Mercredi 13 juin 2018

P8_TA(2018)0258

Cyberdéfense

Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2018/2004(INI))

(2020/C 28/06)

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 du 20 décembre 2013, du 26 juin 2015, du 15 décembre 2016, du 9 mars 2017, du 22 juin 2017, du 20 novembre 2017 et du 15 décembre 2017,

— vu la communication de la Commission du 7 juin 2017 intitulée «Document de réflexion sur l'avenir de la défense européenne» (COM(2017)0315),

— vu la communication de la Commission du 7 juin 2017 intitulée «Lancement du Fonds européen de la défense» (COM(2017)0295),

— vu la communication de la Commission du 30 novembre 2016 sur le plan d'action européen de la défense (COM(2016)0950),

— vu la communication conjointe de la Commission et de la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité du 7 février 2013 au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» (JOIN(2013)0001),

— vu le document de travail des services de la Commission du 13 septembre 2017 intitulé «Assessment of the EU 2013 Cybersecurity Strategy» (Évaluation de la stratégie de cybersécurité de l'Union européenne en 2013) (SWD(2017)0295),

— vu le cadre stratégique de cyberdéfense de l'Union européenne du 18 novembre 2014,

— vu les conclusions du Conseil du 10 février 2015 sur la cyberdiplomatie,

— 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 de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 13 septembre 2017 au Parlement européen et au Conseil intitulée «Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide» (JOIN(2017)0450),

Mercredi 13 juin 2018

— vu le «Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations [1]» (manuel de Tallinn sur le droit international applicable aux cyberopérations),

— 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 [2],

— vu les travaux de la Commission mondiale sur la stabilité du cyberespace,

— vu la communication de la Commission du 28 avril 2015 intitulée «Le programme européen en matière de sécurité» (COM(2015)0185),

— vu la communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 6 avril 2016 au Parlement européen et au Conseil intitulée: «Cadre commun en matière de lutte contre les menaces hybrides: une réponse de l'Union européenne» (JOIN(2016)0018),

— vu sa résolution du 3 octobre 2017 sur la lutte contre la cybercriminalité [3],

— vu la déclaration conjointe du 8 juillet 2016 des présidents du Conseil européen et de la Commission ainsi que du secrétaire général de l'Organisation du traité de l'Atlantique Nord (OTAN), les ensembles communs de propositions pour la mise en œuvre de la déclaration commune approuvés par les ministres de l'OTAN et de l'Union européenne le 6 décembre 2016 et le 5 décembre 2017, ainsi que les rapports sur l'état d'avancement de la mise en œuvre de ceux-ci adoptés le 14 juin et le 5 décembre 2017,

— vu sa résolution du 22 novembre 2012 sur la sécurité et la défense du cyberespace [4],

— vu sa résolution du 22 novembre 2016 sur l'Union européenne de la défense [5],

— vu la proposition de la Commission du 13 septembre 2017 d'un règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) (COM(2017)0477),

— vu sa résolution du 13 décembre 2017 sur le rapport annuel sur la mise en œuvre de la politique extérieure et de sécurité commune (PESC) [6],

— vu sa résolution du 13 décembre 2017 sur le rapport annuel sur la mise en œuvre de la politique de sécurité et de défense commune (PSDC) [7],

— vu l'article 52 de son règlement intérieur,

— vu le rapport de la commission des affaires étrangères (A8-0189/2018),

A. considérant que les défis, les menaces et les attaques informatiques et hybrides constituent une menace importante pour la sécurité, la défense, la stabilité et la compétitivité de l'Union, de ses État membres et de ses citoyens; que la cyberdéfense intègre clairement des dimensions militaires et civiles;

---

[1] Cambridge University Press, février 2017, ISBN 9 781 316 822 524, https://doi.org/10.1017/9781316822524.
[2] JO L 194 du 19.7.2016, p. 1.
[3] Textes adoptés de cette date, P8_TA(2017)0366.
[4] JO C 419 du 16.12.2015, p. 145.
[5] Textes adoptés de cette date, P8_TA(2016)0435.
[6] Textes adoptés de cette date, P8_TA(2017)0493.
[7] Textes adoptés de cette date, P8_TA(2017)0492.

B. considérant que l'Union et les États membres sont confrontés à une menace sans précédent prenant la forme de cyberattaques politiques d'État ainsi que de cybercriminalité et de terrorisme;

C. considérant que le cyberespace est largement reconnu par les forces armées comme le cinquième domaine opérationnel, favorisant ainsi le développement des capacités de cyberdéfense; que des débats ont lieu sur la question de savoir si le cyberespace constitue le cinquième domaine de la guerre;

D. considérant que la clause de défense mutuelle de l'article 42, paragraphe 7, du traité sur l'Union européenne prévoit que les États membres se doivent mutuellement aide et assistance par tous les moyens en leur pouvoir en cas d'agression armée sur le territoire d'un État membre; que cela n'affecte pas le caractère spécifique de la politique de sécurité et de défense de certains États membres; que la clause de solidarité de l'article 222 du traité sur le fonctionnement de l'Union européenne complète la clause de défense mutuelle en prévoyant que les États membres de l'Union sont tenus d'agir conjointement lorsque l'un d'eux est victime d'une attaque terroriste ou d'une catastrophe naturelle ou d'origine humaine; que la clause de solidarité implique le recours à des structures civiles et militaires;

E. considérant que, si la cyberdéfense demeure une compétence clé des États membres, l'Union européenne a un rôle vital à jouer pour offrir une plateforme de coopération européenne et pour veiller à ce que ces nouveaux efforts soient étroitement coordonnés au niveau international et dans le cadre de l'architecture de sécurité transatlantique dès le début, afin d'éviter les faiblesses et l'inefficacité qui caractérisent nombre de projets de défense classiques; que nous devons aller au-delà du renforcement de notre coopération et de notre coordination; que nous devons garantir une prévention efficace en renforçant la capacité de détection, de défense et de dissuasion de l'Union; qu'il est indispensable de disposer d'une cyberdéfense et d'une cyberdissuasion crédibles afin de garantir une cybersécurité effective dans l'Union, tout en veillant à ce que les États les moins préparés ne deviennent pas la cible facile de cyberattaques, et qu'une capacité consistante de cyberdéfense devrait être entièrement intégrée à la PSDC ainsi qu'à l'union de la défense en cours d'érection; considérant que nous nous trouvons dans une situation de pénurie récurrente de spécialistes de la cyberdéfense hautement qualifiés; qu'une étroite coordination en matière de protection des forces armées contre les cyberattaques est nécessaire à la mise en place d'une politique de sécurité et de défense commune (PSDC) efficace;

F. considérant que les États membres de l'Union font souvent l'objet de cyberattaques menées par des acteurs étatiques et non étatiques hostiles et dangereux à l'encontre de cibles civiles et militaires; considérant que la vulnérabilité actuelle s'explique principalement par la fragmentation des stratégies et des capacités de défense au niveau européen, ce qui ouvre une brèche et permet aux agences de renseignement étrangères d'exploiter régulièrement les failles de sécurité des systèmes et réseaux informatiques essentiels à la sécurité du continent; considérant que les gouvernements des États membres, très souvent, n'ont pas informé les acteurs concernés assez rapidement, ce qui a empêché ceux-ci de remédier à temps aux failles de leurs produits et services; considérant que ces attaques requièrent d'urgence un renforcement et un étoffement des capacités offensives et défensives de l'Union au niveau civil et militaire afin d'éviter toute répercussion transfrontalière économique ou sociétale des incidents de cybersécurité;

