Conseil de
l'Union européenne

Bruxelles, le 7 novembre 2017
(OR. en)

13943/17

CYBER 168
TELECOM 263
ENFOPOL 506
JAI 996
MI 771
COSI 258
JAIEX 90
RELEX 933
IND 285
CSDP/PSDC 597
COPS 333
POLMIL 124

NOTE POINT "I/A"

Origine:	Secrétariat général du Conseil
Destinataire:	Comité des représentants permanents/Conseil
Nº doc. préc.:	12762/5/16 REV 5
N° doc. Cion:	12211/17, 12210/17
Objet:	Projet de conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil - Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide - Adoption

1. Lors de la réunion du groupe horizontal "Questions liées au cyberespace", du 26 septembre 2017, la Commission a présenté son paquet "cybersécurité" où figure notamment une communication conjointe intitulée "Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide"[1]. Il y est question de la capacité de l'UE à se protéger des cybermenaces en envisageant des mesures visant à mettre en place une résilience, une dissuasion et une défense plus efficaces en vue de renforcer la cybersécurité de l'UE, ainsi qu'à fournir encouragement et soutien aux États membres afin qu'ils continuent de développer et de maintenir des capacités à la fois plus nombreuses et de meilleure qualité en matière de cybersécurité.

[1] Doc. 12211/17.

2. Les discussions qui ont suivi la présentation de la Commission ont clairement montré qu'il importait de penser l'avenir d'un point de vue stratégique pour ce qui est des questions soulevées dans la communication conjointe, et de prendre un engagement politique pour atteindre les objectifs et adopter les initiatives qui y sont prévus.

3. Lors de la réunion du groupe horizontal "Questions liées au cyberespace", du 6 octobre 2017, la présidence a présenté le premier projet de conclusions du Conseil[2], s'inspirant des observations et contributions écrites initiales des États membres. La discussion a permis de rationnaliser la structure et de cibler les messages, tout en tenant dûment compte de l'ensemble des processus en cours, y compris celui relatif à la transposition de la directive SRI en droit national.

4. Les trois cycles de discussions supplémentaires intervenus lors des réunions du groupe horizontal "Questions liées au cyberespace", du 13 et 30 octobre et du 6 novembre, ainsi que les contributions écrites communiquées par les délégations, ont permis de faire aboutir les négociations au niveau du groupe et d'élaborer le texte de compromis final[3].

5. Sur cette base, il est demandé au Coreper d'inviter le Conseil à approuver le projet de conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil - Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide, dont le texte figure en annexe.

---

[2] Doc. 12762/17.
[3] Doc. 12762/5/17 REV5.

ANNEXE

Projet de conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil - Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide

Le Conseil de l'Union européenne,

1. RECONNAISSANT l'importance de la cybersécurité pour la prospérité, la croissance et la sécurité de l'UE et l'intégrité de nos sociétés libres et démocratiques et des processus qui les sous-tendent à l'ère numérique, en termes de protection tant de l'État de droit que des droits de l'homme et des libertés fondamentales de chacun;

2. SOULIGNANT la nécessité de traiter la cybersécurité dans le cadre d'une approche cohérente au niveau national, mondial et de l'UE, étant donné que les cybermenaces peuvent avoir des répercussions sur notre démocratie, ainsi que sur la prospérité, la stabilité et la sécurité qui sont les nôtres;

3. NOTE qu'un niveau élevé de cyber-résilience dans toute l'UE est également important pour assurer la confiance dans le marché unique numérique et la poursuite du développement d'une Europe numérique;

4. RÉAFFIRMANT que l'UE s'emploiera sans relâche à promouvoir un cyberespace ouvert, mondial, libre, pacifique et sûr dans lequel tant les droits de l'homme que les libertés fondamentales, en particulier le droit à la liberté d'expression, l'accès à l'information, la protection des données, la vie privée et la sécurité, ainsi que les valeurs et principes fondamentaux de l'UE, sont pleinement appliqués et respectés, à la fois au sein de l'UE et au niveau mondial, et SOULIGNANT l'importance cruciale d'assurer un équilibre approprié entre les droits de l'homme et les libertés fondamentales, d'une part, et le respect des exigences de la politique de sécurité intérieure de l'UE, d'autre part[4];

5. CONSCIENT que le droit international, y compris la charte des Nations unies dans son intégralité, le droit international humanitaire et le droit international relatif aux droits de l'homme, s'appliquent dans le cyberespace et INSISTANT dès lors sur la nécessité de poursuivre les efforts pour veiller au respect du droit international dans le cyberespace;

[4] Doc. 12650/17.

