COMMISSION
EUROPÉENNE

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

Bruxelles, le 19.7.2017
JOIN(2017) 30 final

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»

1. INTRODUCTION

L'Union européenne fait actuellement face à l'un des plus grands défis de son histoire dans le domaine de la sécurité. Les menaces qui pèsent sur elle ont un visage de moins en moins conventionnel; elles sont tantôt physiques (comme les nouvelles formes de terrorisme), tantôt numériques (telles les cyberattaques complexes). Certaines prennent des formes plus subtiles, à visée coercitive, par exemple les campagnes de désinformation et la manipulation médiatique. Elles ont pour objectif de saper des valeurs fondamentales de l'Europe telles que la dignité humaine, la liberté et la démocratie. Les cyberattaques coordonnées qui ont récemment frappé la planète, et dont l'origine s'est révélée difficile à déterminer, ont mis au jour les points faibles de nos sociétés et de nos institutions.

En avril 2016, la Commission européenne et la haute représentante ont adopté une communication conjointe en matière de lutte contre les menaces hybrides[1] (ci-après le «cadre commun»). Ce cadre, qui reconnaît la nature transfrontière et complexe des menaces hybrides, propose une approche du renforcement de la résilience globale de nos sociétés qui implique l'ensemble des instances de gouvernement. Le Conseil[2] a accueilli favorablement l'initiative et les actions proposées et a invité la Commission et la haute représentante à rendre compte de leur état d'avancement en juillet 2017. Si l'Union européenne peut aider les États membres à renforcer leur résilience aux menaces hybrides, la responsabilité première en la matière incombe aux États membres, dans la mesure où la lutte contre les menaces hybrides touche à la sécurité nationale et à la défense.

Le cadre commun en matière de lutte contre les menaces hybrides est un élément important de l'approche globale plus intégrée de l'UE en matière de sécurité et de défense. Il contribue à la création d'une Europe qui protège, conformément à l'appel lancé en ce sens par le président Juncker dans le discours sur l'état de l'Union de septembre 2016. En 2016, l'Union européenne a également jeté les bases d'un renforcement de la politique de défense européenne pour répondre aux attentes des citoyens, qui veulent être mieux protégés. La stratégie globale de l'UE pour la politique étrangère et de sécurité de l'Union européenne[3] a mis en lumière la nécessité d'une approche intégrée établissant un lien entre la résilience intérieure et l'action extérieure de l'Union européenne et préconise la mise en place de synergies entre la politique de défense et les politiques concernant le marché intérieur, l'industrie ainsi que les services répressifs et de renseignement. À la suite de l'adoption, en novembre 2016, du plan d'action européen de la défense, la Commission a présenté des initiatives concrètes qui contribueront à améliorer la capacité de l'Union européenne à répondre aux menaces hybrides en favorisant la résilience des chaînes d'approvisionnement de la défense et en renforçant le marché unique de la défense. Le 7 juin 2017, la Commission a notamment lancé le Fonds européen de la défense et proposé de lui accorder un financement de 600 millions d'euros jusqu'en 2020 et de 1,5 milliard d'euros par an au-delà de 2020. La communication sur l'union de la sécurité[4] a établi la nécessité de lutter contre les menaces

[1] Communication conjointe 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) 18 final.
[2] Conclusions du Conseil sur la lutte contre les menaces hybrides, communiqué de presse 196/16 du 19 avril 2016.
[3] Présentée le 28 juin 2016 au Conseil européen par la haute représentante.
[4] COM(2016) 230 final du 20.4.2016.

hybrides et l'importance d'assurer une plus grande cohérence entre les actions internes et externes dans le domaine de la sécurité.

Les dirigeants de l'Union ont mis la sécurité et la défense au cœur du débat sur l'avenir de l'Europe[5], comme l'atteste la déclaration de Rome du 25 mars 2017, qui trace les contours d'une Union sûre et sécurisée, déterminée à renforcer sa sécurité et sa défense communes. Le 8 juillet 2016, le président du Conseil européen, le président de la Commission européenne et le secrétaire général de l'OTAN ont signé à Varsovie une déclaration commune visant à conférer un nouvel élan et une nouvelle teneur au partenariat stratégique UE-OTAN. La déclaration commune énonce sept domaines concrets – dont la lutte contre les menaces hybrides – dans lesquels la coopération entre les deux organisations devrait être renforcée. Un ensemble commun de quarante-deux propositions de mise en œuvre a ensuite été approuvé par les Conseils de l'UE et de l'OTAN, et un premier rapport faisant état d'avancées considérables a été publié en juin 2017[6].

Dans son document de réflexion sur l'avenir de la défense européenne[7], présenté en juin 2017, la Commission expose différents scénarios visant à lutter contre les menaces croissantes qui pèsent sur la sécurité et la défense de l'Europe et à renforcer les capacités de défense propres de l'Europe à l'horizon 2025. Dans les trois scénarios, la sécurité et la défense sont considérées comme des parties intégrantes du projet européen qui sont nécessaires pour protéger et promouvoir nos intérêts à l'intérieur comme à l'extérieur de nos frontières. L'Europe doit devenir un garant de la sécurité et assurer progressivement sa propre sécurité. Aucun État membre ne peut relever seul les défis à venir, en particulier celui de la lutte contre les menaces hybrides. La coopération en matière de défense et de sécurité n'est donc pas optionnelle; c'est une nécessité pour parvenir à une Europe qui protège.

Le présent rapport vise à rendre compte de l'état d'avancement des actions entreprises et à exposer les prochaines étapes de leur mise en œuvre dans les quatre domaines proposés dans le cadre commun: améliorer la connaissance de la situation; renforcer la résilience; renforcer la capacité des États membres et de l'Union à prévenir les crises, à y faire face et à s'en remettre de manière concertée; et renforcer la coopération avec l'OTAN afin de garantir la complémentarité des mesures. Le présent rapport devrait être lu en liaison avec les rapports d'avancement mensuels sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective.

2. RECONNAÎTRE LE CARACTÈRE HYBRIDE D'UNE MENACE

Les activités hybrides deviennent monnaie courante dans l'environnement de sécurité européen. L'intensité de ces activités est en hausse et suscite de plus en d'inquiétude concernant de possibles immixtions dans les élections, des campagnes de désinformation, des cyberactivités malveillantes et des actes hybrides commis par des auteurs cherchant à radicaliser et à manipuler les membres vulnérables de la société pour les faire agir à leur

[5] La «feuille de route de Bratislava» du Conseil européen du 16 septembre 2016 et la déclaration des dirigeants de vingt-sept États membres et du Conseil européen, du Parlement européen et de la Commission européenne, dite «déclaration de Rome», du 25 mars 2017.

[6] http://www.consilium.europa.eu/fr/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation

[7] Document de réflexion sur l'avenir de la défense européenne, 7.6.2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_fr.pdf

place. Les vulnérabilités à l'égard des menaces hybrides ne s'arrêtent pas aux frontières des États. Ces menaces appellent aussi une réponse coordonnée à l'échelon de l'UE et de l'OTAN. L'évolution de la situation depuis avril 2016 montre que, même si les menaces continuent souvent d'être évaluées isolément, on discerne et on appréhende de mieux en mieux, au sein de l'Union, la nature hybride de certaines activités observées et la nécessité d'une action coordonnée. L'Union européenne poursuivra ses efforts visant à améliorer la connaissance de la situation et la coopération.

