Conseil de l'Union européenne
Secrétariat général

Bruxelles, le 11 mars 2022

CM 2164/22

CYBER
COPEN
COPS
COSI
DATAPROTECT
IND
JAI
JAIEX
POLMIL
RELEX
TELECOM

COMMUNICATION

CONVOCATION ET ORDRE DU JOUR PROVISOIRE

Correspondant:	cyber@consilium.europa.eu
Tél./Fax:	+32 2 281 3607
Objet:	Groupe Horizontal sur les Questions Cyber
Date:	15 mars 2022
Heure:	9:45
Lieu:	CONSEIL BÂTIMENT JUSTUS LIPSIUS Rue de la Loi 175, 1048 BRUXELLES

Format: 1+1 pour les délégations, 2+2 pour la présidence, la Commission et le SGC

Session du matin – 09h45

1. Adoption de l'ordre du jour

2. **Directive NIS2**
   – Retour des réunions techniques avec le Parlement des 10 et 11 mars 2022
   – Discussion sur les points soulevés lors du GHQC du 8 mars 2022
   – Discussion sur la clause d'exclusion (article 2)
   – Discussion sur l'administration publique
   – Discussion sur la juridiction (Article 24)

3. **Projet de conclusions du Conseil sur le Rapport spécial de la Cour des comptes européenne - « Déploiment des réseaux 5G au sein de l'UE : des retards et des questions de sécurité encore sans réponse »**
   – Présentation par la Présidence
   – Discussion
   6982/22

Session de l'après-midi – 14h45

4. **Boite à outils cyberdiplomatique *(CONFIDENTIEL UE/EU CONFIDENTIAL)*[1]**
   – Présentation par le SEAE
   – Présentation de la Commission
   – Discussion

5. **Régimes de sanctions Cyber : revue des désignations (RESTREINT-UE)**
   – Présentation par le SEAE
   – Discussion

6. **Retour d'expérience sur la gestion des incidents Cyber ayant affecté l'UE ces derniers mois**[2]
   – Présentation par le SEAE
   – Présentation de la Commission
   – Discussion

7. **Processus onusiens en matière de Cybersécurité**
   – Présentation par le SEAE
   – Discussion

8. **Points divers**

NB: Les documents du Conseil sont disponibles sur le Portail des délégués.

---

[1] Ce point sera présenté en présence de l'ENISA et du CERT-EU.

[2] Ce point sera présenté en présence du réseau des CSIRT (Centres de réponse aux incidents de sécurité informatique) et de CyCLONe (réseau pour la préparation et la gestion des crises cyber par les États membres).

* * *

* Cette réunion va traiter des informations classifiées au niveau : "***CONFIDENTIEL UE/EU CONFIDENTIAL***".

Conformément aux règles de sécurité du Conseil, tous les délégués présents lors de l'examen de ces points, doivent posséder une **habilitation de sécurité personnelle (HSP) valide, au minimum du niveau "*CONFIDENTIEL UE/EU CONFIDENTIAL*" afin d'accéder à la salle de réunion lorsque les points seront discutés.**

Les délégués sont priés de noter que, conformément au règlement de sécurité du Conseil, seules les personnes titulaires d'une HSP valide et ayant le besoin d'en connaître, peuvent participer aux réunions quand ces informations classifiées doivent être discutées.

Les délégations sont priées de transmettre la liste des participants **au plus tard le 11 mars 2022 à 17:00 heures à l'adresse courriel suivante wp-cyber@consilium.europa.eu** afin de permettre à la direction Prévention et Sécurité de s'assurer que tous les participants disposent d'une HSP valide pour la réunion.

Vous devez envoyer les informations suivantes pour chaque délégué participant à la réunion : nom(s) de famille, prénom, nationalité, date de naissance, le nom de l'organisation/institution d'appartenance du délégué.

Sur la base de ces informations, si la direction Prévention et Sécurité ne dispose d'aucune information sur l'HSP des délégués, nous vous en informerons et votre autorité nationale de sécurité ou toute autre autorité nationale compétente ou l'officier de sécurité de votre organisation devra envoyer un certificat de l'HSP valide à l'attention de l'équipe en charge de la gestion des habilitations du secrétariat général du Conseil à l'adresse courriel suivante: security.clearances@consilium.europa.eu

1. **Veuillez noter que les certificats envoyés par les délégués eux-mêmes ne seront pas acceptés.**

2. Veuillez indiquer la référence de la réunion dans le sujet pour un traitement plus rapide.

3. Il est dans l'intérêt des participants de s'assurer que leur habilitation de sécurité personnel n'a pas expiré.

Aucune admission à la discussion d'un point classifié ne sera accordée aux délégués pour lesquels la direction Prévention et Sécurité n'a aucun certificat d'habilitation de sécurité personnelle enregistré ou qui ne peut pas présenter un certificat original et valide pour accéder à des informations classifiées de l'UE, délivré par leurs autorités nationales de sécurité ou par d'autres autorités nationales compétentes ou l'officier de sécurité de leur organisation.

Lors de la discussion des points *CONFIDENTIEL UE/EU CONFIDENTIAL*, **tous les appareils électroniques doivent être éteints**. S'ils ne peuvent pas être facilement désactivés, ils ne peuvent pas être conservés dans la salle de réunion.