Conseil de
l'Union européenne

Bruxelles, le 20 octobre 2021
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	19 octobre 2021
Destinataire:	délégations
Nº doc. préc.:	12534/21
Objet:	Conclusions du Conseil - Explorer le potentiel de l'initiative consistant à créer une unité conjointe de cybersécurité, en complément de la réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs - Conclusions du Conseil (19 octobre 2021)

La présidence a présenté un premier projet de conclusions du Conseil intitulées "Explorer le potentiel de l'initiative consistant à créer une unité conjointe de cybersécurité, en complément de la réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs" lors de la vidéoconférence informelle des membres du groupe horizontal, le 19 octobre 2021.

ANNEXE

Conclusions du Conseil - Explorer le potentiel de l'initiative consistant à créer une unité conjointe de cybersécurité, en complément de la réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs

LE CONSEIL DE L'UNION EUROPÉENNE,

RAPPELANT:

– ses conclusions sur la stratégie de cybersécurité de l'UE pour la décennie numérique[1];

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

– ses conclusions sur la cyberdiplomatie[3];

– ses conclusions relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique")[4];

– ses conclusions sur la sécurité et la défense[5];

– le cadre d'action de l'UE en matière de cyberdéfense[6];

– ses conclusions intitulées "Façonner l'avenir numérique de l'Europe"[7];

– la décision d'exécution (UE) 2018/1993 du Conseil du 11 décembre 2018 concernant le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise;

1 7290/21.
2 10086/18.
3 6122/15 + COR 1.
4 10474/17.
5 8396/21.
6 15585/14.
7 8711/20.

– ses conclusions sur la communication conjointe au Parlement européen et au Conseil intitulée "Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide"[8];

– ses conclusions sur le renforcement des capacités en matière de cybersécurité dans l'UE[9];

1. MET EN AVANT l'importance que revêt la cybersécurité pour construire une Europe résiliente, numérique et verte; SOULIGNE que la cybersécurité est indispensable à la prospérité et à la sécurité de l'UE et de ses États membres, de ses citoyens, de ses entreprises et de ses institutions, ainsi qu'à la préservation de l'intégrité de nos sociétés libres et démocratiques;

2. EST CONSCIENT de la nature transfrontière et transsectorielle de nombreuses menaces en matière de cybersécurité, ainsi que des risques et des implications potentielles des incessantes campagnes marquées par des actes de cybermalveillance plus efficaces, plus sophistiqués, plus ciblés, plus complexes, plus persistants et/ou plus généralisés[10]. La pandémie de COVID-19 a mis encore davantage en lumière les vulnérabilités de nos sociétés et les dommages que les incidents de cybersécurité majeurs peuvent causer à l'économie, à la démocratie, aux services essentiels et aux infrastructures critiques, plus particulièrement dans le secteur de la santé. Elle a également exacerbé l'importance de la connectivité ainsi que la dépendance de la société à l'égard de réseaux et de systèmes d'information fiables, dignes de confiance et sûrs. Enfin, elle a mis en évidence la nécessité d'un internet mondial, ouvert, libre, stable et sûr, ainsi que d'une confiance dans les produits, processus et services des technologies de l'information et de la communication (TIC) et dans leur sécurité, y compris la nécessité d'une chaîne d'approvisionnement résiliente;

---

8 14435/17 + COR 1.
9 7737/19.
10 Voir le rapport 2020 de l'ENISA concernant le panorama des menaces.

