COMMISSION
EUROPÉENNE

LA HAUTE REPRÉSENTANTE DE
L'UNION POUR LES AFFAIRES
ÉTRANGÈRES ET LA
POLITIQUE DE SÉCURITÉ

Bruxelles, le 13.6.2018
JOIN(2018) 14 final

RAPPORT CONJOINT AU PARLEMENT EUROPÉEN, AU CONSEIL EUROPÉEN ET AU CONSEIL

sur la mise en oeuvre du cadre commun en matière de lutte contre les menaces hybrides pour la période comprise en juillet 2017 et juin 2018

INTRODUCTION

La communication conjointe intitulée «Cadre commun en matière de lutte contre les menaces hybrides — une réponse de l'Union européenne»[1] place la connaissance de la situation, la résilience et la réaction au cœur de l'action de l'UE visant à lutter contre les menaces hybrides. L'amélioration de notre capacité à détecter et à comprendre les activités hybrides malveillantes à un stade précoce et le renforcement de la résilience des infrastructures critiques (par exemple dans les domaines des transports, des communications, de l'énergie, de l'espace et de la finance) de nos sociétés et de nos institutions sont essentiels pour accroître notre aptitude à résister aux attaques et à les surmonter. La lutte contre les menaces hybrides impose que des mesures soient prises à la fois par les États membres et par les institutions européennes. Le premier rapport sur la mise en œuvre des 22 actions définies dans le cadre commun a été présenté au Conseil le 19 juillet 2017[2]. La présente mise à jour de 2018 donne un aperçu des progrès réalisés depuis l'été dernier.

Des progrès considérables ont été accomplis dans les quatre domaines d'action prioritaires:

- Amélioration de la connaissance de la situation
- Accroissement de la résilience
- Renforcement de la capacité des États membres et de l'Union à prévenir les crises, à y faire face et à s'en remettre rapidement et de manière concertée
- Intensification de la coopération avec l'OTAN afin de garantir la complémentarité des mesures

RECONNAITRE LE CARACTERE HYBRIDE D'UNE MENACE

Action n° 1: ***Les États membres invités à lancer une étude sur les risques hybrides***

Le groupe des Amis de la présidence, présidé par la présidence tournante, a été mis en place par le Conseil pour faire avancer les travaux. En décembre 2017, les États membres ont lancé une étude en vue d'évaluer leurs principales vulnérabilités face aux menaces hybrides. La présidence devrait présenter au COREPER un rapport fondé sur les réponses des États membres, avant la fin du mois de juin 2018.

Dans la perspective de l'expiration de son mandat, fin juin 2018, le groupe des Amis de la présidence, réuni en avril, a entamé des discussions au sujet de son prochain mandat en s'appuyant sur la proposition de la présidence. Le mandat actuel serait prolongé jusqu'en 2020 et son contenu serait élargi; conformément au projet actuel, le mandat inclurait des tâches liées à l'examen de solutions possibles pour renforcer le niveau de préparation et de résilience des États membres, à l'observation de l'évolution sur le plan national et à la coordination des politiques sur les questions hybrides, au soutien des travaux du Conseil sur la coopération entre l'UE et l'OTAN dans le domaine de la lutte contre les menaces hybrides ainsi qu'à l'échange d'informations et à l'élaboration d'une position commune sur les menaces hybrides.

[1] JOIN(2016) 18 final.

[2] Rapport conjoint au Parlement européen et au Conseil sur la mise en œuvre du «cadre commun en matière de lutte contre les menaces hybrides – une réponse de l'Union européenne», JOIN(2017) 30 final.

ORGANISER LA REPONSE DE L'UE: AMELIORER LA CONNAISSANCE DE LA SITUATION

Action nº 2: ***Création d'une cellule de fusion de l'UE contre les menaces hybrides***

La cellule de fusion de l'UE contre les menaces hybrides, établie au sein du Centre de situation et du renseignement de l'UE dans le cadre de la capacité unique d'analyse du renseignement à des fins civiles et militaires de l'UE, recourt à la fois à des analystes civils et militaires et aux services de renseignement et de sécurité des États membres. Elle a atteint sa pleine capacité opérationnelle en juillet 2017, comme elle l'a montré au cours de l'exercice parallèle et coordonné de 2017 avec l'OTAN (PACE17). La cellule de fusion de l'UE contre les menaces hybrides reçoit et analyse des informations classifiées et de source ouverte sur les menaces hybrides, émanant d'un large éventail de parties prenantes. Les rapports et les analyses sont ensuite transmis aux institutions de l'UE et aux États membres afin d'éclairer la prise de décision. La cellule de fusion de l'UE contre les menaces hybrides a livré à ce jour plus d'une centaine de produits ayant trait aux menaces hybrides. La CERT-UE (équipe d'intervention en cas d'urgence informatique pour les institutions de l'UE) contribue aux activités de la cellule de fusion en échangeant des informations sur les cybermenaces actuelles ou émergentes. Cependant, dans les domaines des menaces chimiques, biologiques, radiologiques et nucléaires ainsi que du cyberespace et du contre-renseignement, les compétences spécifiques sont actuellement limitées.

Pour amplifier ces travaux, la cellule de fusion de l'UE contre les menaces hybrides a mis en place un réseau de points de contact nationaux. À ce jour, 26 États membres sur 28 ont désigné des personnes de contact qui se réunissent régulièrement pour partager leurs compétences avec la cellule.

Par ailleurs, ce réseau trouve son pendant dans un réseau conjoint équivalent de la Commission et du SEAE, axé sur l'obtention de résultats au regard de diverses actions menées en matière de résilience. Les réunions se tiennent chaque mois et portent principalement sur des questions thématiques, notamment les transports, les infrastructures, l'énergie, la cybersécurité et les activités de renseignement hostiles.

Au niveau stratégique, la cellule de fusion de l'UE contre les menaces hybrides développe ses relations avec le Centre européen d'excellence pour la lutte contre les menaces hybrides d'Helsinki en participant à des ateliers, à des exercices et à des débats ordinaires sur différents thèmes en vue de renforcer les compétences en matière de lutte contre les menaces hybrides.

Dans le cadre de la déclaration commune, les contacts interservices avec la branche d'analyse des menaces hybrides de l'OTAN sont quotidiens et permanents. Une évaluation parallèle et coordonnée inédite sur un thème hybride a été publiée en septembre 2017 et les produits à livrer en 2018 seront axés sur les défis hybrides émanant de pays du voisinage méridional et oriental.

Action nº 3: ***Communication stratégique***

La communication stratégique dans l'UE est passée à la vitesse supérieure car de nombreux acteurs différents renforcent leurs capacités. La communication intitulée «Lutter contre la désinformation en ligne: une approche européenne»[3] du 26 avril 2018 constate que la désinformation est une menace hybride et définit un certain nombre d'actions, dont la création d'un réseau renforcé entre la Commission, le service européen pour l'action extérieure (SEAE) et les États membres. Les expériences positives de la task force East Stratcom, créée conformément au mandat donné par le Conseil européen en mars 2015, doivent être étayées et

[3] COM(2018) 236 final

consolidées, comme proposé dans la communication conjointe intitulée «Face aux menaces hybrides: protéger les Européens»[4].