G. considérant que les frontières entre l'ingérence civile et militaire deviennent floues dans le cyberespace;

H. considérant qu'un grand nombre de cyberincidents sont imputables à un défaut de résistance et de robustesse des infrastructures de réseau privées et publiques, à des bases de données mal protégées ou sécurisées et à d'autres failles dans les infrastructures d'information critiques; que seuls quelques États membres endossent la responsabilité de la protection de leurs réseaux et systèmes d'information, ainsi que des données associées, comme partie intégrante de leurs obligations respectives de diligence, ce qui explique le manque général d'investissement dans la formation et les technologies de pointe en matière de sécurité, mais aussi dans l'élaboration de lignes directrices appropriées;

I. considérant que les droits à la vie privée et à la protection des données sont définis dans la charte des droits fondamentaux de l'Union européenne et à l'article 16 du traité sur le fonctionnement de l'Union européenne et qu'ils sont régis par le règlement général de l'Union sur la protection des données, qui entrera en vigueur le 25 mai 2018;

J. considérant qu'une cyberpolitique active et efficace permet de dissuader les ennemis et de perturber leurs capacités, en anticipant et en diminuant leur capacité d'attaque;

K. considérant que plusieurs groupes et organisations terroristes utilisent le cyberespace comme un outil peu coûteux de recrutement, de radicalisation et de diffusion de la propagande terroriste; que les groupes terroristes, les acteurs non étatiques et les réseaux criminels transnationaux ont recours à des cyberopérations pour collecter des fonds de façon anonyme, recueillir des renseignements et développer des cyberarmes pour mener des campagnes de cyberterreur, pour perturber, endommager ou détruire des infrastructures critiques, attaquer des systèmes financiers et poursuivre d'autres activités illégales ayant des implications pour la sécurité des citoyens européens;

L. considérant que la cyberdissuasion et la défense des forces armées ainsi que des infrastructures critiques européennes se sont imposées comme des questions essentielles dans les débats sur la modernisation de la défense, les efforts de défense communs de l'Europe, l'évolution future des forces armées et de leurs opérations et l'autonomie stratégique de l'Union;

M. considérant que plusieurs États membres ont investi massivement dans la création de commandements de cyberdéfense dotés de personnel suffisant pour relever ces nouveaux défis et améliorer leur cyberrésilience, mais qu'il reste bien davantage à faire, car il est de plus en plus difficile de contrer les cyberattaques au niveau des États membres; que les cybercommandements des États membres sont dotés de mandats offensifs et défensifs variables selon le pays; que les autres structures de cyberdéfense restent éparpillées et varient largement d'un État membre à l'autre; que la cyberdéfense et la cyberdissuasion sont des activités qu'il est préférable d'aborder sous l'angle de la coopération à l'échelle européenne et en coordination avec nos partenaires et alliés, car son domaine opérationnel ne connaît pas de frontières nationales ou organisationnelles; que la cybersécurité militaire est étroitement liée à la cybersécurité civile et qu'il convient par conséquent de créer davantage de synergies entre les professionnels civils et militaires du domaine; que les entreprises privées ont acquis une spécialisation solide dans ce domaine, ce qui pose des questions fondamentales en matière de gouvernance et de sécurité sur la capacité des États à défendre leurs citoyens;

N. considérant, compte tenu de l'absence d'une réaction suffisamment rapide face à l'évolution permanente de la sécurité cybernétique, qu'il est urgent de renforcer les capacités de cyberdéfense de l'Union et qu'une rapidité de réaction et un niveau de préparation adaptés sont des éléments clés qui permettront de garantir la sécurité dans ce domaine;

O. considérant que la coopération structurée permanente (CSP) et le Fonds européen de la défense (FED) constituent de nouvelles initiatives dotées de la portée nécessaire pour favoriser un écosystème à même d'offrir des opportunités aux PME et aux jeunes entreprises et pour faciliter les projets de coopération dans le domaine de la cyberdéfense, qui contribueront toutes deux à façonner le cadre réglementaire et institutionnel;

P. considérant que les États membres participant à la CSP se sont engagés à veiller à ce que les efforts de coopération en matière de cyberdéfense, notamment en matière d'échange d'informations, de formation et de soutien opérationnel, s'intensifient;

Q. considérant que parmi les dix-sept projets sélectionnés pour la CSP, deux concernent la cyberdéfense;

R. considérant que le FED doit soutenir la compétitivité mondiale de l'industrie européenne de la défense et l'innovation en son sein en investissant dans les technologies numériques et les cybertechnologies et faciliter la mise en place de solutions intelligentes en offrant aux PME et aux jeunes entreprises la possibilité de participer à cet effort collectif;

S. considérant que l'Agence européenne de la défense (AED) a lancé un certain nombre de projets afin de répondre aux besoins des États membres en matière de développement des capacités de cyberdéfense, y compris des projets d'enseignement et de formation, notamment la plateforme de coordination de la formation et des exercices en matière de cyberdéfense, l'harmonisation de la demande pour le soutien à la formation et aux exercices en matière de cyberdéfense par le secteur privé et le projet de plateformes informatiques de simulation en matière de cybersécurité *(cyber ranges)*;

T. considérant qu'il existe d'autres projets européens en cours dans les domaines de la sensibilisation aux cyberincidents, de la détection de programmes malveillants et du partage d'informations (plateforme d'échange d'informations sur les logiciels malveillants [MISP]), système multi-agents de détection de menaces persistantes avancées);

U. considérant que les besoins de renforcement des capacités et de formation dans le domaine de la cyberdéfense sont considérables et en hausse, et que la façon la plus efficace de les satisfaire est de coopérer à l'échelle de l'Union et de l'OTAN;

V. considérant que les missions et les opérations de la PSDC, comme toutes les initiatives modernes, dépendent en grande partie de systèmes informatiques opérationnels; que les menaces informatiques dirigées contre les missions et les opérations de la PSDC peuvent exister à différents niveaux, allant de la couche tactique (missions et opérations de la PSDC) et de la couche opérationnelle (réseaux européens) à, plus largement, l'infrastructure informatique mondiale;

W. considérant que les systèmes de commandement et de contrôle, les échanges d'informations et l'organisation logistique reposent sur des infrastructures informatiques plus ou moins strictement sécurisées, en particulier aux niveaux tactique et opérationnel; que ces systèmes constituent une cible de prédilection pour les agents malveillants cherchant à compromettre les missions; considérant que les cyberattaques peuvent avoir des répercussions considérables sur les infrastructures de l'Union; considérant en particulier que toute cyberattaque contre des infrastructures énergétiques européennes entraînerait de graves répercussions et doit par conséquent être évitée;

X. considérant qu'il est évident que la cyberdéfense doit être dûment prise en compte à toutes les étapes de la planification des missions et opérations de PSDC, qu'elle exige un suivi constant et que des capacités adéquates doivent être disponibles afin de l'intégrer pleinement à la planification des missions et de fournir l'appui critique nécessaire;

Y. considérant que le réseau du Collège européen de sécurité et de défense (CESD) est le seul prestataire européen de formation pour les structures, les missions et les opérations de la PSDC; que, d'après les plans actuels, son rôle dans la mise en commun des capacités de formation européennes devrait progresser fortement dans le domaine de la cyberdéfense;