***Action nº 1**: les États membres, avec l'appui de la Commission et de la haute représentante, le cas échéant, sont invités à lancer une étude sur les risques hybrides afin de recenser les principales vulnérabilités, y compris certains indicateurs liés aux menaces hybrides, susceptibles d'affecter les réseaux et les structures nationaux et paneuropéens.*

Le Conseil a mis en place un «groupe des Amis de la présidence» composé d'experts des États membres et chargé d'élaborer une enquête générique qui leur permettrait de mieux recenser les indicateurs clés de menaces hybrides, de les intégrer dans des systèmes d'alerte précoce et dans les mécanismes d'évaluation des risques existants et de les partager, le cas échéant. Le mandat a été approuvé et les travaux ont déjà commencé. L'enquête générique devrait être prête avant la fin 2017 et les enquêtes proprement dites pourraient être menées par la suite. La protection contre les menaces hybrides devrait contribuer au renforcement mutuel. Les États membres sont donc encouragés à effectuer ces enquêtes le plus rapidement possible car elles fourniront des informations utiles sur le degré de vulnérabilité et de préparation dans les différents pays d'Europe.

a. AMÉLIORER LA CONNAISSANCE DE LA SITUATION

Le partage des travaux d'analyse et d'évaluation des services de renseignement est essentiel pour réduire l'incertitude et améliorer la connaissance de la situation. Des progrès significatifs ont été accomplis au cours de l'année écoulée. La cellule de fusion de l'UE contre les menaces hybrides a été créée et est aujourd'hui totalement opérationnelle, la task-force «East Stratcom» est en place et la Finlande a ouvert le centre européen de lutte contre les menaces hybrides. Maints travaux ont porté sur l'analyse des outils et leviers de désinformation ou de propagande et ont permis de constater que la coopération se déroule bien entre la task-force «East Stratcom» de l'UE, la cellule de fusion de l'UE contre les menaces hybrides et l'OTAN. On dispose ainsi d'une bonne base pour continuer à renforcer la culture d'analyse et d'évaluation des menaces pesant sur notre sécurité intérieure et extérieure dans une perspective hybride.

Cellule de fusion contre les menaces hybrides

***Action nº 2**: création d'une cellule de fusion de l'UE contre les menaces hybrides au sein de la structure existante de Centre de situation et du renseignement de l'UE, capable de recevoir et d'analyser les informations classifiées et de source ouverte sur les menaces hybrides. Les États membres sont invités à mettre en place des points de contact nationaux sur les menaces hybrides, chargés de coopérer et d'entretenir une communication sécurisée avec la cellule de fusion de l'UE contre les menaces hybrides.*

La cellule de fusion de l'UE contre les menaces hybrides a été établie au sein du Centre de situation et du renseignement de l'UE pour recevoir et analyser des informations classifiées et de source ouverte sur les menaces hybrides, émanant de différentes parties prenantes. Une fois réalisée, l'analyse est partagée au sein de l'UE et parmi les États membres et elle alimente le

processus de prise de décision de l'UE, notamment en fournissant des éléments à intégrer dans les évaluations des risques pour la sécurité réalisées à l'échelon de l'UE. La division «Renseignement» de l'État-major de l'UE contribue au travail de la cellule de fusion en réalisant des analyses militaires. À ce jour, plus de cinquante évaluations et documents d'information sur les questions hybrides ont été produits. Depuis janvier 2017, la cellule rédige un périodique (*Hybrid Bulletin*) qui analyse les menaces et questions hybrides actuelles et est directement distribué au sein des institutions et organes de l'UE ainsi que dans les points de contact nationaux[8]. La cellule jouit, comme prévu, d'une pleine capacité opérationnelle depuis mai 2017. Enfin, des contacts interservices réguliers existent avec la Branche Analyse des menaces hybrides récemment instaurée à l'OTAN, tant pour partager les enseignements tirés de la création de la cellule de fusion que pour échanger des informations (dans le respect de la réglementation de l'UE en matière d'échange d'informations classifiées). La cellule de fusion de l'UE contre les menaces hybrides est en train de déterminer les nouvelles initiatives à prendre pour renforcer la coopération et jouera un rôle essentiel dans le cadre des exercices parallèles UE-OTAN prévus pour l'automne 2017, au cours desquels la capacité de réaction de la cellule de fusion de l'UE contre les menaces hybrides sera mise à l'épreuve et les enseignements tirés seront pris en considération.

Communication stratégique

Action nº 3: la haute représentante étudiera avec les États membres les moyens d'actualiser et de coordonner les capacités en matière de fourniture de communications stratégiques proactives et d'optimiser le recours à des spécialistes du suivi des médias et à des experts linguistiques.

Ces derniers mois, l'amplification des campagnes de désinformation et la propagation systématique de fausses informations dans les médias sociaux font partie d'un éventail de moyens utilisés pour nuire à des adversaires. Lorsque les médias sociaux sont plébiscités par la population, des informations qui paraissent fiables et fondées peuvent influencer l'opinion publique en faveur de certains individus, organisations ou gouvernements. Ces tactiques hybrides ont un objectif plus large consistant à semer la confusion dans nos sociétés et à jeter le discrédit sur les gouvernements démocratiques et nos structures, institutions et élections. Les fausses informations sont souvent propagées par l'intermédiaire de plateformes en ligne (voir également l'action nº 17). La Commission et la haute représentante se félicitent des récentes mesures prises par les plateformes en ligne et les éditeurs de médias d'informations pour lutter contre la désinformation. La Commission continuera d'encourager de telles initiatives spontanées.

La haute représentante a mis en place la task-force «East Stratcom», qui anticipe les cas et les campagnes de désinformation et y réagit. Il en résulte une amélioration considérable de la communication sur les politiques de l'Union dans les pays du voisinage oriental et un renforcement de l'environnement médiatique dans ces pays. Au cours des deux dernières années, la task-force a révélé plus de 3 000 cas de désinformation dans 18 langues. Le lancement prochain d'un nouveau site web (*#EUvsdisinformation*) doté d'un outil de recherche en ligne améliorera sensiblement l'accès des utilisateurs. Toutefois, les travaux de recherche et d'analyse montrent que le nombre de canaux de désinformation et de messages diffusés quotidiennement est nettement plus élevé. Le projet «EU-STRAT», financé par

[8] À ce jour, vingt et un États membres ont désigné des points de contact nationaux. Il s'agit de personnes travaillant dans les capitales des États membres et jouant un rôle stratégique en matière de résilience.

Horizon 2020, porte sur l'analyse de la politique et des médias dans les pays du partenariat oriental.

La haute représentante invite les États membres à soutenir le travail des task-forces «Stratcom» dans le but de contrer plus efficacement la multiplication des menaces hybrides. Cela aidera la task-force «South» à améliorer la communication et les contacts avec le monde arabe, y compris en arabe, et contribuera à déjouer les mystifications et à établir la vérité sur l'Union européenne et ses politiques. L'interaction avec les journalistes locaux contribuera à garantir la transculturation des informations. Les deux task-forces, appuyées par la cellule de fusion de l'UE contre les menaces hybrides, ont pour mission de soutenir et de compléter l'action des États membres en la matière. De plus, la Commission cofinance le réseau européen des communications stratégiques, un réseau collaboratif de vingt-six États membres qui partage les analyses, les bonnes pratiques et les idées en ce qui concerne le recours aux communications stratégiques dans la lutte contre l'extrémisme violent, y compris en matière de désinformation.

Centre d'excellence pour la «lutte contre les menaces hybrides»

Action nº 4: les États membres sont invités à envisager de mettre en place un centre d'excellence pour la «lutte contre les menaces hybrides».

En réponse à l'invitation à créer un centre d'excellence, lancée en avril 2017, la Finlande a institué le centre européen de lutte contre les menaces hybrides. Dix États membres de l'UE[9], la Norvège et les États-Unis en sont membres, et l'Union européenne et l'OTAN ont été invitées à soutenir son comité directeur[10]. Le centre a pour mission d'encourager un dialogue stratégique et d'effectuer des recherches et des analyses en collaboration avec les communautés d'intérêt pour améliorer la résilience et la capacité de réaction, et ainsi contribuer à la lutte contre les menaces hybrides. Il doit aussi accueillir dans l'avenir des exercices de préparation aux menaces hybrides. Le centre a déjà établi des contacts étroits avec la cellule de fusion de l'UE contre les menaces hybrides, et les travaux des deux organisations devraient se compléter. L'UE examine actuellement les moyens d'apporter un soutien concret au centre.

b. RENFORCER LA RÉSILIENCE

Le cadre commun place la résilience (par exemple dans les domaines des transports, des communications, de l'énergie, de la finance ou des infrastructures de sécurité régionales) au cœur de l'action de l'UE visant à résister à la propagande et aux campagnes d'information, aux tentatives de sape ciblant les affaires, les sociétés et les flux économiques, ainsi qu'aux attaques dirigées contre les technologies de l'information et les infrastructures y afférentes. Le renforcement de la résilience y est considéré comme une action préventive et dissuasive destinée à rendre les sociétés plus fortes et à éviter l'intensification des crises à l'intérieur comme à l'extérieur de l'Union. L'apport de l'Union consiste à aider les États membres et les partenaires à renforcer leur résilience, en s'appuyant sur un large éventail d'instruments et de programmes existants. Des progrès importants ont été réalisés en ce qui concerne les actions visant à renforcer la résilience dans des domaines tels que la cybersécurité, les infrastructures

[9] Allemagne, Estonie, Espagne, France, Lettonie, Lituanie, Pologne, Finlande, Suède et Royaume-Uni.
[10] Les autres États membres de l'UE et les alliés membres de l'OTAN peuvent adhérer au centre.

critiques, la protection du système financier contre les utilisations illicites ainsi que la lutte contre l'extrémisme violent et la radicalisation.