Les travaux de la task force East Stratcom consistent, pour l'essentiel, à aider les délégations de l'UE situées dans la région du Partenariat oriental et en Russie principalement ainsi que, dans une certaine mesure, en Asie centrale à améliorer la transmission de messages positifs et à accroître la proximité avec les publics nationaux ou régionaux. La Commission soutient ces activités dans le cadre d'un programme régional d'information et de communication pluriannuel. De plus, la task force East Stratcom coordonne régulièrement ses actions avec les États membres et l'OTAN. Outre le contrôle de la désinformation, la task force East Stratcom mène des activités de sensibilisation, dans les pays du Partenariat oriental et les États membres, à l'impact de la désinformation russe. Elle a également intensifié la formation du personnel en poste dans les pays du Partenariat oriental pour renforcer ses capacités de communication stratégique et sa résilience face à la désinformation. Une coopération accrue avec le quartier général de l'OTAN et les centres d'excellence de Riga et d'Helsinki est prévue à l'avenir; elle consistera notamment à échanger des analyses et à organiser des séminaires de formation pour les journalistes de la région du Partenariat oriental ou de Russie.

Dans le sillage de la nouvelle stratégie de l'UE pour les Balkans occidentaux, une task force axée sur ces pays a été mise en place pour assurer une communication plus efficace sur les politiques de l'UE et atteindre un plus large public dans la région, tout en sensibilisant aux activités de désinformation qui ciblent les Balkans occidentaux et en luttant contre celles-ci. La task force et la Commission ont mis en place une coopération étroite visant à accentuer les éléments stratégiques et ciblés de la communication et de la diffusion de messages à l'égard de la région, en s'appuyant sur les bonnes pratiques et en privilégiant les campagnes thématiques. Cependant, la sensibilisation aux menaces croissantes dont les institutions en particulier sont la cible est insuffisante. Il est nécessaire d'instaurer une culture de sensibilisation à la sécurité et de renforcer les capacités des institutions à faire face aux menaces hybrides.

La task force South, créée en 2017, a modifié son mandat pour tenir compte d'un abandon progressif du prisme de la lutte contre le terrorisme au profit d'une approche plus nuancée destinée à améliorer la communication et à intensifier les contacts avec le monde arabe, y compris en langue arabe. Étant donné que Daesh ou groupe «État islamique» n'est pas l'unique menace en termes de radicalisation, la task force s'emploie à atténuer la désinformation généralisée et la perception erronée de l'UE. À cette fin, elle élabore, en étroite collaboration avec la Commission, des discours positifs sur l'Union européenne et ses politiques pour que l'UE soit mieux comprise, elle communique de manière plus stratégique sur les activités de l'UE dans le monde arabe et promeut les valeurs et les intérêts partagés. La Commission soutient ces activités dans le cadre d'un programme régional d'information et de communication pluriannuel.

<u>Action n° 4:</u> ***Centre d'excellence pour la «lutte contre les menaces hybrides»***

Le Centre européen d'excellence pour la lutte contre les menaces hybrides, créé en 2017, sert de pôle d'expertise à l'appui des efforts déployés individuellement et collectivement par les pays participants pour lutter contre les menaces hybrides, au moyen de la recherche, de la formation, de l'éducation et d'exercices. La participation à ce Centre est ouverte tant aux États membres de l'UE qu'aux pays alliés de l'OTAN. L'Italie, les Pays-Bas, le Danemark et la République tchèque l'ont rejoint récemment, ce qui porte le nombre de pays membres à 16. L'UE et l'OTAN sont toutes deux présentes dans le comité de pilotage en tant qu'observatrices.

[4] Reference to be inserted when known

En 2018, le Centre a approuvé un budget et un plan de travail, élaboré son cadre conceptuel et créé les trois communautés d'intérêt suivantes: influences hybrides, vulnérabilités et résilience, stratégie et défense. Un sous-groupe consacré aux acteurs non étatiques a été mis en place. Il examine les modes opératoires de différents groupes terroristes et intermédiaires. Le Centre a publié un certain nombre d'analyses hybrides et a accueilli plusieurs réunions de haut niveau en vue de dégager une compréhension commune des menaces hybrides, de partager les bonnes pratiques et de rechercher des réponses communes dans l'ensemble de l'UE et des communautés de l'OTAN.

ORGANISER LA REPONSE DE L'UE: RENFORCER LA RESILIENCE

Pour renforcer la résilience, il convient de prendre des mesures dans de nombreux domaines d'action. Ces mesures ne doivent pas nécessairement être axées sur le caractère hybride des menaces, mais conjuguées, elles peuvent faire en sorte qu'une UE plus résiliente soit mieux à même de faire face aux menaces hybrides. Par conséquent, s'il y a lieu dans la description des progrès réalisés dans chacune des actions mentionnées ci-après, il est fait référence au cadre politique spécifique et aux mesures prises par l'Union, notamment celles relevant des travaux en faveur d'une union de la sécurité. Le présent rapport doit donc être lu en liaison avec les rapports mensuels sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, adoptés le même jour[5].

Action n° 5: Protection et résilience des infrastructures critiques

La Commission a élaboré un projet de manuel des indicateurs de vulnérabilité et de la résilience face aux menaces hybrides qui pèsent sur les infrastructures critiques de l'UE. Ce projet de manuel est actuellement en cours de validation au moyen de consultations avec les États membres. La version finale devrait être adoptée en novembre 2018. Par ailleurs, les indicateurs de vulnérabilité seront testés au cours de l'exercice parallèle et coordonné de 2018 avec l'OTAN (PACE18), ainsi que par les États membres qui auront manifesté leur intérêt. Il conviendra de veiller tout particulièrement à poursuivre l'élaboration d'indicateurs de détection qui faciliteront les alertes rapides au tout début d'attaques hybrides contre des infrastructures critiques. Les menaces hybrides seront également prises en considération lors de la prochaine évaluation de la directive européenne sur la protection des infrastructures critiques. Par ailleurs, la Commission renforce le soutien scientifique pour examiner les caractéristiques multiples et transversales des menaces hybrides et se concentre en particulier sur l'identification des vulnérabilités, la détection précoce et les indicateurs, la résilience, la sensibilisation et les exercices.

Afin de protéger les principaux actifs de l'Union, la Commission a en outre présenté une proposition de règlement établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union européenne, s'ils sont susceptibles de porter atteinte à la sécurité ou à l'ordre public[6]. Cette proposition porte sur les investissements directs de personnes ou d'entreprises de pays tiers, qui peuvent, entre autres, avoir des répercussions sur les infrastructures critiques (notamment dans les domaines de l'énergie, des transports, des communications, du stockage de données, de l'espace et dans d'autres installations sensibles), les technologies critiques (y compris l'intelligence artificielle, la cybersécurité, les technologies pouvant avoir des applications à double usage), la sécurité de l'approvisionnement en intrants essentiels ou des investissements qui permettent d'avoir accès à des informations sensibles ou ont la capacité de contrôler de telles informations.

