Conseil de
l'Union européenne

Bruxelles, le 23 mars 2021
(OR. en)

7290/21

CYBER 80
TELECOM 124
COPEN 144
CODEC 443
COPS 107
COSI 50
CSC 119
CSCI 45
IND 70
RECH 117
ESPACE 21

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	22 mars 2021
Destinataire:	délégations
Objet:	Conclusions du Conseil sur la stratégie de cybersécurité de l'UE pour la décennie numérique - Conclusions du Conseil approuvées par le Conseil lors de sa session du 22 mars 2021

Les délégations trouveront en annexe les conclusions du Conseil sur la stratégie de cybersécurité de l'UE pour la décennie numérique, approuvées par le Conseil lors de sa session du 22 mars 2021.

ANNEXE

Conclusions du Conseil sur la stratégie de cybersécurité de l'UE pour la décennie numérique

LE CONSEIL DE L'UNION EUROPÉENNE,

RAPPELANT:

- ses conclusions relatives à la communication conjointe au Parlement européen et au Conseil du 25 juin 2013 concernant la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé[1];

- ses conclusions sur la gouvernance de l'Internet[2];

- ses conclusions sur la communication conjointe au Parlement européen et au Conseil du 20 novembre 2017 intitulée: "Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide"[3];

- ses conclusions sur le renforcement des capacités en matière de cybersécurité dans l'UE[4];

- ses conclusions sur l'importance de la 5G pour l'économie européenne et sur la nécessité d'atténuer les risques pour la sécurité liés à la 5G[5];

- ses conclusions sur l'avenir d'une Europe fortement numérisée après 2020: "Stimuler la compétitivité numérique et économique dans l'ensemble de l'Union et la cohésion numérique"[6];

- ses conclusions intitulées "Efforts complémentaires pour renforcer la résilience et lutter contre les menaces hybrides"[7];

- ses conclusions intitulées "Façonner l'avenir numérique de l'Europe"[8];

---

1 12109/13.
2 16200/14.
3 14435/17 + COR 1.
4 7737/19.
5 14517/19.
6 9596/19.
7 14972/19.

- ses conclusions sur la diplomatie numérique[9];

- ses conclusions sur le renforcement de la résilience et la lutte contre les menaces hybrides, y compris la désinformation, dans le contexte de la pandémie de COVID-19[10];

- ses conclusions sur la cyberdiplomatie[11];

- ses conclusions sur la réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs[12];

- ses conclusions relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique")[13];

- ses conclusions sur des lignes de conduite de l'UE concernant le renforcement des cybercapacités externes[14];

- ses conclusions intitulées "Une relance au service de la transition vers une industrie européenne plus dynamique, résiliente et compétitive"[15];

- ses conclusions sur la cybersécurité des dispositifs connectés[16];

- ses conclusions intitulées "Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité"[17];

- sa résolution sur le chiffrement - La sécurité grâce au chiffrement et malgré le chiffrement[18];

---

8 8711/20.
9 12804/20.
10 14064/20.
11 6122/15 + COR 1.
12 10086/18.
13 10474/17.
14 10496/18.
15 13004/20.
16 13629/20.
17 14540/16.
18 13084/1/20 REV 1.

- et la déclaration des États membres du 15 octobre 2020 intitulée "Building the next generation cloud for businesses and the public sector in the EU" (Construire l'informatique en nuage de la prochaine génération pour les entreprises et le secteur public dans l'UE);

RAPPELANT les conclusions du Conseil européen des 1er et 2 octobre 2020 sur la COVID-19, le marché unique, la politique industrielle, la dimension numérique et les relations extérieures[19], ainsi que les conclusions du Conseil européen du 20 juin 2019 sur la désinformation et les menaces hybrides et sur un nouveau programme stratégique 2019-2024[20];

RAPPELANT la stratégie globale pour la politique étrangère et de sécurité de l'Union européenne du 28 juin 2016 intitulée "Vision partagée, action commune: une Europe plus forte";

RAPPELANT les communications de la Commission européenne du 19 décembre 2020 sur le thème "Façonner l'avenir numérique de l'Europe"[21] et du 24 juillet 2020 relative à la stratégie de l'UE pour l'union de la sécurité[22];

RAPPELANT la communication conjointe de la Commission européenne et du haut représentant du 2 décembre 2020 sur un nouveau programme UE – États-Unis pour un changement planétaire[23];

