Parlement européen
2019-2024

TEXTES ADOPTÉS

P9_TA(2021)0412

État des capacités de cyberdéfense de l'Union

Résolution du Parlement européen du 7 octobre 2021 sur l'état des capacités de cyberdéfense de l'Union (2020/2256(INI))

Le Parlement européen,

– vu le traité sur l'Union européenne (traité UE) et le traité sur le fonctionnement de l'Union européenne (traité FUE),

– vu le document intitulé «Vision partagée, action commune: une Europe plus forte – Une stratégie globale pour la politique étrangère et de sécurité de l'Union européenne», présenté par la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité et vice-présidente de la Commission européenne (HR/VP) le 28 juin 2016,

– vu les conclusions du Conseil européen des 20 décembre 2013, 26 juin 2015, 15 décembre 2016, 9 mars 2017, 22 juin 2017, 20 novembre 2017 et 15 décembre 2017,

– vu la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union[1],

– vu les conclusions du Conseil du 19 juin 2017 relatives à un cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance («boîte à outils cyberdiplomatique»),

– vu la communication conjointe de la Commission et du haut représentant de l'Union européenne pour les affaires étrangères et la politique de sécurité du 13 septembre 2017 intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide» (JOIN(2017)0450),

– vu la déclaration conjointe sur la coopération entre l'UE et l'OTAN signée en juillet 2018,

– vu la décision (PESC) 2019/797 du 17 mai 2019 du Conseil concernant des mesures restrictives contre les cyberattaques menaçant l'Union ou ses États membres,

– vu les conclusions du Conseil du 10 décembre 2019 sur les efforts complémentaires

[1] JO L 194 du 19.7.2016, p. 1.

pour renforcer la résilience et lutter contre les menaces hybrides,

– vu le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications[1] (règlement sur la cybersécurité),

– vu les conclusions du Conseil du 16 juin 2020 sur l'action extérieure de l'UE concernant la prévention du terrorisme et de l'extrémisme violent et la lutte contre ces phénomènes,

– vu les conclusions du Conseil et des représentants des gouvernements des États membres, réunis au sein du Conseil, sur l'établissement d'un pacte en matière de PSDC civile,

– vu la décision (PESC) 2020/1127 du Conseil du 30 juillet 2020 modifiant la décision (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres[2],

– vu la décision (PESC) 2020/1537 du Conseil du 22 octobre 2020 modifiant la décision (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres[3],

– vu la communication de la Commission du 24 juillet 2020 relative à la stratégie de l'UE pour l'union de la sécurité (COM(2020)0605),

– vu la communication conjointe de la Commission et du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité du 16 décembre 2020 intitulée «La stratégie de cybersécurité de l'UE pour la décennie numérique» (JOIN(2020)0018),

– vu la proposition de directive du Parlement européen et du Conseil, présentée par la Commission, concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 du 16 décembre 2020 (COM(2020)0823),

– vu la proposition de directive du Parlement européen et du Conseil, présentée par la Commission, sur la résilience des entités critiques du 16 décembre 2020 (COM(2020)0829),

– vu les conclusions du Conseil du 9 mars 2021 sur la stratégie de cybersécurité de l'UE pour la décennie numérique,

– vu la déclaration du Conseil européen du 25 mars 2021,

– vu le rapport du groupe de travail ouvert du 10 mars 2021,

– vu le programme de désarmement des Nations unies intitulé «Assurer notre avenir

---

1 JO L 151 du 7.6.2019, p. 15.
2 JO L 246 du 30.7.2020, p. 12.
3 JO L 351 I du 22.10.2020, p. 5.

commun»,

– vu les objectifs de développement durable (ODD) des Nations unies, et notamment l'objectif 16, qui vise à promouvoir l'avènement de sociétés pacifiques et inclusives aux fins du développement durable,

– vu le document d'analyse nº 09/2019 de la Cour des comptes européenne sur la défense européenne,

– vu sa résolution du 13 juin 2018 sur la cyberdéfense[1],

– vu l'article 54 de son règlement intérieur,

– vu le rapport de la commission des affaires étrangères (A9-0234/2021),

A. considérant que l'Union et ses États membres doivent encore développer une stratégie de cybersécurité qui fixe des objectifs réalistes, précis et ambitieux et qui définit de manière claire des mesures tant dans le domaine militaire que dans le domaine civil, et dans les zones de recoupement de ces domaines; que toutes les institutions de l'Union et tous les États membres de l'Union doivent davantage coopérer à tous les niveaux pour élaborer cette stratégie, dont l'objet principal devrait être de renforcer la résilience et, ainsi, de développer une coopération et des cybercapacités civiles et militaires nationales communes meilleures et plus solides afin de répondre aux défis persistants en matière de sécurité;

B. considérant que l'Union européenne est attachée à l'application du droit international existant dans le cyberespace, en particulier à l'application de la charte des Nations unies, qui invite les États membres à régler les différends internationaux par des moyens pacifiques et à s'abstenir, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations unies;

C. considérant que ces dernières années ont vu se multiplier les cyberopérations malveillantes menées contre l'Union et ses États membres par des acteurs étatiques et non étatiques qui ont révélé des vulnérabilités dans les réseaux indispensables à la sécurité européenne; que les acteurs informatiques hostiles gagnent en diversité et en sophistication et se multiplient; que ces attaques exigent d'accorder la priorité au renforcement des moyens de défense et au développement des cybercapacités européennes; que des cyberattaques lourdes de conséquences peuvent avoir lieu à tout moment et que les parties prenantes au niveau tant européen que national devraient être encouragées à prendre les mesures nécessaires pour maintenir constamment de réelles capacités de cyberdéfense en temps de paix;

D. considérant que la pandémie de COVID-19 et la hausse de l'insécurité informatique ont montré que des accords internationaux sont nécessaires; que le nombre de cyberattaques s'est considérablement accru durant la pandémie de COVID-19 et que l'Union et ses États membres ont détecté des cybermenaces et des activités informatiques malveillantes ciblant des opérateurs essentiels, y compris des attaques visant à perturber des infrastructures critiques dans le domaine de l'énergie, des transports et de la santé,

---

[1] JO C 28 du 27.1.2020, p. 57.

ainsi que d'importantes ingérences étrangères qui ont rendue floue la limite entre paix et hostilités; que le plan de relance pour l'Europe prévoit des investissements supplémentaires dans la cybersécurité;

