Avis du Comité économique et social européen sur la communication conjointe au Parlement européen et au Conseil — «La politique de cyberdéfense de l'UE»

(avis d'initiative)

(2023/C 293/04)

Rapporteur: **Anastasis YIAPANIS**

Corapporteur: **Alberto MAZZOLA**

Décision de l'assemblée plénière	20.9.2022
Base juridique	Article 52, paragraphe 2, du règlement intérieur Avis d'initiative
Compétence	Commission consultative des mutations industrielles (CCMI)
Adoption en section	27.3.2023
Adoption en session plénière	14.6.2023
Session plénière n°	579
Résultat du vote (pour/contre/abstentions)	208/1/2

1. **Conclusions et recommandations**

1.1. Le Comité économique et social européen (CESE) adhère à la proposition de politique de cyberdéfense de l'Union européenne (UE), mais aurait espéré que la société civile organisée se voie attribuer un rôle plus important dans l'élaboration de cette proposition. À ce stade, il est difficile pour le Comité d'évaluer si les futures initiatives décrites dans la communication conjointe seront mises en œuvre et si elles produiront les résultats escomptés. Il invite donc instamment les institutions et les États membres de l'Union européenne à donner la priorité aux initiatives annoncées et à les faire progresser rapidement.

1.2. Le CESE insiste sur la nécessité de prendre des mesures supplémentaires afin de renforcer la capacité de l'Union à détecter les cybermenaces et recommande que le financement de la recherche et du développement soit axé sur le développement de capacités de pointe au sein de l'UE. La coopération entre les secteurs privé et public est essentielle et ne doit pas se faire à sens unique. Le CESE considère qu'il est nécessaire de favoriser la coordination au niveau de l'Union pour remédier à la fragmentation et garantir la coopération et les investissements conjoints entre les États membres.

1.3. Le CESE est favorable à la création d'un Centre de coordination de l'UE en matière de cyberdéfense (EUCDCC) et recommande que les États membres s'engagent à fournir des réponses rapides à tout moment de la journée, 7 jours sur 7, et qu'ils évaluent le niveau de préparation en matière de cybersécurité et l'efficacité des mécanismes de réponse aux crises cyber de l'UE, en examinant en particulier les capacités militaires de même que les secteurs critiques tels que recensés par la directive (UE) 2022/2555 du Parlement européen et du Conseil [1] (directive SRI 2). Le Comité approuve l'extension du mandat du Centre de compétences européen en matière de cybersécurité (ECCC) qui le charge d'assister le Centre de coordination de l'UE en matière de cyberdéfense dans ses travaux.

1.4. Le CESE estime qu'en vue de renforcer l'autonomie stratégique et la souveraineté de l'Union européenne en matière de cybersécurité, il conviendrait de mettre au point une plateforme dynamique permettant le partage d'informations et la conduite de tests en temps réel, ou d'adopter une telle plateforme existante dans le secteur privé, de manière à repérer les lacunes à combler dans les capacités actuelles. Cette plateforme pourrait également être utilisée pour diffuser les bonnes pratiques, signaler les cyberincidents et dresser une liste exhaustive des cybercriminels dans l'UE.

---

[1] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

1.5. Le CESE souligne la nécessité pour l'Union d'être mieux préparée aux cyberattaques telles que celles perpétrées par la Russie en Ukraine, qui ciblent en particulier les infrastructures critiques. La coopération entre les écosystèmes civils et militaires, notamment au moyen de simulations de cyberattaques, est indispensable à la gestion efficace des crises, ainsi que pour garantir l'interopérabilité et éviter la duplication des efforts et des investissements.

1.6. Le CESE est d'avis que les investissements dans le domaine de la cyberdéfense devraient être consacrés en priorité à la protection des citoyens et des infrastructures critiques de l'Union, laquelle passe notamment par un recours à des fournisseurs de matériel et de logiciels de confiance. Il insiste sur l'importance de mettre à jour les priorités et les investissements en temps utile, sur la base d'une concertation entre l'UE et ses États membres, avec la participation des acteurs privés concernés.