Z. considérant que la déclaration du sommet de l'OTAN à Varsovie en 2016 a pris acte du cyberespace comme domaine opérationnel dans lequel l'OTAN doit se défendre aussi efficacement qu'elle le fait dans les domaines aérien, terrestre et maritime;

AA. considérant que l'Union et l'OTAN ont contribué à l'amélioration des capacités de cyberdéfense des États membres par des projets de recherche à double usage coordonnés par l'AED et l'OTAN et par l'amélioration de la cyberrésilience des États membres grâce au soutien fourni par l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA);

AB. considérant qu'en 2014, l'OTAN a intégré les opérations de cybersécurité dans sa défense collective et qu'en 2016, elle a élevé le cyberespace au rang de terrain d'opération au même titre que la terre, l'air et la mer; que l'Union et l'OTAN sont des partenaires complémentaires dans le renforcement de leurs capacités de cyberrésilience et de cyberdéfense; que la cybersécurité et la cyberdéfense constituent déjà l'un des piliers les plus solides de la coopération entre les deux organisations et un domaine critique dans lequel elles ont toutes deux des capacités uniques; considérant que l'Union et l'OTAN sont convenus d'un vaste programme de coopération dans leur déclaration commune du 8 juillet 2016; que quatre des 42 propositions de coopération plus étroite concernent la cybersécurité et la cyberdéfense, auxquelles s'ajoutent d'autres propositions visant à affronter les menaces hybrides de manière plus générale; qu'elles ont été complétées par une nouvelle proposition relative à la cybersécurité et à la cyberdéfense présentée le 5 décembre 2017;

AC. considérant que le groupe d'experts gouvernementaux des Nations unies sur la sécurité de l'information a conclu son dernier cycle de délibérations; que, bien qu'il ait été dans l'incapacité de produire un rapport de consensus en 2017, les rapports de 2015 et de 2013 s'appliquent, y compris – comme ces rapports l'affirment – le droit international, et en particulier la charte des Nations unies, essentielle au maintien de la paix et de la stabilité, ainsi qu'à la promotion d'un environnement ouvert, sûr, pacifique et accessible des technologies de l'information et de la communication;

AD. considérant que le cadre récemment mis en place pour une réponse diplomatique commune de l'Union européenne face aux actes de cybermalveillance (la «boîte à outils cyberdiplomatique»), destiné à étoffer les capacités de l'Union et des États membres de sorte qu'ils puissent influer sur le comportement d'agresseurs potentiels, prévoit le recours à des mesures proportionnées dans le cadre de la PESC, notamment à des mesures restrictives;

AE. considérant que différents États – la Russie, la Chine et la Corée du Nord, entre autres, mais aussi des acteurs non étatiques (y compris des organisations criminelles) inspirés, employés ou soutenus par des États, des agences de sécurité ou des entreprises privées – ont été impliqués dans des actes de cybermalveillance à visée politique, économique ou de sécurité comprenant des attaques contre des infrastructures critiques, des activités de cyberespionnage, la surveillance de masse de citoyens de l'Union, la participation à des campagnes de désinformation, la diffusion de maliciels (Wannacry, NotPetya, etc.) ainsi que la limitation de l'accès à l'internet et du fonctionnement de systèmes informatiques; considérant que de telles activités enfreignent le droit international, les droits de l'homme et les droits fondamentaux de l'Union et mettent en péril la démocratie, la sécurité, l'ordre public et l'autonomie stratégique de l'Union, et appellent par conséquent une réponse commune de l'Union, par exemple le recours à sa boîte à outils cyberdiplomatique ou, lorsque des entreprises privées sont coupables, des sanctions telles que des amendes ou la limitation de l'accès au marché intérieur;

AF. considérant que de telles attaques à grande échelle ont été lancées à de nombreuses reprises contre des infrastructures informatiques, notamment contre l'Estonie en 2007, la Géorgie en 2008 et, actuellement, contre l'Ukraine de manière quasi quotidienne; que des capacités de cyberdéfense offensive sont également utilisées contre les États membres de l'Union et de l'OTAN à une échelle sans précédent;

AG. considérant que les technologies de cybersécurité, valables à la fois dans les domaines militaire et civil, sont des technologies à double usage qui offrent de nombreuses possibilités de développer des synergies entre leurs acteurs civils et militaires dans un certain nombre de domaines, comme par exemple le chiffrement, les outils de gestion de la sécurité et des vulnérabilités, la détection des intrusions et les systèmes de prévention;

AH. considérant qu'au cours des prochaines années, le développement des cybertechnologies aura des répercussions dans de nouveaux domaines, tels que l'intelligence artificielle, l'internet des objets, la robotique et les appareils mobiles, et que tous ces éléments pourraient également avoir des conséquences sur le plan de la sécurité pour la défense;

AI. considérant que les commandements de cyberdéfense mis en place par plusieurs États membres peuvent contribuer significativement à la protection des infrastructures civiles clés et que les connaissances liées à la cyberdéfense sont souvent tout aussi utiles dans le domaine civil;

Développement des capacités de cyberdéfense et de cyberdissuasion

1. souligne qu'une politique de cyberdéfense commune et une capacité solide de cyberdéfense devraient former un socle sur lequel bâtir l'Union européenne de la défense;

2. se félicite de l'initiative de la Commission en faveur d'un paquet «Cybersécurité» destiné à favoriser la cyber-résilience, la dissuasion et la défense de l'Union;

3. rappelle que la cyberdéfense présente des dimensions à la fois militaires et civiles et qu'il est par conséquent indispensable de mettre en place une démarche politique intégrée ainsi qu'une coopération étroite entre les parties prenantes militaires et civiles;

4. appelle de ses vœux le développement cohérent des capacités de cyberdéfense dans l'ensemble des institutions et organes de l'Union, ainsi que dans les États membres, et à l'élaboration des solutions politiques et concrètes nécessaires pour surmonter les obstacles politiques, législatifs et organisationnels restants qui s'opposent à la coopération en matière de cyberdéfense; estime essentiel de mettre en place une coopération et des échanges réguliers et renforcés entre les acteurs publics concernés aux niveaux européen et national en matière de cyberdéfense;

5. insiste fortement sur la nécessité, dans le cadre de l'Union européenne de la défense en gestation, de mettre au premier plan les capacités de cyberdéfense des États membres et de les intégrer, dans la mesure du possible, dès le début, afin de garantir une efficacité maximale; exhorte par conséquent les États membres à coopérer étroitement lors de la mise en place de leurs commandements de cyberdéfense respectifs, en s'appuyant sur une feuille de route claire, contribuant ainsi à un processus coordonné par la Commission, le Service européen pour l'action extérieure (SEAE) et l'AED afin de rationaliser davantage les structures de cyberdéfense dans les États membres, d'appliquer les mesures de court terme à disposition dans les plus brefs délais et d'encourager le partage des connaissances; est d'avis que nous devrions développer un réseau européen sécurisé pour les informations et les infrastructures critiques; prend acte du fait que de solides capacités d'attribution sont essentielles à une cyberdéfense et à une cyberdissuasion efficaces et que la mise en place d'une prévention efficace exigerait l'acquisition de compétences technologiques spécialisées bien plus approfondies; exhorte les États membres à accroître les ressources financières et humaines consacrées au sujet, en particulier au niveau des experts en sciences criminalistiques, afin d'améliorer l'attribution des cyberattaques; souligne que cette coopération devrait également être mise en œuvre grâce au renforcement de l'ENISA;