Le forum de consultation pour l'énergie durable dans le secteur de la défense et de la sécurité,

[5] COM(2018) 470 final.

[6] COM(2017) 487 final

seconde phase (FC SEDSS II), de l'Agence européenne de défense continuera de soutenir l'élaboration du document conceptuel préparé par le groupe d'experts sur la protection des infrastructures énergétiques critiques (PCEI), qui est appelé à devenir un document d'orientation stratégique au niveau de l'UE. Celui-ci propose un cadre visant à recenser les meilleures pratiques de gestion, pour les ministères de la défense, dans le renforcement de la protection et de la résilience de toutes les infrastructures énergétiques critiques liées à la défense (IEC).

<u>Action n° 6:</u> ***Accroître la sécurité d'approvisionnement énergétique de l'UE et renforcer la résilience des infrastructures nucléaires***

À la suite de l'engagement pris en septembre 2017 (communication conjointe «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide»[7]), la Commission continuera de soutenir le Centre européen d'échange et d'analyse d'informations dans le domaine de l'énergie en matière de cybersécurité.

Afin d'éviter les crises en matière d'approvisionnement en gaz, les États membres transposent actuellement le règlement relatif à la sécurité de l'approvisionnement en gaz, adopté l'an passé, tandis que la Commission facilite sa mise en œuvre et la coopération entre les États membres au sein des groupes de risques. Les évaluations communes des risques doivent être notifiées à la Commission au plus tard le 1er octobre 2018. La Commission recevra les plans d'action préventifs et les plans d'urgence d'ici au 1er mars 2019. Les États membres devraient conclure les dispositifs de solidarité bilatéraux au plus tard le 1er décembre 2018.

Afin de combler le vide réglementaire concernant la préparation aux risques dans le secteur de l'électricité, le règlement sur la préparation aux risques, qui est en cours de négociation, comporterait des règles sur l'évaluation des risques, l'obligation pour les États membres d'élaborer un plan de préparation aux risques contenant certains éléments contraignants, des modalités de gestion de situations de crise et de contrôle de la sécurité d'approvisionnement. Les plans de préparation aux risques devraient également inclure des accords sur la coopération régionale, notamment des modalités de gestion de situations de crises de l'électricité simultanées. Lors de la mise en œuvre du règlement sur la préparation aux risques, les États membres devraient élaborer le premier plan national de préparation aux risques deux ans après l'entrée en vigueur dudit règlement. Ultérieurement, les plans devraient être mis à jour tous les trois ans. Le futur règlement sur la préparation aux risques nécessitera aussi la réalisation, à intervalles réguliers, d'exercices communs, entre les États membres, simulant une crise de l'électricité. La Commission a déjà commencé les préparatifs de tels exercices avec les États membres intéressés, le Centre commun de recherche et le groupe de coordination pour l'électricité.

En ce qui concerne la résilience des infrastructures nucléaires, les échanges d'informations avec et entre les États membres et la Commission sur les questions de sécurité nucléaire seront améliorés à court terme, et une étude portant sur des initiatives supplémentaires est prévue. Une analyse de la réglementation sur les garanties nucléaires sera effectuée, ce qui permettra éventuellement d'aider les États membres à mieux gérer les sources (radioactives) scellées de haute activité. À plus long terme, la Commission a l'intention de renforcer les activités dans le domaine nucléaire, dès lors que les États membres ont un intérêt commun, et qu'il existe un avantage admis par tous, à échanger des informations et à travailler en collaboration. Elle se penchera également sur les mesures qu'il conviendra de prendre pour la mise en œuvre effective, dans l'UE, de la Convention internationale sur la protection physique des matières nucléaires et des installations nucléaires.

[7] JOIN(2017) 450 final

En ce qui concerne le secteur de la défense, le forum de consultation pour l'énergie durable dans le secteur de la défense et de la sécurité a élaboré la «feuille de route pour la gestion de l'énergie durable dans le domaine de la défense et de la sécurité» pour aider le secteur de la défense à améliorer la gestion énergétique des infrastructures. Ce forum continuera d'étudier les pistes susceptibles de rendre le secteur de la défense plus efficace dans l'utilisation des ressources énergétiques et examinera plusieurs technologies, aux fins de projets de production d'électricité, que le secteur de la défense pourrait exploiter (par exemple, l'énergie éolienne, l'énergie solaire, les réseaux intelligents, le stockage de l'énergie, les biocarburants, la biomasse et la valorisation énergétique des déchets).

Dans ce contexte, le programme «Énergie et Environnement» de l'Agence européenne de défense a poursuivi ses travaux dans le cadre du projet de recherche «Smart Blue Water Camps» afin d'étudier les possibilités d'interventions technologiques pour une gestion durable de l'eau dans les camps militaires «à domicile» et, dans le cadre du contrat de recherche «Smart Camps Technical Demonstrator», pour examiner la faisabilité de l'intégration d'un plus large éventail de technologies environnementales ou énergétiques à plus grande échelle dans un environnement militaire afin de prendre en compte des considérations liées à l'énergie, à l'eau et aux déchets, tout en améliorant le coût et l'efficacité militaire des missions du PSDC.

<u>Action nº 7</u>: Transports et sécurité de la chaîne d'approvisionnement

Pour tous les domaines des transports, à savoir l'aviation civile, les transports maritimes et les transports terrestres, la Commission a intensifié le dialogue avec les États membres, le secteur et d'autres parties prenantes sur les nouvelles menaces de nature hybride qui pèsent sur la sécurité, afin d'acquérir des connaissances et de tirer les enseignements de l'expérience acquise.

Dans le cadre des activités de mise en œuvre et de la révision du plan d'action de la stratégie de sécurité maritime européenne, la Commission s'emploie à analyser les tendances dans le domaine de la sécurité maritime (y compris la piraterie et les litiges maritimes), qui pourraient perturber la navigation et les routes commerciales et avoir une incidence sur les intérêts de l'UE. Compte tenu du fait que les États membres de l'UE et les pays de l'EEE contrôlent plus de 40 % de la flotte marchande mondiale et que l'UE constitue un bloc commercial majeur, les attaques hybrides sur les routes commerciales maritimes auraient des effets perturbateurs importants sur la chaîne de valeur et d'approvisionnement en Europe. L'analyse des risques et le contrôle de nouvelles menaces dans le domaine maritime pourraient déboucher sur des propositions visant la mise à jour de la législation en matière de transports, le cas échéant. Ils constituent aussi la base des efforts continus visant à améliorer l'appréciation de la situation maritime, notamment dans le contexte du développement de l'environnement commun de partage de l'information (CISE). Trois nouveaux projets ont été attribués récemment (début 2018) dans le cadre d'un nouvel appel à propositions destiné à aider les États membres à améliorer l'interopérabilité des TI entre les autorités maritimes nationales).