Protéger les infrastructures critiques

Action nº 5: la Commission, en coopération avec les États membres et les parties prenantes, recensera des outils communs, y compris des indicateurs, destinés à améliorer la protection et la résilience des infrastructures critiques contre les menaces hybrides dans les secteurs concernés.

Dans le contexte du programme européen de protection des infrastructures critiques (EPCIP), la Commission a fait progresser les travaux visant à déterminer des outils communs, notamment des indicateurs de vulnérabilité, destinés à améliorer la résilience des infrastructures critiques contre les menaces hybrides dans les secteurs concernés. En mai 2017, la Commission a organisé un atelier sur les menaces hybrides pesant sur les infrastructures critiques, auquel ont participé presque tous les États membres, des gestionnaires d'infrastructures critiques, la cellule de fusion de l'UE contre les menaces hybrides ainsi que l'OTAN en qualité d'observateur. Une feuille de route commune ainsi que les étapes du travail futur ont été approuvées sur la base d'un questionnaire envoyé aux autorités nationales des États membres. La Commission consultera de nouveau les parties prenantes à l'automne afin d'adopter des indicateurs avant la fin 2017.

L'Agence européenne de défense s'emploie à recenser les lacunes en matière de capacités et de recherche communes découlant du lien entre les infrastructures énergétiques et les capacités de défense. L'Agence européenne de défense élaborera un document conceptuel à l'automne 2017 ainsi que des actions pilotes de mise au point de méthodes holistiques.

Renforcer la sécurité d'approvisionnement énergétique de l'UE

Action nº 6: la Commission, en coopération avec les États membres, soutiendra les efforts visant à diversifier les sources d'énergie et à promouvoir les normes de sûreté et de sécurité destinées à accroître la résilience des infrastructures nucléaires.

La Commission a présenté des propositions concrètes dans le cadre du paquet sur la sécurité d'approvisionnement en décembre 2016, et le Conseil et le Parlement européen sont parvenus, en avril 2017, à un accord sur le nouveau règlement relatif à la sécurité de l'approvisionnement en gaz, qui vise à prévenir les crises d'approvisionnement. Les nouvelles règles garantiront que les États membres suivent une approche commune, coordonnée à l'échelon régional, en ce qui concerne les mesures relatives à la sécurité d'approvisionnement. L'UE sera ainsi plus à même de se préparer aux pénuries de gaz et d'y faire face en cas de crise ou d'attaque hybride. Pour la première fois, le principe de solidarité s'appliquera: les États membres pourront aider leurs voisins en cas de crise ou d'attaque grave, afin que les foyers et les entreprises d'Europe ne subissent pas de coupure complète et généralisée.

L'UE a aussi progressé dans la mise au point de projets clés visant à diversifier ses voies et sources d'approvisionnement énergétique, conformément au cadre stratégique pour une union de l'énergie et à la stratégie européenne pour la sécurité énergétique. Par exemple, en ce qui concerne le corridor gazier sud-européen, des travaux de construction concrets sont en cours sur tous les grands projets de gazoducs: l'extension du gazoduc du Caucase du Sud, du gazoduc transanatolien et du gazoduc transadriatique, du Shah Deniz II, en amont, ainsi que l'extension du corridor gazier sud-européen vers l'Asie centrale, et notamment vers le Turkménistan. Les importations de gaz naturel liquéfié (GNL) en Europe sont en hausse et

proviennent de nouvelles sources, comme les États-Unis. L'exemple du terminal de Lituanie montre que les projets de diversification peuvent réduire la dépendance vis-à-vis d'un fournisseur unique. Le fait de réaliser davantage d'efforts en matière d'énergie et de mieux utiliser les sources d'énergie locales, notamment les sources renouvelables, contribue également à la diversification des voies et des sources d'approvisionnement.

Dans le domaine de la sûreté nucléaire, la Commission soutient activement – notamment grâce à des ateliers avec les autorités et les régulateurs nationaux – la mise en œuvre cohérente et efficace de la directive sur la sûreté nucléaire et de la directive sur les normes de base, que les États membres doivent avoir transposées avant la fin de 2017 pour la première et avant la fin de 2018 pour la seconde. En outre, le programme Euratom de recherche et de formation contribue au renforcement de la sûreté nucléaire.

Transports et sécurité de la chaîne d'approvisionnement

Action n° 7: la Commission suivra les menaces émergentes dans le secteur des transports et actualisera la législation, le cas échéant. Dans la mise en œuvre de la stratégie de sûreté maritime de l'UE et de la stratégie de l'UE sur la gestion des risques en matière douanière, ainsi que de leurs plans d'action, la Commission et la haute représentante (dans le cadre de leurs compétences respectives), en coordination avec les États membres, examineront la réponse à apporter aux menaces hybrides, notamment celles concernant les infrastructures critiques de transport.

Conformément à sa communication sur l'union de la sécurité, la Commission soutient la réalisation d'évaluations des risques pour la sécurité au niveau de l'UE avec les États membres, le Centre de situation et du renseignement de l'UE et les agences concernées afin de mettre en évidence les menaces pour la sécurité des transports et de soutenir l'élaboration de mesures d'atténuation efficaces et proportionnées. Le crash du vol MH17 de la Malaysia Airlines dans l'est de l'Ukraine en 2014 a attiré l'attention sur le risque lié au survol des zones de conflit. Conformément aux recommandations de la task-force européenne de haut niveau sur les zones de conflit[11], la Commission a mis au point, avec le soutien d'experts nationaux de l'aéronautique et de la sécurité et en collaboration avec le SEAE, une méthode d'«évaluation commune du risque au niveau de l'UE» permettant d'échanger des informations classifiées et d'établir un tableau commun des risques. En mars 2017, l'Agence européenne de la sécurité aérienne (AESA) a publié le premier bulletin d'information sur les zones de conflit[12], sur la base des résultats de cette évaluation commune du risque au niveau de l'UE. La Commission envisage d'étendre les activités d'évaluation du risque menées dans le domaine de la sécurité aérienne à d'autres modes de transport (ferroviaire ou maritime, par exemple), et des propositions seront présentées en 2018. En juin 2017, la Commission, le SEAE et les États membres ont entamé un exercice d'évaluation des risques pour la sécurité ferroviaire afin de recenser les points faibles et de déterminer les éventuelles mesures à prendre pour atténuer les risques.