6. RAPPELANT ses conclusions sur la stratégie de cybersécurité de l'UE[5], la gouvernance de l'Internet[6], le renforcement du système de cyber-résilience de l'UE[7], la cyberdiplomatie[8] et un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance[9], l'amélioration de la justice pénale dans le cyberespace[10], la sécurité et la défense dans le contexte de la stratégie globale de l'UE[11], le cadre commun en matière de lutte contre les menaces hybrides[12] et l'examen à mi-parcours de la stratégie de sécurité intérieure renouvelée pour l'Union européenne 2015-2020[13];

7. RECONNAISSANT que le cadre prévu par la convention sur la cybercriminalité du Conseil de l'Europe (la convention de Budapest) offre une base solide donnant la possibilité à un groupe de pays diversifié d'appliquer une norme juridique efficace aux différentes législations nationales et à la coopération internationale en matière de lutte contre la cybercriminalité;

8. CONSCIENT de la nécessité de donner une nouvelle impulsion à la mise en œuvre du cadre stratégique de cyberdéfense de 2014 et de l'actualiser pour poursuivre l'intégration de la cybersécurité et de la défense dans la politique de sécurité et de défense commune (PSDC) ainsi que dans une stratégie plus large en matière de sécurité et de défense;

9. RECONNAISSANT qu'une industrie européenne compétitive à l'échelle mondiale est un élément important pour parvenir à un niveau élevé de cybersécurité sur le plan national et dans l'ensemble de l'UE;

10. RAPPELANT que, conformément à l'article 4, paragraphe 2, du traité sur l'Union européenne, la sécurité nationale reste de la seule responsabilité de chaque État membre,

---

5 Doc. 12109/13 et 6225/13 (Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions - Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé (COM JOIN (2013) 1 final)).

6 Doc. 16200/14 et 6460/14 (Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions - Politique et gouvernance de l'Internet: le rôle de l'Europe à l'avenir (COM(2014) 72 final)).

7 Doc. 14540/16 et 11013/16 (Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions - Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité (COM 2016(410) final)).

8 Doc. 6122/15.

9 Doc. 9916/17.

10 Doc. 10007/16.

11 Doc. 9178/17.

12 Doc. 7688/16 (Communication conjointe au Parlement européen et au Conseil - Cadre commun en matière de lutte contre les menaces hybrides: une réponse de l'Union européenne).

13 Doc. 12650/17.

PAR LES PRÉSENTES CONCLUSIONS

11. SE FÉLICITE que la communication conjointe au Parlement européen et au Conseil intitulée "Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide" mette en avant un objectif ambitieux en matière de renforcement de la cybersécurité au sein de l'UE, contribuant aussi à l'autonomie stratégique de l'UE visée dans ses conclusions sur la stratégie globale pour la politique étrangère et de sécurité de l'Union européenne[14] en visant à bâtir une Europe numérique plus sûre, contribuant à la confiance, consciente de sa force, compétitive, ouverte sur le monde, respectueuse des valeurs partagées de l'UE en matière d'internet mondial ouvert, libre, pacifique et sûr – et parvenant par conséquent à un haut niveau de résilience permettant de prévenir, de décourager, de déceler les cybermenaces, d'y réagir et d'être en mesure d'apporter une réponse conjointe aux cybermenaces dans l'ensemble de l'UE; et

12. INVITE les États membres, ainsi que les institutions, agences et organes de l'UE à coopérer, dans le respect des domaines de compétences de chacun et du principe de subsidiarité et de proportionnalité, pour répondre aux objectifs stratégiques énoncés dans les présentes conclusions; et

13. SOULIGNE la nécessité, pour l'UE, ses États membres et le secteur privé, d'assurer un financement suffisant, dans le respect des ressources disponibles, pour soutenir le développement de la cyber-résilience et les efforts de recherche et de développement en matière de cybersécurité dans toute l'UE, ainsi que pour renforcer la coopération visant à prévenir, à décourager, à déceler les cybermenaces, à y réagir et à être en mesure d'apporter une réponse conjointe aux cyberincidents majeurs et aux actes de cybermalveillance dans l'ensemble de l'UE;

[14] Doc. 13202/16.