6. est conscient que, pour de nombreux États membres, le fait de posséder leurs propres capacités de cyberdéfense est crucial pour leur stratégie de sécurité et constitue une part essentielle de leur souveraineté nationale; souligne cependant que, compte tenu de l'absence de frontières dans le cyberespace, l'échelle et les connaissances requises pour une action réellement complète et efficace garantissant l'objectif d'autonomie stratégique de l'Union dans le cyberespace sont inaccessibles pour un État membre opérant seul; qu'une action intensifiée et coordonnée de la part de tous les États membres au niveau de l'Union est par conséquent indispensable; relève, dans ce contexte, que l'Union et ses États membres se trouvent confrontés à des contraintes temporelles quant à la mise en place de telles forces et doivent agir sans délai; fait observer que grâce aux initiatives européennes telles que le marché unique numérique, l'Union est bien placée pour jouer un rôle de premier plan dans l'élaboration de stratégies européennes en matière de cyberdéfense; rappelle que le développement de la cyberdéfense au niveau européen doit favoriser la capacité de l'Union à se protéger; se félicite, à cet égard, du mandat permanent et du renforcement proposés du rôle de l'ENISA;

7. demande instamment aux États membres, dans ce contexte, d'utiliser au mieux le cadre fourni par la CSP et le FED pour proposer des projets de coopération;

8. prend note du travail accompli par l'Union et ses États membres dans le domaine de la cyberdéfense; prend acte, en particulier, des projets de l'AED relatifs aux plateformes informatiques de simulation en matière de cybersécurité (*cyber ranges*), du «Cyber Defence Strategic Research Agenda» (programme de recherche stratégique dans le domaine de la cyberdéfense) et de la mise au point de dispositifs de sensibilisation aux cyberincidents à destination des états-majors;

9. accueille avec satisfaction les cyberprojets qui seront lancés dans le cadre de la CSP, à savoir une plateforme d'échange d'informations sur les cyberincidents, la création d'équipes d'intervention rapide en matière de cybersécurité et la mise en place d'une assistance mutuelle en matière de cybersécurité; souligne que ces deux projets mettent l'accent sur une cyberpolitique défensive qui s'appuie sur le partage d'informations concernant les cybermenaces grâce à une plateforme des États membres mise en réseau et sur la création d'équipes d'intervention rapide en cas d'incident informatique, qui permettront aux États membres de s'entraider afin de garantir un niveau accru de cyberrésilience et de détecter, de reconnaître et d'atténuer collectivement les cybermenaces; invite la Commission et les États membres à s'appuyer sur les projets de la CSP relatifs à la mise en place d'équipes nationales d'intervention rapide en cas d'incident informatique et à l'assistance mutuelle dans le domaine de la cybersécurité, et à créer une équipe européenne d'intervention rapide en matière de cybersécurité chargée de coordonner, de détecter et de contrer les cybermenaces collectives en soutien à l'action des États membres participants;

10. observe que la capacité de l'Union à développer des projets de cyberdéfense repose sur la maîtrise des technologies, des équipements, des services et des données et de leur traitement, et nécessite de s'appuyer sur une base d'acteurs industriels de confiance;

11. rappelle qu'un des objectifs des efforts engagés afin d'améliorer l'homogénéité des systèmes de commandement est de s'assurer de disposer de moyens de commandement interopérables avec ceux des pays non membres de l'Alliance atlantique ainsi qu'avec ceux des partenaires de circonstance, et de garantir la fluidité des échanges d'informations afin d'accélérer la boucle décisionnelle et de conserver la maîtrise de l'information dans un contexte de risque cyber;

12. recommande de trouver des moyens de compléter les projets de défense intelligente de l'OTAN (la mise au point d'une capacité de cyberdéfense multinationale, d'une plateforme d'échange d'informations sur les logiciels malveillants, ou encore d'une formation et d'un entraînement multinationaux à la cyberdéfense, par exemple);

13. est conscient des mutations à l'œuvre dans des domaines tels que la nanotechnologie, l'intelligence artificielle, les mégadonnées, les déchets d'équipements électriques et électroniques et la robotique de pointe; exhorte les États membres et l'Union à prêter une attention particulière à l'exploitation que pourraient en faire des acteurs étatiques hostiles et des groupes criminels organisés; demande que davantage de formations soient dispensées et que les capacités soient étoffées, de sorte à se prémunir contre l'apparition de systèmes criminels perfectionnés, comme les fraudes à l'identité complexes et la contrefaçon de marchandises;

14. souligne la nécessité d'instaurer une terminologie plus claire concernant la sécurité dans le cyberespace, et de mettre en place une approche globale et intégrée ainsi que des efforts communs pour contrer les cybermenaces et les menaces hybrides, afin de détecter et de supprimer les refuges d'extrémistes et de criminels en ligne, en renforçant et en intensifiant le partage d'informations entre l'Union et ses agences telles qu'Europol, Eurojust, l'EAD et l'ENISA;

15. souligne le rôle de plus en plus important de l'intelligence artificielle en matière de cybercriminalité et de défense; demande instamment à l'Union et aux États membres d'accorder une attention particulière à ce domaine, tant au stade de la recherche que lors du développement concret de leurs capacités de cyberdéfense;

16. insiste fortement sur la nécessité de prendre des mesures supplémentaires pour réduire la vulnérabilité informatique éventuelle des véhicules aériens sans pilote, armés ou non, qui sont en phase de déploiement;

Cyberdéfense des missions et opérations de la PSDC

17. souligne que la cyberdéfense devrait être considérée comme une tâche opérationnelle dans le cadre des missions et des opérations de la PSDC et qu'elle devrait être incluse dans tous les processus de planification de la PSDC, afin de garantir que la cybersécurité est constamment prise en compte tout au long du processus de planification, ce qui réduit les carences en matière de vulnérabilité informatique;

18. reconnaît que la planification d'une mission ou d'une opération réussie de PSDC demande un savoir-faire important en matière de cyberdéfense ainsi que des réseaux et une infrastructure informatiques sécurisés, tant au siège opérationnel qu'au cours de la mission même, de sorte à évaluer les menaces de manière précise et à fournir une protection adaptée sur le terrain; invite le SEAE et les États membres qui mettent des états-majors à disposition pour des opérations de PSDC à renforcer le savoir-faire en matière de cyberdéfense qu'ils apportent dans le cadre des missions et des opérations de l'Union; relève la limite à laquelle est confrontée toute mission de PSDC dans la préparation face aux cyberattaques;

19. souligne qu'il est nécessaire de joindre une évaluation approfondie du paysage des cybermenaces à toutes les planifications de mission et d'opération de la PSDC; relève que la classification des menaces établie par l'ENISA fournit un modèle adapté pour une telle évaluation; recommande la création d'une capacité d'évaluation de la cyber-résilience pour les états-majors de la PSDC;

20. souligne, en particulier, qu'il importe de restreindre au minimum nécessaire l'empreinte numérique et la surface d'attaque des missions et opérations de la PSDC; prie instamment les planificateurs de tenir compte de ce constat dès le début du processus de planification;