E. considérant que le cyberespace est maintenant reconnu comme un domaine d'opérations; que les cybermenaces sont capables de compromettre tous les domaines militaires traditionnels et que ces domaines dépendent de la fonctionnalité du cyberespace, et non l'inverse; considérant que les conflits peuvent avoir lieu dans tous les domaines physiques (terrestre, aérien, maritime et spatial) et virtuels (cyberespace), et peuvent être amplifiés par des éléments de guerre hybride, tels que des campagnes de désinformation utilisant les TIC, des guerres par procuration, l'utilisation offensive et défensive de capacités informatiques ainsi que des attaques stratégiques contre des prestataires de services numériques visant à désorganiser des infrastructures critiques ainsi que nos institutions démocratiques et à engendrer des pertes financières considérables;

F. considérant que le Service européen pour l'action extérieure (SEAE), la Commission et l'Agence européenne de défense (AED) devraient aider les États membres à se coordonner et à redoubler d'efforts pour mettre à disposition des capacités et des technologies de cyberdéfense, en abordant tous les aspects du développement des capacités, y compris la doctrine, le commandement, l'organisation, le personnel, la formation, l'industrie, les technologies, les infrastructures, la logistique, l'interopérabilité et les ressources;

G. considérant que pendant l'élaboration du catalogue des besoins (2017), qui est utilisé pour recenser toute l'étendue des besoins militaires de la politique de sécurité et de défense commune (PSDC) dans le contexte de plusieurs scénarios types, les capacités de cyberdéfense sont apparues comme une priorité élevée;

H. considérant que la réussite de l'exécution des missions et des opérations de l'Union dépend de plus en plus d'un accès ininterrompu à un cyberespace sécurisé, et nécessite par conséquent des cybercapacités opérationnelles résilientes;

I. considérant que le cadre stratégique de cyberdéfense de l'UE mis à jour en 2018 a mis en évidence des priorités telles que le développement des capacités de cyberdéfense et la protection des réseaux de communication et d'information relevant de la PSDC;

J. considérant que, dans son discours sur l'état de l'Union de 2021, la présidente de la Commission a souligné la nécessité d'une politique de cyberdéfense de l'Union;

K. considérant que l'intégration croissante de l'intelligence artificielle (IA) dans les cybercapacités des forces de défense (systèmes cyber-physiques, y compris les liaisons de communication et de données entre les véhicules dans un système en réseau) peut entraîner des vulnérabilités aux attaques de guerre électronique telles que le brouillage, l'usurpation ou le piratage;

L. considérant que le relèvement du niveau de la cybersécurité et de la cyberdéfense dans l'Union devra nécessairement accompagner celui des ambitions numériques et géopolitiques de l'Europe pour assurer leur concrétisation, et engendrera une plus grande résilience, tout en permettant de tenir tête à la sophistication croissante et à la multiplication des cyberattaques; qu'une Union dotée d'une solide culture en matière de

cybersécurité et de technologies de cybersécurité robustes, notamment de la capacité d'identifier et d'attribuer les actes de malveillance de manière rapide et efficace et d'y répondre adéquatement, serait en mesure de protéger ses citoyens ainsi que la sécurité de ses États membres;

M. considérant que les organisations terroristes internationales ont acquis une grande expertise et expérience de la cyberguerre et que les auteurs de cyberattaques utilisent des technologies de pointe pour rechercher des vulnérabilités dans les systèmes et les appareils ainsi que pour lancer des attaques informatiques de grande envergure et à très grande échelle;

N. considérant que le secteur de la défense et l'industrie spatiale sont confrontés à une concurrence mondiale sans précédent et à des évolutions technologiques majeures avec l'émergence de technologies informatiques de pointe; que la Cour des comptes de l'Union européenne a relevé des lacunes capacitaires dans les domaines des technologies de l'information et de la communication, de la cyberguerre et de l'IA; que l'Union européenne est importatrice nette de produits et de services de cybersécurité, ce qui augmente le risque de dépendance technologique et de vulnérabilité face aux opérateurs extérieurs à l'Union européenne; qu'un socle de compétences communes de l'Union en matière d'IA devrait venir combler les lacunes techniques et garantir que les États membres ne disposant pas de la technologie adéquate ni de l'expertise industrielle ou de la capacité à mettre en œuvre des systèmes fondés sur l'IA dans leurs propres ministères de la défense ne soient pas laissés de côté;

O. considérant que le scandale du logiciel espion Pegasus a révélé qu'un grand nombre de journalistes, de militants dans le domaine des droits de l'homme, de représentants élus et d'autres citoyens de l'Union ont été espionnés; que différents acteurs étatiques tels que la Russie, la Chine et la Corée du Nord ont commis des actes de cybermalveillance visant des objectifs politiques, économiques ou de sécurité et qui incluent des attaques contre des infrastructures critiques, du cyberespionnage et une surveillance de masse des citoyens de l'Union, le soutien à des campagnes de désinformation, la diffusion de logiciels malveillants et la restriction de l'accès à l'internet et du fonctionnement des systèmes informatiques; que ces actes bafouent et enfreignent le droit international, les droits de l'homme et les droits fondamentaux dans l'Union et mettent en péril la démocratie, la sécurité, l'ordre public et l'autonomie stratégique de l'Union, et devraient donc faire l'objet une réponse conjointe de l'Union, par exemple en utilisant le cadre pour une réponse diplomatique conjointe de l'Union, y compris les mesures restrictives prévues dans la boîte à outils cyberdiplomatique;

P. considérant que le Conseil a décidé pour la première fois, le 30 juillet 2020, d'appliquer des mesures restrictives à l'encontre de personnes, d'entités et d'organismes impliqués dans diverses cyberattaques, afin de mieux prévenir et décourager les actes de cybermalveillance ainsi qu'à mieux y faire face; que le cadre juridique du régime de sanctions de l'Union en matière de cyberattaques a été adopté en mai 2019;

Q. considérant que les cadres d'attribution constituent un élément central de la cyberdiplomatie et des stratégies de dissuasion;

R. considérant que, ces dernières années, la coopération entre l'Union et l'OTAN s'est intensifiée dans de nombreux domaines, y compris ceux de la cybersécurité et de la cyberdéfense, conformément à la déclaration conjointe UE-OTAN de 2016;

S. considérant que les rapports de consensus de 2010, 2013 et 2015 du groupe d'experts gouvernementaux des Nations unies, tels qu'approuvés par son Assemblée générale, constituent un cadre normatif universel pour la stabilité du cyberespace, qui consiste à reconnaître que le droit international en vigueur, y compris la charte des Nations unies dans son intégralité, s'applique dans le cyberespace, tout comme les onze normes volontaires non contraignantes de comportement responsable des États, ainsi que les mesures de confiance et le renforcement des capacités;