Avec l'adoption du paquet «garde-frontières et garde-côtes»[8], en septembre 2016, le Parlement européen et le Conseil ont introduit, dans les règlements fondateurs de l'Agence européenne de garde-frontières et de garde-côtes, de l'Agence européenne de contrôle des pêches (AECP) et de l'Agence européenne pour la sécurité maritime (AESM), un article commun leur conférant la tâche de renforcer la coopération, chacune dans le cadre de son mandat, tant entre elles qu'avec les autorités nationales exerçant des fonctions de garde-

[8] Règlement (UE) 2016/1624 relatif au corps européen de garde-frontières et de garde-côtes.

côtes[9], afin d'améliorer l'appréciation de la situation maritime et de soutenir une action cohérente et rentable. Sur ce sujet, une étude visant à recenser les points communs et les moyens de renforcer l'interopérabilité et la coopération dans le domaine de l'évaluation des risques entre les autorités exerçant des fonctions de garde-côtes a été publiée en 201710.

Parmi les questions et les nouvelles menaces liées aux transports - notamment les ports mais pas uniquement - figurent les cybermenaces pesant sur la sûreté aérienne, le brouillage de GPS et l'usurpation (spoofing), les menaces sur les satellites ou les problèmes dans le Grand Nord et l'Arctique. Le Centre d'excellence pour la lutte contre les menaces hybrides d'Helsinki contribue également à l'analyse de ces menaces hybrides liées aux transports, et a récemment entrepris une étude sur la protection des ports.

Les autorités douanières de l'UE jouent un rôle fondamental, en ce qu'elles garantissent la sécurité aux frontières extérieures et la sécurité de la chaîne d'approvisionnement, et qu'elles contribuent ainsi à la sécurité de l'Union européenne. La Commission œuvre à l'amélioration significative du système d'informations anticipées sur les marchandises et de gestion des risques en matière douanière pour que les douanes dans l'UE puissent obtenir toutes les informations nécessaires, partager ces informations de manière plus efficace entre les États membres, appliquer des dispositions communes et spécifiques aux États membres en matière de risque et cibler plus efficacement les envois à risque. L'une des principales priorités du plan d'action de l'UE dans les domaines chimique, biologique, radiologique et nucléaire («CBRN»)[11] est de garantir la sécurité aux frontières et la capacité de détection en ce qui concerne l'entrée illégale de matières CBRN. L'adaptation des systèmes d'information sur les marchandises est essentielle pour renforcer la surveillance et les contrôles fondés sur des chaînes d'approvisionnement internationales afin qu'aucune matière CBRN n'entre illégalement sur le territoire de l'UE. Le quinzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective fournit de plus amples informations sur les mesures prises par l'UE pour renforcer la préparation aux risques CBRN, et notamment sur les actions lancées au niveau de l'UE dans le cadre du plan d'action de la Commission visant à améliorer la préparation aux risques en matière de sécurité chimique, biologique, radiologique et nucléaire.

Afin de supprimer les obstacles à la mobilité militaire dans l'UE, la haute représentante et la Commission ont présenté, le 28 mars 2018, un plan d'action pour étudier les possibilités d'utilisation civilo-militaire du réseau transeuropéen, simplifier les formalités douanières pour les transports militaires et lever les barrières réglementaires et procédurales pour le transport de marchandises dangereuses à des fins militaires. La Commission a proposé un budget de 6,5 milliards d'euros au titre du groupe de programmes «Défense» du cadre financier pluriannuel, qui serait mis en œuvre par l'intermédiaire du mécanisme pour l'interconnexion en Europe pour soutenir les infrastructures de transport afin de les adapter aux exigences de mobilité militaire. L'objectif est de permettre un double usage, civil et militaire, des infrastructures de transport.

---

[9] Les fonctions de garde-côtes sont les suivantes: 1) sécurité maritime et gestion de la navigation; 2) sinistres maritimes et service d'assistance en mer; 3) inspection et contrôle des pêches; 4) contrôle des frontières maritimes; 5) protection de l'environnement maritime; 6) prévention et répression du trafic et de la contrebande, et application du droit maritime connexe; 7) recherche et sauvetage en mer; 8) contrôle et surveillance maritimes; 9) activités douanières maritimes; 10) gestion des accidents et des catastrophes maritimes et 11) sécurité maritime des navires et des ports.

[10] https://publications.europa.eu/en/publication-detail/-/publication/217db2fc-15d6-11e7-808e-01aa75ed71a1/language-en

[11] COM(2017) 610 final du 18.10.2017.

<u>Action nº 8</u>: Accroître la résilience des moyens spatiaux

La proposition de la Commission relative à un programme spatial de l'Union[12] intègre des aspects liés à la sécurité, y compris dans Copernicus, les télécommunications gouvernementales par satellite et le cadre de soutien à la surveillance de l'espace et au suivi des objets en orbite, qui couvriraient la résilience face aux menaces hybrides, en plus des mesures déjà en place pour Galileo et EGNOS.

La surveillance de l'espace et le suivi des objets en orbite[13] visent à garantir le maintien à long terme des infrastructures, équipements et services spatiaux européens et nationaux. Ce cadre de soutien a commencé à fournir ses premiers services de prévention des collisions et de surveillance de la fragmentation et de la rentrée incontrôlée d'objets spatiaux en juillet 2016. Les centres d'opérations nationaux pour la surveillance de l'espace et le suivi des objets en orbite et le centre satellitaire de l'UE ont mis en place des mesures de sécurité des données, qui tiennent compte des recommandations du Conseil relatives aux aspects de sécurité de la politique en matière de données relatives à la surveillance spatiale[14].

En ce qui concerne Galileo, la Commission prend de nouvelles mesures pour garantir une meilleure protection de la fourniture de données qui sont essentielles au bon fonctionnement des infrastructures critiques tributaires de la navigation par satellite pour la datation et la synchronisation. Il est envisagé d'utiliser Galileo pour fournir des services dans les infrastructures critiques, telles que les réseaux énergétiques, les réseaux de télécommunications et les places financières. Dans ce contexte, la proposition de règlement de la Commission établissant un cadre pour le filtrage des investissements directs étrangers cite les programmes européens de radionavigation par satellite (GNSS), Galileo et EGNOS, comme exemples de projets ou de programmes présentant un intérêt pour l'Union, qui pourraient être utiles pour le filtrage des investissements directs étrangers conformément à la proposition de règlement[15].

L'initiative de l'UE pour des télécommunications gouvernementales par satellite permettra de fournir un accès garanti à des télécommunications par satellite sécurisées pour les missions essentielles, les opérations de sécurité et les infrastructures de l'Union et de ses États membres. Il s'agit d'un outil important pour lutter contre les menaces hybrides qui pèsent sur de nombreuses infrastructures, et notamment dans les domaines de l'espace, des transports et de l'énergie.

