriefing by the Presidency
  - b) Next steps regarding the procedure on the seat: Proposal by the Presidency
- 4. Priorities of the Horizontal Working Party Enhancing Resilience and Countering Hybrid Threats (ERCHT): Presentation by the Chair of the HWP ERCHT**

**5. Cyber Diplomacy Toolbox [CONFIDENTIEL UE/EU CONFIDENTIAL]**

- a) Continuation of discussion
- b) Information by the EEAS

**6. Information points**

- a) UN High Level Panel on Digital Cooperation by the EEAS
- b) EU Cyber Forum by the EEAS
- c) UN Security Council arria-formula meeting on cyber-attacks against critical infrastructure by the EEAS
- d) EU Cyber Net by EU Cyber Net

**7. Developments in UN First and Third Committee**

- a) First Committee (GGE and OEWG): Input by the EEAS and the Netherlands followed by an exchange of views
- b) Third Committee (cybercrime): Information by the EEAS

**8. AOB**

\* \* \*

**\*Note:** This meeting will cover information classified ***CONFIDENTIEL UE/EU CONFIDENTIAL*** please see **item 5** 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 *CONFIDENTIEL UE/EU CONFIDENTIAL* level.**

**A maximum of 1 participant per delegation can attend.**

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.

**List of participants**

Delegations are requested to forward to [WP-CYBER@consilium.europa.eu](mailto:WP-CYBER@consilium.europa.eu) by **09 September 2020 18:00 (Brussels time)** the following details for the 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 him/her to the meeting.

**Personnel Security Clearance**

In accordance with the Council Decision on the Security Rules for Protecting EU Classified Information (2013/488/EU), all delegates attending those meetings must be in possession of a valid EU security clearance up to the level CONFIDENTIEL UE/EU CONFIDENTIAL.

**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.

**Only in case a Personnel Security Clearance Certificate for the delegate concerned has not yet been transmitted to the Security Office, a copy should be sent by National Security Authority or other competent national authority or your organisation's security officer to the following email address, also by 09 September 2020 18:00 (Brussels time)**  
[security.clearances@consilium.europa.eu](mailto:security.clearances@consilium.europa.eu)

**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 CONFIDENTIEL UE/EU CONFIDENTIAL items, all electronic devices must be switched off.**

---

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

NB: Please send a list of your delegates to this meeting as soon as possible to the email address [access.general@consilium.europa.eu](mailto:access.general@consilium.europa.eu)