1.7. L'Union doit maintenir et développer les capacités nécessaires pour sécuriser son économie numérique, la société, la démocratie et les technologies critiques, ainsi que pour fournir des services essentiels en matière de cybersécurité. Pour garantir l'autonomie stratégique de l'Union, il est crucial de réduire ses dépendances à l'égard des pays tiers. Le CESE estime qu'il est essentiel que l'UE adopte une approche à moyen terme pour acquérir son autonomie s'agissant des technologies clés, et il plaide résolument en faveur de la mise en place d'infrastructures de recherche et de production par des entreprises établies dans l'UE, ainsi que d'une politique industrielle européenne adéquate et axée sur un écosystème cyber autonome.

1.8. Les PME devraient bénéficier d'un soutien ciblé et avoir accès à des programmes de financement leur permettant de renforcer leur résilience face aux cyberattaques, ainsi qu'à des possibilités d'assistance, de formation et d'éducation concernant les risques relatifs à la cybersécurité et les moyens de s'en prémunir. L'Union européenne devrait prévoir un mécanisme d'incitation favorisant une familiarisation progressive des PME aux questions de cybersécurité ainsi que la création de PME innovantes actives dans ce domaine.

1.9. Le CESE se félicite de l'intention de la Commission européenne de créer une Académie des compétences cyber et lui demande de coordonner et de financer des programmes de formation à grande échelle et des programmes d'enseignement et de formation professionnels auxquels tous les États membres peuvent participer et qui visent à constituer une main-d'œuvre qualifiée pour l'ensemble des agences et organisations concernées par la cyberdéfense, ainsi que pour les réseaux civils privés.

1.10. Le Comité tient pour essentiel de sensibiliser les citoyens à la cybersécurité afin de réduire l'exposition aux cyberattaques et demande que soient créés des cursus d'éducation et des programmes de formation tout au long de la vie qui auront pour principal objectif de renforcer les compétences et les connaissances en matière de cybersécurité. Le CESE est favorable à ce que les questions de cybersécurité soient intégrées dans toutes les futures politiques de l'Union et à ce que l'on informe le grand public sur les cybermenaces.

1.11. Le CESE estime que, dans les domaines militaires, une coopération étroite avec les alliés de l'OTAN doit être centrée sur la pleine coordination et la réciprocité, la mise sur pied de projets conjoints de recherche, développement et innovation, le partage de bonnes pratiques, la création de vastes programmes de formation et des simulations de cyberattaques, l'objectif premier étant d'améliorer la capacité de réaction commune.

1.12. Le Comité invite le haut représentant à examiner les dialogues bilatéraux existants sur la cybersécurité et à nouer des dialogues supplémentaires avec d'autres pays et des organisations internationales compétentes, de manière à établir un cadre mondial pour le respect du droit international dans le cyberespace en mettant un accent particulier sur la réciprocité. Le Comité considère que l'Union européenne, compte tenu de son ancrage solide dans les libertés démocratiques fondamentales, est bien placée pour prendre la tête des débats à l'échelle internationale sur l'avenir de la cybersécurité, en particulier au sein des Nations unies.

1.13. L'Union européenne devrait s'opposer fermement à tout type de système de notation sociale à l'encontre des citoyens. Le CESE souhaite affirmer explicitement qu'une véritable démocratie ne peut exister sans une protection effective des données à caractère personnel. Il estime en outre qu'une gestion responsable et efficace des données est essentielle pour faire de l'hyperconnectivité un avantage concurrentiel.

2. **Introduction et observations générales**

2.1. L'expansion du numérique dans les sociétés s'accompagne d'un grand nombre de cybermenaces engendrées par les avancées technologiques. Ces dernières années, les cyberattaques se sont considérablement multipliées et sont devenues beaucoup plus élaborées, menaçant la sécurité des entités publiques comme privées. Qu'il s'agisse de rançongiciels, de logiciels malveillants, d'attaques par courriels, de violations de données, de désinformation, d'attaques collectives par saturation de service (ACSS) ou d'autres formes d'attaques, ces pratiques posent toutes une menace constante et continue à la sécurité de l'Union dans son ensemble.