Des efforts considérables en matière de sécurité aérienne et de gestion du trafic aérien ont également été réalisés dans le cadre des projets de recherche portant sur la sécurité au titre du 7e programme-cadre et d'Horizon 2020. Dans le domaine de l'aviation civile, la Commission,

11 https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

12 https://ad.easa.europa.eu/czib-docs/page-1

en concertation avec l'Agence européenne de la sécurité aérienne et les parties prenantes, est en train d'élaborer deux nouvelles initiatives visant à renforcer la cybersécurité, qui portent également sur les menaces hybrides: l'établissement de l'équipe d'intervention en cas d'urgence informatique dans le domaine de l'aviation, et la création d'une task-force sur la cybersécurité au sein de l'entreprise commune pour la recherche sur la gestion du trafic aérien dans le ciel unique européen (SESAR), qui est chargée de la gestion du trafic aérien dans le ciel unique européen. L'Agence européenne de défense fournit des informations militaires en ce qui concerne la cybernétique dans l'aviation à l'entreprise commune SESAR, mais aussi à l'Agence européenne de la sécurité aérienne, via la «plateforme européenne de coordination stratégique sur la cybersécurité», qui, à la demande des États membres et de l'industrie, contribuera à coordonner au niveau de l'UE toutes les activités liées au secteur aéronautique. Conformément à la feuille de route sur la cybersécurité dans le secteur aéronautique, l'Agence européenne de la sécurité aérienne a analysé les règles existantes afin d'en détecter les lacunes, et a notamment œuvré à la définition et à l'établissement du centre européen pour la cybersécurité dans l'aviation; celui-ci est désormais opérationnel et coopère avec l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'UE (CERT-UE) (le protocole d'accord a été signé en février 2017), en produisant des analyses des menaces dans le secteur aéronautique, et avec Eurocontrol (une feuille de route en matière de coopération a été adoptée), tandis qu'un site web pour la diffusion d'analyses de source ouverte a été mis en place. D'ici à l'automne 2017, un programme de normalisation et un mécanisme d'échange d'informations sécurisé seront adoptés.

Gestion des risques en matière douanière

Sur le plan douanier, la Commission œuvre à l'amélioration significative du système d'informations anticipées sur les marchandises et de gestion des risques en matière douanière. Ce système couvre l'ensemble des risques douaniers, y compris en ce qui concerne les menaces pour la sécurité et l'intégrité des chaînes d'approvisionnement internationales et pour les infrastructures critiques concernées (par exemple les menaces directes que représentent les importations pour les installations portuaires, les aéroports ou les frontières terrestres). L'amélioration vise à garantir que les douanes de l'UE obtiennent toutes les informations nécessaires de la part des opérateurs en ce qui concerne les mouvements de marchandises, qu'elles puissent assurer un partage plus efficace de ces informations entre les États membres, qu'elles appliquent, en matière de risque, tant des règles communes que des règles spécifiques aux États membres, et qu'elles soient en mesure de repérer plus efficacement les envois à risque en coopérant de façon plus intensive avec d'autres autorités, en particulier d'autres organismes de répression et de sécurité. Les développements informatiques indispensables à la mise en œuvre de cette amélioration par la Commission sont actuellement en phase de démarrage, et les investissements nécessaires à l'échelon central seront lancés dans les mois à venir.

Espace

Action nº 8: dans le contexte de la stratégie spatiale et du plan d'action européen de la défense, la Commission proposera d'accroître la résilience des infrastructures spatiales contre les menaces hybrides, notamment par une éventuelle extension de la portée de la surveillance de l'espace et du suivi des objets en orbite pour couvrir les menaces hybrides, par la préparation de la prochaine génération de télécommunications gouvernementales par satellite au niveau européen et par l'introduction de Galileo dans les infrastructures critiques tributaires de la synchronisation temporelle.

Lorsqu'elle préparera le cadre réglementaire sur les télécommunications gouvernementales par satellite (GovSatCom) et sur la surveillance de l'espace et le suivi des objets en orbite en 2018, la Commission incorporera dans son évaluation les aspects liés à la résilience face aux menaces hybrides. Conformément à la stratégie spatiale, lors de la préparation de l'évolution de Galileo et de Copernicus, la Commission évaluera l'apport potentiel de ces services en matière d'atténuation de la vulnérabilité des infrastructures critiques. Le rapport d'évaluation devrait être prêt à l'automne 2017 et la proposition sur la prochaine génération de Copernicus et de Galileo devrait être présentée en 2018. L'Agence européenne de défense travaille sur des projets collaboratifs de développement des capacités dans le domaine des communications spatiales, du positionnement à des fins militaires, de la navigation et de la datation, ainsi que de l'observation de la terre. Tous les projets seront axés sur les exigences en matière de résilience, compte tenu des menaces hybrides actuelles et émergentes.

Les capacités de défense

Action nº 9: la haute représentante, le cas échéant avec le soutien des États membres, en liaison avec la Commission, présentera des propositions d'adaptation des capacités de défense et des propositions de développement importantes pour l'UE dans le but spécifique de lutter contre les menaces hybrides pesant sur un ou plusieurs États membres.

En 2016 et 2017, l'Agence européenne de défense a réalisé trois exercices de simulation basés sur des scénarios impliquant des menaces hybrides, en concertation avec la Commission, le SEAE et des experts des États membres. Les conclusions de ces exercices seront utilisées aux fins du réexamen du plan de développement des capacités, afin que les développements de capacités essentielles qui en résulteront, et qui sont nécessaires à la lutte contre les menaces hybrides, figurent parmi les nouvelles priorités de l'UE en matière de développement des capacités. Le travail de réexamen du catalogue des besoins 2005 tiendra compte de la dimension relative aux menaces hybrides. En avril 2017, l'Agence européenne de défense a achevé un rapport d'analyse sur les conséquences militaires que pourraient avoir des attaques hybrides dirigées contre des infrastructures portuaires critiques, rapport qui sera examiné lors d'un atelier avec des experts maritimes en octobre 2017. Une autre analyse spécifique portant sur le rôle des forces militaires dans la lutte contre les minidrones est prévue pour 2018. En outre, les priorités en termes de capacités visant à renforcer la résilience face aux menaces hybrides recensées par les États membres pourraient également être admissibles à une aide au titre du Fonds européen de la défense dès 2019. La Commission invite les colégislateurs à faire en sorte que l'adoption soit rapide et prie les États membres de présenter des propositions relatives à des projets de capacités visant à renforcer la résilience de l'UE face aux menaces hybrides.

Action nº 10: la Commission, en collaboration avec les États membres, améliorera la sensibilisation aux menaces hybrides et la résilience face à celles-ci dans le cadre des mécanismes de préparation et de coordination existants, et notamment du comité de sécurité sanitaire.

Afin d'améliorer la préparation et la résilience face aux menaces hybrides, y compris le renforcement des capacités au sein des systèmes de santé et des systèmes alimentaires, la Commission soutient les États membres en organisant des formations et des exercices de simulation, en facilitant l'élaboration d'orientations sur la base de l'échange d'expériences et en finançant des actions conjointes. Ces activités de soutien sont menées au titre du cadre de sécurité sanitaire de l'UE relatif aux menaces transfrontières graves pour la santé et du programme de santé publique pour la mise en œuvre du règlement sanitaire international, un socle législatif qui a force obligatoire pour 196 pays (dont les États membres) et qui vise à

prévenir et contrer les risques transfrontières graves pour la santé publique dans le monde entier. Afin de tester la préparation et la réaction intersectorielles dans le secteur de la santé, les services de la Commission mèneront, à l'automne 2017, un exercice sur les menaces hybrides complexes et multidimensionnelles. La Commission et les États membres préparent actuellement une action commune relative à la vaccination, qui porte entre autres sur la prévision de l'approvisionnement et de la demande de vaccins et sur la recherche en matière de processus innovants de fabrication de vaccins, dans le but de renforcer l'approvisionnement en vaccins et d'améliorer la sécurité sanitaire au niveau de l'UE (2018-2020). La Commission collabore également avec l'Autorité européenne de sécurité des aliments et le Centre européen de prévention et de contrôle des maladies pour s'adapter aux techniques d'investigation scientifique avancées de manière à pouvoir identifier les menaces sanitaires et leur origine avec plus de précision et, en conséquence, gérer rapidement les foyers constituant une menace pour la sécurité des aliments. La Commission a mis en place un réseau de bailleurs de fonds en faveur de la recherche (Collaboration mondiale en matière de recherche pour la préparation aux maladies infectieuses) afin de pouvoir réagir de manière coordonnée en matière de recherche dans les 48 heures qui suivent l'apparition de tout foyer de maladie significatif.