État des capacités de cyberdéfense de l'Union

1. souligne qu'une politique de cyberdéfense commune et une coopération accrue au niveau de l'Union visant à mettre en place des capacités communes et améliorées de cyberdéfense sont des éléments essentiels pour bâtir une Union européenne de la défense plus solide et plus approfondie et nécessitent une combinaison complexe de capacités techniques, stratégiques et opérationnelles; indique que le concept de cyberdéfense renvoie à des actions, des instruments et des processus proportionnés et conformes au droit international, qui peuvent comprendre des éléments tant militaires que civils et qui ont pour objectif de protéger, notamment, les réseaux de communication et d'information relevant de la PSDC ainsi que les missions et opérations de PSDC et d'apporter une assistance aux États membres; souligne qu'il est urgent de développer et de renforcer tant les capacités de cyberdéfense militaires communes que celles des États membres;

2. rappelle que la nature transfrontière du cyberespace, ainsi que le nombre important de cyberattaques et leur complexité croissante, nécessitent une réaction coordonnée au niveau de l'Union, y compris par la mobilisation des capacités de soutien communes des États membres et l'appui des États membres aux mesures prévues dans la boîte à outils cyberdiplomatique de l'Union, ainsi que l'intensification de la coopération UE-OTAN sur la base du partage d'informations entre les équipes chargées de la gestion des crises cyber, le partage des bonnes pratiques et le renforcement de la formation, de la recherche et des exercices dans ce domaine;

3. salue le cadre stratégique de cyberdéfense en tant qu'outil de soutien au développement des capacités de cyberdéfense des États membres; souligne que la révision du cadre stratégique de cyberdéfense devrait avant tout mettre en lumière les lacunes et les vulnérabilités existantes dans les structures militaires nationales et de l'Union; souligne la nécessité de renforcer la coordination entre les institutions, les agences et les organes de l'Union, entre et avec les États membres, ainsi qu'avec le Parlement européen, afin de garantir que le cadre stratégique de cyberdéfense actualisé permette la réalisation des objectifs de l'Union en matière de cyberdéfense;

4. invite le SEAE et la Commission à poursuivre, en coopération avec les États membres, l'élaboration d'un ensemble complet de mesures et d'une politique cohérente en matière de sécurité informatique afin de renforcer la résilience, mais aussi la coordination en matière de cyberdéfense; demande instamment le renforcement de la coopération avec l'équipe civile d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union (CERT-UE) afin de protéger les réseaux utilisés par l'ensemble des institutions, des organes et des agences de l'Union, en étroite collaboration avec les directions des systèmes d'information respectives de ces entités, ainsi que l'amélioration de la communication des institutions, organes et agences de l'Union avec les États membres; invite le Parlement à s'assurer de sa contribution aux

résultats produits par la CERT-UE afin de garantir un niveau de sécurité informatique qui lui permettra de recevoir toutes les informations classifiées et non classifiées nécessaires à l'exercice des responsabilités qui lui incombent en vertu des traités, y compris en conséquence du processus actuel visant à remplacer l'accord interinstitutionnel de 2002 sur l'accès à l'information dans le domaine de la sécurité et de la défense; demande au SEAE de garantir des niveaux appropriés de cybersécurité pour ses actifs, ses locaux et ses activités, y compris son siège, les délégations de l'Union et les missions et opérations de la PSDC;

5. prend acte de l'objectif du cadre stratégique de cyberdéfense de 2018 consistant à mettre en place un réseau CERT militaire de l'Union; invite les États membres à accroître sensiblement les capacités de partage d'informations classifiées afin de faciliter le partage d'informations là où il est utile et nécessaire, et à mettre en place un réseau européen rapide et sécurisé de détection, d'évaluation et de lutte contre les cyberattaques;

6. rappelle que les priorités fixées en 2018 dans le cadre du plan de développement des capacités de l'UE portaient sur la nécessité de développer un éventail complet de capacités et ont désigné les capacités de cyberdéfense comme une priorité essentielle; que le plan soulignait que les technologies de surveillance cyber et de cyberdéfense sont essentielles pour contrer les menaces de sécurité; salue l'appui apporté par l'AED aux États membres dans le développement de leurs capacités de sorte à améliorer leur résilience informatique, notamment leur capacité à détecter toute cyberattaque, à y résister et à s'en remettre; prend note des différentes activités engagées par les États membres dans le cadre de l'AED, notamment de son projet CyDRE, dont l'objectif est d'élaborer une architecture d'entreprise pour les opérations liées au cyberespace, notamment sa portée, ses fonctionnalités et ses exigences, sur la base de la législation nationale et européenne;

7. invite les États membres à définir une norme commune de communication qui pourrait être utilisée pour les informations classifiées et non classifiées, afin de faciliter une action rapide et de garantir l'existence d'un réseau sécurisé de protection contre les cyberattaques.

8. se félicite de l'examen annuel coordonné en matière de défense (EACD), le premier examen complet en matière de défense à l'échelle de l'Union, qui est l'un des principaux outils à l'appui de la cohérence globale des dépenses, de la planification et de la coopération en matière de défense des États membres, et qui devrait contribuer à promouvoir les investissements dans le développement des cybercapacités de défense;

9. salue les progrès déjà accomplis dans le cadre du programme européen de développement industriel dans le domaine de la défense (PEDID) sous la forme de plusieurs projets pertinents concernant le renseignement, la sécurisation des communications et la cyberdéfense; salue, en particulier, l'appel lancé en faveur d'une boîte à outils de cyberdéfense facilement déployable et interconnectée et le fait que le Fonds européen de la défense (FED) contribuera également au renforcement de la résilience et à l'amélioration de la préparation, de la réactivité et de la coopération dans le domaine cyber, à condition que cette priorité soit fixée lors de la négociation des programmes de travail concernés du FED; souligne que la capacité de l'Union à développer des projets de cyberdéfense dépend de la maîtrise des technologies, des équipements, des services et des données ainsi que de leur traitement et nécessite de

s’appuyer sur une base d’acteurs sectoriels de confiance, et exige la mise en œuvre intégrale de la directive relative aux marchés publics dans le domaine de la défense[1] ainsi que le contrôle de son application; invite les États membres à tirer parti du FED pour développer ensemble des capacités de cyberdéfense;

