

Bruxelles, le 20 avril 2023  
(OR. en)

---

---

**Dossier interinstitutionnel:  
2023/0109(COD)**

---

---

8512/23  
ADD 1

CYBER 92  
TELECOM 108  
CADREFIN 51  
FIN 448  
BUDGET 6  
IND 181  
JAI 471  
MI 314  
DATAPROTECT 110  
RELEX 481  
CODEC 662

#### **NOTE DE TRANSMISSION**

---

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	19 avril 2023
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2023) 209 final - Annexe
Objet:	ANNEXES du RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir

---

Les délégations trouveront ci-joint le document COM(2023) 209 final - Annexe.

---

p.j.: COM(2023) 209 final - Annexe

Strasbourg, le 18.4.2023  
COM(2023) 209 final

ANNEX

**ANNEXES**

**du**

**RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir**

## ANNEXE

Le règlement (UE) 2021/694 est modifié comme suit:

(1) À l'annexe I, la section «Objectif spécifique n° 3 — Cybersécurité et confiance» est remplacé par le texte suivant:

«Objectif spécifique 3 - Cybersécurité et confiance

Le programme stimule le renforcement, la création et l'acquisition des capacités essentielles pour sécuriser l'économie numérique, la société et la démocratie dans l'Union en renforçant le potentiel industriel et la compétitivité de l'Union en matière de cybersécurité, et en améliorant la capacité des secteurs privé et public à protéger les citoyens et les entreprises des cybermenaces, y compris en soutenant la mise en œuvre de la directive (UE) 2016/1148.

Les actions initiales et, le cas échéant, les actions ultérieures relevant du présent objectif comprennent:

1. Un co-investissement avec les États membres dans des équipements, des infrastructures et des savoir-faire avancés en matière de cybersécurité qui sont essentiels pour protéger les infrastructures critiques et le marché unique numérique dans son ensemble. Un tel co-investissement pourrait comprendre des investissements dans des installations quantiques et des ressources de données pour la cybersécurité, l'appréciation de la situation dans le cyberspace, **notamment des SOC nationaux et des SOC transfrontières constituant le cyberbouclier européen**; ainsi que d'autres outils à mettre à la disposition des secteurs public et privé dans toute l'Europe.
2. L'extension des capacités technologiques existantes et la mise en réseau des centres de compétence des États membres, en veillant à ce que ces capacités répondent aux besoins du secteur public et de l'industrie, notamment par le biais de produits et services qui renforcent la cybersécurité et la confiance au sein du marché unique numérique.
3. Un large déploiement de solutions de pointe efficaces en matière de cybersécurité et de confiance dans tous les États membres. Ce déploiement comprend notamment le renforcement de la sécurité et de la sûreté des produits, depuis leur conception jusqu'à leur commercialisation.
4. Un soutien comblant le déficit de compétences en matière de cybersécurité, par exemple en alignant les programmes de compétences en matière de cybersécurité, en les adaptant aux besoins sectoriels spécifiques et en facilitant l'accès à des formations spécialisées ciblées.

***5. La promotion de la solidarité entre les États membres en ce qui concerne la préparation et la réaction aux incidents majeurs de cybersécurité par le déploiement de services de cybersécurité par-delà les frontières, y compris un soutien à l'assistance mutuelle entre les autorités publiques et la création d'une réserve de fournisseurs de services de cybersécurité de confiance au niveau de l'Union.»;***

(2) À l'annexe II, la section «Objectif spécifique n° 3 — Cybersécurité et confiance» est remplacé par le texte suivant:

«Objectif spécifique 3 - Cybersécurité et confiance

3.1. Le nombre d'infrastructures ou d'outils de cybersécurité, ou les deux, faisant l'objet de marchés publics conjoints

3.2. Le nombre d'utilisateurs et de communautés d'utilisateurs ayant accès à des installations européennes de cybersécurité

***3.3 Le nombre de mesures d'aide à la préparation et à la réaction aux incidents de cybersécurité dans le cadre du mécanisme d'urgence dans le domaine de la cybersécurité»***

ANNEXE [...]