Chapitre I

ASSURER UNE CYBER-RÉSILIENCE EFFICACE DE L'UE ET LA CONFIANCE DANS LE MARCHÉ UNIQUE NUMÉRIQUE

14. SOULIGNE que c'est à chaque État membre qu'il incombe en premier lieu d'améliorer sa propre cybersécurité et de veiller à répondre aux cyberincidents et aux crises tandis que l'UE peut apporter une forte valeur ajoutée en termes de soutien à la coopération entre les États membres. Dans ce contexte, MET L'ACCENT sur la nécessité, pour tous les États membres, de mettre les ressources nécessaires à la disposition des autorités nationales chargées de la cybersécurité afin de garantir la prévention et la détection des cyberincidents et des crises dans l'ensemble de l'UE ainsi que la réaction face à ceux-ci;

15. SOULIGNE qu'il est nécessaire, dans la mesure du possible, de recourir aux mécanismes, aux structures et aux organisations existants au niveau de l'UE;

16. SALUE:

- les progrès accomplis dans la transposition de la directive SRI par les États membres et INSISTE sur la nécessité de parvenir à une mise en œuvre complète et effective d'ici mai 2018 comme le prévoit ladite directive[15];

- les travaux réalisés au sein du groupe de coopération SRI pour améliorer la coopération stratégique et l'échange d'informations entre les États membres;

- le travail accompli au sein du réseau des centres de réponse aux incidents de sécurité informatique (CSIRT), en particulier pour renforcer la coopération opérationnelle des États membres, en instaurant la confiance envers le partage d'informations dans le cadre de la gestion d'incidents de cybersécurité de grande ampleur et, sur la base des conclusions nationales des États membres, pour fournir des éléments pour une appréciation commune de la situation à l'échelle de l'Union;

- les travaux effectués dans le cadre du partenariat public-privé contractuel sur la cybersécurité.

[15] Sans préjudice de la compétence des États membres pour la transposition de la directive SRI, en particulier en ce qui concerne les opérateurs de services essentiels.

17. SE FÉLICITE qu'il ait été confirmé dans la communication conjointe qu'un cryptage fort et fiable est extrêmement important pour veiller au respect qui convient en matière de droits de l'homme et de libertés fondamentales dans l'UE ainsi que pour assurer la confiance des citoyens à l'égard du marché unique numérique, compte tenu de la nécessité, pour les autorités répressives, d'avoir accès aux données dont elles ont besoin pour leurs enquêtes, et de la confirmation du fait que l'identification et la communication numériques sécurisées jouent toutes deux un rôle essentiel pour assurer l'efficacité de la cybersécurité dans l'UE;

18. SALUE le projet énoncé dans la communication conjointe visant à augmenter le niveau d'ambition en matière de tenue régulière des exercices paneuropéens de cybersécurité combinant les réactions à différents niveaux, en s'appuyant sur les expérience tirées des exercices Cyber Europe, étant donné qu'il s'agira d'un élément important pour renforcer la capacité des États membres et des institutions de l'UE à réagir aux cyberincidents majeurs;

19. DEMANDE à l'UE et à ses États membres de mener régulièrement des exercices stratégiques de cybersécurité dans les différentes formations du Conseil, en s'appuyant sur l'expérience acquise au cours de l'exercice EU CYBRID 2017; et

20. Sans préjudice de l'issue du processus législatif:

- SALUE la proposition de doter l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) d'un mandat fort et permanent ayant pour objectif principal de soutenir et de développer une coopération plus étroite entre les États membres, d'augmenter leurs capacités et d'accroître la confiance à l'égard d'une Europe numérique;

- RÉAFFIRME que la future ENISA devrait s'appuyer sur l'expérience et l'expertise acquises au sein des États membres et de l'UE et soutenir l'élaboration et la mise en œuvre cohérentes des politiques et règlementations existantes et futures de l'UE en matière de cybersécurité, tout en veillant à ce que toutes les compétences de l'ENISA soient développées afin de compléter celles des États membres;

- RÉAFFIRME l'objectif visant à accroître la confiance à l'égard d'une Europe numérique en renforçant le sentiment de sécurité inspiré par les solutions et innovations numériques, y compris l'internet des objets, le commerce électronique et la gouvernance électronique, notamment par un Cadre européen de certification de cybersécurité d'envergure mondiale[16]. Il s'agit d'une exigence essentielle pour renforcer la confiance dans les produits et services numériques et la sécurité de ceux-ci ainsi que pour protéger les infrastructures critiques, les données des pouvoirs publics, des citoyens et des entreprises, et cette exigence jouera un rôle important dans l'adoption d'une approche fondée sur la sécurité dès la conception pour les produits, les services et les processus dans le marché unique numérique;

