Conseil de
l'Union européenne

Bruxelles, le 20 mars 2019
(OR. en)

7737/19

CYBER 101	**RELEX 287**
COPEN 118	**TELECOM 141**
COPS 92	**DAPIX 109**
COSI 52	**CATS 43**
DATAPROTECT 98	**CSC 111**
IND 102	**CSCI 47**
JAI 313	**IA 106**
JAIEX 44	**EJUSTICE 44**
POLMIL 31	

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	19 mars 2019
Destinataire:	délégations
Nº doc. préc.:	6866/19
Objet:	Conclusions du Conseil sur le renforcement des capacités en matière de cybersécurité dans l'UE

Les délégations trouveront en annexe les conclusions du Conseil sur le renforcement des capacités en matière de cybersécurité dans l'UE, adoptées par le Conseil des affaires générales qui s'est tenu le 19 mars 2019.

ANNEXE

Conclusions du Conseil sur le renforcement des capacités en matière de cybersécurité dans l'UE

Le Conseil de l'Union européenne,

1. RAPPELANT ses conclusions sur la communication conjointe intitulée "Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide"[1];

2. RAPPELANT ses conclusions sur la réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs[2];

3. RAPPELANT ses conclusions sur le renforcement des cybercapacités externes[3];

4. RÉAFFIRMANT qu'un niveau élevé de sécurité des réseaux et des systèmes d'information peut être assuré par l'amélioration des capacités des États membres et des institutions, agences et organes de l'UE en matière de cybersécurité et le renforcement de leur cyber-résilience en résultant;

5. SALUANT les progrès réalisés par les États membres en vue de renforcer les centres de réponse aux incidents de sécurité informatique (CSIRT);

6. SE FÉLICITANT de la création du réseau des CSIRT par les États membres, avec le soutien actif de la Commission et de l'ENISA, ainsi que de la coopération renforcée au niveau stratégique par l'intermédiaire du groupe de coopération SRI, composé des États membres, de la Commission et de l'ENISA;

---

1 14435/17 (Conclusions du Conseil du 20 novembre 2017 sur la communication conjointe au Parlement européen et au Conseil "Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide").

2 10086/18 (Conclusions du 26 juin 2018 sur la réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs).

3 10496/18 (Conclusions du Conseil du 26 juin 2018 sur des lignes de conduite de l'UE concernant le renforcement des cybercapacités externes).

7. INSISTANT sur le rôle clé que joue le groupe de coopération SRI pour fournir les orientations nécessaires afin d'harmoniser autant que possible l'approche en ce qui concerne la transposition de la directive SRI[4] dans l'ensemble de l'UE ainsi que pour résoudre les problèmes pertinents en matière de cybersécurité;

8. RECONNAISSANT le soutien que la Commission fournit actuellement aux États membres pour renforcer les capacités des CSIRT au moyen du mécanisme pour l'interconnexion en Europe;

9. RECONNAISSANT le soutien apporté aux services répressifs en matière de renforcement des capacités dans la lutte contre la cybercriminalité par l'intermédiaire du Fonds pour la sécurité intérieure et du CEPOL;

10. SALUANT la mise à jour du cadre stratégique de cyberdéfense de l'UE pour soutenir davantage le renforcement des capacités de cyberdéfense des États membres;

11. SE FÉLICITANT des progrès réalisés par les États membres dans la mise en œuvre de la directive SRI;

12. NOTANT que la cybersécurité est un domaine complexe, interdépendant et en constante évolution qui exige que le cadre politique et juridique soit adapté aux nouvelles tendances technologiques et aux technologies émergentes telles que l'intelligence artificielle, les chaînes de blocs et l'informatique quantique;

---

[4] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016).