21. prend note de l'analyse des besoins de formation de l'AED, qui a mis en évidence des lacunes importantes en matière de compétences et de savoir-faire dans le domaine de la cyberdéfense parmi les décideurs, pas uniquement au sein des États membres, et se félicite des initiatives de l'AED relatives à des cours à destination des hauts responsables dans les États membres venant en soutien à la planification des missions et des opérations de la PSDC;

Instruction et formation dans le domaine de la cyberdéfense

22. relève que la rationalisation du paysage européen de l'éducation et de la formation en matière de cyberdéfense atténuerait sensiblement les menaces, et invite l'Union et les États membres à renforcer leur coopération en matière d'éducation, de formation et d'exercices;

23. appuie vivement le programme Erasmus militaire et les autres initiatives communes en matière de formation et d'échange, qui visent à améliorer l'interopérabilité des forces armées des États membres et le développement d'une culture stratégique commune par une intensification des échanges de jeunes membres du personnel militaire, en gardant à l'esprit qu'il importe d'instaurer une telle interopérabilité entre tous les États membres et alliés de l'OTAN; estime toutefois que les échanges en matière de formation et d'éducation dans le domaine de la cyberdéfense devraient aller au-delà de cette initiative et inclure des militaires de tous âges et de tous grades ainsi que des étudiants de tous les centres universitaires d'études sur la cybersécurité;

24. souligne que davantage de spécialistes doivent être formés dans le domaine de la cyberdéfense; invite les États membres à faciliter la coopération entre les établissements universitaires civils et les académies militaires afin de pallier ce manque, l'objectif étant de créer davantage de possibilités dans le domaine de l'éducation et de la formation à la cyberdéfense et à consacrer davantage de ressources à une formation opérationnelle spécialisée en la matière, y compris à propos de l'intelligence artificielle; demande aux académies militaires d'intégrer l'éducation à la cyberdéfense dans leurs programmes, afin d'aider à l'élargissement des équipes de spécialistes en cyberespace disponibles pour les besoins des missions de la PSDC;

25. invite tous les États membres à informer, sensibiliser et conseiller d'une manière adéquate et proactive les entreprises, les écoles et les citoyens au sujet de la cybersécurité et des principales menaces numériques; salue à cet égard les cyberguides qui constituent un outil destiné à orienter les citoyens et les organisations vers une meilleure stratégie de cybersécurité, à renforcer les connaissances en la matière, et à améliorer la cyber-résilience générale;

26. relève que, compte tenu de la nécessité de disposer de personnel plus spécialisé, les États membres ne devraient pas se concentrer uniquement sur le recrutement de personnel compétent des forces armées, mais aussi sur la fidélisation des spécialistes recherchés;

27. salue la mise en œuvre, par 11 États membres (la Belgique, l'Allemagne, l'Estonie, l'Irlande, la Grèce, la Lettonie, les Pays-Bas, l'Autriche, le Portugal, la Finlande et la Suède) parties au projet «Cyber Ranges Federation», du premier de quatre projets de cyberdéfense lancés dans le cadre du programme de mise en commun et de partage de l'AED; exhorte les autres États membres à se joindre à cette initiative; invite les États membres à promouvoir une plus grande accessibilité mutuelle à la formation en ligne en matière de cyberdéfense et aux *cyber ranges*; relève à cet égard que le rôle de l'ENISA ainsi que son savoir-faire devraient également être pris en compte;

28. estime que de telles initiatives contribuent à améliorer la qualité de la formation dans le domaine de la cyberdéfense à l'échelon de l'Union, en particulier par la création de vastes plateformes techniques et la mise en place d'une communauté d'experts européens; estime que les forces armées européennes peuvent renforcer leur attrait en dispensant des formations complètes en matière de cyberdéfense pour attirer et fidéliser les spécialistes du cyberespace; souligne la nécessité de mettre en évidence les défaillances des systèmes informatiques tant des États membres que des institutions de l'Union; constate que les erreurs humaines constituent l'une des défaillances des systèmes de sécurité cybernétique les plus souvent recensées et, dès lors, appelle à organiser des formations régulières du personnel des institutions de l'Union tant militaire que civil;

29. invite l'AED à lancer la plateforme de coordination de la formation et des exercices en matière de cyberdéfense (CD TEXP) afin qu'elle apporte son appui au projet «Cyber Ranges Federation» dès que possible, en mettant l'accent sur le renforcement de la coopération en matière d'exigences harmonisées, en encourageant la recherche sur la cyberdéfense et les innovations technologiques, et en aidant collectivement les pays tiers à renforcer leurs capacités afin de créer de la résilience en matière de cyberdéfense; invite la Commission et les États membres à compléter ces initiatives par la création d'un centre d'excellence européen pour la formation en matière de cyberdéfense, qui offrira une formation spécialisée aux recrues les plus prometteuses, en soutien à la cyberformation des États membres participants;

30. salue la mise en place, au sein du CESD, de la plateforme d'éducation, de formation, d'exercices et d'évaluation en matière de cyberdéfense, afin d'élargir les possibilités de formation et d'enseignement dans les États membres;

31. encourage l'intensification des échanges dans le domaine de la sensibilisation aux cyberincidents grâce à des exercices de simulation informatique et à la coordination des efforts respectifs en matière de développement des capacités afin d'atteindre une plus grande interopérabilité, de mieux intervenir en cas de futures attaques et de mieux les prévenir; demande que de tels projets soient menés avec les alliés de l'OTAN, les forces armées des États membres de l'Union européenne et d'autres partenaires ayant une vaste expérience de la lutte contre les cyberattaques afin de développer l'état de préparation opérationnelle, des procédures communes et des normes pour faire face de manière globale à différentes cybermenaces; se félicite à cet égard de la participation de l'Union à des cyberexercices comme les exercices de cyberdéfense offensive et défensive;

32. rappelle qu'il importe d'adopter une cyberhygiène irréprochable pour avoir un cyberespace résistant; invite toutes les parties prenantes publiques et privées à organiser des formations régulières sur la cyberhygiène pour tous les membres de leur personnel;

33. recommande d'intensifier les échanges de savoir-faire et d'expérience entre les forces armées, les forces de police et les autres organes étatiques des États membres activement impliqués dans la lutte contre les cybermenaces;

Coopération entre l'Union européenne et l'OTAN dans le domaine de la cyberdéfense

34. rappelle qu'au vu de leurs valeurs communes et de leurs intérêts stratégiques partagés, l'Union et l'OTAN assument une responsabilité particulière et disposent des capacités pour répondre d'une manière plus efficace à la multiplication des défis dans les domaines de la cybersécurité et de la cyberdéfense en coopérant étroitement à la recherche d'éventuelles complémentarités, à la prévention des doubles emplois et au respect de leurs compétences respectives;

35. invite le Conseil à envisager, en collaboration avec d'autres institutions et structures européennes compétentes, des moyens de fournir, dans les meilleurs délais, un soutien à l'échelle de l'Union à l'intégration du cyberdomaine dans les doctrines militaires des États membres, d'une manière harmonisée et en étroite coopération avec l'OTAN;