- SOULIGNE que les travaux législatifs visant à renforcer la certification de cybersécurité au niveau de l'UE devront répondre aux besoins du marché et des utilisateurs et s'appuyer sur les expériences relatives aux capacités et aux processus de certification existants dans l'UE (par exemple, le cadre SOG-IS) et devraient fournir un cadre capable de s'adapter rapidement aux futures évolutions technologiques de pointe dans le domaine du numérique;

- SOULIGNE que le renforcement de la certification de cybersécurité dans l'UE devrait couvrir tout l'éventail des exigences en matière de sécurité, jusqu'aux plus élevées, pour lesquelles la résistance aux capacités des attaquants doit être démontrée. Les principaux facteurs de réussite consisteraient à garantir un processus fiable, transparent et indépendant pour la certification de sécurité afin de promouvoir la disponibilité d'appareils, de logiciels et de services inspirant confiance et sûrs au sein du marché unique et au-delà; à reconnaître l'expertise respective de l'industrie européenne, des pouvoirs publics et des spécialistes de l'évaluation par le biais de normes européennes et mondiales[17]; à respecter le rôle des États membres dans le processus de certification en particulier en ce qui concerne l'évaluation à des niveaux de sécurité plus élevés et notamment en liaison avec l'évaluation des besoins essentiels et des compétences en matière de sécurité. Un tel cadre de certification devrait également faire en sorte que tout système de certification à l'échelle de l'UE soit proportionnel au niveau d'assurance nécessaire pour l'utilisation des produits, des services et/ou des systèmes associés liés aux technologies de l'information et de la communication (TIC) et il permet aux entreprises de toutes tailles de pratiquer le commerce transfrontalier afin de se développer et de vendre de nouveaux produits, à la fois au sein de l'UE et en dehors des marchés de celle-ci;

---

16 Grâce à des normes mondiales élaborées dans l'esprit du Code de pratique de l'OMC concernant les obstacles techniques au commerce.

17 Grâce à des normes européennes et mondiales élaborées dans l'esprit du Code de pratique de l'OMC concernant les obstacles techniques au commerce.

21. SALUE l'intention de mettre en place un réseau de centres de compétences en matière de cybersécurité pour stimuler le développement et le déploiement des technologies dans le domaine de la cybersécurité et de donner un nouvel élan à l'innovation de l'industrie de l'UE sur la scène mondiale dans le développement de la prochaine génération de technologies de pointe, telles que l'intelligence artificielle, l'informatique quantique, les chaînes de blocs et les identités numériques sécurisées;

22. SOULIGNE qu'il est nécessaire que le réseau de centres de compétences en matière de cybersécurité soit inclusif à l'égard de tous les États membres et de leurs centres d'excellence et de compétence existants et accorde une attention particulière à la complémentarité; et compte tenu de cela,

23. PREND NOTE du projet de centre européen de recherche en cybersécurité dont le rôle principal devrait être d'assurer la complémentarité et d'éviter les doubles emplois au sein du réseau de centres de compétences en matière de cybersécurité et avec d'autres agences de l'UE; SOULIGNE que le réseau de centres de compétences en matière de cybersécurité devrait traiter un éventail de questions allant de la recherche à l'industrie et devrait donc contribuer, entre autres, à la réalisation de l'objectif d'autonomie stratégique de l'Europe;

24. dans la perspective du réseau proposé de centres de compétences en matière de cybersécurité, RÉAFFIRME qu'il est nécessaire que l'UE, par l'intermédiaire de ses États membres, développe une capacité européenne dans le domaine de l'évaluation de la force de la cryptographie utilisée dans les produits et services mis à la disposition des citoyens, des entreprises et des pouvoirs publics au sein du marché unique numérique tout en reconnaissant que les politiques en matière de cryptographie sont un aspect essentiel de la sécurité nationale et relèvent par conséquent de la compétence des États membres;

25. INVITE tous les parties prenantes concernées à accroître les investissements dans les applications de nouvelles technologies en matière de cybersécurité afin de contribuer à assurer la cybersécurité dans tous les secteurs de l'économie européenne;

26. SOULIGNE qu'il importe de fournir de façon crédible, fiable et coordonnée des services en matière de cybersécurité aux institutions de l'UE et DEMANDE à la COMMISSION et à d'autres institutions de l'UE de continuer à renforcer l'équipe CERT-UE conformément à ces objectifs et de garantir également des ressources adéquates à cette fin;