1. SOULIGNE que la cybersécurité est essentielle à l'édification d'une Europe résiliente, verte et numérique et SE FÉLICITE de la communication conjointe au Parlement européen et au Conseil intitulée "La stratégie de cybersécurité de l'UE pour la décennie numérique", qui expose le nouveau cadre de l'action de l'UE dans le domaine de la "résilience, de la souveraineté technologique et du leadership" et en ce qui concerne la manière de protéger ses citoyens, ses entreprises et ses institutions contre les cyber-incidents et les cybermenaces, tout en renforçant la confiance des particuliers et des organisations dans la capacité de l'UE à promouvoir des réseaux et des systèmes d'information ainsi que des infrastructures et une connectivité sûrs et fiables, ainsi qu'à favoriser et à protéger un cyberespace mondial, ouvert, libre, stable et sûr, fondé sur les droits de l'homme, les libertés fondamentales, la démocratie et l'état de droit;

---

19 EUCO 13/20.
20 EUCO 9/19.
21 COM(2020) 67 final du 19.2.2020.
22 COM(2020) 605 final du 24.7.2020.
23 JOIN(2020) 22 final du 2.12.2020.

2. CONSIDÈRE que la pandémie de COVID-19 a placé au premier rang des priorités de notre quotidien le besoin accru de confiance dans les outils et systèmes des technologies de l'information et de la communication (TIC) et leur sécurité; SOULIGNE que la cybersécurité et l'internet mondial et ouvert sont essentiels au fonctionnement de l'administration et des institutions publiques, tant au niveau national qu'au niveau de l'UE, ainsi que pour notre société et l'économie dans son ensemble;

3. INSISTE sur la nécessité de sensibiliser davantage aux questions liées au cyberespace aux niveaux politique et stratégique de la prise de décision en fournissant aux décideurs des connaissances et des informations pertinentes et SOULIGNE la nécessité de conscientiser davantage le grand public et de promouvoir la cyberhygiène;

4. APPELLE à promouvoir et à protéger les valeurs fondamentales de l'UE que sont la démocratie, l'état de droit, les droits de l'homme et les libertés fondamentales, y compris le droit à la liberté d'expression et d'information, le droit à la liberté de réunion et d'association ainsi que le droit au respect de la vie privée dans le cyberespace; SE FÉLICITE, à cet égard, que les efforts soutenus se poursuivent en vue de protéger les défenseurs des droits de l'homme, la société civile et les universitaires qui travaillent sur des questions telles que la cybersécurité, la confidentialité des données, la surveillance et la censure en ligne en fournissant de nouvelles orientations pratiques, en promouvant les bonnes pratiques et en intensifiant les efforts déployés par l'UE pour prévenir les violations des droits de l'homme et les atteintes à ces droits ainsi que l'utilisation abusive des technologies émergentes, notamment par le recours à des mesures diplomatiques, le cas échéant, ainsi qu'au contrôle des exportations de ces technologies; MET EN EXERGUE, dans ce contexte, l'importance que revêtent le plan d'action de l'UE en faveur des droits de l'homme et de la démocratie 2020-2024 et les orientations de l'UE relatives à la liberté d'expression en ligne et hors ligne;

5. INSISTE SUR LE FAIT que parvenir à une autonomie stratégique tout en préservant une économie ouverte est un objectif clé de l'Union afin qu'elle puisse déterminer elle-même sa trajectoire et ses intérêts économiques. Il s'agit notamment d'accroître la capacité à opérer des choix autonomes dans le domaine de la cybersécurité afin de renforcer le leadership numérique et les capacités stratégiques de l'UE; RAPPELLE qu'il s'agit aussi de recenser et de réduire les dépendances stratégiques et d'accroître la résilience dans les écosystèmes industriels les plus sensibles et dans des domaines spécifiques; SOULIGNE que cela peut consister à diversifier les chaînes de production et d'approvisionnement, à stimuler et à attirer les investissements et la production en Europe, à explorer des solutions alternatives et des modèles circulaires et à encourager une vaste coopération industrielle entre les États membres;

6. compte tenu du déficit de compétences numériques et de cybersécurité qui existe dans la main-d'œuvre, INSISTE sur l'importance de répondre à la demande de main-d'œuvre formée dans le domaine du numérique et de la cybersécurité, notamment en développant, en conservant et en attirant les meilleurs talents, par exemple grâce à l'éducation et à la formation, afin de pouvoir numériser notre société d'une manière sécurisée du point de vue de la cybersécurité; ENCOURAGE la participation accrue des femmes et des filles aux filières scientifiques, technologiques, d'ingénierie et de mathématiques (STIM) de l'enseignement ainsi qu'au perfectionnement professionnel dans le domaine des TIC et à la reconversion dans les compétences numériques, ce qui est l'un des moyens de combler la fracture numérique entre les femmes et les hommes;