3. RÉAFFIRME que la cyberrésilience est essentielle et qu'il importe de continuer à développer le cadre européen de gestion des crises en matière de cybersécurité[11] visant à apporter en temps utile une réponse efficace au niveau de l'UE aux incidents et crises de cybersécurité majeurs, ainsi que de l'intégrer davantage aux mécanismes horizontaux et sectoriels de réaction aux crises existant déjà dans l'UE; INSISTE sur le rôle que jouent le Conseil et le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) afin d'assurer une coordination et une réaction en temps utile au niveau politique de l'Union pour les situations de crise, que celles-ci trouvent leur origine dans l'Union ou en dehors, qui ont une incidence ou une importance politique considérables; SOULIGNE qu'il importe de tester ces cadres et mécanismes lors d'exercices réguliers;

4. RAPPELLE que les activités menées au niveau de l'UE en ce qui concerne les incidents et crises de cybersécurité majeurs se déroulent dans le respect des principes de subsidiarité, de proportionnalité, de complémentarité, de non-duplication et de confidentialité; RÉAFFIRME que c'est avant tout aux États membres qu'incombe la responsabilité de réagir aux incidents et crises de cybersécurité majeurs qui les concernent; RAPPELLE qu'il importe de respecter les compétences des États membres, ainsi que leur responsabilité exclusive en matière de sécurité nationale, conformément à l'article 4, paragraphe 2, du traité sur l'Union européenne, y compris dans le domaine de la cybersécurité;

5. RAPPELLE par ailleurs qu'il importe de respecter les compétences et les mandats des institutions, organes et agences de l'UE. Le haut représentant, la Commission et d'autres institutions, organes et agences de l'UE ont également un rôle essentiel à jouer, découlant du droit de l'Union, notamment en raison des répercussions que les incidents et crises de cybersécurité majeurs peuvent avoir sur le marché unique, ainsi que sur le fonctionnement des institutions, organes et agences de l'UE eux-mêmes;

---

[11] 10086/18.

6. INSISTE sur la nécessité d'éviter les doubles emplois inutiles et de rechercher la complémentarité et la valeur ajoutée dans la poursuite du développement du cadre européen de gestion des crises en matière de cybersécurité, et de veiller à l'aligner sur les mécanismes, initiatives, réseaux, processus et procédures existants aux niveaux national et européen; SOULIGNE qu'il importe de rationaliser les processus et structures existants afin d'en réduire la complexité et, dans un souci de cohésion de l'Union, d'en améliorer l'accessibilité et la réactivité pour les personnes qui sollicitent une assistance et de la solidarité;

7. RECONNAÎT l'applicabilité du droit international, y compris de la charte des Nations unies dans son intégralité, du droit international humanitaire et du droit relatif aux droits de l'homme dans le cyberespace; et ENCOURAGE l'adhésion aux normes, règles et principes volontaires non contraignants en matière de comportement responsable des États dans le cyberespace, approuvés par tous les États membres des Nations unies;

8. SE FÉLICITE des progrès accomplis au cours des dernières années au sein du Conseil, en particulier au sein du groupe horizontal "Questions liées au cyberespace" et d'autres groupes concernés du Conseil, ainsi que dans la mise en place d'autres initiatives, réseaux et mécanismes de coopération et de partage d'informations entre les États membres, notamment le groupe de coopération SRI et le réseau des CSIRT, établis par la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016, le réseau européen pour la préparation et la gestion des crises cyber (réseau CyCLONe), ainsi que les projets pertinents liés à la cyberdéfense lancés dans le cadre de la coopération structurée permanente (CSP)[12], la force d'action anticybercriminalité européenne (J-CAT), le réseau judiciaire européen en matière de cybercriminalité (RJEC), les contributions volontaires des États membres au Centre de situation et du renseignement de l'UE (INTCEN), et la coordination et la coopération dans le contexte de la boîte à outils cyberdiplomatique;

[12] En particulier, le projet intitulé "équipes d'intervention rapide en cas d'incident informatique et assistance mutuelle dans le domaine de la cybersécurité" coordonné par la Lituanie, le projet sur le "centre de coordination dans le domaine du cyber et de l'information" coordonné par l'Allemagne, et le projet sur la "plateforme de partage d'informations en matière de réaction aux menaces et incidents informatiques" coordonné par la Grèce.