Action n° 11: la Commission encourage les États membres à mettre en place et à exploiter pleinement, de façon prioritaire, un réseau regroupant les 28 CSIRT et le CERT-EU (équipe d'intervention interinstitutionnelle de l'UE en cas d'urgence informatique) et un cadre de coopération stratégique. En coordination avec les États membres, elle s'assurera de la conformité des initiatives relatives aux cybermenaces mises en place dans certains secteurs (aéronautique, énergétique et maritime, par exemple) avec les capacités intersectorielles couvertes par la directive SRI, aux fins de la mise en commun d'informations, d'expertises et de réactions rapides.

Les récentes cyberattaques mondiales, qui ont consisté à désactiver des milliers de systèmes informatiques au moyen de rançongiciels et de logiciels malveillants, ont une nouvelle fois mis en lumière la nécessité de renforcer de toute urgence les actions en faveur de la cyber-résilience et de la cybersécurité au sein de l'UE. Comme annoncé dans l'examen à mi-parcours de la stratégie pour le marché unique numérique, la Commission et la haute représentante réexaminent actuellement la stratégie de cybersécurité de l'UE de 2013, et prévoient notamment l'adoption d'un train de mesures pour septembre 2017. L'objectif sera de permettre une réaction intersectorielle plus efficace face à ces menaces et de renforcer ainsi la confiance dans la société et l'économie numériques, mais aussi de revoir le mandat de l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information), afin de définir son rôle dans le nouvel écosystème de la cybersécurité. Le Conseil européen[13] s'est félicité de l'intention de la Commission de revoir la stratégie de cybersécurité.

L'adoption de la directive sur la sécurité des réseaux et de l'information[14], en juillet 2016, a marqué une étape décisive vers la construction d'une résilience à l'échelon européen en matière de cybersécurité. La directive établit les premières règles européennes en matière de cybersécurité, améliore les capacités liées à la cybersécurité et renforce la coopération entre les États membres. Elle exige aussi que les entreprises exerçant leurs activités dans des secteurs critiques prennent les mesures de sécurité appropriées et signalent tout cyberincident grave à l'autorité nationale concernée. Ces secteurs comprennent l'énergie, les transports,

[13] Conclusions du Conseil européen des 22 et 23 juin 2017.

[14] 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 (JO L 194 du 19.7.2016, p. 1).

l'eau, les soins de santé, la banque et les infrastructures des marchés financiers. Les marchés électroniques, les services d'informatique en nuage et les moteurs de recherche devront en faire autant. Le groupe de coopération sur les services de réseau et d'information (établi par la Commission en 2016), qui est chargé d'éviter la fragmentation du marché, veillera à une mise en œuvre cohérente dans différents secteurs et au niveau transfrontière. Dans ce contexte, la directive sur la sécurité des réseaux et de l'information est considérée comme le cadre de référence pour toutes les initiatives sectorielles dans le domaine de la cybersécurité. En outre, elle crée le réseau des centres de réponse aux incidents de sécurité informatique (CSIRT), qui regroupe toutes les parties prenantes. Parallèlement, la Commission et le CERT-EU suivent activement la situation en matière de cybermenaces et ils échangent des informations avec les autorités nationales pour faire en sorte que les systèmes informatiques des institutions de l'UE soient sûrs et résilients face aux cyberattaques. L'incident causé en mai 2017 par le rançongiciel WannaCry a donné au réseau CSIRT l'occasion d'entamer des échanges d'informations opérationnelles et de coopérer par la diffusion de conseils. L'équipe d'intervention interinstitutionnelle de l'UE en cas d'urgence informatique était en contact étroit avec le Centre européen de lutte contre la cybercriminalité (EC3) d'Europol, les centres de réponse aux incidents de sécurité informatique (CSIRT) des pays touchés, les unités spécialisées en cybercriminalité et les partenaires clés du secteur afin de réduire la menace et d'aider les victimes. Les échanges de rapports de situation nationaux ont aidé l'ensemble de l'UE à acquérir une connaissance commune de la situation. Cette expérience a permis au réseau d'être mieux préparé pour les incidents ultérieurs (tels que NonPetya). Plusieurs problèmes ont aussi été détectés et sont en cours de résolution.

<u>Action nº 12</u>: la Commission, en coordination avec les États membres, coopérera avec l'industrie dans le cadre d'un partenariat public-privé contractuel en matière de cybersécurité dans le but de développer et de tester des technologies afin d'améliorer la protection des utilisateurs et des infrastructures contre les cyberaspects des menaces hybrides.

En juillet 2016, la Commission, en coordination avec les États membres, a signé avec l'industrie un partenariat public-privé contractuel en matière de cybersécurité, prévoyant d'investir jusqu'à 450 millions d'euros dans le cadre du programme de l'UE pour la recherche et l'innovation Horizon 2020, afin de développer et de tester des technologies visant à améliorer la protection des utilisateurs et des infrastructures contre les cybermenaces et les menaces hybrides. Ce partenariat a débouché sur le premier programme de recherche stratégique paneuropéen, axé sur le renforcement de la résilience des infrastructures critiques et de celle des citoyens face aux cyberattaques. Il a amélioré la coordination entre les parties prenantes, ce qui a conduit à des gains d'efficience et d'efficacité en matière de financement de la cybersécurité dans le cadre d'Horizon 2020. Le partenariat s'intéresse en parallèle aux questions qui ont trait à la certification en matière de cybersécurité des technologies de l'information et des communications, ainsi qu'aux moyens de résoudre le problème de la grave pénurie de professionnels ayant des compétences en cybersécurité. Compte tenu des besoins considérables dans la recherche civile et du niveau élevé de résilience requis dans le domaine de la défense, le groupe chargé de la recherche et de la technologie cybernétiques à l'Agence européenne de défense (AED) apporte sa contribution dans les domaines de recherche retenus par l'organisation européenne pour la cybersécurité dans son programme stratégique de recherche et d'innovation.

<u>Action nº 13</u>: la Commission fournira des orientations aux détenteurs d'actifs dans des réseaux intelligents en vue de l'amélioration de la cybersécurité de leurs installations. Dans le contexte de l'initiative sur l'organisation du marché de l'électricité, la Commission envisagera de proposer des «plans de préparation aux risques» et des règles de procédure permettant des échanges

d'informations et garantissant une solidarité entre les États membres en cas de crise, y compris des règles en matière de prévention et d'atténuation des cyberattaques.

Dans le secteur de l'énergie, la Commission est en train d'élaborer une stratégie sectorielle en matière de cybersécurité avec la mise en place de la plateforme d'experts en énergie sur la cybersécurité, afin de renforcer la mise en œuvre de la directive SRI. Une étude de février 2017 a recensé les meilleures techniques disponibles pour renforcer le niveau de cybersécurité des compteurs intelligents, à l'appui de cette plateforme. La Commission a également créé une plateforme internet (*Incident and Threat Information Sharing EU Centre*) pour l'analyse et le partage des informations relatives aux cybermenaces et aux cyberincidents dans le secteur de l'énergie.

Renforcer la résilience du secteur financier face aux menaces hybrides

Action nº 14: la Commission, en collaboration avec l'ENISA[15], les États membres, les instances internationales, européennes et nationales compétentes et les établissements financiers, encouragera et facilitera les plateformes et les réseaux d'échanges d'informations sur les menaces et examinera les éléments qui entravent l'échange de telles informations.

Reconnaissant que les cybermenaces comptent parmi les risques majeurs pour la stabilité financière, la Commission a révisé le cadre réglementaire relatif aux services de paiement dans l'Union européenne, qui doit maintenant être mis en œuvre. La directive révisée sur les services de paiement[16] a introduit de nouvelles dispositions renforçant la sécurité des instruments de paiement et l'authentification des clients afin de réduire la fraude, particulièrement dans les paiements en ligne. Le nouveau cadre législatif sera applicable à partir de janvier 2018. Actuellement, la Commission, assistée de l'Autorité bancaire européenne et en concertation avec les parties prenantes, élabore des normes techniques réglementaires pour une authentification forte des clients et une communication sécurisée commune afin d'assurer effectivement la sécurité des opérations de paiement; ces normes devraient être publiées avant la fin de 2017. Par ailleurs, sur le plan international, la Commission a collaboré étroitement avec les partenaires du G7 à l'élaboration des principes fondamentaux de la cybersécurité dans le secteur financier («*G7 fundamental principles of cyber security in the financial sector*»), qui ont été approuvés en octobre 2016 par les ministres des finances et les gouverneurs des banques centrales du G7. Ces principes s'adressent aux entités du secteur financier (privées et publiques) et contribuent à une approche coordonnée de la cybersécurité au sein du secteur financier, le but étant que des solutions communes soient mises en œuvre face aux cybermenaces, en particulier face à leur multiplication et à leur sophistication croissante.