7. RAPPELLE que l'approche commune et globale de l'UE en matière de cyberdiplomatie vise à contribuer à la prévention des conflits, à l'atténuation des menaces en matière de cybersécurité et au renforcement de la stabilité des relations internationales; dans ce contexte, RÉAFFIRME qu'il est attaché au règlement des différends internationaux en matière de cyberespace par des moyens pacifiques, et que l'ensemble des efforts diplomatiques déployés par l'UE devraient, en priorité, être axés sur la promotion de la sécurité et de la stabilité dans le cyberespace au moyen d'une coopération internationale renforcée, ainsi que sur la réduction du risque de perceptions erronées, d'escalade et de conflits qui peuvent découler d'incidents liés aux TIC, et SOUTIENT la poursuite de l'élaboration et de la mise en place de mesures de confiance aux niveaux régional et international; RÉITÈRE l'appel lancé par l'Assemblée générale des Nations unies, approuvé par consensus, pour que les États membres des Nations unies s'inspirent des recommandations figurant dans les rapports des groupes d'experts gouvernementaux des Nations unies en ce qui concerne l'utilisation qu'ils font des TIC, et RÉAFFIRME que le droit international, en particulier la charte des Nations unies dans son intégralité, s'applique dans le cyberespace;

8. RÉAFFIRME que, en vue de façonner de manière significative les règles et les normes internationales dans les domaines des technologies émergentes et de l'infrastructure technique et logique essentielle à la disponibilité et à l'intégrité générales du noyau public de l'internet, de sorte que ces règles et normes soient conformes aux valeurs universelles et européennes, il est essentiel de poursuivre leur développement au sein de l'Union, dans le cadre d'une approche associant de multiples parties prenantes. Cela permettra de garantir que l'internet reste mondial, ouvert, libre, stable et sûr, que l'utilisation et le développement des technologies numériques respectent les droits de l'homme et que celles-ci soient exploitées de façon licite, sûre et éthique; PREND NOTE de la future stratégie de normalisation et S'ENGAGE à mener des actions de sensibilisation proactives et coordonnées afin de promouvoir le leadership de l'UE ainsi que les objectifs de celle-ci au niveau international, y compris au sein de divers organismes internationaux de normalisation et grâce à la coopération avec des partenaires partageant les mêmes valeurs, la société civile, le monde universitaire et le secteur privé;

9. SOUTIENT RÉSOLUMENT le modèle multipartite de gouvernance de l'internet et de cybersécurité et s'engage à renforcer les échanges réguliers et structurés avec les parties prenantes, y compris le secteur privé, le monde universitaire et la société civile, au sein des enceintes internationales, notamment dans le cadre de l'appel de Paris pour la confiance et la sécurité dans le cyberespace; PLAIDE EN FAVEUR d'un accès universel, abordable et égal à l'internet, comblant les fractures numériques, et, en particulier, PROMEUT l'autonomie des femmes, des jeunes filles et des personnes en situation de vulnérabilité ou de marginalisation, tant dans le cadre de l'élaboration des politiques que de l'utilisation de l'internet;

10. SOULIGNE la nécessité d'inclure la cybersécurité dans les investissements et initiatives numériques au cours des années à venir et de contribuer progressivement à la mise en place de conditions de concurrence équitables en matière de cybersécurité et PREND NOTE du plan de la Commission visant à accroître les dépenses publiques et à mobiliser des investissements privés dans le domaine de la cybersécurité; INSISTE SUR l'importance des petites et moyennes entreprises (PME) dans l'écosystème de la cybersécurité et PREND ACTE des instruments financiers pertinents disponibles pour soutenir le fait d'accorder une forte priorité à la cybersécurité dans le contexte de la transformation numérique pendant la durée du cadre financier pluriannuel (CFP) 2021-2027 ainsi qu'au niveau de la facilité pour la reprise et la résilience (FRR);