36. demande la mise en œuvre des mesures qui ont déjà été arrêtées; demande que de nouvelles initiatives soient définies afin d'approfondir la coopération entre l'Union européenne et l'OTAN, en tenant également compte des possibilités de coopération au sein du Centre d'excellence pour la cyberdéfense en coopération et de l'école des systèmes d'information et de communication de l'OTAN, qui ont pour objectif d'accroître les capacités de formation à la cyberdéfense dans les systèmes informatiques et cybersystèmes, tant en ce qui concerne les logiciels que le matériel; relève que cela pourrait inclure un dialogue avec l'OTAN sur la possibilité pour l'Union de rejoindre le Centre d'excellence afin d'améliorer la complémentarité et la collaboration; salue la création récente du centre d'excellence européen pour la lutte contre les menaces hybrides; exhorte toutes les institutions et tous les alliés concernés à se réunir régulièrement pour discuter de leurs activités afin d'éviter les chevauchements et d'encourager une approche coordonnée en matière de cyberdéfense; estime qu'il est essentiel d'encourager, sur la base de la confiance mutuelle, les échanges de renseignements sur les cybermenaces entre les États membres de l'Union et avec l'OTAN;

37. est convaincu qu'il est important et utile de renforcer la coopération entre l'Union européenne et l'OTAN dans le domaine de la cyberdéfense en tant que moyen de prévenir, de détecter et de dissuader les cyberattaques; invite, dès lors, les deux organisations à renforcer leur coopération et leur coordination opérationnelles, ainsi qu'à intensifier leurs efforts conjoints de renforcement des capacités, en particulier sous la forme d'exercices communs et de formation commune du personnel de cyberdéfense civil et militaire et par la participation des États membres aux projets de défense intelligente de l'OTAN; estime qu'il est essentiel que l'Union et l'OTAN intensifient le partage de renseignements afin de permettre l'attribution formelle des cyberattaques et, par conséquent, d'imposer des sanctions restrictives aux responsables; exhorte les deux organisations à coopérer plus étroitement également sur les aspects informatiques de la gestion des crises;

38. salue les échanges de concepts qui visent à intégrer les exigences et les normes en matière de cyberdéfense dans la planification et la conduite des missions et des opérations en vue de favoriser l'interopérabilité, et souhaite que ces échanges donnent lieu à une coopération plus opérationnelle destinée à assurer l'aspect de cyberdéfense des missions respectives et la synchronisation des approches opérationnelles;

39. accueille avec satisfaction l'accord mis en place entre le centre de réponse aux incidents de sécurité informatique de l'Union européenne (CERT-UE) et la capacité OTAN de réaction aux incidents informatiques (NCIRC), qui a pour but de faciliter l'échange d'informations, le soutien logistique, les évaluations conjointes de la menace, le recrutement de personnel et le partage des bonnes pratiques, l'objectif étant toujours d'assurer la capacité de réponse aux menaces en temps réel; souligne qu'il importe d'encourager l'échange d'informations entre le CERT-UE et le NCIRC et d'accroître le degré de confiance; estime que des informations détenues par le CERT-UE pourraient probablement être utiles à la recherche en matière de cyberdéfense et à l'OTAN, et qu'elles devraient donc être partagées sous réserve du strict respect de la législation européenne en matière de protection des données;

40. salue la coopération entre les deux organisations dans le domaine des exercices de cyberdéfense; constate la participation de représentants de l'Union à l'exercice annuel de cyberdéfense de l'OTAN, «Cyber Coalition»; prend acte de l'avancée que représente la participation de l'Union à l'exercice 2017 de gestion de crise de l'OTAN, dans le cadre des exercices parallèles et coordonnés 2017 (PACE) et salue en particulier l'inclusion d'un volet consacré à la cyberdéfense; demande instamment aux deux organisations d'intensifier leurs efforts à cet égard;

41. exhorte l'Union européenne et l'OTAN à organiser des exercices réguliers au niveau stratégique, recueillant la participation des plus hauts responsables politiques des deux organisations; salue, à cet égard, l'exercice estonien «EU CYBRID 2017», premier exercice de l'Union auquel le secrétaire général de l'OTAN ait participé;

42. observe qu'il existe une marge de progression non négligeable pour rendre le programme de coopération dans le domaine de la cyberdéfense plus ambitieux et plus concret, de sorte qu'il dépasse le niveau conceptuel de la coopération dans le cadre d'opérations spécifiques; exhorte les deux organisations à mettre en œuvre concrètement et efficacement ce qui existe déjà et à présenter des propositions plus ambitieuses en vue du prochain examen de la mise en œuvre de la déclaration commune;

43. salue le cyberpartenariat OTAN-industrie (NICP) établi en 2014 et demande à l'Union de s'engager dans le travail commun de ce partenariat afin de créer un lien entre la coopération qu'elle a avec l'OTAN et les leaders de l'industrie spécialisés dans les cybertechnologies pour améliorer la cybersécurité grâce à une collaboration continue mettant notamment l'accent sur: la formation, les exercices et l'éducation pour les représentants de l'OTAN, de l'Union et de l'industrie; l'intégration de l'Union et de l'industrie dans les projets de défense intelligente de l'OTAN; le partage collaboratif d'informations et les bonnes pratiques communes dans le cadre de la préparation et de la récupération entre l'OTAN, l'Union et l'industrie; la poursuite du développement commun des capacités en matière de cyberdéfense; et les réponses concertées aux cyberincidents, au moment et à l'endroit opportuns;

44. prend note des travaux en cours sur la proposition de règlement portant révision du règlement (UE) nº 526/2013 concernant l'ENISA et établissant un cadre européen de certification et d'étiquetage en matière de sécurité des TIC; invite l'ENISA à signer un accord avec l'OTAN afin d'intensifier leur coopération dans la pratique, y compris concernant le partage d'informations et la participation à des exercices de cyberdéfense;

Normes internationales applicables au cyberespace

45. demande l'intégration des capacités de cyberdéfense dans la politique étrangère et de sécurité commune et l'action extérieure de l'UE et de ses États membres, en tant que mission transversale, et invite à une coordination plus étroite en matière de cyberdéfense entre les États membres, les institutions européennes, l'OTAN, les Nations unies, les États-Unis et d'autres partenaires stratégiques, en particulier en ce qui concerne les règles, les normes et les mesures de contrôle applicables au cyberespace;

46. regrette qu'après plusieurs mois de négociations, le groupe d'experts gouvernementaux des Nations unies de 2016-2017 ait été dans l'incapacité de produire un rapport de consensus; rappelle que, comme l'indique le rapport de 2013, le droit international existant et la charte des Nations unies en particulier – qui interdit la menace ou l'utilisation de la force contre l'indépendance politique de tout État, y compris les cyberopérations coercitives destinées à perturber les infrastructures techniques essentielles à la conduite de procédures de participation officielles, y compris les élections, dans un autre État – s'applique et devrait être imposé dans le cyberespace; relève que le rapport de 2015 dudit groupe d'experts énumère un ensemble de normes s'appliquant à un comportement responsable des États, notamment l'interdiction, pour les États, d'exercer ou de soutenir en toute connaissance de cause des cyberactivités contraires aux obligations qui leur incombent en vertu des règles internationales; invite l'Union à jouer un rôle majeur dans les débats en cours et futurs sur les normes internationales et leur mise en œuvre dans le cyberespace;

47. constate la pertinence du manuel de Tallinn 2.0 comme point de départ pour débattre et comme analyse des modalités d'application du droit international en vigueur dans le cyberespace; invite les États membres à commencer à analyser et à appliquer les avis que les experts ont exprimés dans le manuel de Tallinn et à s'entendre sur de futures normes volontaires de relations internationales; signale en particulier que tout utilisation offensive de cybercapacités devrait reposer sur le droit international;