10. se félicite du renforcement de la coopération entre les États membres dans le domaine de la cyberdéfense et du commandement, du contrôle, des communications, de l’informatique, du renseignement, de la surveillance et de la reconnaissance (C4ISR) dans le cadre de la coopération structurée permanente (CSP), y compris par la mise en œuvre de projets concrets tels que les équipes d’intervention rapide en cas d’incident informatique et l’assistance mutuelle dans le domaine de la cybersécurité; rappelle que le FED et la CSP offrent d’excellents moyens de développer les capacités en matière de cybersécurité et d’accélérer les initiatives de cybersécurité, notamment au moyen de la plateforme de partage d’informations en matière de réaction aux menaces et incidents informatiques et du Centre de coordination dans le domaine du cyber et de l’information; invite tous les États membres à garantir une cohérence et à mettre l’accent sur les capacités informatiques en définissant une approche stratégique commune concernant les priorités; demande que la recherche, l’innovation et le partage d’expertise soient encouragés afin de réaliser le plein potentiel de la CSP et du FED; salue la décision du Conseil du 5 novembre 2020 d’autoriser des pays tiers à participer à des projets de CSP dans certains cas particuliers, lorsqu’ils peuvent apporter une valeur ajoutée ainsi qu’une expertise technique et des capacités supplémentaires, et à condition qu’ils remplissent un ensemble prédéfini de conditions politiques, juridiques et de fond; souligne qu’il pourrait être dans l’intérêt stratégique de l’Union que des États membres et des pays tiers participent, de manière exceptionnelle et au cas par cas, à des projets de CSP liés au domaine cyber dans le but de réaliser des objectifs plus ambitieux, sur la base d’une réelle réciprocité;

11. souligne que la cyberdéfense est considérée comme une tâche opérationnelle pour toutes les missions de CSP, et que la cyberrésilience et les capacités connexes doivent être mises en place, testées et déployées avant le début des processus de planification de la PSDC; rappelle que la réussite des missions et des opérations de l’Union dépend de plus en plus d’un accès ininterrompu à un cyberespace sécurisé et nécessite par conséquent des cybercapacités opérationnelles solides et résilientes ainsi que des réponses appropriées aux attaques contre les installations, les missions et les opérations militaires; souligne que, conformément au pacte en matière de PSDC civile, les missions de la PSDC civile doivent être cyberrésilientes et soutenir les pays hôtes si nécessaire, y compris au moyen d’un suivi, d’un tutorat et de conseils; recommande d’envisager des possibilités de soutien au renforcement des capacités de nos partenaires, au moyen, par exemple, de l’extension du mandat des missions de formation de l’UE pour qu’il comprenne aussi les aspects liés à la cyberdéfense ou du lancement de missions de cybersécurité civiles;

12. se félicite de la décision du Conseil du 14 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l’Union ou ses États membres, qui permet de prendre des mesures restrictives ciblées pour décourager et contrer les cyberattaques

---

[1] Directive 2009/81/CE du Parlement européen et du Conseil du 13 juillet 2009 relative à la coordination des procédures de passation de certains marchés de travaux, de fournitures et de services par des pouvoirs adjudicateurs ou entités adjudicatrices dans les domaines de la défense et de la sécurité (JO L 216 du 20.8.2009, p. 76).

constituant une menace pour l'Union ou ses États membres, y compris les cyberattaques contre des pays tiers ou des organisations internationales; se félicite de l'application de telles mesures restrictives en juillet et octobre 2020, laquelle constitue une étape crédible dans le déploiement de la boîte à outils cyberdiplomatique de l'Union, y compris donc des mesures restrictives, et le renforcement du dispositif de cyberdissuasion de l'Union; appelle de ses vœux la mise en place et l'application stricte d'un système de mesures restrictives proportionnées de contention des cyberattaques, dans le respect de la vision européenne de l'internet, à savoir un réseau unique, ouvert, neutre, libre, sûr et non fragmenté;

13. rappelle qu'étant donné la double nature des cybertechnologies, la sécurité des produits et services civils est essentielle pour le domaine militaire et contribue donc à améliorer la cyberdéfense; accueille par conséquent favorablement les travaux menés par l'ENISA, qui associent les États membres et les parties prenantes intéressées en vue fournir à l'Union des schémas de certification pour les produits, services et processus TIC afin de relever le niveau global de cybersécurité au sein du marché unique numérique; insiste sur le rôle pionnier que joue l'Union dans l'élaboration de normes qui façonnent le paysage de la cybersécurité, contribuent à une concurrence loyale au sein de l'Union et sur la scène mondiale, et apportent une réponse aux mesures extraterritoriales ainsi qu'aux risques pour la sécurité des pays tiers; prend également acte du rôle important joué par l'ENISA dans le soutien apporté aux initiatives de recherche et aux autres formes de coopération visant à renforcer la cybersécurité; souligne l'importance que revêtent les investissements dans la cyberdéfense et les capacités en matière de cyberdéfense en vue de renforcer la résilience et les capacités stratégiques de l'Union et de ses États membres; insiste, à cet égard, sur l'importance du programme pour une Europe numérique et d'Horizon Europe, en particulier de son pôle «Sécurité civile pour la société»; signale l'importance des instruments financiers idoines disponibles dans le cadre financier pluriannuel (CFP) 2021-2027 ainsi que dans la facilité pour la reprise et la résilience (FRR);

14. salue les progrès réalisés par certains États membres de l'Union dans la mise en place de cybercommandements au sein de leurs armées;

Vision stratégique – Parvenir à la résilience en matière de cyberdéfense

15. note que les orientations stratégiques sur la sécurité et la défense renforceront et orienteront la mise en œuvre des ambitions de l'Union en matière de sécurité et de défense et traduiront ces ambitions en besoins capacitaires, y compris et en priorité dans le domaine de la cyberdéfense, ce qui renforcera la capacité de l'Union et de ses États membres à détecter, attribuer, empêcher, décourager et prévenir les actes de cybermalveillance ainsi qu'à mieux y faire face et à s'en remettre en renforçant sa position, son appréciation de la situation, son cadre juridique et éthique, ses outils, ses procédures et ses partenariats;

16. insiste sur le fait que les orientations stratégiques devraient approfondir la culture stratégique dans le domaine cyber et éliminer tout chevauchement des capacités et des missions; souligne qu'il est essentiel de surmonter la fragmentation et la complexité actuelles de l'architecture cyber globale au sein de l'Union et de définir une vision commune pour déterminer comment garantir la sécurité et la stabilité dans le cyberespace;