2.2. Le CESE se félicite de la communication conjointe sur «La politique de cyberdéfense de l'UE» ([2]) et juge qu'il est à présent temps d'agir d'urgence et de manière coordonnée au niveau de l'Union, en associant à la fois les écosystèmes du cyberespace civil et militaire et en veillant à ce qu'un cadre adéquat soit mis en place en ce qui concerne les investissements dans les capacités de cyberdéfense. Toutefois, le Comité fait observer que, dans sa communication, la Commission se contente de déclarer son intention d'agir et de dresser une liste des futures initiatives de l'UE qui devraient aboutir. De l'avis du Comité, il est impossible de déterminer si ces futurs engagements seront effectivement respectés, étant donné que les négociations qui auront lieu à l'avenir entre les colégislateurs influenceront sans nul doute le résultat final du plan d'action de l'Union en matière de cybersécurité.

2.3. La cybersécurité figure parmi les premières priorités de l'UE en matière de menaces pour la sécurité depuis l'attaque russe contre le réseau satellitaire KA-SAT, qui a perturbé les communications au sein des forces armées ukrainiennes, et le récent scandale impliquant Éric Léandri, qui aurait effectué des missions de cyberespionnage pour le compte de certaines entreprises de défense. Si le RGPD, en vigueur depuis plusieurs années, constitue un acte législatif européen très efficace, il est évident que la quantité croissante de données disponibles entraîne une certaine vulnérabilité, et le risque de voir des tiers franchir la limite de la légalité augmente chaque jour.

2.4. Compte tenu de la nature transnationale des cyberattaques, la coordination au niveau de l'Union est nécessaire pour réduire la fragmentation actuelle et veiller à ce que les États membres soient prêts à coopérer et à consentir des investissements conjoints. Cette coordination est particulièrement importante pour parer aux futures éventualités de menaces ciblant un État membre, auquel cas tous les autres États membres devraient avoir la possibilité de lui fournir un soutien immédiat.

3. **Agir ensemble pour renforcer la cyberdéfense**

3.1. Le Comité prend note des initiatives ambitieuses annoncées, à savoir l'établissement d'un Centre de coordination de l'UE en matière de cyberdéfense (EUCDCC), la mise au point du projet CyDef-X, la création d'équipes d'intervention rapide en cas d'incident informatique (CRRT), le lancement d'une initiative de l'UE en matière de cybersolidarité et l'examen de la possibilité d'élaborer des schémas de certification de cybersécurité pour les produits, les services et les processus dans le domaine des TIC. Le CESE recommande que tous les États membres s'engagent à pouvoir fournir une réponse rapide à tout moment de la journée, 7 jours sur 7, et que l'EUCDCC participe à l'évaluation et à l'établissement de rapports réguliers en ce qui concerne la préparation des États membres en matière de cybersécurité et l'efficacité du mécanisme européen de réponse aux crises cyber, en mettant l'accent à la fois sur les capacités militaires et sur les secteurs critiques recensés dans la directive SRI 2. Chaque État membre devrait disposer d'experts spécialement formés pour intervenir en cas d'incident de cybersécurité et évaluer régulièrement leur capacité à intervenir dans d'autres États membres.

3.2. Bien que la communication présente une longue liste d'améliorations à introduire de façon progressive, le CESE aurait espéré y trouver une feuille de route explicite quant à la mise en œuvre de ces initiatives, assortie d'instructions de gouvernance et de délais clairs pour leur soumission et leur adoption. En outre, le Comité aurait espéré que la société civile organisée se voie attribuer un rôle plus important dans l'élaboration de cette proposition.