27. SALUE l'appel visant à reconnaître l'importance du rôle des chercheurs tiers spécialisés en sécurité dans la détection de failles dans les produits et les services existants et DEMANDE aux États membres d'échanger les meilleures pratiques en matière de divulgation coordonnée des failles;

28. INSISTE SUR la responsabilité de chacun en matière de cybersécurité et INVITE l'UE et ses États membres à promouvoir les compétences numériques et l'éducation aux médias, ce qui aiderait les utilisateurs à protéger leurs informations numériques en ligne et les sensibiliserait aux risques qu'ils encourent lorsqu'ils placent des données personnelles sur internet;

29. SE FÉLICITE de l'importance donnée dans la communication conjointe à l'éducation, à l'hygiène informatique et à la sensibilisation en matière de cybersécurité dans les États membres et l'UE;

30. DEMANDE À LA COMMISSION de fournir rapidement une analyse d'impact relative à l'initiative établissant un réseau de centres de compétences en cybersécurité et un centre européen de recherche et de compétences en cybersécurité et de proposer, d'ici la mi-2018, les instruments juridiques pertinents pour la mise en œuvre de cette initiative;

31. INVITE les États membres:

- à faire figurer en bonne place la sensibilisation à la cybersécurité dans les campagnes d'information et à stimuler la cybersécurité dans les programmes universitaires, d'éducation et de formation professionnelle. Une attention particulière devrait être accordée à l'éducation des jeunes et à la promotion des compétences numériques, afin de former des professionnels prêts à affronter l'avenir et les défis dans les domaines de la sécurité, de l'économie et des services;

- à redoubler d'efforts dans le lancement de programmes de haut niveau spécialisés en matière de cybersécurité afin de combler le manque actuel de professionnels de la cybersécurité dans l'UE;

- à établir un réseau de coopération efficace entre les points de contact en matière d'éducation dans le cadre de l'ENISA. Le réseau des points de contact devrait viser à renforcer la coordination et l'échange des meilleures pratiques entre les États membres en ce qui concerne l'éducation et la sensibilisation à la cybersécurité, ainsi que la formation, les exercices et le renforcement des capacités;

- à envisager d'appliquer les règles de la directive SRI également aux administrations publiques qui participent à des activités sociétales ou économiques critiques, si elles ne sont pas déjà couvertes par la législation nationale et si cela est jugé approprié, et à organiser des formations liées à la cybersécurité également dans les administrations publiques, compte tenu du rôle qu'elles jouent dans notre société et dans notre économie.

Chapitre II

RENFORCER LA CAPACITÉ DE L'UE À PRÉVENIR, À DISSUADER ET À DÉCELER LES ACTES DE CYBERMALVEILLANCE AINSI QU'À Y RÉPONDRE

32. SOULIGNE qu'un cyberincident ou une crise de cybersécurité de nature particulièrement grave pourrait constituer un motif suffisant pour qu'un État membre invoque la clause de solidarité de l'UE[18] et/ou la clause d'assistance mutuelle[19];

33. SALUE l'adoption du "cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance", qui contribue à la prévention des conflits, à la coopération et à la stabilité dans le cyberespace par la définition de mesures relevant de la PESC, et notamment de mesures restrictives, qui peuvent être utilisées pour prévenir les actes de cybermalveillance et y répondre, et DEMANDE au SEAE et aux États membres de mener régulièrement des exercices dans ce cadre;

[18] Article 222 du TUE.
[19] Article 42, paragraphe 7, du TUE.

34. SOULIGNE la nécessité d'apporter une réponse efficace au niveau de l'UE aux incidents et crises de cybersécurité majeurs, tout en respectant les compétences des États membres, ainsi que d'intégrer la question de la cybersécurité dans les mécanismes de gestion des crises qui existent déjà au niveau de l'UE[20]. Pour y parvenir, DEMANDE que la réponse apportée au niveau de l'UE aux incidents de cybersécurité majeurs fasse régulièrement l'objet d'exercices - sur le plan de la réponse tant diplomatique-stratégique que technique -, sur la base des cadres et procédures pertinents, y compris en les affinant le cas échéant[21];

35. SOULIGNE l'importance d'avoir des mécanismes de réponse et d'échange d'informations bien intégrés entre les différents acteurs dont le rôle est essentiel pour assurer la cybersécurité en Europe, y compris entre les organismes compétents de l'UE et les autorités des États membres. Ces mécanismes devront être testés et vérifiés dans le cadre des exercices de cybersécurité menés au niveau de l'UE et être formalisés par des accords appropriés, le cas échéant;