17. souligne que cette fragmentation s'accompagne de graves préoccupations quant au manque de ressources et de personnel au niveau de l'Union, entrave à la création d'un environnement numérique entièrement sûr, et insiste par conséquent sur la nécessité de renforcer ces deux postes; prie instamment le HR/VP et/ou les États membres d'accroître les ressources financières et humaines consacrées à la cyberdéfense, en particulier le nombre d'analystes en cyberrenseignement et d'experts en investigation numérique, ainsi que d'améliorer leur formation dans les domaines de la prise de décision et de l'élaboration des politiques, de la mise en œuvre de ces dernières, de la réaction aux incidents informatiques et des enquêtes à leur sujet, y compris leurs compétences en matière de cybersécurité afin de renforcer la capacité de l'Union à repérer et à attribuer les cyberattaques, et donc à proposer une réponse politique, civile et militaire adéquate dans un délai court; demande un financement supplémentaire de la CERT-UE et du Centre de situation et du renseignement de l'UE (INTCEN) ainsi qu'un soutien plus appuyé aux États membres pour la création et le renforcement des centres d'opérations de sécurité (COS) afin de former un réseau de COS couvrant toute l'Union, ce qui permettrait de renforcer la coopération civilo-militaire de sorte à pouvoir émettre en temps utile des alertes concernant les incidents de cybersécurité;

18. fait remarquer qu'une formation militaire européenne harmonisée dans le domaine cyber améliorerait sensiblement le niveau de confiance parmi les États membres et permettrait d'accroître le nombre de procédures opérationnelles standardisées, de définir des règles plus claires et d'améliorer l'application de ces dernières; prend acte, à cet égard, de l'important travail de formation réalisé par le Collège européen de sécurité et de défense (CESD) dans le domaine de la cyberdéfense et se félicite de la création de la plateforme d'enseignement, de formation, d'évaluation et d'exercices (ETEE) dans le domaine cyber, qui vise à assurer la formation en cybersécurité et en cyberdéfense du personnel civil et militaire ainsi qu'à permettre l'harmonisation et la standardisation nécessaires des formations liées au domaine cyber; souligne que le CESD devrait bénéficier davantage des Fonds structurels de l'Union afin de pouvoir accroître sa contribution à la promotion des compétences de cyberdéfense dans l'Union, en particulier au vu du besoin accru d'experts cyber de haut niveau; invite les États membres à encourager la conclusion de partenariats avec le monde universitaire visant à promouvoir des programmes de recherche et développement en matière de cybersécurité afin de développer de nouveaux outils communs ainsi que de nouvelles technologies et compétences communes applicables à la fois au secteur civil et au secteur militaire; souligne l'importance de l'éducation pour sensibiliser le public et améliorer les compétences des citoyens afin qu'ils puissent se défendre contre les cyberattaques;

19. souligne que les politiques de cyberdéfense de l'Union doivent intégrer les questions de genre et faire preuve d'ambition pour réduire l'écart entre les hommes et les femmes parmi les professionnels de la cyberdéfense, notamment au moyen de politiques actives d'inclusion des femmes et de programmes de formation conçus spécifiquement pour les femmes;

20. rappelle que la cyberdéfense comprend des dimensions civiles et militaires et exige par conséquent une coopération, des synergies et une cohérence plus fortes entre les différents instruments; souligne qu'il convient d'abord d'analyser et de discuter des problèmes de coopération et de coordination, mais aussi, par la suite, d'examiner les lacunes en matière de ressources humaines et techniques, tant au niveau national qu'au niveau de l'Union; relève qu'une intégration réussie des ressources militaires et civiles ne peut être assurée que par des formations et des exercices incluant toutes les parties

concernées; attire l'attention, à cet égard, sur l'exercice «Locked Shields» de l'OTAN, qui est un des meilleurs exemples de test et d'amélioration des capacités de cyberdéfense tant civiles que militaires; invite dès lors le HR/VP et la Commission à élaborer une approche stratégique intégrée et à encourager les synergies ainsi qu'une étroite coopération entre le réseau CERT militaire, la CERT-UE et le réseau des CSIRT;

21. se félicite de la communication conjointe du HR/VP et de la Commission intitulée «La stratégie de cybersécurité de l'UE pour la décennie numérique», qui vise à renforcer les synergies et la coopération entre les missions en matière de cybersécurité civiles, de défense et spatiales; estime que la stratégie constitue une étape importante dans le renforcement de la cyber-résilience de l'Union et des États membres, confortant ainsi la position prépondérante de l'Union en matière de numérique et ses capacités stratégiques;

22. préconise la création d'une unité conjointe de cybersécurité en vue de renforcer la coopération et de remédier à l'insuffisance du partage d'informations entre les institutions, les organes et les agences de l'Union, en garantissant ainsi un réseau d'information rapide et sûr et en permettant la pleine exploitation des structures, des ressources et des capacités existantes; note le rôle important que pourrait jouer l'unité conjointe de cybersécurité dans la protection de l'Union contre de graves cyberattaques transfrontalières en s'appuyant sur le concept de partage d'informations intersectoriel; souligne l'importance de la coordination afin d'éviter la duplication des structures et des responsabilités au cours de la conception; salue, à cet égard, la recommandation de la Commission du 23 juin 2021, qui prévoit que la mise en place d'interfaces spécifiques avec l'unité conjointe de cybersécurité devrait être conçue de sorte à permettre le partage d'informations avec la communauté de cyberdéfense, notamment par l'intermédiaire de la représentation du SEAE; souligne par ailleurs que les représentants des projets de CSP pertinents devraient soutenir l'unité conjointe de cybersécurité, notamment en ce qui concerne la connaissance de la situation et la préparation;