<u>Action nº 9</u>: Adaptation des capacités de défense et propositions de développement importantes pour l'UE

Le lancement du Fonds européen de la défense, le 7 juin 2017, représente une avancée majeure, qui contribue à stimuler les efforts des États membres pour renforcer et soutenir la collaboration dans le domaine de la défense en Europe, de manière à répondre efficacement aux défis stratégiques. Dans le cadre du volet «capacités» du Fonds, l'UE complètera en particulier le financement national de projets de développement collaboratifs en matière de défense. À cette fin, la Commission a proposé, en juin 2017, un règlement établissant un programme européen de développement industriel dans le domaine de la défense, doté d'un budget de 500 millions d'euros pour la période 2019-2020. Le Parlement européen et le Conseil sont parvenus à un accord provisoire sur ce projet de règlement, le 22 mai 2018. Dans le prochain cadre financier pluriannuel de l'UE, la Commission a proposé un Fonds européen intégré de la défense, doté d'une enveloppe budgétaire ambitieuse de 13 milliards d'euros,

[12] COM(2018) 447 final du 6.6.2018.

[13] Décision nº 541/2014/UE du Parlement européen et du Conseil du 16 avril 2014 établissant un cadre de soutien à la surveillance de l'espace et au suivi des objets en orbite

[14] Politique en matière de données relatives à la surveillance spatiale (14698/12) du 9.10.2012

[15] Voir l'annexe de COM(2017) 487 final.

prévoyant d'affecter plus de 8,90 milliards d'euros à des projets collaboratifs de développement des capacités de défense.L'impact potentiel de la lutte contre les menaces hybrides sur le développement des capacités sera intégré dans le plan de développement des capacités révisé, qui doit être approuvé par les États membres en juin 2018.

<u>Action nº 10</u>: Mécanismes de préparation et de coordination en matière de santé

La préparation en matière de santé est une composante très importante de la préparation globale face aux risques CBRN. C'est la raison pour laquelle la Commission a pris des mesures dans le cadre de son plan d'action visant à renforcer la préparation aux risques en matière de sécurité chimique, biologique, radiologique et nucléaire. Des efforts ont été notamment déployés pour encourager les initiatives visant à partager efficacement l'expertise.

La Commission a ainsi mis en place Chimera, un exercice concernant les secteurs de la santé, de la protection civile et de la sécurité dans toute l'UE et dans des pays tiers, destiné à tester les plans de préparation et d'intervention face à des menaces transfrontières graves. Cet exercice avait notamment comme scénario fictif la dissémination délibérée d'une maladie transmissible, conjuguée à des cyberattaques contre des infrastructures critiques, y compris des hôpitaux, afin de tester les mécanismes, les systèmes et les outils de communication existants au niveau national et de l'UE en réponse à une menace hybride. L'exercice à l'échelle de l'UE a eu lieu les 30 et 31 janvier 2018 à Luxembourg. Il a contribué à renforcer les capacités intersectorielles et à améliorer l'interopérabilité et la coordination entre les secteurs de la santé, de la protection civile et de la sécurité au niveau de l'UE et des États membres ainsi que la collaboration avec les partenaires internationaux. L'exercice a également permis de recenser les responsabilités actuelles et les rôles de toutes les parties prenantes dans la gestion des crises en réponse aux menaces hybrides. Le système d'alerte précoce et de réaction (SAPR), le système d'alerte intersectoriel de la Commission (ARGUS), le système commun de communication et d'information d'urgence (CECIS) et le dispositif intégré pour une réaction au niveau politique dans les situations de crise du Conseil (IPCR) ont été testés et leur interaction vérifiée. Le quinzième rapport sur les progrès accomplis dans la mise en place d'union de la sécurité réelle et effective fournit de plus amples informations sur les mesures prises par l'UE pour renforcer la préparation face aux risques CBRN.

En avril 2018, la Commission a publié une communication et soumis une proposition de recommandation du Conseil visant à renforcer la coopération de l'UE dans la lutte contre les maladies à prévention vaccinale dans le but de la voir adoptée avant la fin de l'année 2018. Elle vise à remédier à la réticence à la vaccination, à accroître la viabilité des programmes de vaccination et à renforcer l'efficacité de la recherche et du développement dans le domaine des vaccins.

En ce qui concerne le Corps médical européen, l'équipe médicale d'urgence norvégienne est entrée dans le classement de l'Organisation mondiale de la santé (OMS), ce qui signifie qu'elle respecte les normes de qualité minimale. La première réunion régionale des équipes médicales d'urgence de la région européenne de l'OMS s'est tenue en avril 2018; elle était organisée conjointement par la Commission, l'Organisation mondiale de la santé et les autorités sanitaires belges, qui présidaient le groupe régional.

Actuellement, des travaux de préparation, en étroite collaboration avec la European Burns Association et les États membres, sont en cours pour mettre sur pied un mécanisme de gestion de catastrophes de masse impliquant des victimes de brûlures. Au début d'octobre 2018, la Commission et les États membres se réuniront dans le cadre d'un atelier pour finaliser ces travaux.

<u>Action nº 11</u>: Réseau des CSIRT (centres de réponse aux incidents de sécurité informatique), CERT-UE et directive SRI

La CERT-UE diffuse des produits d'évaluation des cybermenaces concernant des secteurs critiques, de manière périodique et ad hoc. Pour différents modes de transport (aérien, maritime et terrestre), la Commission assure un suivi régulier et veille à ce que les initiatives sectorielles concernant les cybermenaces soient cohérentes avec les capacités intersectorielles couvertes par la directive relative à la sécurité des réseaux et des systèmes d'information (directive SRI).

En septembre 2017, l'Agence européenne de défense et la présidence estonienne du Conseil de l'UE ont organisé un exercice de simulation informatique stratégique pour les ministres de la défense de l'Union, baptisé CYBRID17, dont l'objectif était de sensibiliser à la coordination en cas d'incident en matière de cybersécurité au niveau politique et aux effets potentiels de cyber-campagnes offensives. Cet exercice était axé sur l'analyse de la situation, les mécanismes de réaction en cas de crise et la communication stratégique. L'Agence européenne de défense transférera les éléments de cet exercice sur la cyber-plateforme du Collège européen de sécurité et de défense destinée à coordonner l'éducation, la formation, l'évaluation et les exercices, qui sera lancée en septembre 2018. L'organisation d'exercices de haut niveau similaires par les présidences de l'UE est envisagée à l'avenir.

<u>Action nº 12</u>: Partenariat public-privé contractuel en matière de cybersécurité

La Commission a signé un partenariat public-privé sur la cybersécurité avec l'organisation européenne pour la cybersécurité (ECSO) afin de stimuler la compétitivité et les capacités d'innovation du secteur européen de la sécurité numérique et de la protection de la vie privée. L'UE va investir jusqu'à 450 millions d'euros dans ce partenariat pour la protection des utilisateurs et des infrastructures contre les cyberattaques. Ce partenariat devrait engendrer des investissements à hauteur de 1,8 milliard d'euros d'ici à 2020.