11. ATTEND AVEC INTÉRÊT la mise en œuvre rapide du règlement relatif au Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et au Réseau de centres nationaux de coordination, y compris l'établissement et la mise en place opérationnelle, sans tarder, du Centre européen de compétences en matière de cybersécurité, à Bucarest. Une prompte adoption du programme de celui-ci contribuera à maximiser les effets des investissements visant à renforcer le leadership de l'Union et son autonomie stratégique dans le domaine de la cybersécurité tout en soutenant les capacités et compétences technologiques, ainsi qu'à accroître la compétitivité de l'Union au niveau mondial, avec le concours de l'industrie et des milieux universitaires en matière de cybersécurité, y compris les PME et les centres de recherche, qui bénéficieront d'une collaboration plus systématique, plus inclusive et plus stratégique, eu égard à la cohésion de l'Union et de tous ses États membres;

12. SE FÉLICITE des travaux en cours menés par l'ENISA, ainsi que par les États membres et les parties prenantes intéressées, en vue de fournir à l'UE des schémas de certification pour les produits, services et processus TIC qui devraient contribuer à relever le niveau global de cybersécurité au sein du marché unique numérique; dans ce contexte, ATTEND AVEC INTÉRÊT le programme de travail glissant de l'Union en vue d'élaborer des schémas de certification de cybersécurité de l'UE dans le cadre du règlement sur la cybersécurité (CSA); RECONNAÎT, dans ce contexte, le rôle central de l'UE dans l'élaboration de normes qui sont susceptibles de façonner le paysage de la cybersécurité et contribuent à assurer une concurrence loyale au sein de l'UE et sur la scène internationale, à promouvoir l'accès au marché ainsi qu'à faire face aux risques pour la sécurité tout en garantissant l'applicabilité du cadre législatif de l'UE;

13. RÉAFFIRME qu'il importe d'évaluer la nécessité d'une législation horizontale, précisant également les conditions nécessaires pour la mise sur le marché, sur le long terme, en vue de traiter tous les aspects pertinents de la cybersécurité des dispositifs connectés, tels que la disponibilité, l'intégrité et la confidentialité; SALUE, à cet égard, la tenue d'une discussion visant à examiner le champ d'application d'une telle législation et ses liens avec le cadre de certification de cybersécurité défini dans le CSA, dans le but de relever le niveau de sécurité au sein du marché unique numérique; ATTIRE L'ATTENTION SUR LE FAIT que les exigences en matière de cybersécurité devraient être définies conformément à la législation pertinente de l'Union, y compris le CSA, le nouveau cadre législatif (NCL), le règlement relatif à la normalisation européenne et une éventuelle législation horizontale à venir, afin d'éviter toute ambiguïté et toute fragmentation de la législation;

14. EST CONSCIENT de l'importance que revêtent une approche globale et horizontale en matière de cybersécurité dans l'Union, dans le plein respect des compétences et des besoins des États membres, ainsi qu'un soutien continu à l'assistance technique et à la coopération pour renforcer la capacité des États membres; compte tenu de l'évolution du paysage des cybermenaces, PREND ACTE de la nouvelle proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, qui s'appuie sur la directive SRI, et réaffirme son soutien au renforcement et à l'harmonisation des cadres nationaux de cybersécurité et à une coopération soutenue entre les États membres; en outre, SOULIGNE la nécessité d'un alignement et d'une meilleure articulation de la législation sectorielle dans ce domaine;

15. PREND NOTE de la proposition de la Commission visant à aider les États membres à mettre en place et à renforcer des centres des opérations de sécurité (COS) afin de créer un réseau de COS dans l'ensemble de l'UE, pour mieux surveiller et anticiper les signes d'attaques sur les réseaux; dans ce contexte, ATTEND les plans détaillés de la Commission concernant le réseau de COS, dans le respect des compétences des États membres. RAPPELLE les efforts déployés par les États membres, avec le soutien de l'UE, pour mettre en place des CSIRT sectoriels, nationaux et régionaux et des centres nationaux ou européens d'échange et d'analyse d'informations (ISAC) dans le cadre d'un réseau efficace de partenariats en matière de cybersécurité dans l'Union; ATTEND AVEC INTÉRÊT d'explorer le potentiel de ce réseau pour renforcer les COS ainsi que la complémentarité et la coordination de ces derniers avec les réseaux et acteurs existants (en particulier le réseau des CSIRT), afin de promouvoir une culture de partage d'informations efficace, sûre et fiable; SOULIGNE que ce processus s'appuiera sur les travaux menés dans le contexte des initiatives en matière d'intelligence artificielle et de calcul à haute performance, ainsi que par les pôles européens d'innovation numérique.