3.3. Le CESE est d'avis que les États membres doivent renforcer leur capacité interne à contrer les cybermenaces tout en prenant part à des projets de coopération et en partageant des informations et de bonnes pratiques avec les autres États membres. Il y a lieu de réaliser sans tarder des investissements dans les capacités de cyberdéfense, d'accélérer le déploiement des technologies ([3]) dans tous les États membres et d'améliorer la préparation collective à détecter les cyberattaques, s'en prémunir et s'en remettre. Le CESE estime qu'en vue de soutenir l'autonomie de l'Union européenne en matière de cybersécurité, il conviendrait de mettre au point une plateforme dynamique permettant le partage d'informations et la conduite de tests en temps réel, ou d'adopter une telle plateforme existante dans le secteur privé, laquelle viserait principalement à repérer les lacunes à combler dans les capacités actuelles.

3.4. Le CESE partage le point de vue selon lequel les opérations militaires dans le cyberespace devraient, à ce stade, continuer à relever strictement de la compétence des États membres; le Comité est favorable à la coopération annoncée entre les équipes militaires d'intervention en cas d'urgence informatique de l'UE (milCERT), les centres de réponse aux incidents de sécurité informatique (CSIRT) et l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'UE (CERT-UE).

3.5. La directive SRI 2 et la directive sur la résilience des entités critiques ([4]), récemment adoptées, prévoient déjà des obligations nationales et sectorielles spécifiques au cadre de cyberdéfense de l'Union. D'autres mesures sont nécessaires pour améliorer la capacité de détection collective de l'Union, et le CESE préconise des investissements dans la recherche et le développement en vue de développer des capacités de pointe au niveau de l'UE.

([2]) Communication conjointe de la Commission européenne au Parlement européen et au Conseil sur «La politique de cyberdéfense de l'UE».

([3]) Notamment l'accélérateur d'innovation de défense pour l'Atlantique Nord (DIANA), une initiative de l'OTAN.

([4]) Directive sur la résilience des entités critiques.

4. **Sécuriser l'écosystème de défense de l'UE**

4.1. Le CESE estime que l'écosystème de défense a été transformé par des complexités qui lui sont inhérentes et par des défis technologiques qui évoluent rapidement, et que la question de la cybersécurité est désormais commune aux secteurs militaire et civil, et concerne également les citoyens de l'Union. La coopération entre les écosystèmes civil et militaire est désormais plus importante que jamais; elle devrait contribuer à la gestion efficace des crises et permettre de progresser en continu, d'assurer l'interopérabilité, mais aussi d'éviter la duplication ou la multiplication des efforts et des investissements. Les États membres devraient être prêts à réaliser des tests de résistance des infrastructures critiques nationales, de sorte à évaluer et améliorer la résilience face aux futures cyberattaques.

4.2. Le CESE est d'avis que les investissements dans le domaine de la cyberdéfense devraient être consacrés en priorité à la protection des citoyens et des infrastructures critiques de l'Union. Compte tenu de l'évolution rapide de la transformation numérique et du paysage de menaces, le Comité réclame instamment que soient mis à jour, en temps utile, les priorités et les investissements, sur la base d'une concertation entre l'UE et ses États membres, en prévoyant également une consultation approfondie des acteurs privés concernés. Les appareils de l'internet des objets sont souvent moins bien protégés que les appareils traditionnels. Dès lors, le CESE demande qu'un niveau de sécurité minimal soit garanti par l'intermédiaire de plateformes de gestion de l'identité et de l'accès. En outre, dans la mesure où la certification constitue une méthode essentielle de renforcement du niveau de sécurité, le Comité réclame une nouvelle approche de l'UE en matière de certification, qui mettrait davantage l'accent sur la sécurité de l'internet des objets.