23. rappelle qu'étant donné que les capacités de cyberdéfense comportent souvent une dimension duelle, leur amélioration nécessite également une expertise civile en matière de sécurité des réseaux et de l'information; souligne que la prolifération de systèmes à double usage librement commercialisés peut devenir problématique, car ces systèmes sont exploités par un nombre croissant d'acteurs hostiles étatiques et non étatiques; invite la Commission et les États membres à actionner plusieurs leviers importants, tels que la certification et la surveillance de la responsabilité des acteurs privés; souligne que l'innovation technologique est principalement portée par des entreprises privées et que, par conséquent, la coopération avec le secteur privé et les parties prenantes civiles, y compris les industries et les entités participant à la gestion des infrastructures critiques, ainsi qu'avec les PME, la société civile, les organisations et le monde universitaire est essentielle et devrait être renforcée; prend note de la proposition de révision de la directive sur la sécurité des réseaux et des systèmes d'information (SRI) et de la proposition de directive relative à la résilience des entités critiques, qui visent à protéger les infrastructures critiques et à renforcer la sécurité de la chaîne d'approvisionnement ainsi qu'à intégrer les acteurs réglementés dans l'écosystème numérique; rappelle que chaque État membre devrait disposer d'une politique spécifique en matière de gestion des risques de cybersécurité concernant les chaînes d'approvisionnement qui traite, en particulier, la question des fournisseurs de confiance; rappelle par ailleurs que la directive SRI devrait respecter les compétences des États membres et renvoie aux avis de la sous-commission SEDE concernant ces deux

propositions;

24. salue le lancement, le 29 septembre 2020, du réseau européen pour la préparation et la gestion des crises cyber (réseau CyCLONe), qui a encore amélioré l'échange d'informations en temps opportun et la capacité d'appréciation de la situation en comblant le fossé entre les niveaux technique et politique de l'Union; note également qu'une capacité effective de cyberdéfense exige de passer d'une culture du partage d'informations basée sur le «besoin d'en connaître» à une culture basée sur la «nécessité de partager»;

25. se félicite du plan d'action de la Commission relatif aux synergies entre les industries civile, spatiale et de la défense, et rappelle l'interdépendance étroite de ces trois secteurs dans le domaine de la cyberdéfense; constate que, contrairement à d'autres domaines militaires, l'infrastructure utilisée pour «créer» le cyberespace est principalement aux mains d'entités commerciales établies pour la plupart en dehors de l'Union, ce qui entraîne une dépendance industrielle et technologique vis-à-vis de tiers; est fermement convaincu que l'Union doit renforcer sa souveraineté technologique et stimuler l'innovation en investissant dans l'utilisation éthique de nouvelles technologies de sécurité et de défense, telles que l'intelligence artificielle et l'informatique quantique; encourage fortement la création au sein des États membres d'un programme de recherche et développement axé sur l'IA; insiste cependant sur le fait que l'utilisation militaire de l'IA doit respecter le droit international relatif aux droits de l'homme et le droit international humanitaire, et que l'Union doit jouer un rôle moteur dans l'élaboration d'un cadre réglementaire mondial pour l'IA fondé sur des valeurs démocratiques et sur une approche intégrant l'humain aux processus;

26. prend acte des travaux importants menés par le Centre satellitaire de l'Union européenne (CSUE) et insiste sur le fait que l'Union doit disposer de ressources adéquates dans les domaines de l'imagerie spatiale et du recueil du renseignement; demande à l'Agence de mener une analyse et de rédiger un rapport sur la sécurité et/ou les vulnérabilités des satellites de l'Union et des États membres à l'égard des débris spatiaux et des cyberattaques; souligne que le CSUE devrait bénéficier de davantage de Fonds structurels de l'Union pour pouvoir continuer de contribuer aux actions de l'Union; souligne que les capacités de cyberdéfense sont essentielles pour garantir le partage sûr et résilient d'informations avec le CSUE, qu'il s'agisse de sécurité depuis l'espace ou de sécurité dans l'espace, afin de préserver et de renforcer l'autonomie stratégique nécessaire de l'Union en matière d'appréciation de la situation; souligne la nécessité pour l'Union de s'efforcer d'empêcher la militarisation de l'espace;

27. salue la décision du Conseil relative à la création à Bucarest du Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, qui recevra et orientera les financements liés à la cybersécurité d'Horizon Europe et du programme pour une Europe numérique, et se dit en faveur d'une coopération harmonieuse avec son réseau de centres nationaux de coordination; souligne l'importance du Centre pour l'exécution des projets et des initiatives pertinents en matière de cybersécurité qui contribueront à la création de nouvelles capacités essentielles à la résilience de l'Union et au renforcement de la coordination entre les secteurs civil et militaire de la cybersécurité; souligne que le Centre de compétences en matière de cybersécurité doit réunir les principales parties prenantes européennes, notamment des entreprises, des organisations universitaires et de recherche et d'autres associations de la société civile concernées, en vue de renforcer et de diffuser l'expertise

en matière de cybersécurité dans toute l'Union;

28. souligne l'importance du chiffrement et de l'accès légal aux données chiffrées; rappelle que le chiffrement des données et le renforcement ainsi que l'usage le plus large possible de ces capacités peuvent contribuer de manière significative à la cybersécurité des États, des sociétés et de l'industrie; appelle de ses vœux un programme de «souveraineté numérique européenne» afin de promouvoir et de renforcer les capacités actuelles en matière d'outils cyber et de chiffrement, sur la base des droits fondamentaux européens et de valeurs telles que le respect de la vie privée, la liberté d'expression et la démocratie, avec pour objectif d'améliorer la compétitivité de l'Europe sur le marché de la cybersécurité et de stimuler la demande intérieure;

29. se félicite des futures «stratégie et vision militaires de l'UE sur le cyberespace en tant que domaine d'opérations» qui définiront le cyberespace comme un domaine d'opérations pour la PSDC de l'Union; demande une évaluation continue des vulnérabilités des infrastructures d'information des missions de la PSDC ainsi que la mise en œuvre de normes harmonisées communes en matière d'éducation, de formation et d'exercices en matière de cyberdéfense à l'appui des missions PSDC;

30. regrette que les limitations actuelles des systèmes classifiés de la capacité militaire de planification et de conduite (MPCC) de l'Union entravent ses capacités; demande par conséquent au SEAE de fournir rapidement à la MPCC un système de communication et d'information de pointe, autonome et sûr, capable de traiter des données classifiées de l'Union pour ses missions et opérations de la PSDC et doté d'un niveau de protection et de résilience adapté ainsi que d'un quartier général pour les forces déployées;