16. PREND NOTE de la possible mise en place d'un système de connectivité sécurisé, s'appuyant sur l'infrastructure européenne de communication quantique (EuroQCI) et le programme de communication gouvernementale par satellite de l'Union européenne (Govsatcom), et RECONNAÎT que tout éventuel développement à venir devrait être fondé sur un cadre solide en matière de cybersécurité et tenir compte de l'ensemble des infrastructures de communications électroniques, telles que les systèmes de réseaux spatiaux, terrestres et sous-marins;

17. ATTEND AVEC INTÉRÊT les discussions avec la Commission, l'ENISA, les opérateurs des deux serveurs racines du DNS de l'UE et la communauté multipartite visant à évaluer le rôle joué par lesdits opérateurs de serveurs racines pour ce qui de garantir que l'internet reste accessible et non fragmenté à l'échelle mondiale; SE FÉLICITE de la poursuite du débat portant sur l'intention de la Commission de développer un autre service, européen, pour accéder à l'internet mondial (initiative "DNS4EU"), fondé sur un modèle transparent conforme aux normes et règles les plus récentes en matière de sécurité, de protection des données et de vie privée dès la conception et par défaut, afin de contribuer à accroître la résilience, tout en maintenant et en renforçant la connectivité internationale pour tous les États membres;

18. RECONNAÎT la nécessité d'un effort conjoint de la Commission et des États membres pour accélérer l'adoption des normes clés de l'internet, notamment l'IPv6, et des normes de sécurité internet bien établies, étant donné qu'elles contribuent de manière déterminante à relever le niveau global de sécurité, de résilience, d'ouverture et d'interopérabilité de l'internet mondial, tout en renforçant la compétitivité de l'industrie de l'UE et, en particulier, des opérateurs d'infrastructure internet;

19. INSISTE SUR l'importance d'une approche coordonnée ainsi que sur l'élaboration et la mise en œuvre de mesures efficaces au niveau national pour renforcer la cybersécurité des réseaux 5G; SOUTIENT les prochaines mesures à prendre en faveur de la cybersécurité des réseaux 5G, telles qu'elles sont présentées dans l'appendice de la stratégie de cybersécurité de l'Union européenne et sur la base des résultats du rapport relatif aux effets de la recommandation de la Commission sur la sécurité des réseaux 5G, par exemple en ce qui concerne la définition d'une approche globale et à long terme portant sur l'ensemble de la chaîne de valeur et de l'écosystème de la 5G; en vue de renforcer encore l'approche coordonnée en matière de sécurité des réseaux 5G, INVITE INSTAMMENT les États membres, les institutions de l'UE et les autres parties prenantes concernées à continuer de procéder à leur bilan périodique, ainsi qu'à poursuivre l'échange d'informations et de bonnes pratiques au sein du groupe de travail ad hoc du groupe de coopération SRI, spécialisé en matière de cybersécurité de la 5G, et à informer régulièrement le Conseil des progrès accomplis; tout en mettant l'accent sur la responsabilité des États membres en matière de protection de la sécurité nationale, MET EN AVANT la ferme volonté qui est la sienne d'appliquer les mesures de la boîte à outils de l'UE relative à la 5G, d'en achever rapidement la mise en œuvre et de poursuivre les efforts visant à garantir la sécurité des réseaux 5G et le développement de futures générations de réseaux. L'étroite coopération entre les États membres, la Commission et l'ENISA en matière de sécurité des réseaux 5G pourrait servir d'exemple pour d'autres questions dans le domaine de la cybersécurité, dans le respect des compétences des États membres et des principes de subsidiarité et de proportionnalité;

20. MESURE l'intérêt qu'il y a à intégrer davantage la cybersécurité dans les mécanismes de gestion de crise de l'UE et de tester ceux-ci dans le cadre d'exercices pertinents et SOULIGNE qu'il importe de renforcer la coopération et le partage d'informations entre les différentes cybercommunautés au sein de l'UE, ainsi que de relier les initiatives, structures et procédures existantes (telles que l'IPCR, le réseau des CSIRT, le groupe de coopération SRI, le réseau CyCLONe, le Centre européen de lutte contre la cybercriminalité, le Centre de situation et du renseignement de l'UE (INTCEN) et d'autres organes compétents de l'UE) en cas de cyber-incidents et de cybermenaces transfrontières et de grande ampleur; TENANT COMPTE des progrès déjà accomplis dans ce domaine, ATTEND la proposition de la Commission concernant le processus, les étapes et un calendrier de mise en place de l'unité conjointe de cybersécurité, en vue d'apporter une valeur ajoutée, de définir des orientations claires et de rationaliser le cadre européen de gestion des crises en matière de cybersécurité, y compris en termes d'état de préparation, de connaissance partagée de la situation, de renforcement de la réaction coordonnée et d'exercices, d'une façon transparente et progressive, tout en évitant les doubles emplois et les chevauchements et en respectant les compétences des États membres;