Transports

Action nº 15: la Commission et la haute représentante (dans leurs domaines de compétence respectifs), en coordination avec les États membres, examineront la réponse à apporter aux menaces hybrides, et notamment aux menaces ayant trait à des cyberattaques dans le secteur des transports.

[15] Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information.
[16] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (JO L 337 du 23.12.2015, p. 35).

La mise en œuvre du plan d'action pour la stratégie de sûreté maritime de l'UE[17] permettra de rompre avec le fonctionnement en vase clos des autorités civiles et militaires dans le domaine de l'échange d'informations et de l'utilisation partagée des ressources. Une démarche englobant l'ensemble de l'administration a eu pour effet d'accroître la coopération entre divers acteurs. Un programme de recherche stratégique commun de la Commission et du SEAE associant les sphères civile et militaire devrait être mené à bien avant la fin de l'année 2017 et s'achever par un dernier atelier sur la protection des infrastructures maritimes critiques. À l'avenir, ces travaux pourraient être élargis et porter également sur la menace émergente que représentent les interférences en dehors des eaux nationales pour les conduites sous-marines, le transfert d'énergie, les fibres optiques et les câbles de communication traditionnels.

Une récente étude[18] a examiné la capacité d'évaluation des risques des autorités nationales exerçant des fonctions de garde-côtes. Elle a mis en évidence les obstacles les plus importants à la collaboration et a émis des recommandations quant aux solutions pratiques à appliquer afin de renforcer la coopération entre les autorités maritimes à l'échelon de l'UE et à l'échelon national dans ce domaine spécifique. L'évaluation des risques est essentielle pour contrer les menaces maritimes; elle est encore plus déterminante pour l'appréciation et la prévention des menaces hybrides, car celles-ci appellent des considérations supplémentaires, plus complexes. Les résultats de cette étude seront présentés à différents forums de garde-côtes, afin que les recommandations émises puissent être analysées et mises en œuvre pour renforcer la coopération dans ce domaine, les principaux objectifs étant la préparation et la capacité de réaction aux menaces hybrides.

Combattre le financement du terrorisme

Action nº 16: la Commission mettra à profit la mise en œuvre du plan d'action destiné à renforcer la lutte contre le financement du terrorisme pour contribuer aussi à la lutte contre les menaces hybrides.

Les auteurs de menaces hybrides et leurs partisans ont besoin d'argent pour exécuter leurs plans. Les efforts déployés par l'UE contre le crime organisé et le financement du terrorisme dans le cadre du programme européen en matière de sécurité et du plan d'action destiné à renforcer la lutte contre le financement du terrorisme peuvent également contribuer à la lutte contre les menaces hybrides. En décembre 2016, la Commission a présenté trois propositions législatives, portant notamment sur l'introduction de sanctions pénales en lien avec le blanchiment de capitaux et les paiements illicites en espèces, ainsi que sur le gel et la confiscation des avoirs[19].
Tous les États membres devaient transposer pour le 26 juin 2017 la quatrième directive antiblanchiment[20], et en juillet 2016, la Commission a présenté une proposition législative ciblée destinée à compléter et à renforcer ladite directive par des mesures supplémentaires[21].

---

[17] http://data.consilium.europa.eu/doc/document/ST-17002-2014-INIT/fr/pdf, ainsi que le 2e rapport sur la mise en œuvre du plan d'action pour la stratégie de sûreté maritime de l'UE, présenté aux États membres le 21 juin 2017.
[18] Étude intitulée «Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions», 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies.
[19] Troisième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2016) 831 final].
[20] Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) nº 648/2012 du Parlement européen et du Conseil et abrogeant la directive

Le 26 juin 2017, la Commission a publié l'évaluation supranationale des risques prévue par la quatrième directive antiblanchiment. Elle a également présenté une proposition de règlement visant à empêcher l'importation et le stockage dans l'Union de biens culturels exportés illicitement depuis un pays tiers[22]. Dans le courant de cette année, la Commission rendra compte de son évaluation en cours de la nécessité de prendre des mesures supplémentaires pour surveiller le financement du terrorisme au sein de l'UE. Actuellement, elle réexamine aussi la législation relative à la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces[23].

Le huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective donne de plus amples précisions sur l'état d'avancement de la mise en œuvre du plan d'action destiné à renforcer la lutte contre le financement du terrorisme.

Promouvoir les valeurs communes de l'UE et des sociétés inclusives, ouvertes et résilientes

Renforcer la résilience face à la radicalisation et à l'extrémisme violent

La radicalisation religieuse et idéologique, les conflits ethniques et les conflits de minorités peuvent naître à l'instigation d'acteurs extérieurs, soit du fait d'un soutien apporté à des groupes spécifiques, soit du fait de manœuvres visant à attiser les conflits entre groupes. D'autres périls sont apparus, tels que les menaces provenant d'acteurs isolés, les nouvelles voies de radicalisation, notamment dans le contexte de la crise migratoire, ainsi que la montée de l'extrémisme de droite (incluant la violence contre les migrants) et les risques de polarisation. Alors que les travaux sur la radicalisation se poursuivent dans le contexte de l'union de la sécurité, ils peuvent aussi avoir une utilité indirecte en rapport avec les menaces hybrides, sachant que des personnes vulnérables à la radicalisation peuvent être manipulées par des auteurs de menaces hybrides.

Action nº 17: la Commission met en œuvre les actions de lutte contre la radicalisation figurant dans le programme européen en matière de sécurité et analyse la nécessité de renforcer les procédures de retrait des contenus illicites, en demandant aux intermédiaires de faire preuve de diligence dans la gestion des réseaux et des systèmes.

Prévenir la radicalisation

La Commission continue d'apporter une réponse multidimensionnelle à la radicalisation, comme elle l'a exposé dans sa communication de juin 2016 sur le soutien à la prévention de la radicalisation conduisant à l'extrémisme violent[24], dans laquelle elle définit des actions clés, telles que la promotion d'une éducation ouverte à tous et des valeurs communes, la lutte contre la propagande extrémiste en ligne et contre la radicalisation en milieu carcéral, le

2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission (Texte présentant de l'intérêt pour l'EEE) (JO L 141 du 5.6.2015, p. 73).

[21] Pour plus de détails, consulter le «troisième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective» [COM(2016) 831 final] et le huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2017) 354 final].

[22] COM(2017) du 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final.

[23] Huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2017) 354 final].

[24] https://ec.europa.eu/transparency/regdoc/rep/1/2016/FR/1-2016-379-FR-F1-1.PDF

renforcement de la coopération avec les pays tiers, et l'intensification de la recherche afin de mieux comprendre la nature évolutive de la radicalisation et de mieux éclairer les réponses politiques. Le réseau de sensibilisation à la radicalisation (RSR) a été au premier plan de l'action de la Commission pour aider les États membres dans ce domaine, en collaboration avec les acteurs de terrain locaux au niveau des communautés. Le huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective donne plus de précisions à cet égard[25].

Radicalisation et discours haineux en ligne

Dans le droit fil du programme européen en matière de sécurité[26], la Commission a pris des mesures pour réduire le volume de contenus illicites disponibles en ligne, notamment par l'intermédiaire de l'unité de l'UE chargée, au sein d'Europol, du signalement des contenus sur Internet, et du Forum de l'UE sur l'internet[27]. Des progrès significatifs ont également été accomplis dans le cadre du code de conduite pour lutter contre les discours haineux illégaux en ligne[28]. Le huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective donne plus de précisions à cet égard[29]. Ces actions seront renforcées, compte tenu également des conclusions du Conseil européen[30], du sommet du G7[31] et du sommet du G20 à Hambourg[32].