En ce qui concerne la cybersécurité, la communication conjointe intitulée «*Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide*»[16] de septembre 2017 met en place des mesures visant à insuffler une dynamique importante dans les structures et les capacités de l'UE en matière de cybersécurité. Toutefois, l'insuffisance des investissements et le manque de coordination empêchent l'UE d'avoir une cybersécurité efficace. L'UE cherche à y remédier, comme l'indique la communication conjointe.

<u>Action nº 13</u>: Résilience du secteur de l'énergie

En juin 2018, la Commission mettra en place un groupe de travail sectoriel sur l'énergie dans le cadre du groupe de coopération SRI pour examiner les particularités du secteur de l'énergie et fournir des indications aux États membres sur la mise en œuvre de la directive relative à la sécurité des réseaux et des systèmes d'information (directive SRI) pour ce secteur. Dans le même temps, la Commission s'emploie à élaborer des orientations spécifiques en matière de cybersécurité, qui dépassent le cadre de la directive SRI pour recenser les bonnes pratiques de cybersécurité dans le secteur de l'énergie et s'adressent aux opérateurs qui ne sont pas couverts par ladite directive. La Commission continuera d'organiser des événements de partage d'information sur les questions de cybersécurité dans le secteur de l'énergie pour sensibiliser, échanger les bonnes pratiques, renforcer la coopération (par-delà les frontières et entre les gestionnaires de réseau de transport et les gestionnaires de réseau de distribution), examiner les mesures physiques, les nouveaux risques, ainsi que l'éducation et les compétences.

[16] JOIN(2017) 450 final

À long terme, la Commission mettra en place un code de réseau pour des règles sectorielles en matière de cybersécurité, comme proposé dans la refonte du règlement «électricité»[17], actuellement soumise à la procédure législative.

Action nº 14: Résilience du secteur financier: plateformes et réseaux d'échanges d'informations

Le plan d'action Fintech de la Commission aborde les obstacles susceptibles d'entraver les échanges d'informations sur les cybermenaces entre les acteurs des marchés financiers, et propose des solutions possibles pour y remédier. Par ailleurs, la CERT-UE joue un rôle dans l'échange d'informations sur les incidents.

Action nº 15: Résilience face aux cyberattaques dans le secteur des transports

La protection des modes de transport contre les cyberattaques est une priorité majeure pour la Commission. Dans le domaine de l'aviation civile, le renforcement de la cybersécurité a bien progressé, mais la vulnérabilité des systèmes face à une défaillance technique ou à des menaces pesant sur la cybersécurité ne peut jamais être exclue, comme l'a montré la récente panne informatique chez Eurocontrol qui a eu des répercussions sur la moitié des vols en Europe. La Commission travaille en étroite coopération avec l'Agence européenne de la sécurité aérienne dans ce domaine de transports. La CERT-UE a signé un accord de niveau de service avec Eurocontrol et un protocole de coopération avec l'Agence européenne de la sécurité aérienne pour aider ces entités et leurs parties prenantes à réagir face aux cybermenaces.

Dans le domaine des transports maritimes, le secteur a publié des lignes directrices sur la cybersécurité, qui ont ensuite été examinées et adoptées au niveau de l'Organisation maritime internationale, dans une perspective et selon une approche essentiellement mondiales. La cybersécurité dans les installations portuaires et les ports européens demeure une priorité politique majeure, qui est étudiée et fait l'objet de discussions régulières avec les États membres, le secteur et les parties prenantes dans le cadre de la mise en œuvre et du suivi de la directive sur la sécurité des réseaux et de l'information.

La Commission a l'intention de mettre au point une boîte à outils globale et interactive de gestion des connaissances en matière de cybersécurité, comportant des recommandations de bonnes pratiques pour aider les responsables de la sécurité et les professionnels du secteur des transports à mieux détecter, évaluer et atténuer les risques en matière de cybersécurité.

Action nº 16: Lutte contre le financement du terrorisme

L'an passé, la Commission a déployé des efforts considérables pour combattre le financement du terrorisme, comme l'indiquent les rapports réguliers sur la sécurité de l'Union. Plus récemment, dans son train de mesures en matière de sécurité présenté en avril 2018[18], la Commission a pris de nouvelles dispositions pour renforcer la coopération entre les autorités chargées de la lutte contre les formes graves de criminalité et le terrorisme et améliorer l'accès aux informations financières, avec une proposition de directive[19] visant à faciliter l'utilisation des informations financières et d'autres informations à des fins de prévention et de détection d'infractions pénales graves, et d'enquêtes et de poursuites en la matière. Le quinzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective contient de plus amples informations sur les récents travaux entrepris au niveau de l'UE pour lutter contre le financement du terrorisme.

---

17 Proposition de règlement du Parlement européen et du Conseil sur le marché intérieur de l'électricité (refonte) - COM/2016/0861 final

18 COM(2018) 211 final.

19 COM(2018) 213 final

Afin d'harmoniser les sanctions en cas d'infractions pénales de blanchiment de capitaux, la Commission a proposé une législation dont l'adoption est prévue vers la mi-2018. En outre, la cinquième directive anti-blanchiment a été adoptée en mai 2018 pour renforcer un certain nombre de mesures, telles que le renforcement des contrôles de pays tiers à haut risque, les contrôles des plateformes de change de monnaies virtuelles, les mesures de transparence applicables aux instruments prépayés, les nouvelles compétences des cellules de renseignement financier et l'accès rapide aux informations relatives aux titulaires de comptes bancaires et de comptes de paiement, au moyen de registres centralisés ou de systèmes électroniques de recherche de données pour les cellules de renseignement financier.

Action n° 17: Actions de lutte contre la radicalisation et analyse de la nécessité de renforcer les procédures de retrait des contenus illicites

Ces dernières années, la prévention de la radicalisation violente, tant en ligne que hors ligne, est devenue une priorité pour la Commission. Pour intensifier les efforts au niveau de l'UE, la Commission a mis en place un groupe d'experts de haut niveau sur la radicalisation, chargé de fournir des recommandations sur la coordination, la portée et l'impact des politiques de l'UE en matière de prévention. Ce groupe d'experts a rendu son rapport final le 18 mai 2018, dans lequel il recommande notamment de mettre en place un mécanisme de coopération de l'UE.

En ce qui concerne la lutte contre les contenus illicites en ligne, suite à l'adoption de la recommandation de la Commission du 1er mars 2018, l'accent est mis sur la réduction de l'accessibilité à ce type de contenus. La Commission a lancé une étude d'impact visant à déterminer si les efforts actuellement déployés sont suffisants ou si des mesures supplémentaires s'imposent afin d'assurer la détection et le retrait rapides et proactifs des contenus illicites en ligne, y compris d'éventuelles mesures législatives destinées à compléter le cadre réglementaire en vigueur. Les travaux de la Commission dans ce domaine sont décrits de manière circonstanciée dans le quinzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective.