21. MET L'ACCENT à la fois sur le fait qu'il importe de favoriser la coopération et l'échange d'informations entre les acteurs concernés de la cybersécurité et les autorités compétentes dans le domaine de la sécurité et de la justice pénale, par exemple les autorités répressives et judiciaires, et sur la nécessité d'étendre et d'améliorer la capacité de ces autorités à enquêter sur la cybercriminalité et à engager des poursuites en la matière, ainsi que de promouvoir les négociations internationales et les règles de l'UE concernant l'accès transfrontière aux preuves électroniques; Indépendamment de l'environnement technologique du moment, il est essentiel de préserver les pouvoirs des autorités compétentes dans le domaine de la sécurité et de la justice pénale grâce à un accès licite leur permettant d'accomplir les missions prescrites et autorisées par la loi. Ces lois prévoyant des pouvoirs d'exécution doivent toujours respecter pleinement le droit à un procès équitable et d'autres garanties, ainsi que les droits fondamentaux, en particulier le droit au respect de la vie privée et du caractère privé des communications et le droit à la protection des données à caractère personnel;

22. RÉAFFIRME son soutien au développement, à la mise en œuvre et à l'utilisation du chiffrement fort, qui est un moyen nécessaire pour protéger les droits fondamentaux et la sécurité numérique des citoyens, des pouvoirs publics, des entreprises et de la société et, dans le même temps, EST CONSCIENT de la nécessité de veiller à ce que les autorités compétentes dans le domaine de la sécurité et de la justice pénale, par exemple les autorités répressives et judiciaires, puissent exercer leurs pouvoirs légaux, tant en ligne que hors ligne, pour protéger nos sociétés et nos citoyens. Les autorités compétentes doivent être en mesure d'accéder aux données de manière licite et ciblée, dans le plein respect des droits fondamentaux et des lois applicables en matière de protection des données, tout en préservant la cybersécurité. SOULIGNE que toute mesure prise doit soigneusement respecter l'équilibre entre ces intérêts et les principes de nécessité, de proportionnalité et de subsidiarité;

23. SOUTIENT et PROMEUT la convention de Budapest sur la cybercriminalité et les travaux en cours sur le deuxième protocole additionnel à cette convention. Continue en outre de participer aux échanges multilatéraux sur la cybercriminalité, y compris dans le cadre de processus liés au Conseil de l'Europe, à l'Office des Nations unies contre la drogue et le crime (ONUDC) et à la Commission pour la prévention du crime et la justice pénale (CPCJP), afin d'assurer une coopération internationale renforcée en matière de lutte contre la cybercriminalité, y compris par l'échange de bonnes pratiques et de connaissances techniques et le soutien au renforcement des capacités, tout en respectant, en promouvant et en protégeant les droits de l'homme et les libertés fondamentales;

24. Alors que la sécurité nationale reste de la seule responsabilité de chaque État membre, EST CONSCIENT de l'importance que revêt la coopération stratégique en matière de renseignement sur les cybermenaces et les actes de cybermalveillance, et INVITE donc les États membres à continuer, par l'intermédiaire de leurs autorités compétentes, de contribuer aux travaux de l'INTCEN, véritable plaque tournante de l'UE pour l'appréciation de la situation et l'évaluation des menaces concernant les questions liées au cyberespace, et à étudier la proposition relative à la mise en place éventuelle d'un groupe de travail des États membres en matière de cyber-renseignement, qui vienne renforcer la capacité spécifique de l'INTCEN dans ce domaine, et dont les travaux feraient fond sur des contributions volontaires des États membres en matière de renseignement, sans préjudice des compétences de ces derniers;

25. SOULIGNE l'importance que revêt un cadre de sécurité solide et cohérent pour protéger l'ensemble du personnel, des données, des réseaux de communication et des systèmes d'information ainsi que des processus décisionnels de l'UE sur la base de règles globales, cohérentes et homogènes. À cette fin, il conviendrait en particulier d'accroître la résilience et d'améliorer la culture de sécurité de l'UE face aux cybermenaces et de renforcer la sécurité des réseaux classifiés et non classifiés de l'UE, tout assurant une gouvernance adéquate et en veillant à ce que des ressources et des capacités suffisantes soient mises à disposition, y compris dans le cadre du renforcement du mandat de la CERT-UE. SE FÉLICITE, dans ce contexte, des discussions en cours sur l'établissement de règles communes en matière de sécurité de l'information tenant dûment compte des règles de sécurité du Conseil aux fins de la protection des informations classifiées de l'UE, ainsi que de la définition de règles communes contraignantes en matière de cybersécurité pour l'ensemble des institutions, organes et organismes de l'UE;