13. INSISTANT sur le fait que les programmes d'enseignement et de formation liés à la cybersécurité ainsi que les campagnes d'information et de sensibilisation sur les menaces pour la sécurité à destination des utilisateurs finaux sont essentiels afin de réduire les risques en matière de cybersécurité;

14. SOULIGNANT que les cyberexercices sont des instruments efficaces pour évaluer et améliorer encore le niveau de préparation de l'UE et de ses États membres en vue de réagir aux incidents et crises de cybersécurité majeurs;

15. RÉAFFIRMANT que le cyberespace ne connaît pas de frontières, et, par conséquent, que les perspectives et la coopération transfrontières et transsectorielles constituent des éléments essentiels des activités et des initiatives dans le domaine du renforcement des cybercapacités;

16. SOULIGNANT l'importance de la coopération entre le secteur public, le secteur privé et les milieux universitaires, en particulier au moyen de projets collaboratifs;

17. SOULIGNANT l'importance de la coopération civilo-militaire, qui œuvre en faveur d'objectifs communs dans le domaine cyber pour veiller à répondre de manière efficace et cohérente aux cybermenaces,

18. NOTE les progrès réalisés par un groupe d'États membres dans le développement d'équipes d'intervention rapide en cas d'incident informatique en vue d'approfondir la coopération volontaire dans le domaine cyber grâce à l'assistance mutuelle;

19. SE FÉLICITE des discussions en cours au sein du Conseil sur la proposition de règlement du Parlement européen et du Conseil établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination, présentée par la Commission;

20. ENCOURAGE la participation active aux travaux menés actuellement par le groupe de coopération SRI, en particulier en ce qui concerne le renforcement des cybercapacités;

21. ENCOURAGE les travaux que le groupe de coopération SRI mène actuellement sur la réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs;

22. INVITE les États membres à s'appuyer sur leurs stratégies nationales de cybersécurité et à accorder une place importante à la cybersécurité, en tenant compte des exigences sectorielles;

23. INVITE les États membres à réaliser des évaluations et des contrôles constants de l'impact des mesures prises pour renforcer la cyber-résilience et développer les cybercapacités au niveau national;

24. INVITE les États membres à intégrer la cybersécurité et la littératie numérique dans les programmes à tous les niveaux d'enseignement (primaire, secondaire, supérieur, apprentissage tout au long de la vie), sur la base, le cas échéant, des profils d'emploi actuels et futurs;

25. INVITE les États membres à mener des campagnes de sensibilisation à la cybersécurité et des initiatives dans le domaine de l'hygiène cybernétique destinées au grand public et aux utilisateurs finaux, en ciblant les employés du secteur public;

26. ENCOURAGE les États membres à mener des exercices de cybersécurité au niveau national, à mener de tels exercices et/ou à y participer au niveau de l'UE afin de tester les aspects stratégiques et technologiques et de s'y former, et à développer les compétences nécessaires de manière efficace et sur le plan pratique;

27. INVITE les États membres à développer encore les capacités techniques et opérationnelles de leurs CSIRT en matière de cybersécurité dans la cadre de la prévention et de l'atténuation des incidents et de la réponse à ces derniers;

28. INVITE la Commission et l'ENISA à continuer d'aider les États membres à développer les capacités du réseau des CSIRT pour mieux coopérer, partager des informations sur les incidents et répondre efficacement aux incidents transfrontières majeurs;

29. INVITE les États membres à continuer d'aider les services répressifs à développer des compétences spécifiques en collaboration avec les autorités européennes compétentes afin de lutter efficacement contre la cybercriminalité au niveau de l'UE;

30. INVITE les États membres à accroître les investissements destinés au renforcement des cybercapacités;

31. DEMANDE à la Commission et à l'ENISA d'organiser des formations et des programmes de sensibilisation à la cybersécurité pour le personnel des institutions, agences et organes de l'UE;

32. INVITE l'UE et ses États membres à partager des informations et des bonnes pratiques sur une base volontaire afin de contribuer à la définition des principaux besoins en matière de renforcement des cybercapacités et aux réponses à leur donner au niveau national et à celui de l'UE;

33. INVITE l'UE et ses États membres à soutenir la recherche en matière de cybersécurité et à promouvoir la cybersécurité dans d'autres domaines d'étude, en rassemblant plusieurs branches de la recherche et du développement liées à la cybersécurité dans un ensemble intégré, ainsi qu'à favoriser l'excellence de la recherche portant sur la cybersécurité;

34. INVITE l'UE et ses États membres à développer la recherche dans le domaine de la cybersécurité en reflétant les besoins de la société et en intégrant les résultats de la recherche dans le marché;

35. DEMANDE à l'UE et à ses États membres de prendre la cybersécurité en considération dans les procédures de passation de marchés dans le domaine des TIC, le cas échéant.