31. demande une intégration plus poussée de la cybersécurité dans les mécanismes de réaction aux crises de l'Union et l'interconnexion des initiatives, structures et procédures existantes dans les diverses communautés cyber afin de renforcer l'assistance mutuelle et la coopération opérationnelle entre les États membres, en particulier en cas de cyberattaques majeures, de sorte à accroître l'interopérabilité et à parvenir à une définition commune de la cyberdéfense; insiste avec force sur l'importance de mener d'autres d'exercices, mais à une fréquence plus élevée, et des discussions stratégiques fondées sur des scénarios portant sur la gestion de crise, y compris sur la clause d'assistance mutuelle (article 42, paragraphe 7, du traité UE), dans l'hypothèse d'une cyberattaque grave, potentiellement de même niveau qu'une agression armée; demande que de telles initiatives viennent consolider la définition commune des procédures de mise en œuvre de l'assistance mutuelle et/ou de la clause de solidarité, conformément à l'article 42, paragraphe 7, du traité UE et à l'article 222 du traité FUE, y compris dans le but spécifique de mettre en œuvre ces procédures pour les cyberattaques dirigées contre les États membres de l'Union; salue le communiqué du sommet de l'OTAN de Bruxelles du 14 juin 2021, qui réaffirme l'engagement pris par l'OTAN d'employer la totalité des capacités à sa disposition à tout moment à des fins de dissuasion, de défense et de contre-attaque actives face au vaste éventail de cybermenaces, y compris le recours à l'article 5 «au cas par cas»; se félicite des discussions plus approfondies sur l'articulation entre le cadre de gestion des crises de cybersécurité de l'Union et la boîte à outils cyberdiplomatique;

32. fait remarquer que l'Union européenne est de plus en plus mêlée à des conflits hybrides avec des adversaires géopolitiques; souligne que ces actes sont d'une nature particulièrement déstabilisante et dangereuse, car ils brouillent les limites entre guerre et

paix, déstabilisent les démocraties et sèment le doute dans l'esprit des populations visées; rappelle que ces attaques sont rarement assez graves en elles-mêmes pour déclencher l'article 5 du traité de l'Atlantique Nord ou l'article 42, paragraphe 7, du traité UE, mais qu'elles ont tout de même des effets stratégiques cumulatifs et qu'elles ne peuvent pas être réellement combattues par des mesures de rétorsion de la part de l'État membre attaqué; estime que l'Union devrait par conséquent s'efforcer de trouver une solution pour combler ce vide juridique en réinterprétant l'article 42, paragraphe 7, du traité UE et l'article 222 du traité FUE d'une manière qui prévoirait un droit à une défense collective en dessous du seuil de défense collective et permettrait l'adoption par les États membres, sur la base du volontariat, de contre-mesures collectives, et qu'elle devrait travailler avec ses alliés pour trouver une solution similaire au niveau international; souligne qu'il s'agit du seul véritable moyen de surmonter la paralysie face aux menaces hybrides, et que cela pourrait permettre de rendre plus coûteuses les attaques pour nos adversaires;

33. rappelle que des capacités d'attribution communes robustes sont un des principaux outils nécessaires au renforcement des capacités de l'Union et des États membres et qu'elles forment une composante essentielle d'une cyberdéfense et d'une cyberdissuasion efficaces; souligne que l'amélioration de l'échange d'informations techniques, d'analyses et de renseignements sur les menaces entre les États membres au niveau de l'Union pourrait permettre une attribution collective au niveau de l'Union; admet que, dans une certaine mesure, la cyberdéfense est plus efficace si elle comporte également certains moyens et mesures offensifs, sous réserve que leur usage soit conforme au droit international; souligne que l'attribution explicite des cyberattaques est un instrument de dissuasion utile; propose d'envisager l'attribution publique conjointe des cyberactivités malveillantes, y compris la possibilité de créer sous les auspices du SEAE des rapports sur les comportements dans le cyberespace, afin de permettre à des acteurs spécifiques de synthétiser à l'échelle de l'Union les informations relatives aux cyberactivités malveillantes menées contre les États membres et soutenues par des États;

34. considère essentielle la coopération en matière de cybersécurité entre l'Union et l'OTAN, qui pourrait permettre et renforcer une attribution formelle collective des incidents informatiques malveillants, et par conséquent l'application de sanctions et de mesures restrictives; fait observer que l'on pourrait mettre en place une véritable résilience et une dissuasion efficace si les auteurs des cyberattaques connaissaient le catalogue des contre-mesures possibles, leur proportionnalité, leur caractère approprié et leur conformité avec le droit international, en particulier avec la charte des Nations unies (en fonction de la gravité, de l'ampleur et de la cible des cyberattaques);

35. salue la proposition du HR/VP d'encourager et de faciliter la mise en place d'un groupe de travail des États membres de l'Union en matière de cyber-renseignement au sein de l'INTCEN, afin de faire progresser la coopération stratégique en matière de renseignement sur les cybermenaces et les actes de cybermalveillance et de continuer à soutenir les capacités d'analyse de la situation et la prise de décision en ce qui concerne une réponse diplomatique conjointe; appelle de ses vœux davantage de progrès en ce qui concerne la série de propositions communes, en particulier l'interaction actuelle entre la cellule de fusion de l'Union contre les menaces hybrides et la branche d'analyse des menaces hybrides de l'OTAN sur le plan du partage d'informations sur les situations et d'analyses ainsi que de la coopération tactique et opérationnelle;

Renforcer les partenariats et le rôle de l'Union dans le contexte international

36. estime que la coopération en matière de cyberdéfense avec l'OTAN joue un rôle important pour prévenir et dissuader les cyberattaques impactant la sécurité collective des États membres ainsi que pour y répondre; invite les États membres à partager sans réserve les éléments probants et les renseignements dont ils disposent afin d'alimenter les listes de sanctions cyber; demande une coordination accrue avec l'OTAN dans ce domaine au moyen de la participation à des exercices de cybersécurité et à des formations conjointes, telles que les exercices parallèles et coordonnés (PACE);

37. est d'avis que l'Union et l'OTAN devraient se coordonner dans les domaines où des acteurs hostiles menacent les intérêts euro-atlantiques en matière de sécurité; s'inquiète de l'attitude systématiquement agressive dont font preuve notamment la Chine, la Russie et la Corée du Nord dans le cyberespace, y compris par de nombreuses cyberattaques contre des institutions publiques et des entreprises privées; estime que la coopération entre l'Union et l'OTAN devrait se concentrer sur les problèmes concernant les domaines du cyber, des menaces hybrides, des technologies émergentes et disruptives, de l'espace, du contrôle des armements et de la non-prolifération; appelle de ses vœux une coopération entre l'Union et l'OTAN garantissant des réseaux à haut débit résilients, abordables et sécurisés conformes aux normes de sécurité européennes et nationales et à même de sécuriser des réseaux d'information nationaux et internationaux capables de chiffrer les données et les communications sensibles;