26. FAISANT FOND sur les efforts déployés par l'UE en matière de cyberdiplomatie, S'ENGAGE à accroître l'efficacité de la boîte à outils cyberdiplomatique et ATTEND AVEC INTÉRÊT d'approfondir les discussions sur son champ d'application et son utilisation, sur la base des enseignements tirés de l'application faite jusqu'à présent de cet instrument. Ces discussions devraient contribuer à promouvoir la sécurité au niveau international en encourageant le dialogue et en alimentant une conception commune des questions de cybersécurité, en renforçant la prévention, la stabilité et la coopération et en faisant progresser la confiance et le renforcement des capacités et, si nécessaire, par l'application de mesures restrictives, afin d'empêcher, de décourager et de prévenir les actes de cybermalveillance visant l'intégrité et la sécurité de l'UE et de ses États membres, ainsi que d'y faire face, contribuant ainsi à assurer la sécurité et à la stabilité internationales et à consolider la cyberposture de l'UE, dans le plein respect des compétences et prérogatives nationales. Il convient notamment d'accorder une attention particulière à la nécessité de prévenir et de contrer les cyberattaques ayant des effets systémiques susceptibles d'affecter nos chaînes d'approvisionnement, nos infrastructures critiques et nos services essentiels, ainsi que nos institutions et processus démocratiques, et de compromettre notre sécurité économique, y compris par le vol de propriété intellectuelle facilité par les technologies de l'information et de la communication. Les États membres et les institutions de l'UE devraient également poursuivre leur réflexion sur l'articulation entre le cadre européen de gestion des crises en matière de cybersécurité, la boîte à outils cyberdiplomatique et les dispositions de l'article 42, paragraphe 7, du TUE et de l'article 222 du TFUE, notamment en travaillant sur la base de scénarios afin de parvenir à une compréhension commune des modalités pratiques de mise en œuvre de l'article 42, paragraphe 7, du TUE;

27. RECONNAÎT l'importance qu'il y a à renforcer la coopération avec les organisations internationales et les pays partenaires afin de faire progresser la compréhension commune du paysage des cybermenaces, d'établir des dialogues et des mécanismes de coopération, de définir, le cas échéant, des réponses diplomatiques coopératives et d'améliorer le partage d'informations, y compris par l'éducation, la formation et les exercices. En particulier, SOULIGNE qu'un partenariat transatlantique solide dans le domaine de la cybersécurité contribue à notre sécurité, à notre stabilité et à notre prospérité communes et PREND ACTE des dispositions relatives à la coopération en matière de cybersécurité que contient l'accord de commerce et de coopération UE-Royaume-Uni. RAPPELANT les grandes réalisations de la coopération UE-OTAN en matière de cybersécurité dans le cadre de la mise en œuvre des déclarations conjointes de Varsovie et de Bruxelles, de 2016 et 2018 respectivement, réaffirme l'importance que revêt une coopération approfondie, mutuellement bénéfique et dans laquelle les deux parties se renforcent mutuellement, par l'éducation, la formation, les exercices et une réponse coordonnée aux actes de cybermalveillance, dans le plein respect de l'autonomie décisionnelle et des procédures décisionnelles des deux organisations et sur la base des principes de transparence, de réciprocité et d'inclusion;

28. Afin de contribuer à un cyberespace mondial, ouvert, libre, stable et sûr, qui revêt une importance sans cesse grandissante pour le maintien de la prospérité, de la croissance, de la sécurité, du bien-être, de la connectivité et de l'intégrité de nos sociétés, S'ENGAGE à participer sans relâche aux processus de normalisation au sein des organisations internationales, en particulier les processus liés à la Première Commission des Nations unies, en promouvant l'applicabilité du droit international dans le cyberespace et l'adhésion aux normes, aux règles et aux principes en matière de comportement responsable des États dans le cyberespace, et en y contribuant, y compris en encourageant la mise en place rapide d'un programme d'action pour un comportement responsable des États dans le cyberespace, en tant que prolongement constructif, inclusif et consensuel des actuels processus du groupe d'experts gouvernementaux et du groupe de travail à composition non limitée des Nations unies;