4.3. L'Union européenne doit renforcer sa résilience aux cyberattaques et élaborer des stratégies efficaces de cyberdissuasion. Il importe de protéger les infrastructures critiques contre les cyberattaques de toute nature, y compris au moyen des systèmes de défense de l'UE. Le Comité estime qu'il est dans l'intérêt stratégique de l'Union de maintenir et de développer les capacités nécessaires pour sécuriser son économie numérique, la société et la démocratie, afin de parvenir à une souveraineté numérique totale, puisqu'il s'agit du seul moyen de protéger les technologies critiques et de fournir des services essentiels efficaces en matière de cybersécurité. Il est également crucial, pour l'autonomie stratégique de l'Union, de réduire les dépendances à l'égard des pays tiers. Le CESE estime que les agences sectorielles de l'UE (ENISA, AESA, AFE, EMA, ABE, ESA, HADEA, etc.) devraient être associées à ce processus et fournir des orientations pour l'élaboration de mécanismes de cybersécurité.

4.4. La pandémie de COVID-19 a accéléré la transition numérique et transformé les activités traditionnelles en travail hybride et/ou à distance, donnant ainsi lieu à de nouvelles relations de travail et de nouvelles attentes, ainsi qu'à une nouvelle classe de nomades numériques, dont le nombre ne cesse de croître. Le CESE attire l'attention sur les rapides mutations que connaît le marché du travail, qui ont mené à l'adoption d'une architecture «zéro confiance» par les entreprises, au moyen de solutions de gestion des identités et des accès (IAM, *Identity and Access Management*) et de gestion des accès privilégiés (PAM, *Privileged Access Management*). Le Comité considère que ce type de gestion des ressources des entreprises offre de nouvelles solutions aux cybermenaces, et qu'il convient donc d'aider le secteur privé à renforcer le niveau de sécurité de ses solutions numériques innovantes.

4.5. Le CESE déplore que la Commission se contente de déclarer qu'«[u]n plan de mise en œuvre pourrait être établi en coopération avec les États membres», et est d'avis qu'un tel plan devrait être obligatoire, élaboré conjointement avec les États membres et mis en œuvre au plus tôt. Le Comité est préoccupé par l'approche trop superficielle adoptée par la Commission et demande instamment aux institutions de l'Union européenne et aux États membres de favoriser une progression rapide dans la mise en place des initiatives annoncées.

5. **Investir dans les capacités de cyberdéfense**

5.1. Alors que les avancées technologiques progressent rapidement, le cyberespace est devenu le tout nouveau terrain de guerre, après la terre, la mer, les airs et l'espace. Ces évolutions ont aussi ouvert de vastes possibilités de criminalité aux acteurs malveillants du cyberespace, des pirates informatiques indépendants aux criminels professionnels, voire aux acteurs étatiques.

5.2. Il est capital d'investir dans la recherche et le développement, et le CESE se félicite des fonds spécifiques existants au titre du programme pour une Europe numérique, du Fonds européen de la défense, du programme Horizon Europe et des plans nationaux pour la reprise et la résilience. Toutefois, le Comité apprécierait de voir naître davantage de projets transnationaux axés sur la coopération et l'interopérabilité entre les systèmes de cyberdéfense de tous les États membres, ainsi que davantage de synergies entre les instruments de financement, en particulier pour accompagner les PME innovantes.

5.3. Le Comité fait observer que, selon la stratégie de cybersécurité de l'UE adoptée en 2020, l'unité conjointe de cybersécurité doit être créée cette année; il attend des informations sur la finalisation du processus et sur la préparation de l'Union européenne à réagir aux cyberincidents de grande ampleur. Le CESE s'attend à ce que cette unité améliore la connaissance de l'Union quant à la situation en matière de cybersécurité ainsi que sa capacité globale à réagir aux menaces et à s'en relever.