Les plateformes en ligne ont un rôle clé à jouer dans le combat contre les contenus illicites ou potentiellement dommageables. Dans le cadre de la stratégie pour le marché unique numérique, comme indiqué dans l'examen à mi-parcours[33], la Commission assurera une meilleure coordination des dialogues avec les plateformes, en s'attachant aux mécanismes et solutions techniques pour le retrait des contenus illicites. Le cas échéant, l'objectif devrait être d'appuyer ces mécanismes par des orientations sur des aspects tels que la notification et le retrait des contenus illicites. La Commission formulera également des orientations concernant les règles en matière de responsabilité.

Renforcer la coopération avec les pays tiers

***Action nº 18:** en collaboration avec la Commission, la haute représentante lancera une étude sur les risques hybrides dans les régions du voisinage. La haute représentante, la Commission et les États membres feront usage des instruments à leur disposition pour renforcer les capacités des partenaires et améliorer leur résilience aux menaces hybrides. Des missions de la PSDC pourraient être déployées, indépendamment ou en complément des instruments de l'UE, pour aider les partenaires à renforcer leurs capacités.*

[25] COM(2017) 354 final.
[26] Pour en savoir plus, voir le huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2017) 354 final].
[27] Pour en savoir plus, voir le huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2017) 354 final].
[28] Code de conduite visant à combattre les discours de haine illégaux en ligne, 31 mai 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[29] Pour en savoir plus, voir le huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2017) 354 final].
[30] Conclusions du Conseil des 22 et 23 juin 2017.
[31] Sommet du G7 à Taormina, Italie, les 26 et 27 mai 2017.
[32] Sommet du G20 à Hambourg, Allemagne, les 7 et 8 juillet 2017.
[33] Cf. ci-dessus la communication de la Commission COM(2017) 228 final.

L'Union européenne met à présent davantage l'accent, dans le domaine de la sécurité, sur le renforcement des capacités et de la résilience dans les pays partenaires, notamment en tirant parti du lien entre sécurité et développement, en renforçant la dimension «sécurité» de la politique européenne de voisinage révisée et en engageant des dialogues en matière d'antiterrorisme et de sécurité avec les pays du pourtour méditerranéen. Dans cette optique, une étude sur les risques a été lancée dans le cadre d'un projet pilote en coopération avec la République de Moldavie dans le but de contribuer à recenser les principales vulnérabilités du pays et de garantir que l'aide de l'UE porte spécifiquement sur ces aspects. Les résultats du projet pilote ont montré que l'étude en elle-même avait été jugée utile. En s'appuyant sur l'expérience acquise, la Commission et le SEAE feront des recommandations quant à la priorité à donner aux actions relevant du volet «Efficacité, communications stratégiques, protection des infrastructures critiques et cybersécurité».

À l'avenir, d'autres pays voisins pourraient bénéficier de cette étude, en partant de cette première expérience, sous réserve que des adaptations reflétant les différentes situations locales et les menaces spécifiques dans les pays respectifs soient apportées et que tout double-emploi avec les dialogues en cours en matière d'antiterrorisme et de sécurité soit évité. Sur un plan plus général, le 7 juin 2017, la Commission et la haute représentante ont adopté une communication conjointe intitulée «Une approche stratégique de la résilience dans l'action extérieure de l'UE»[34]. L'objectif est d'aider les pays partenaires à devenir plus résilients face aux défis mondiaux d'aujourd'hui. Cette communication prend acte de la nécessité de passer d'une approche d'endiguement des crises à une approche à long terme, plus structurelle, des vulnérabilités, en mettant l'accent sur l'anticipation, la prévention et la préparation.

La cyber-résilience pour le développement

L'UE soutient les pays situés en dehors de l'Europe afin de renforcer la résilience de leurs réseaux d'information. La numérisation croissante renferme une dimension «sécurité» qui soulève des difficultés particulières en matière de résilience des systèmes de réseaux d'information à l'échelle mondiale, car les cyberattaques ne connaissent pas de frontières. L'UE aide les pays tiers à étoffer leurs capacités pour qu'ils soient en mesure de prévenir les défaillances accidentelles et les cyberattaques ou d'y répondre de manière adéquate. À la suite d'un projet pilote en matière de cybersécurité mené dans l'ancienne République yougoslave de Macédoine, au Kosovo[35] et en Moldavie, qui s'est achevé en 2016, la Commission lancera un nouveau programme pour renforcer la cyber-résilience de pays tiers, principalement en Afrique et en Asie, au cours de la période 2017-2020, mais également en Ukraine. Son objectif est d'accroître la sécurité et la préparation des infrastructures et des réseaux d'information critiques dans des pays tiers sur la base d'une approche impliquant l'ensemble des instances de gouvernement, en assurant simultanément le respect des droits de l'homme et de l'État de droit.

Sûreté aérienne

[34]Communication conjointe au Parlement européen et au Conseil: Une approche stratégique de la résilience dans l'action extérieure de l'UE, JOIN (2017) 21 final.

[35] Cette désignation est sans préjudice des positions sur le statut et est conforme à la résolution 1244 du Conseil de sécurité des Nations unies ainsi qu'à l'avis de la CIJ sur la déclaration d'indépendance du Kosovo.

L'aviation civile reste une cible majeure et symbolique pour les terroristes mais pourrait aussi être visée dans le cadre d'une campagne hybride. L'UE s'est dotée d'un cadre solide en matière de sûreté aérienne; cependant, les vols en provenance de pays tiers risquent d'être plus vulnérables. Conformément à la résolution 2309 (2016) du Conseil de sécurité de l'ONU, la Commission multiplie les démarches pour renforcer les capacités des pays tiers. En janvier 2017, elle a lancé une nouvelle évaluation intégrée des risques en vue de hiérarchiser et de coordonner les efforts dans le domaine du renforcement des capacités à l'échelon de l'UE et des États membres, ainsi qu'avec les partenaires internationaux. En 2016, la Commission a lancé un projet quadriennal relatif à la sûreté dans l'aviation civile en Afrique et dans la péninsule arabique qui vise à lutter contre la menace terroriste planant sur l'aviation civile. Le projet est axé sur le partage d'expertise entre les États partenaires et les experts des États membres de la Conférence européenne de l'aviation civile, ainsi que sur les activités de tutorat, de formation et d'accompagnement. Ces activités devraient encore s'intensifier au cours de l'année 2017.

c. 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. La surveillance et les exercices réguliers se poursuivront.

Action nº 19: ***en coordination avec les États membres, la haute représentante et la Commission mettront en place un protocole opérationnel commun et procéderont à des exercices réguliers visant à améliorer les capacités de prise de décisions stratégiques en réaction aux menaces hybrides complexes, en s'appuyant sur les procédures de gestion des crises et le dispositif intégré pour une réaction au niveau politique dans les situations de crise.***

Le cadre commun recommandait l'établissement de mécanismes permettant de réagir rapidement à des événements déclenchés par des menaces hybrides, à coordonner avec les mécanismes de réaction[36] et systèmes d'alerte précoce de l'UE. À cette fin, les services de la Commission et le SEAE ont mis au point le protocole opérationnel de l'UE de lutte contre les menaces hybrides (*EU Playbook*)[37], qui précise les modalités de coordination, de fusion et d'analyse des renseignements, de contribution au processus décisionnel, de réalisation des exercices et de la formation, ainsi que de la coopération avec les organisations partenaires, notamment l'OTAN, en cas de menace hybride. De son côté, l'OTAN a élaboré un protocole pour une interaction renforcée entre l'OTAN et l'UE en matière de prévention et de neutralisation des menaces hybrides dans les domaines de la cyberdéfense, des communications stratégiques, de la connaissance des situations et de la gestion de crise. Le protocole de l'UE sera testé à l'automne 2017, dans le cadre de l'exercice parallèle et coordonné de l'Union européenne, qui implique une interaction avec l'OTAN.

[36] Le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise (IPCR) du Conseil, le système ARGUS de la Commission et le mécanisme de réaction aux crises (CRM) du SEAE.
[37] Document de travail des services de la Commission (2016) 227 adopté le 7 juillet 2016.