Le code de conduite signé avec Facebook, Twitter, Google (YouTube) et Microsoft pour lutter contre les discours haineux illégaux diffusés en ligne donne des résultats rapides et positifs. Il a permis à ces entreprises de réaliser d'importants progrès dans l'analyse et la suppression sans délais des discours jugés haineux et illégaux qui leur sont signalés. Le 3e exercice de suivi de la Commission sur la mise en œuvre du code, publié en janvier 2018, a montré qu'en moyenne, 70 % des contenus haineux sont retirés et que les discours haineux signalés sont examinés dans un délai de 24 heures, comme prévu par le code de conduite. Ce code est devenu une norme pour le secteur et la récente décision d'Instagram et de Google + d'y adhérer est encourageante. En mars 2018, la Commission a également proposé des mesures supplémentaires pour les plateformes en ligne, telles que la détection automatisée, la transparence et le retour d'informations aux utilisateurs, ainsi que des garanties destinées à protéger la liberté d'expression[20].

Au-delà des actions déjà entreprises pour lutter contre la radicalisation et les discours haineux en ligne, il convient de prendre des mesures visant à prévenir et à atténuer les menaces liées au cyberespace pour les élections.

Action n° 18: Renforcement de la coopération avec les régions du voisinage et les pays tiers

L'Union européenne a accordé davantage d'attention au renforcement des capacités et à l'amélioration de la résilience dans les pays partenaires dans le domaine de la sécurité, notamment en développant la dimension «sécurité» de la politique européenne de voisinage révisée. Dans le but de renforcer les capacités des partenaires dans la lutte contre les menaces

[20] COM(2018) 1177 final

hybrides, des études spécifiques sur les risques hybrides sont actuellement lancées afin de déterminer la vulnérabilité des points sensibles de ces pays et de leur apporter un soutien ciblé. Le SEAE, en coordination avec la Commission, a mené une enquête avec la République de Moldavie. En 2018, la Jordanie et la Géorgie ont officiellement demandé à l'UE de faire l'objet d'enquêtes sur leur vulnérabilité; dans un premier temps, le questionnaire doit être adapté aux besoins spécifiques de ces deux pays. Des travaux complémentaires consacrés au renforcement des capacités en matière de cybersécurité, en particulier pour des infrastructures critiques, ont été entrepris en Ukraine par l'intermédiaire de missions d'assistance technique. Enfin, la Commission a également lancé, au début de 2018, un nouveau programme complet visant à augmenter la cyberrésilience de pays tiers, notamment en Afrique et en Asie.

L'UE continue d'examiner des plans et des programmes de renforcement des capacités en matière de sécurité nucléaire avec l'Agence internationale de l'énergie atomique et le gouvernement américain dans le groupe de travail sur la surveillance des frontières. Le centre européen de formation à la sécurité nucléaire (EUSECTRA) organise des formations sur la prévention et la détection dans le domaine de la sécurité nucléaire ainsi que les réactions en cas d'accident nucléaire. Le plan d'action de la Commission visant à améliorer la préparation aux risques en matière de sécurité chimique, biologique, radiologique et nucléaire prévoit des actions axées sur la coopération avec des partenaires internationaux majeurs, y compris dans le cadre de dialogues sur la lutte contre le terrorisme et sur la sécurité avec les pays tiers concernés.

L'initiative relative aux centres d'excellence CBRN financés par l'UE, qui concerne la quasi-totalité des partenaires du voisinage[21], continue d'œuvrer à l'amélioration des capacités nationales et régionales des pays partenaires dans les domaines de la prévention, de la préparation et de la réaction à ces menaces, y compris celles pesant sur les structures de sécurité militaire («hard security»).

Dans les pays du voisinage oriental et méridional, des formations de protection civile et des exercices sont organisés dans le cadre des programmes régionaux de prévention, de préparation et de réaction aux catastrophes naturelles et d'origine humaine (PPRD). La troisième phase du PPRD Sud a débuté en 2018, tandis que la deuxième phase du PPRD Est s'achèvera en novembre 2018, à moins que le délai ne soit prolongé. Il convient de maintenir des liens étroits avec les centres d'excellence CBRN régionaux et les programmes PPRD Sud et Est.

PRÉVENIR LES CRISES, Y FAIRE FACE ET S'EN REMETTRE

Si les politiques de longue durée menées à l'échelon national et de l'Union permettent d'atténuer les conséquences, il demeure essentiel, à court terme, de renforcer la capacité des États membres et de l'Union à prévenir les menaces hybrides, à y faire face et à s'en remettre à bref délai et de manière concertée. Une réaction rapide aux événements déclenchés par des menaces hybrides est primordiale. Des progrès importants ont été enregistrés dans ce domaine au cours de l'année écoulée, avec, notamment, la mise en place dans l'UE d'un protocole opérationnel définissant le processus de gestion de crise en cas d'attaque hybride. Le suivi régulier et les exercices se poursuivront.

Action n° 19: ***Mise en place d'un protocole opérationnel commun et exercices visant à améliorer les capacités de prise de décisions stratégiques en réaction aux menaces hybrides complexes***

Le protocole opérationnel de l'UE a été arrêté dans un document de travail conjoint en juin 2016. Il définit les principes fondamentaux de la réaction pan-institutionnelle en cas de

[21] Avec les centres d'excellence NRBC régionaux à Rabat, Alger, Amman et Tbilissi.

crise. Durant EUPACE17, le protocole a été testé dans un scénario hybride et s'est révélé être un outil précieux pour faciliter l'interconnexion entre les services. En outre, il a établi les points de contact pour l'interaction entre les différents niveaux d'intervention, à savoir politique, stratégique, opérationnel et technique, ainsi qu'entre les trois principaux mécanismes de réaction aux crises de l'UE (pour les crises extérieures), ARGUS (la plateforme informatique interne de la Commission pour l'échange d'informations) et le dispositif intégré pour une réaction au niveau politique dans les situations de crise du Conseil. Le protocole a également fait ses preuves au cours de l'exercice parallèle CMX17 avec l'OTAN. Le prochain exercice relevant de la série PACE18 aura lieu en novembre 2018 et, en fonction des enseignements tirés, une mise à jour du protocole sera envisagée.

En septembre et octobre 2017, l'UE a organisé le premier exercice parallèle et coordonné avec l'OTAN (PACE17), qui consistait à tester le niveau de préparation et l'interaction entre les deux organisations en cas de crise hybride de grande ampleur. Dans la phase préparatoire, de nombreux échanges de personnel ont eu lieu dans les quatre domaines traités dans les manuels d'instructions hybrides: alerte précoce/connaissance de la situation; communication stratégique; cyberdéfense; prévention et réaction aux crises. L'ampleur de l'interaction entre les personnels de l'UE et de l'OTAN durant EUPACE17 est sans précédent. De surcroît, l'OTAN a participé pour la première fois à une table ronde sur le dispositif intégré pour une réaction au niveau politique dans les situations de crise, présidée par la Présidence du Conseil, et des hauts fonctionnaires de l'UE ont participé aux discussions du Conseil de l'Atlantique Nord. Le processus de retour d'expérience s'est concentré sur plusieurs aspects, notamment l'interaction entre les mécanismes de réaction en cas de crise de l'UE et de l'OTAN et les difficultés liées à l'échange d'informations classifiées entre les services des deux organisations, y compris la nécessité de sécuriser les communications, notamment dans le but d'assurer, à l'avenir, un échange rapide et sûr, tout en respectant pleinement l'obligation de contrôle de l'autorité d'origine.