5.4. Le CESE approuve l'extension du mandat du Centre de compétences européen en matière de cybersécurité (ECCC) qui le charge d'assister le Centre de coordination de l'UE en matière de cyberdéfense dans ses activités. Par ailleurs, ce réseau pourrait contribuer à la souveraineté numérique de l'Europe en bâtissant une base industrielle européenne compétitive pour les capacités technologiques clés, notamment par des travaux réalisés dans le cadre de partenariats public-privé contractuels. Les partenariats public-privé se sont révélés être l'approche la plus efficace pour améliorer la cybersécurité de l'écosystème numérique dans son ensemble, mais ils ne peuvent pas être introduits de manière unidirectionnelle: les institutions publiques doivent également partager avec le secteur privé les renseignements dont elles disposent.

5.5. Le CESE fait valoir que pour faire face aux futures tentatives de piratage basées sur l'informatique quantique, l'Union doit investir sans délai dans des technologies de pointe telles que la cryptographie post-quantique. Le CESE estime qu'il est essentiel que l'UE adopte une approche à moyen terme pour acquérir son autonomie et plaide résolument en faveur de la mise en place d'infrastructures de recherche et de production par des entreprises établies dans l'UE. Le CESE tient pour important d'accroître les ressources de l'Union allouées à la recherche et à l'innovation dans le domaine numérique et de soutenir les investissements des opérateurs et des fournisseurs dans les nouvelles fonctionnalités techniques de sécurité, y compris celles qui sont liées à de nouvelles tendances telles que la réalité augmentée et le métavers. Il est particulièrement crucial de créer une infrastructure européenne d'informatique en nuage distribuée, fondée sur les réglementations européennes dans des domaines comme le stockage et le traitement des données ([5]).

5.6. Les PME devraient bénéficier d'une attention particulière et avoir accès à des programmes de financement leur permettant de renforcer leur résilience face aux cyberattaques, ainsi qu'à des programmes d'assistance, de formation et d'éducation qui les aident à comprendre les risques relatifs à la cybersécurité et les moyens de s'en prémunir. L'Union européenne devrait prévoir un mécanisme d'incitation favorisant une familiarisation progressive des PME aux questions de cybersécurité.

5.7. Selon les estimations de la Commission, le déficit de compétences en cybersécurité se chiffre à un demi-million de personnes. Par conséquent, le CESE accueille favorablement la proposition de créer une Académie des compétences cyber. Il est évident que les efforts déployés au niveau des États membres ne suffisent pas à réduire le déficit de compétences. C'est pourquoi le Comité propose qu'en sus du lancement de l'Académie des compétences cyber, la Commission s'appuie sur la nouvelle dynamique créée par l'Année européenne des compétences pour coordonner et financer, au niveau de l'UE, des programmes de formation à grande échelle et des programmes d'enseignement et de formation professionnels auxquels tous les États membres peuvent participer et qui visent à constituer une main-d'œuvre qualifiée pour l'ensemble des agences et organisations concernées par la cyberdéfense, ainsi que pour les réseaux civils privés. Une attention particulière doit être accordée à la formation de la main-d'œuvre, en particulier dans les domaines des sciences, de la technologie, de l'ingénierie et des mathématiques (STEM).

5.8. En outre, le CESE tient pour essentiel de sensibiliser les citoyens à la cybersécurité afin de réduire l'exposition aux cyberattaques, en particulier s'agissant de la cybercriminalité ordinaire qui cible la population dans son ensemble. Le Comité demande que soient créés des cursus d'éducation et des programmes de formation tout au long de la vie qui auront pour principal objectif de renforcer les compétences en matière de cybersécurité, de familiariser les citoyens à cette question, notamment les jeunes, et de rendre ce domaine plus attrayant à leurs yeux. Le CESE est favorable à ce que les questions de cybersécurité soient intégrées dans toutes les futures politiques de l'Union et à ce que l'on informe le grand public sur les cybermenaces, notamment par l'intermédiaire de programmes gratuits de formation destinés à la population dans son ensemble, d'applications mobiles informatives gratuites ou de communications diffusées à la télévision aux heures de grande écoute. En parallèle de ces actions, il y a lieu de promouvoir des avancées culturelles généralisées à tous les niveaux de la société, en vue de progresser vers une approche axée sur la cybersécurité.