9. RAPPELLE les cadres de coopération existants entre les institutions, organes et agences de l'UE, tels que la coopération structurée entre l'ENISA et la CERT-UE, ainsi que le protocole d'accord entre l'ENISA, l'Agence européenne de défense (AED), le Centre européen de lutte contre la cybercriminalité (EC3) d'Europol et la CERT-UE; SOULIGNE qu'il importe de continuer à échanger régulièrement avec le Conseil des informations sur l'évolution de ces cadres de coopération;

10. MET EN AVANT qu'il importe de renforcer la coopération et le partage d'informations entre les différentes cybercommunautés au sein de l'UE et de ses États membres à tous les niveaux nécessaires, à savoir technique, opérationnel et stratégique/politique, ainsi que de relier les mécanismes, réseaux, structures, processus et procédures existants de gestion de crises lorsque cela soutient et améliore le traitement des incidents et des crises de cybersécurité majeurs;

11. PREND ACTE des progrès accomplis par un groupe d'États membres dans la création d'une capacité opérationnelle conjointe intitulée "équipes d'intervention rapide en cas d'incident informatique" dans le cadre de la CSP, l'objectif étant d'approfondir la coopération volontaire dans la cybersécurité au moyen d'une assistance mutuelle, y compris en réaction aux incidents et crises de cybersécurité majeurs;

12. PREND ACTE de l'expérience acquise et de la capacité de réaction 24 heures sur 24 et 7 jours sur 7 des services répressifs dans le domaine de la coopération opérationnelle et de l'échange sécurisé d'informations pour lutter contre les cyberattaques transfrontières majeures, dans le cadre du protocole de réaction d'urgence des services répressifs de l'UE;

13. PREND ACTE de la poursuite de la mise en œuvre du cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique"). RAPPELLE que chaque État membre est libre de prendre, au cas par cas et de manière souveraine, sa propre décision eu égard à l'attribution d'un acte de cybermalveillance. RAPPELLE que les mesures prises en vertu du cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance devraient être fondées sur une appréciation commune de la situation convenue entre les États membres. L'INTCEN joue un rôle central en tant que plaque tournante sensibilisant l'UE à la situation et lui fournissant une évaluation des menaces concernant les questions liées au cyberespace, sur la base de contributions volontaires des États membres en matière de renseignement, sans préjudice des compétences de ces derniers.

14. RÉAFFIRME l'importance de l'assistance mutuelle et de la solidarité, conformément à l'article 42, paragraphe 7, du traité sur l'Union européenne et à l'article 222 du traité sur le fonctionnement de l'Union européenne, et APPELLE à la poursuite des exercices comportant une dimension de cybersécurité. RAPPELLE la nécessité de réfléchir à l'articulation entre le cadre européen de gestion des crises en matière de cybersécurité, la boîte à outils cyberdiplomatique et les dispositions des articles susmentionnés en cas d'incidents ou de crises de cybersécurité majeurs. RAPPELLE en outre que les obligations des États membres découlant de l'article 42, paragraphe 7, du traité sur l'Union européenne s'entendent sans préjudice de la spécificité de la politique de sécurité et de défense de certains d'entre eux. RAPPELLE également que l'OTAN reste le fondement de la défense collective des États qui en sont membres.

15. PREND ACTE de la coopération UE-OTAN dans les domaines de la cybersécurité et de la cyberdéfense, y compris du partage d'informations entre la CERT-UE et la capacité OTAN de réaction aux incidents informatiques (NCIRC), dans le respect absolu des principes de transparence, de réciprocité et d'inclusion, ainsi que de l'autonomie décisionnelle des deux organisations.

16. RECONNAÎT l'importance de la coopération, le cas échéant, avec le secteur privé en ce qui concerne les exercices de partage d'informations et la fourniture d'une expertise pertinente ainsi que de solutions et de services fiables, y compris, par exemple, pour soutenir la réaction aux incidents et renforcer l'appréciation de la situation parmi les différentes cybercommunautés.