La planification de l'exercice parallèle et coordonné 2018, pour lequel l'UE sera chef de file, est en cours.

<u>Action n° 20</u>: Examen de l'applicabilité et des implications pratiques de l'article 222 du TFUE et de l'article 42, paragraphe 7, du TUE en cas d'attaque hybride grave et de grande ampleur

L'applicabilité de la clause de solidarité de l'UE et de son mécanisme d'assistance mutuelle ainsi que leur interaction réciproque et les mécanismes de réaction de l'OTAN, y compris la défense collective conformément à l'article 5, sont examinés en profondeur et testés dans des scénarios d'exercices hybrides. Le centre d'excellence pour la lutte contre les menaces hybrides d'Helsinki est intéressé et prêt à faire avancer les travaux sur le plan tant de la recherche que des exercices et à contribuer au développement d'une vision commune entre les États membres et les pays alliés.

<u>Action n° 21</u>: Intégrer, exploiter et coordonner les capacités d'action militaire dans la lutte contre les menaces hybrides dans le cadre de la politique de sécurité et de défense commune

En réponse à la mission d'intégration des capacités militaires destinées à appuyer la politique étrangère et de sécurité commune/politique de sécurité et de défense commune, l'avis militaire concernant le document intitulé «EU military contribution to countering hybrid threats within the CSDP» a été finalisé en juillet 2017, à la suite d'un séminaire avec des experts militaires en décembre 2016 et suivant les orientations reçues du groupe de travail du Comité militaire de l'Union européenne en mai 2017. Cet avis trouvera son application

concrète dans le plan de mise en œuvre de l'élaboration de concepts. En consultation avec le Centre européen d'excellence pour la lutte contre les menaces hybrides, l'État-major de l'UE est en train de développer un concept sur la manière dont les forces armées peuvent contribuer à la lutte contre les menaces hybrides, notamment par le biais des missions et opérations relevant de la politique de sécurité et de défense commune.

En outre, l'État-major de l'UE et les États membres permettent quotidiennement d'améliorer l'alerte précoce en fournissant des renseignements militaires à la cellule de fusion de l'UE contre les menaces hybrides. La capacité unique d'analyse du renseignement soutient les task forces Stratcom du SEAE en procurant des conseils militaires pour aider à lutter contre les campagnes de désinformation qui ciblent l'UE et les États membres.

Les capacités militaires destinées à lutter contre les menaces hybrides seront mises à l'épreuve lors de l'exercice parallèle et coordonné de 2018 avec l'OTAN (PACE18). Sur la base du scénario hybride PACE18, l'État-major de l'UE et l'état-major international de l'OTAN mèneront des discussions informelles reposant sur ce scénario afin de garantir la complémentarité dans la lutte contre les menaces hybrides, lorsque les besoins se recoupent, conformément au principe d'inclusion, tout en respectant l'autonomie décisionnelle de chaque organisation et les règles applicables en matière de protection des données.

COOPÉRATION UE-OTAN

Action n° 22: ***Coopération UE-OTAN en ce qui concerne la connaissance de la situation, les communications stratégiques, la cybersécurité, ainsi que «la prévention et la gestion des crises»***

La lutte contre les menaces hybrides demeure un domaine clé de l'interaction UE-OTAN. Force est en effet de constater qu'en cas de menace hybride, les ressources et les capacités que les deux organisations peuvent mobiliser sont complémentaires et renforcent la capacité des États membres et des pays alliés à prévenir, décourager et contrer de telles menaces. L'exercice PACE17 a testé les protocoles opérationnels des deux organisations et, par ce moyen, leur aptitude à réunir leurs efforts de manière rapide et efficace pour venir en aide à leurs pays membres touchés. À la lumière des enseignements tirés, ces deux «protocoles opérationnels seront révisés et mis à jour. Dans le domaine de la communication stratégique, des consultations ont eu lieu en vue d'un soutien pour l'Ukraine, la Bosnie-et-Herzégovine, la République de Moldavie et la Géorgie.

En septembre 2017, un atelier UE-OTAN sur la résilience a réuni des experts dans des secteurs stratégiques critiques pour échanger des informations sur leurs activités respectives et étudier des propositions d'actions complémentaires, notamment dans le domaine de la protection des infrastructures critiques.

Le plan d'action sur la mobilité militaire, présenté en 2018, vise à faciliter la circulation des troupes et des équipements militaires et pourrait prendre en considération les défis que risquent de poser les menaces hybrides spécialement conçues pour ralentir les temps de réaction des États membres et des pays alliés; ce domaine pourrait faire l'objet d'un futur exercice parallèle et sera pris en compte dans la série EUPACE19/20.

La coordination des efforts en matière de cyberformation constitue un important domaine d'action et appelle une interaction plus étroite. L'OTAN a également participé en qualité d'observateur à l'exercice de simulation CyberEurope de l'ENISA en juin 2018.

CONCLUSIONS

L'amélioration de la connaissance de la situation et le renforcement de la résilience face à l'évolution des menaces hybrides émanant de diverses sources continuent de poser de multiples difficultés et exigent un effort permanent de la part de l'UE. Le cadre commun comporte un large éventail d'actions allant de l'amélioration de la fusion et de l'échange de l'information au renforcement de la protection des infrastructures critiques et de la cybersécurité, en passant par l'édification de sociétés résilientes face à la radicalisation et à l'extrémisme violent. Le cadre de l'UE en matière de lutte contre les menaces hybrides a permis d'apporter un soutien aux États membres grâce à toute une série de mesures visant à renforcer la capacité de l'UE et des États membres à résister aux épreuves, à réagir de manière coordonnée aux attaques leur portant atteinte et, enfin, à s'en remettre.

La réponse de l'UE aux menaces hybrides a en outre été testée avec succès et mise à l'épreuve conjointement avec l'OTAN au cours de plusieurs exercices. Il est prévu de poursuivre dans cette voie. L'étroite coopération entre tous les acteurs concernés au sein de l'UE et avec l'OTAN est la pierre angulaire des efforts visant au renforcement de la résilience. En outre, l'aide apportée aux pays partenaires du voisinage pour déterminer leurs vulnérabilités et renforcer les capacités de lutte contre les menaces hybrides contribue à une meilleure compréhension de la nature des menaces extérieures et, par voie de conséquence, permet d'améliorer la sécurité dans le voisinage de l'UE.