38. se félicite de l'accord conclu entre la CERT-UE et la capacité de réaction aux incidents informatiques (NCIRC) de l'OTAN afin de garantir la capacité à réagir aux menaces en temps réel par une amélioration de la prévention et de la détection des incidents informatiques ainsi que de la réaction à ceux-ci, à la fois au sein de l'Union et au sein de l'OTAN; souligne également qu'il importe d'accroître les capacités de formation en matière de cyberdéfense appliquée aux TIC et aux systèmes cyber, en coopération avec le Centre coopératif d'excellence pour la cyberdéfense de l'OTAN et l'École des systèmes d'information et de communication de l'OTAN;

39. demande que l'Union et l'OTAN coopèrent de manière encore plus étroite, notamment en ce qui concerne les exigences d'interopérabilité en matière de cyberdéfense, en recherchant d'éventuelles complémentarités et un renforcement mutuellement avantageux des capacités, en poursuivant l'affiliation des structures pertinentes de la PSDC avec le Federated Mission Networking de l'OTAN, en évitant les doubles emplois et en reconnaissant leurs responsabilités respectives; invite à la consolidation de la CSP de l'Union ainsi que de la défense intelligente, de l'initiative d'interconnexion des forces et de l'engagement en matière d'investissements de défense de l'OTAN, et à la promotion de la mise en commun et du partage de sorte à créer de meilleures synergies et à réaliser des gains d'efficacité dans la relation entre fournisseurs et utilisateurs finals; se félicite des progrès réalisés dans la coopération entre l'Union et l'OTAN dans le domaine de la cyberdéfense, notamment en ce qui concerne le partage de concepts et de doctrines, la participation conjointe à des exercices de cybersécurité et les séances d'information mutuelle, en particulier sur la dimension cyber de la gestion de crise; préconise la création d'un centre commun UE-OTAN d'information sur les cybermenaces ainsi que d'un groupe de travail commun sur la cybersécurité;

40. demande une coordination plus étroite en matière de cyberdéfense entre les États membres, les institutions de l'Union, les alliés de l'OTAN, les Nations unies et

l'Organisation pour la sécurité et la coopération en Europe (OSCE); encourage, à cet égard, la poursuite de la promotion des mesures de confiance de l'OSCE concernant le cyberespace et souligne la nécessité d'élaborer des outils de coopération internationale efficaces à l'appui du renforcement des cybercapacités des partenaires, ainsi que de mettre en place et de promouvoir des mesures de confiance et une coopération inclusive avec la société civile et les parties prenantes; se félicite de l'importance accordée à un cyberespace mondial, ouvert, libre, stable et sûr par la stratégie de l'Union pour la coopération dans la région indo-pacifique du 19 avril 2021; appelle de ses vœux le développement actif de liens plus étroits avec les démocraties de la région indo-pacifique partageant les mêmes valeurs, telles que les États-Unis, la Corée du Sud, le Japon, l'Inde, l'Australie et Taïwan, afin de partager des connaissances et des expériences ainsi que des informations permettant de lutter contre les cybermenaces; souligne également l'importance de coopérer avec d'autres pays, en particulier dans le voisinage immédiat de l'Union, pour les aider à renforcer leur capacité de défense contre les cybermenaces; félicite la Commission pour son soutien à des programmes de cybersécurité dans les Balkans occidentaux et les pays partenaires d'Europe orientale; souligne la nécessité urgente de respecter le droit international, y compris la charte des Nations unies dans son intégralité, et d'adhérer au cadre normatif international largement reconnu pour un comportement responsable des États, ainsi que de contribuer à la discussion en cours sur les modalités d'application du droit international dans le cyberespace dans le cadre des Nations unies;

41. souligne qu'il importe de nouer un partenariat solide dans le domaine informatique avec le Royaume-Uni, qui est à la pointe en matière d'arsenal de cyberdéfense; invite la Commission à étudier la possibilité de relancer un processus visant à établir à l'avenir un cadre formel et structuré de coopération dans ce domaine;

42. souligne la nécessité de garantir la paix et la stabilité dans le cyberespace; invite tous les États membres ainsi que l'Union à jouer un rôle moteur lors des discussions et initiatives menées sous les auspices des Nations unies, notamment en proposant un plan d'action, à adopter une approche volontariste pour l'élaboration à l'échelle internationale d'un cadre réglementaire commun et à contribuer à renforcer la responsabilité, le respect des normes émergentes et la prévention d'une utilisation malveillante des technologies numériques, ainsi qu'à promouvoir un comportement responsable des États dans le cyberespace, en s'appuyant sur les rapports de consensus du groupe d'experts gouvernementaux des Nations unies, tels qu'approuvés par l'Assemblée générale des Nations unies; salue les recommandations du rapport final du groupe de travail ouvert, notamment celles concernant l'élaboration d'un plan d'action; exhorte les Nations unies à encourager le dialogue entre les États, les chercheurs, les universitaires, les organisations de la société civile, les acteurs du secteur humanitaire et le secteur privé, de façon à assurer l'inclusivité des processus d'élaboration de nouvelles normes internationales; demande l'intensification de l'ensemble des efforts multilatéraux actuels afin que les cadres juridiques et réglementaires ne soient pas dépassés par les évolutions technologiques et les nouvelles méthodes de guerre; appelle de ses vœux la modernisation de l'architecture de contrôle des armements afin d'éviter l'émergence d'une zone grise numérique; demande que les missions de maintien de la paix des Nations unies soient renforcées par des capacités de cyberdéfense, conformément à la mise en œuvre effective de leurs mandats;

43. rappelle sa position en ce qui concerne l'interdiction de la mise au point, de la production et de l'utilisation des armes entièrement autonomes permettant d'effectuer

des frappes sans intervention humaine notable; invite le HR/VP, les États membres et le Conseil européen à adopter une position commune sur les systèmes d'armes autonomes qui garantisse un véritable contrôle humain des fonctions critiques des systèmes d'armement; exige l'ouverture de négociations internationales sur la mise en place d'un instrument juridiquement contraignant qui interdirait les armes entièrement autonomes;

44. souligne qu'il importe de coopérer avec les parlements nationaux afin d'échanger les bonnes pratiques dans le domaine de la cyberdéfense;

°

° °

45. charge son Président de transmettre la présente résolution au Conseil européen, au Conseil, à la Commission, au vice-président de la Commission/haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, aux agences de l'Union actives dans les domaines de la défense et de la cybersécurité et au secrétaire général de l'OTAN, ainsi qu'aux gouvernements et aux parlements des États membres.