17. INSISTE sur l'importance des canaux de communication sécurisés pour l'échange d'informations classifiées et sensibles. MET EN AVANT la nécessité de réaliser des progrès supplémentaires.

À cet égard, et compte tenu de ce qui précède,

18. PREND ACTE de la recommandation de la Commission sur la création d'une unité conjointe de cybersécurité, en tant qu'initiative à prendre en compte dans la poursuite de la mise en place du cadre européen de gestion des crises en matière de cybersécurité[13].

19. INVITE l'UE et ses États membres à poursuivre leurs efforts en vue de la mise en place d'un cadre européen de gestion des crises en matière de cybersécurité qui soit plus complet et plus efficace, s'appuyant sur des mécanismes existants et sur les progrès déjà accomplis, et à tenir compte du fait que l'initiative de l'unité conjointe de cybersécurité a le potentiel pour compléter ces mécanismes en adoptant une approche progressive. SOULIGNE qu'un processus progressif, transparent et inclusif est essentiel pour renforcer la confiance et, par conséquent, pour poursuivre la mise en place d'un cadre européen de gestion des crises en matière de cybersécurité. Ce processus devrait respecter les rôles, les compétences et les mandats existants des États membres et des institutions, organes et agences de l'UE, ainsi que les principes énoncés dans les présentes conclusions, notamment la proportionnalité, la subsidiarité, l'inclusion, la complémentarité, la non-duplication et la confidentialité des informations. SOULIGNE, dans le même temps, que toute participation ou contribution potentielle des États membres à une éventuelle unité conjointe de cybersécurité est de nature volontaire.

[13] C(2021) 4520 final (doc. 11155/21 et 11155/21 ADD 1).

20. INSISTE sur la nécessité d'instaurer des méthodes de travail et une gouvernance adéquates afin de permettre à tous les États membres de contribuer et de participer aux processus de délibération, de mise en place et de prise de décisions efficace concernant le cadre européen de gestion des crises en matière de cybersécurité, y compris l'éventuelle initiative de l'unité conjointe de cybersécurité. DEMANDE que soient respectées les prérogatives du Conseil en vertu des traités et du principe de coopération loyale.

21. SOULIGNE qu'il importe de recenser et d'associer toutes les cybercommunautés concernées au sein de l'UE et de ses États membres, tout en tenant compte de leurs différents rôles et responsabilités dans les divers types d'incidents et de crises de cybersécurité majeurs. SOULIGNE le rôle déterminant que joue le Conseil, en particulier par l'intermédiaire du groupe horizontal "Questions liées au cyberespace", en termes d'élaboration des politiques et de coordination eu égard à la poursuite de la mise en place du cadre européen de gestion des crises en matière de cybersécurité. INVITE, dès lors, les États membres, la Commission, le Service européen pour l'action extérieure (SEAE), l'INTCEN, la CERT-UE, l'ENISA, Europol (EC3), Eurojust (RJEC), le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité, ainsi que les représentants du réseau des CSIRT, du réseau CyCLONe, du groupe de coopération SRI, de l'AED et des projets pertinents de la CSP, ainsi que d'autres éventuelles parties concernées, à participer à ce processus. La possibilité de mettre sur pied un groupe de travail, comme le propose la recommandation de la Commission, pourrait être étudiée de manière plus approfondie, en assurant une représentation adéquate de tous les États membres et en agissant conformément aux orientations politiques définies par le Conseil, afin de servir d'enceinte provisoire réunissant des représentants de toutes les cybercommunautés concernées dans les États membres et au sein de l'UE. Ce groupe de travail devrait régulièrement rendre compte de ses activités et soumettre d'éventuelles suggestions au Conseil pour discussion, approbation et orientations supplémentaires. En outre, d'autres formes de dialogue au sein des communautés et entre elles pourraient être établies, notamment au moyen d'ateliers, de séminaires, de formations et d'exercices conjoints.