48. confirme son engagement total en faveur d'un cyberespace ouvert, libre, stable et sûr, qui respecte les valeurs essentielles de la démocratie, des droits de l'homme et de l'état de droit, et où les différends internationaux sont réglés par des moyens pacifiques en se fondant sur la charte des Nations unies et sur les principes du droit international; invite les États membres à promouvoir une mise en œuvre plus complète de l'approche européenne commune et globale en matière de cyberdiplomatie et des normes actuellement applicables au cyberespace et à élaborer avec l'OTAN des critères et des définitions à l'échelle de l'Union permettant de déterminer ce qui constitue une cyberattaque afin d'améliorer la capacité de l'Union à parvenir rapidement à une position commune en cas de réalisation d'un acte illicite sur le plan international prenant la forme d'une cyberattaque; soutient fermement la mise en œuvre des normes volontaires et non contraignantes de comportement responsable des États dans le cyberespace, couvrant le respect de la vie privée et les droits fondamentaux des citoyens ainsi que la création de mesures d'instauration de la confiance au niveau régional, qui figurent dans le rapport de 2015 du groupe d'experts gouvernementaux des Nations unies; soutient, dans ce contexte, le travail de la Commission mondiale sur la stabilité du cyberespace, qui tend à élaborer des propositions de normes et de politiques visant à renforcer la sécurité et la stabilité internationales et à orienter les comportements étatiques et non étatiques responsables dans le cyberespace; approuve la proposition selon laquelle les acteurs étatiques et non étatiques ne devraient pas mener ou autoriser sciemment des activités qui endommagent intentionnellement et substantiellement la disponibilité ou l'intégrité générales du noyau public de l'internet, et donc de la stabilité du cyberespace;

49. reconnaît que la majeure partie de l'infrastructure technologique est détenue ou exploitée par le secteur privé et que, par conséquent, il importe de mettre en place une coopération, une consultation et une participation étroites du secteur privé et des groupes de la société civile dans le cadre d'un dialogue pluripartite pour garantir un cyberespace ouvert, libre, stable et sûr;

50. est conscient que, du fait de difficultés liées à leur application, les accords bilatéraux entre États ne produisent pas toujours les résultats escomptés; considère, par conséquent, que la formation de coalitions au sein de groupes de pays partageant les mêmes valeurs et souhaitant établir un consensus constitue un moyen efficace de compléter les efforts pluripartites; souligne le rôle majeur que les autorités locales doivent jouer dans le processus d'innovation technologique et d'échange des données en vue de renforcer la lutte contre la criminalité et les activités terroristes;

51. se félicite de l'adoption par le Conseil du cadre pour des réponses diplomatiques communes de l'Union face aux actes de cybermalveillance, à savoir la boîte à outils cyberdiplomatique de l'Union; soutient la possibilité pour l'Union de prendre des mesures restrictives à l'encontre des ennemis qui attaquent ses États membres dans le cyberespace, y compris de recourir à des sanctions;

52. appelle également de ses vœux une approche proactive claire en matière de cybersécurité et de cyberdéfense et le renforcement général des capacités et des instruments de cyberdiplomatie de l'Union, en tant que mission transversale dans la politique étrangère de l'UE, de sorte qu'ils viennent efficacement appuyer les normes et les valeurs européennes et ouvrir la voie à un consensus sur les règles, les normes et les mesures de contrôle applicables au cyberespace à l'échelle mondiale; observe que le renforcement de la cyber-résilience dans les pays tiers favorise la paix et la sécurité internationales et, en fin de compte, sécurise les citoyens européens;

53. estime que les cyberattaques à l'instar de celles réalisées par les logiciels malveillants NotPetya et WannaCry sont dirigées par un État ou se déroulent avec la connaissance et l'approbation de celui-ci; relève que ces cyberattaques, qui causent des dommages économiques graves et durables et qui constituent une menace pour la vie, sont des violations flagrantes du droit international et des normes juridiques; estime par conséquent que NotPetya et WannaCry constituent des violations du droit international par, respectivement, la Fédération de Russie et la Corée du Nord, et que ces deux pays devraient face à des réponses appropriées et proportionnées de la part de l'Union et de l'OTAN;

54. demande que le Centre européen de lutte contre la cybercriminalité d'Europol devienne un point de contact pour les services répressifs et les agences gouvernementales dédiés à la cybercriminalité dont la responsabilité principale serait de gérer la défense des domaines «point-eu» (.eu) et des infrastructures critiques des réseaux européens lors d'une attaque; souligne que ce point de contact devrait également être mandaté pour échanger des informations et fournir une assistance aux États membres;

55. souligne qu'il est essentiel d'élaborer des normes en matière de protection de la vie privée et de sécurité, de cryptage, de discours de haine, de désinformation et de menaces terroristes;

56. recommande que chaque État membre assume l'obligation d'assister un autre État membre dans le cadre d'une cyberattaque et d'assurer une cyber-responsabilité nationale en étroite coopération avec l'OTAN;

Coopération civilo-militaire

57. invite toutes les parties prenantes à consolider les partenariats de transfert de connaissances, à mettre en œuvre des modèles économiques adaptés et à établir la confiance entre les entreprises et les utilisateurs finals civils et militaires, ainsi qu'à améliorer la transmutation des connaissances théoriques en solutions pratiques, afin de créer des synergies et des solutions de connexion entre les marchés civil et militaire - en substance, un marché unique européen pour la cybersécurité et les produits de cybersécurité - sur la base de procédures transparentes et dans le respect du droit européen et du droit international, en vue de préserver et de renforcer l'autonomie stratégique de l'Union; prend acte du rôle central que jouent les entreprises privées spécialisées en cybersécurité dans l'alerte précoce et l'attribution des cyberattaques;

58. souligne avec force l'importance des activités de recherche et développement, notamment au regard des exigences élevées sur le plan de la sécurité sur le marché de la défense; exhorte l'Union et les États membres à apporter un soutien plus concret à l'industrie européenne de la cybersécurité et aux autres acteurs économiques concernés, à réduire les charges administratives, en particulier pour les petites et moyennes entreprises ainsi que pour les jeunes entreprises (sources fondamentales de solutions innovantes dans le domaine de la cyberdéfense), et à promouvoir une coopération plus étroite avec les organismes de recherche universitaires et les acteurs de plus grande taille, afin de réduire les dépendances vis-à-vis des produits de cybersécurité provenant de sources externes et de créer une chaîne d'approvisionnement stratégique au sein de l'Union pour renforcer son autonomie stratégique; souligne, à cet égard, que le FED et d'autres instruments du cadre financier pluriannuel (CFP) peuvent apporter une contribution précieuse;

59. encourage la Commission à intégrer des éléments de cyberdéfense dans un réseau des centres européens de compétence et de recherche en matière de cybersécurité, en vue également de prévoir des ressources suffisantes pour les cybercapacités et technologies à double usage dans le prochain cadre financier pluriannuel;