5.9. Le CESE estime qu'il est indispensable d'évaluer les profils de risque des fournisseurs et d'appliquer des restrictions pertinentes à ceux considérés comme à haut risque, y compris en procédant aux exclusions nécessaires en ce qui concerne les actifs et applications essentiels définis comme critiques et sensibles dans l'évaluation coordonnée des risques au niveau de l'UE, ainsi qu'en octroyant une certification aux fournisseurs de matériel et de logiciels de confiance.

6. **Établir des partenariats pour relever les défis communs**

6.1. Le niveau de préparation aux futures cyberattaques varie fortement d'un État membre à l'autre. Le CESE considère que la première étape à mettre en place immédiatement est la création d'une plateforme intraeuropéenne de diffusion des bonnes pratiques, où les États membres les plus avancés en matière de cybersécurité pourraient partager leurs connaissances avec les autres pays, et leur faciliter ainsi l'adoption immédiate de telles mesures. Une telle plateforme contribuerait à accroître la confiance mutuelle entre les entités nationales. En outre, le Comité tient pour essentiel de renforcer la coopération entre les acteurs étatiques et non étatiques dans l'ensemble de l'Union afin d'améliorer le niveau de cybersécurité des produits et services sur le marché intérieur. Le CESE propose également que soit créée une plateforme commune européenne permettant de signaler les cyberincidents et comprenant notamment une liste noire de tous les cybercriminels dans l'UE.

([5]) Citons à titre d'exemple l'initiative franco-allemande «Gaia-X».

6.2. Le CESE estime que, dans le domaine militaire, une coopération étroite avec nos alliés de l'OTAN doit être centrée non seulement sur le renforcement des capacités et la détection précoce, mais aussi sur la mise sur pied de projets conjoints de recherche, développement et innovation, le partage de bonnes pratiques et les échanges entre experts, la création de vastes programmes de formation et des simulations de cyberattaques. L'objectif premier de cette coopération doit être d'améliorer la capacité de réaction commune et de créer des synergies pour contrer les futures menaces hybrides, dans la lignée des déclarations conjointes de Varsovie et de Bruxelles, de 2016 et 2018 respectivement. Plusieurs possibilités de coopération entre l'Union européenne et l'OTAN peuvent encore être exploitées, et des progrès immédiats peuvent faire une réelle différence s'agissant de garantir la sécurité de nos citoyens et de nos sociétés.

6.3. Le Comité est d'avis que les discussions au niveau mondial et avec nos partenaires internationaux devraient ouvrir la voie à la promotion d'un cyberespace mondial et ouvert qui protège les droits de l'homme, les libertés fondamentales et l'état de droit, et se concentre sur l'élaboration de normes internationales contraignantes dans les secteurs caractérisés par un développement numérique rapide. Le CESE recommande au haut représentant d'examiner les dialogues bilatéraux existants sur la cybersécurité et de mener des négociations supplémentaires avec d'autres pays et des organisations internationales compétentes, de manière à promouvoir un cadre mondial pour le respect du droit international dans le cyberespace fondé sur une stricte condition de réciprocité.

6.4. Enfin, le Comité estime que l'Union européenne, compte tenu de son ancrage solide dans les libertés démocratiques fondamentales, est bien placée pour prendre la tête des débats à l'échelle internationale sur l'avenir de la cybersécurité, en particulier au sein des Nations unies. L'UE doit également s'engager dans la lutte contre les régimes totalitaires qui exercent un contrôle sur les données des citoyens et violent leurs droits et leurs libertés, et elle devrait également prendre fermement position contre tout type de système de notation sociale à l'encontre des citoyens. Le CESE affirme explicitement qu'une véritable démocratie ne peut exister sans une protection effective des données à caractère personnel, et considère qu'une gestion responsable et efficace des données est fondamentale pour faire de l'hyperconnectivité un atout.

Bruxelles, le 14 juin 2023.

Le président
du Comité économique et social européen
Oliver RÖPKE