<u>Action nº 20</u>: la Commission et la haute représentante, dans leurs domaines respectifs de compétence, examineront l'applicabilité et les 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'article 42, paragraphe 7, du TUE envisage l'agression armée sur le territoire d'un État membre, tandis que l'article 222 du TFUE (clause de solidarité) évoque une attaque terroriste ou une catastrophe naturelle ou d'origine humaine sur le territoire d'un État membre. Ce dernier article est davantage susceptible d'être invoqué en cas d'attaques hybrides, lesquelles se caractérisent par une combinaison d'actions criminelles et subversives. L'invocation de la clause de solidarité déclenche une coordination au niveau du Conseil (dispositif intégré pour une réaction au niveau politique dans les situations de crise, IPCR) et la participation des institutions, agences et organes concernés de l'UE, ainsi que le recours aux programmes et mécanismes d'assistance de l'UE. La décision 2014/415/UE du Conseil prévoit les modalités de mise en œuvre de la clause de solidarité par l'Union. Ces modalités d'application restent valides, et il n'y a pas lieu de réviser ladite décision du Conseil. En cas d'attaque hybride accompagnée d'une agression armée, l'article 42, paragraphe 7 pourrait aussi être invoqué. Dans une telle éventualité, l'aide et l'assistance seraient apportées aussi bien par les États membres que par l'UE. La Commission et la haute représentante continueront à évaluer les moyens les plus efficaces pour faire face à de telles attaques.

Le protocole opérationnel de l'UE susvisé contribue directement à cette évaluation; il sera mis en pratique dans le cadre de l'exercice parallèle et coordonné (PACE) de l'UE en octobre 2017. Cet exercice permettra de tester les divers mécanismes et les capacités d'interaction de l'UE, le but étant d'accélérer la prise de décision lorsque l'ambiguïté créée par une menace hybride nuit à la clarté.

<u>Action nº 21:</u> en coordination avec les États membres, la haute représentante intégrera, exploitera et coordonnera 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 destinée à appuyer la PESC/PSDC, 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

d. COOPÉRATION UE-OTAN

<u>Action nº 22</u>: en coordination avec la Commission, la haute représentante continuera d'entretenir un dialogue informel et renforcera la coopération et la coordination avec l'OTAN en ce qui concerne la connaissance de la situation, les communications stratégiques, la cybersécurité, la prévention et la gestion des crises afin de lutter contre les menaces hybrides, dans le respect des principes d'inclusion et d'autonomie décisionnelle de chaque organisation.

Sur la base de la déclaration commune signée par le président du Conseil européen, le président de la Commission européenne et le secrétaire général de l'OTAN à Varsovie le 8 juillet 2016, l'UE et l'OTAN ont mis au point un ensemble commun de quarante-deux propositions pour sa mise en œuvre, lequel a été approuvé le 6 décembre 2016, lors de

processus parallèles distincts, par les Conseils respectifs de l'UE et de l'OTAN[38]. En juin 2017, la haute représentante/vice-présidente et le secrétaire général de l'OTAN ont publié un rapport sur l'état d'avancement général des quarante-deux actions prévues dans la déclaration commune. La lutte contre les menaces hybrides est l'un des sept domaines de coopération définis dans la déclaration commune, et dix des quarante-deux actions y sont rattachées. Il ressort du rapport que les efforts conjoints entrepris au cours de l'année écoulée ont produit des résultats substantiels. De nombreuses actions spécifiques visant à lutter contre les menaces hybrides ont déjà été mentionnées, en particulier le centre d'excellence européen pour la lutte contre les menaces hybrides, la meilleure appréciation de la situation, l'établissement de la cellule de fusion de l'UE contre les menaces hybrides et son interaction avec la branche d'analyse des menaces hybrides de l'OTAN, nouvellement créée, ainsi que la collaboration entre les équipes de communication stratégique. Pour la première fois, les personnels de l'OTAN et de l'UE vont procéder ensemble à un exercice visant à tester leur réaction à un scénario de menace hybride. Cet exercice doit servir à tester la mise en œuvre de plus d'un tiers des propositions communes. L'UE procédera à son propre exercice parallèle et coordonné cette année et se prépare à jouer un rôle prépondérant en 2018.

Pour ce qui est de la résilience, les personnels de l'UE et de l'OTAN ont commencé à tenir des sessions d'information mutuelle, portant notamment sur le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise. Des contacts réguliers entre personnels de l'OTAN et de l'UE, par exemple lors d'ateliers ou au travers de la participation de l'OTAN au comité directeur de l'Agence européenne de défense, ont permis des échanges d'informations sur les exigences de base de l'OTAN en matière de résilience nationale. D'autres échanges entre la Commission et l'OTAN sur les moyens de renforcer la résilience sont prévus cet automne. Le prochain rapport d'étape sur la coopération entre l'UE et l'OTAN proposera des pistes pour élargir la coopération entre les deux organisations.

3. CONCLUSION

Le cadre commun définit des actions destinées à contribuer à la lutte contre les menaces hybrides et à favoriser la résilience au niveau de l'UE, à l'échelon national, ainsi que chez les partenaires. Tandis que la Commission et la haute représentante obtiennent des résultats dans tous les domaines, en étroite coopération avec les États membres et les partenaires, il est essentiel de maintenir cette dynamique face à des menaces hybrides persistantes et en continuelle évolution. La responsabilité première de la lutte contre les menaces hybrides touchant à la sécurité nationale et au maintien de l'ordre public incombe aux États membres. La résilience nationale et les efforts collectifs pour se protéger contre les menaces hybrides doivent être vus comme des éléments d'une même démarche globale qui se renforcent mutuellement. Les États membres sont, par conséquent, encouragés à effectuer des études sur les risques hybrides dès que possible, car celles-ci fourniront des informations précieuses quant au niveau de vulnérabilité et de préparation dans l'ensemble de l'Europe. En s'appuyant sur les progrès significatifs réalisés en matière de connaissance de la situation, il convient d'exploiter au maximum le potentiel de la cellule de fusion de l'UE contre les menaces hybrides. La haute représentante invite les États membres à soutenir le travail des task-forces «Stratcom» dans le but de contrer plus efficacement la montée des menaces hybrides. L'UE apportera son soutien plein et entier au centre européen de lutte contre les menaces hybrides dirigé par la Finlande.

[38] http://www.consilium.europa.eu/fr/press/press-releases/2016/12/06-eu-nato-joint-declaration/

L’atout unique de l’UE réside dans l’aide apportée aux États membres et aux partenaires pour qu’ils renforcent leur résilience, en s’appuyant sur un large éventail d’instruments et de programmes existants. Les actions menées en vue de renforcer la résilience enregistrent des progrès significatifs dans des domaines tels que les transports, l’énergie, la cybersécurité, les infrastructures critiques, la protection du système financier contre les utilisations illicites ainsi que dans la lutte contre l’extrémisme violent et la radicalisation. L'action de l’UE visant à renforcer la résilience se poursuivra en même temps que la nature des menaces hybrides évoluera. En particulier, l’UE mettra au point des indicateurs dans l’optique d’une amélioration de la protection et de la résilience des infrastructures critiques face aux menaces hybrides dans les secteurs pertinents.

Le Fonds européen de la défense peut cofinancer, avec les États membres, les capacités jugées prioritaires pour renforcer la résilience face aux menaces hybrides. Le paquet de mesures annoncé sur la cybersécurité ainsi que les mesures intersectorielles visant à mettre en œuvre la directive sur la sécurité des réseaux et de l’information fourniront de nouvelles plateformes de lutte contre les menaces hybrides dans l’ensemble de l’UE.

La Commission et la haute représentante invitent les États membres et les parties prenantes à trouver, si nécessaire, un accord dans les meilleurs délais et à assurer l’application rapide et efficace des nombreuses mesures destinées à renforcer la résilience décrites dans cette communication. L’UE va consolider et approfondir la coopération, déjà fructueuse, qu’elle a entamée avec l’OTAN.

L’Union reste déterminée à mobiliser tous les instruments utiles à sa disposition pour faire face aux menaces hybrides complexes. Soutenir les efforts des États membres demeure une priorité pour l’Union, qui agit comme un garant de la sécurité plus fort et plus réactif, aux côtés de ses principaux partenaires.