36. PREND NOTE de la possibilité d'examiner une éventuelle proposition de la Commission relative à la création d'un fonds d'intervention d'urgence en matière de cybersécurité, lequel compléterait les efforts déjà déployés par les États membres, dans le respect des ressources disponibles (conformément en particulier au cadre financier pluriannuel de l'UE), visant à aider les États membres à répondre aux cyberincidents majeurs et à en atténuer les répercussions, pour autant que l'État membre concerné ait mis en place un système prudent de cybersécurité avant l'incident, ce qui comprend la mise en œuvre intégrale de la directive SRI et des cadres bien développés de gestion des risques et de surveillance au niveau national;

37. EST CONSCIENT de l'accroissement des liens entre cybersécurité et cyberdéfense et DEMANDE une intensification de la coopération en matière de cyberdéfense, notamment en encourageant la coopération entre acteurs civils et militaires en cas d'incident, ainsi que la poursuite du renforcement de la cybersécurité des missions et opérations relevant de la PSDC;

---

20 Doc. C(2017) 6100 final.

21 Doc. 9916/17 et C(2017) 6100 final.

38. SOULIGNE la nécessité de pouvoir tirer pleinement parti des initiatives proposées en matière de défense afin d'accélérer le développement de cybercapacités adéquates en Europe,
A CONSCIENCE des possibilités qu'offre l'éventuel développement de projets de cyberdéfense au travers de la CSP, si les États membres qui participent à cette coopération le jugent nécessaire, et
RECONNAÎT le rôle joué par la base industrielle et technologique de défense européenne (BITDE) et la base industrielle plus large en matière de cybersécurité civile pour ce qui est de fournir aux États membres les moyens de préserver leurs intérêts en matière de sécurité et de défense relevant du cyberespace;

39. PREND NOTE de la proposition de la Commission de mettre en place une plateforme de formation et d'enseignement en matière de cyberdéfense d'ici la fin de 2018 et SOULIGNE que cette plateforme devrait élargir les possibilités de formation et d'enseignement dans les États membres tout en veillant à la complémentarité avec d'autres efforts et initiatives de l'UE, notamment le CESD et l'AED;

40. DEMANDE à l'UE et à ses États membres d'être attentifs à la menace de vol de propriété intellectuelle grâce aux technologies de l'information et de la communication, y compris pour ce qui est des secrets industriels ou d'autres informations commerciales confidentielles, avec l'intention d'accorder des avantages concurrentiels à des entreprises ou à certains secteurs commerciaux;

41. EST CONSCIENT de la nécessité de lutter contre la criminalité dans le cyberespace, y compris en ce qui concerne le dark web, l'exploitation sexuelle des enfants en ligne, ainsi que la fraude et la contrefaçon des moyens de paiement autres que les espèces, notamment en s'employant à dresser un tableau plus juste en matière de renseignement, à mener des enquêtes conjointes et à partager le soutien opérationnel;

42. SALUE les efforts déployés par l'UE et ses États membres pour relever les défis posés par les systèmes qui permettent aux criminels et aux terroristes de communiquer par des moyens auxquels les autorités compétentes ne peuvent avoir accès, SOULIGNE que ces efforts doivent tenir compte du fait qu'un cryptage fort et fiable est très important pour la cybersécurité et pour la confiance à l'égard du marché unique numérique, ainsi que pour assurer le respect des droits de l'homme et des libertés fondamentales;

43. INSISTE sur l'importance que revêt la fourniture aux services répressifs d'outils permettant de déceler les actes de cybercriminalité, de mener des enquêtes et d'engager des poursuites en la matière, afin d'éviter que les infractions commises dans le cyberespace passent inaperçues ou restent impunies, et SE FÉLICITE de la contribution que le réseau judiciaire européen en matière de cybercriminalité apporte à la lutte contre la criminalité grâce à la coopération entre autorités judiciaires;

44. SOULIGNE qu'il importe d'assurer une position coordonnée de l'UE afin d'influer efficacement sur les décisions européennes et mondiales relatives à la gouvernance de l'internet au sein de la communauté des parties prenantes, notamment en veillant à la mise en place de bases de données WHOIS relatives aux adresses IP et aux noms de domaines, qui soient précises et rapidement accessibles, afin de protéger les capacités des services répressifs et l'intérêt général;