60. constate que la protection des infrastructures publiques et autres infrastructures civiles critiques, en particulier des systèmes d'information et des données associées, devient une tâche de défense primordiale pour les États membres et, notamment, pour les autorités en charge de la sécurité des systèmes d'information, et qu'elle devrait faire partie, soit des attributions des structures de cyberdéfense nationales, soit de celles desdites autorités; souligne que, pour ce faire, un certain niveau de confiance et la coopération la plus étroite possible seront nécessaires entre les acteurs militaires, les agences de cyberdéfense, les autres autorités compétentes et les industries concernées, et ne pourront être obtenues qu'au moyen d'une définition claire des devoirs, des rôles et des responsabilités des acteurs civils et militaires, et exhorte toutes les parties prenantes à en tenir compte dans le cadre de leur processus de planification; demande davantage de coopération transfrontalière, dans le plein respect de la législation de l'UE sur la protection des données, sur l'application des lois en matière de lutte contre les actes de cybermalveillance;

61. invite tous les États membres à axer leurs stratégies nationales en matière de cybersécurité sur la protection des systèmes d'information et des données qu'ils contiennent et de considérer la protection de ces infrastructures critiques comme faisant partie de leur obligation respective de diligence; exhorte les États membres à adopter et à mettre en œuvre des stratégies, des orientations et des instruments assurant un niveau raisonnable de protection contre toutes les menaces raisonnablement prévisibles, les coûts et le fardeau de la protection étant proportionnels au préjudice probable qui pourrait être subi par les parties concernées; invite les États membres à prendre des mesures adéquates pour obliger les personnes morales relevant de leur juridiction à protéger les données à caractère personnel dont elles ont la charge;

62. est conscient que compte tenu de l'environnement en mutation des cybermenaces, il est souhaitable de mettre en place une coopération renforcée et plus structurée avec les forces de police, notamment dans certains domaines critiques tels que la lutte contre des menaces comme le cyberdjihad, le cyberterrorisme, la radicalisation en ligne et le financement d'organisations extrémistes ou radicales;

63. encourage une coopération étroite entre les agences européenne comme l'AED, l'ENISA et le Centre européen de lutte contre la cybercriminalité dans le cadre d'une approche transversale visant à promouvoir les synergies et éviter les chevauchements;

64. invite la Commission à élaborer, en étroite coopération avec les États membres, l'AED, le Parlement européen et le Service européen pour l'action extérieure, une feuille de route pour une approche de la cyberdéfense européenne, y compris une mise à jour du cadre stratégique de cyberdéfense de l'Union européenne afin de veiller à ce qu'il reste adapté à sa finalité de mécanisme politique permettant de réaliser les objectifs de l'Union en matière de cyberdéfense; relève que ce processus doit s'inscrire dans le cadre d'une approche stratégique élargie de la PSDC;

65. appelle à un renforcement des capacités de cybersécurité dans le cadre de la coopération au développement, ainsi qu'à une éducation continue et à une formation en matière de sensibilisation au cyberespace, en tenant compte du fait que des millions de nouveaux utilisateurs feront leur apparition en ligne dans les prochaines années, pour la plupart dans les pays en développement, renforçant ainsi la résilience des pays et des sociétés vis-à-vis des cybermenaces et des menaces hybrides;

66. appelle à la mise en place d'une coopération internationale et à des initiatives multilatérales pour établir des cadres de cyberdéfense et de cybersécurité rigoureux en vue de lutter contre la captation de l'État par la corruption, la fraude financière, le blanchiment d'argent, le financement du terrorisme et afin de s'attaquer aux problèmes liés au cyberterrorisme, aux cryptomonnaies et aux autres méthodes de paiement alternatives;

67. constate que les cyberattaques, à l'instar de celles menées par le logiciel malveillant NotPetya, se propagent rapidement en causant des dommages aveugles si une résilience généralisée n'est pas mise en place à l'échelon mondial; estime que la formation et l'éducation en matière de cyberdéfense devraient faire partie de l'action extérieure de l'Union et que le renforcement de la cyber-résilience dans les pays tiers favorise la paix et la sécurité internationales et, en fin de compte, sécurise les citoyens européens;

Renforcement institutionnel

68. invite les États membres à s'engager dans une coopération plus ambitieuse dans le cyberdomaine au sein de la CSP; suggère que les États membres lancent un nouveau programme de cybercoopération dans le cadre de la CSP afin de soutenir une planification, un commandement et un contrôle rapides et efficaces des opérations et des missions actuelles et futures de l'Union; note que ce nouveau programme devrait permettre une meilleure coordination des capacités opérationnelles dans le cyberespace et pourrait aboutir à la création d'un commandement commun de la cyberdéfense lorsque le Conseil européen en décidera ainsi;

69. demande à nouveau aux États membres et à la HR/VP de présenter un Livre blanc de l'Union européenne sur la sécurité et la défense; invite les États membres et la HR/VP à faire de la cyberdéfense et de la dissuasion une pierre angulaire du Livre blanc qui porterait à la fois sur la protection du cyberdomaine pour les opérations prévues à l'article 43 du traité sur l'Union européenne et sur la défense commune prévue par son article 42, paragraphe 7;

70. relève que des personnels militaire et civil de haut niveau provenant de chaque État membre devraient avoir la charge de diriger, à tour de rôle, le nouveau programme de cybercoopération de la CSP et devraient rendre compte auprès des ministres de l'Union européenne chargés de la défense en format CSP et auprès de la HR/VP, afin de promouvoir les principes de confiance entre les États membres et les institutions et agences européennes en matière d'échange d'informations et de renseignements;

71. demande à nouveau la création d'un conseil européen de la défense issu de l'actuel comité directeur ministériel de l'AED et de la formation en format CSP des ministres de l'Union européenne chargés de la défense, afin de garantir la hiérarchisation, la mise en place de ressources et une coopération et une intégration efficaces entre les États membres;

72. rappelle qu'il importe de veiller à ce que le Fonds européen de la défense soit maintenu, voire renforcé dans le prochain CFP, grâce à un budget suffisant en faveur de la cyberdéfense;

73. demande que davantage de ressources soient consacrées à la modernisation et à la rationalisation de la cybersécurité et de la diffusion de renseignements entre le Centre de situation et du renseignement de l'UE (INTCEN) du SEAE, le Conseil et la Commission;

Partenariats public-privé

74. est conscient que les entreprises privées jouent un rôle clé dans la prévention, la détection et le confinement des incidents survenant en matière de cybersécurité ainsi que dans les réponses qui y sont apportées, non seulement au titre de fournisseurs de technologie, mais aussi de fournisseurs de services non informatiques;

75. est conscient du rôle que jouent les secteurs privés dans la prévention, la détection et le confinement des incidents survenant en matière de cybersécurité ainsi que dans les réponses qui y sont apportées, de même que dans la stimulation de l'innovation en matière de cyberdéfense, et demande donc la mise en place d'une coopération renforcée avec le secteur privé afin de garantir une compréhension partagée des exigences de l'Union et de l'OTAN et une assistance à la conception de solutions communes;

76. demande à l'Union de procéder à un examen complet des équipements logiciels, informatiques et de communication, ainsi que des infrastructures utilisées dans les institutions afin d'exclure les programmes et appareils potentiellement dangereux et d'interdire ceux qui ont été confirmés comme malveillants, comme Kaspersky Lab;

o

o o

77. charge son président de transmettre la présente résolution au Conseil européen, au Conseil, à la Commission, à la vice-présidente/haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, aux organismes de l'Union spécialisés dans la défense et la cybersécurité, au secrétaire général de l'OTAN, ainsi qu'aux parlements nationaux des États membres.