22. SOULIGNE le rôle du Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et du Réseau de centres nationaux de coordination eu égard à l'éventuelle unité conjointe de cybersécurité, compte tenu notamment de son rôle consistant à renforcer sensiblement les capacités technologiques, les solutions technologiques, ainsi que les capacités et les compétences de l'Union dans le domaine de la cybersécurité.

23. INVITE l'UE et ses États membres à s'engager à poursuivre la mise en place du cadre européen de gestion des crises en matière de cybersécurité, notamment en étudiant le potentiel de l'initiative de l'unité conjointe de cybersécurité, en fixant et en définissant le processus, y compris des étapes et un calendrier, et en précisant les objectifs ainsi que les éventuels rôles et responsabilités. MET L'ACCENT sur la nécessité de consolider, en priorité, les interactions et les réseaux existants au sein de chaque communauté, ainsi que d'établir une cartographie approfondie des éventuelles lacunes et besoins en matière de partage d'informations au sein des cybercommunautés et entre celles-ci, ainsi qu'au sein des institutions, organes et agences de l'UE et entre ceux-ci, et de convenir ensuite des possibles objectifs et priorités essentiels d'une éventuelle unité conjointe de cybersécurité. Sans préjuger du résultat, INSISTE sur la nécessité de se concentrer sur le recensement des besoins en matière de partage d'informations afin de parvenir à une appréciation commune de la situation parmi toutes les communautés concernées. Pour ce qui est du recensement des lacunes et des besoins en matière de partage d'informations, y compris l'éventuelle utilisation de plateformes virtuelles, il convient de continuer à accorder une attention particulière aux canaux de communication sécurisés pour l'échange d'informations classifiées et sensibles, et de SOULIGNER parallèlement qu'il importe d'utiliser les infrastructures existantes. La mise en place d'une approche progressive vise à instaurer un climat de confiance et à jeter les bases d'éventuelles mesures supplémentaires liées au renforcement de la préparation et de la coopération opérationnelle. EST CONSCIENT du fait que des objectifs différents pourraient justifier des solutions différentes et la participation d'un ensemble différent de représentants des cybercommunautés concernées au sein de l'UE et de ses États membres.

24. PRÉCONISE une réflexion plus approfondie concernant une base juridique pour l'éventuelle unité conjointe de cybersécurité tout au long du processus, y compris une évaluation des tâches et des rôles par rapport à ceux assignés à l'ENISA dans la recommandation à la lumière de l'article 7 du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019. APPELLE à poursuivre la réflexion sur les différents éléments de la recommandation sur l'unité conjointe de cybersécurité, y compris en ce qui concerne l'idée des équipes de réaction rapide de l'UE en matière de cybersécurité, ainsi que le plan de l'UE concernant la réaction aux incidents et crises de cybersécurité. MET L'ACCENT sur le fait qu'une éventuelle unité conjointe de cybersécurité doit respecter les compétences, les mandats et les pouvoirs juridiques de ses potentiels futurs participants.

25. INVITE l'Union européenne et ses États membres à prendre en considération le potentiel de l'initiative de l'unité conjointe de cybersécurité, y compris du point de vue des institutions, organes et agences de l'UE, afin de compléter les efforts actuellement déployés au niveau des États membres. SE FÉLICITE de l'intention de la Commission de renforcer la résilience des institutions, organes et agences de l'UE concernés au moyen de sa prochaine proposition de règlement établissant des règles communes contraignantes en matière de cybersécurité pour les institutions, organes et agences de l'UE.

26. En conclusion, RÉAFFIRME son engagement en faveur du renforcement de la cyberrésilience et de la poursuite de la mise en place du cadre européen de gestion des crises en matière de cybersécurité, et ASSURERA LE SUIVI RÉGULIER des progrès accomplis et fournira des orientations supplémentaires pour compléter le cadre européen de gestion des crises en matière de cybersécurité.