45. SOULIGNE l'importance du recours au protocole internet IPv6, celui-ci étant essentiel au développement de l'"internet des objets" à grande échelle, ainsi que pour mieux imputer les infractions commises dans le cyberespace;

46. ENCOURAGE les travaux en cours sur l'accès transfrontière aux preuves électroniques, le traitement de la conservation des données et les défis posés en matière de procédures pénales par les systèmes qui permettent aux criminels et aux terroristes de communiquer par des moyens auxquels les autorités compétentes ne peuvent avoir accès, en tenant compte de la nécessité de respecter les droits de l'homme et les libertés fondamentales, ainsi que la protection des données;

47. APPELLE la Commission:

- à présenter d'ici décembre 2017 un rapport sur l'état des travaux relatifs à la mise en œuvre de mesures concrètes visant à améliorer l'accès transfrontière aux preuves électroniques;
- à présenter début 2018 une proposition législative en vue d'améliorer l'accès transfrontière aux preuves électroniques;

48. INVITE Europol, l'ENISA et Eurojust:

- à continuer de renforcer leur coopération dans le cadre de la lutte contre la cybercriminalité, tant entre eux qu'avec d'autres parties prenantes, y compris les centres de réponse aux incidents de sécurité informatique (CSIRT), Interpol, le secteur privé et les milieux universitaires, en veillant aux synergies et aux complémentarités, conformément à leurs mandats et compétences respectifs.

- à contribuer, conjointement avec les États membres, à une approche coordonnée en matière de réponse des services répressifs de l'UE aux incidents et crises de cybersécurité majeurs, en vue de compléter les procédures exposées dans les cadres pertinents[22];

49. INVITE l'UE et ses États membres à poursuivre leurs efforts en vue:

- de supprimer les obstacles qui entravent les enquêtes en matière de criminalité et l'efficacité de la justice pénale dans le cyberespace, et de renforcer la coopération et la coordination internationales dans le cadre de la lutte contre la criminalité dans le cyberespace;

- de relever les défis posés par les technologies d'anonymisation en tenant compte du fait qu'un cryptage fort et fiable est très important pour la cybersécurité et pour la confiance à l'égard du marché unique numérique;

- d'influer sur les décisions relatives à la gouvernance de l'internet, qui ont une incidence sur la capacité des services répressifs à lutter contre la criminalité dans le cyberespace;

[22] Doc. 9916/17 et C(2017) 6100 final.

Chapitre III

RENFORCER LA COOPÉRATION INTERNATIONALE POUR UN CYBERESPACE OUVERT, LIBRE, PACIFIQUE ET SÛR AU NIVEAU MONDIAL

50. EST CONSCIENT du fait qu'assurer la cybersécurité représente un défi mondial nécessitant une coopération efficace à l'échelle de la planète entre tous les acteurs, et RECONNAÎT qu'une attention particulière doit être accordée à la défense des valeurs démocratiques et des principes d'un cyberespace ouvert, libre, pacifique et sûr au niveau mondial; et, compte tenu de cela,

51. DEMANDE À L'UE et à ses États membres de favoriser la mise en place d'un cadre stratégique pour la prévention des conflits, la coopération et la stabilité dans le cyberespace, fondé sur l'application du droit international existant, et en particulier la charte des Nations unies dans son intégralité, l'élaboration et la mise en œuvre de normes universelles en matière de comportement responsable des États, et les mesures de confiance régionales entre les États;

52. A CONSCIENCE du rôle joué par les Nations unies dans la poursuite de l'élaboration de normes sur le comportement responsable des États dans le cyberespace, et rappelle que les échanges du groupe d'experts gouvernementaux des Nations unies ont donné lieu, au fil des ans, à un ensemble consensuel de normes et de recommandations, que l'Assemblée générale a soutenu à plusieurs reprises, et que les États devraient adopter comme fondement d'un comportement responsable dans le cyberespace;

53. RECONNAÎT que ces normes de comportement responsable des États impliquent que les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites, qu'ils devraient répondre aux demandes d'assistance appropriées présentées par un autre État dont l'infrastructure critique est la cible d'actes informatiques malveillants émanant de leur territoire et qu'ils devraient prendre des mesures appropriées pour protéger leur infrastructure critique des menaces informatiques;