29. RAPPELLE son profond attachement à un multilatéralisme effectif et à un ordre mondial fondé sur des règles et centré sur les Nations unies, ainsi que sa détermination à renforcer la coopération et la coordination avec les organisations internationales et régionales, à savoir le système des Nations unies, l'OTAN, le Conseil de l'Europe, l'OSCE, l'OCDE, l'UA, l'OEA, l'ASEAN, le FRA, le CCG et la LEA, en ce qui concerne les discussions sur les questions liées au cyberespace ainsi que la poursuite et l'extension des dialogues et consultations structurés de l'UE avec les pays tiers concernant le cyberespace. SOULIGNE qu'il soutient activement les Nations unies, notamment en ce qui concerne leur Programme 2030, y compris les objectifs de développement durable, et SE FÉLICITE de la feuille de route du Secrétaire général des Nations unies pour la coopération numérique ainsi que du programme de désarmement du Secrétaire général des Nations unies, qui favorisent l'obligation de rendre des comptes et l'adhésion aux normes en matière de cyberespace et contribuent à la prévention et au règlement pacifique des conflits résultant d'activités malveillantes dans le cyberespace. ACCUEILLE FAVORABLEMENT la proposition du haut représentant pour les affaires étrangères et la politique de sécurité visant à créer un réseau européen informel de cyberdiplomatie en vue d'accroître l'engagement et l'expertise de l'UE et des États membres sur les questions internationales liées au cyberespace afin de renforcer une action de sensibilisation coordonnée;

30. ATTEND AVEC INTÉRÊT la proposition de réexamen du cadre stratégique de cyberdéfense qui sera présentée prochainement; et S'ENGAGE à poursuivre les efforts visant à renforcer les dimensions cybersécurité et cyberdéfense pour faire en sorte qu'elles soient pleinement intégrées dans le domaine plus large de la sécurité et de la défense, en particulier dans le contexte des travaux sur la boussole stratégique. ESTIME que les futures "stratégie et vision militaires de l'UE sur le cyberespace en tant que domaine d'opérations" contribuera à faire avancer ces discussions. SALUE l'initiative prise par l'Agence européenne de défense (AED) d'encourager la coopération entre les CERT militaires, et APPUIE les efforts déployés pour renforcer les synergies civilo-militaires et la coordination en matière de cyberdéfense et de cybersécurité, y compris sur les aspects liés à l'espace, notamment dans le cadre des projets CSP spécifiques;

31. SE FÉLICITE de la proposition visant à élaborer un programme de renforcement des cybercapacités externes de l'UE, de la proposition visant à créer un comité européen pour le renforcement des cybercapacités, ainsi que de la création et de la mise en œuvre de l'EU CyberNet (réseau de l'UE pour le renforcement des cybercapacités) afin d'accroître la cyber-résilience et les cybercapacités dans le monde entier. Dans ce contexte, SE FÉLICITE de la coopération avec les États membres, ainsi qu'avec les partenaires des secteurs public et privé, notamment le Forum mondial sur la cyberexpertise (GFCE) et d'autres organismes internationaux compétents, afin d'assurer la coordination et d'éviter les doubles emplois. En particulier, ENCOURAGE la coopération avec les partenaires des Balkans occidentaux et du voisinage oriental et méridional de l'UE;

32. afin de faire en sorte que tous les pays soient en mesure de tirer parti des avantages sociaux, économiques et politiques de l'internet et de l'utilisation des technologies, S'ENGAGE à aider les pays partenaires à faire face au défi croissant que constituent les actes de cybermalveillance, notamment ceux qui nuisent au développement de leurs économies et de leurs sociétés ainsi qu'à l'intégrité et à la sécurité des systèmes démocratiques, y compris dans le droit fil des efforts déployés dans le cadre du plan d'action pour la démocratie européenne;

33. afin d'assurer l'élaboration, la mise en œuvre et le suivi des propositions présentées dans le cadre de la stratégie de cybersécurité de l'UE, et compte tenu du caractère pluriannuel de certaines des initiatives, ENCOURAGE la Commission et le haut représentant pour les affaires étrangères et la politique de sécurité à établir un plan de mise en œuvre détaillé fixant les priorités et le calendrier des actions prévues. SUIVRA les progrès accomplis dans la mise en œuvre des présentes conclusions au moyen d'un plan d'action qui sera régulièrement examiné et mis à jour par le Conseil en étroite coopération avec la Commission européenne et le haut représentant.