54. A CONSCIENCE du caractère partagé des cybermenaces et des risques informatiques auxquels sont confrontés l'UE, l'OTAN et leurs États membres respectifs et RAPPELLE qu'il importe de poursuivre la coopération UE-OTAN dans le domaine de la cybersécurité et de la défense, dans le plein respect des principes de l'inclusion, de la réciprocité et de l'autonomie des processus décisionnels de l'UE et conformément à ses conclusions du 6 décembre 2016 sur la mise en œuvre de la déclaration commune du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du Traité de l'Atlantique Nord[23];

55. INVITE l'UE et ses États membres à soutenir et à encourager la mise en place de mesures de confiance régionales, qui constituent un élément essentiel pour accroître la coopération et la transparence et réduire les risques de conflit. La mise en œuvre de mesures de confiance dans la cybersécurité dans le cadre de l'OSCE et d'autres structures régionales renforcera la prévisibilité du comportement des États et contribuera à stabiliser davantage le cyberespace;

56. AFFIRME À NOUVEAU que l'UE continuera à défendre ses valeurs fondamentales en protégeant les droits de l'homme et les libertés fondamentales sur la base des orientations de l'UE en matière de droits de l'homme relatives à la liberté en ligne. L'UE souligne également qu'il est important que toutes les parties prenantes participent à la gouvernance de l'internet, y compris les milieux universitaires, la société civile et le secteur privé;

57. DEMANDE à l'UE et à ses États membres de favoriser le renforcement des capacités en matière de cybersécurité dans les pays tiers, en accordant une attention particulière aux pays du voisinage européen et aux pays en développement qui connaissent une évolution rapide de la connectivité, en relation avec la lutte contre la cybercriminalité et le renforcement de la cyber-résilience, dans le respect des valeurs fondamentales de l'UE. Pour faire avancer les efforts de l'UE dans ce domaine, il conviendrait de mettre en place un réseau de l'UE pour le renforcement des cybercapacités et d'élaborer des lignes directrices de l'UE sur le renforcement des capacités en matière de cybersécurité, de manière complémentaire avec les structures et mécanismes existants;

[23] Doc. 15283/16.

58. SOULIGNE les progrès accomplis dans la coopération UE-OTAN en matière de cyberdéfense et de cybersécurité, et l'évolution à cet égard sur le plan de la formation, de l'enseignement et des concepts, tout en évitant la duplication inutile des efforts lorsque les besoins se recoupent, ainsi qu'en renforçant l'interopérabilité au moyen des exigences et des normes en matière de cyberdéfense, et APPELLE à poursuivre la coopération dans le cadre d'exercices axés sur la cyberdéfense (au niveau du personnel) et à partager les bonnes pratiques en matière de gestion de crises, tout en évitant la duplication inutile des efforts lorsque les besoins se recoupent, dans le strict respect du cadre d'action de l'UE en matière d'exercices et des principes de l'inclusion, de la réciprocité et de l'autonomie des processus décisionnels de l'UE;

59. EST CONSCIENT que la Convention sur la cybercriminalité du Conseil de l'Europe, également connue sous le nom de Convention de Budapest, offre une norme juridique efficace pour éclairer les législations nationales en matière de cybercriminalité. DEMANDE à tous les pays de concevoir des cadres juridiques nationaux appropriés et de poursuivre leur coopération dans l'actuel cadre international défini par la Convention de Budapest;

60. RAPPELLE les résultats obtenus dans le cadre des cyberdialogues bilatéraux de l'UE et invite à redoubler d'efforts pour faciliter la coopération avec les pays tiers en matière de cybersécurité;

61. RAPPELLE que l'UE dispose d'un mécanisme de contrôle des exportations solide et juridiquement contraignant, fondé sur les décisions et bonnes pratiques développées dans le cadre des régimes internationaux de non-prolifération, PREND NOTE des discussions menées actuellement au sein du Conseil en vue de déterminer comment améliorer encore le fonctionnement de ces contrôles, et INVITE les États membres à continuer de traiter, dans le cadre des régimes internationaux de contrôle des exportations pertinentes (comme l'Arrangement de Wassenaar), les applications des nouvelles technologies critiques en matière de cybersécurité, afin d'assurer un contrôle efficace des technologies critiques de demain dans ce domaine.

62. Dans le prolongement des conclusions du Conseil européen du 19 octobre 2017[24], les présentes conclusions seront mises en œuvre au moyen d'un plan d'action que le Conseil doit adopter avant la fin de l'année 2017. Destiné à être utilisé comme un document évolutif, ce plan d'action sera régulièrement réexaminé et actualisé par le Conseil.

---

[24] Doc. EUCO 14/17.