COMMISSION
EUROPÉENNE

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

Bruxelles, le 6.4.2016
JOIN(2016) 18 final

COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL

Cadre commun en matière de lutte contre les menaces hybrides

une réponse de l'Union européenne

1. INTRODUCTION

Au cours de ces dernières années, l'environnement de sécurité de l'Union européenne a considérablement évolué. Les grands défis pour la paix et la stabilité dans le voisinage oriental et méridional de l'UE ne cessent de souligner la nécessité d'une adaptation et d'une augmentation des capacités de l'Union en tant que pourvoyeur de sécurité, un accent marqué étant mis sur la relation étroite entre la sécurité extérieure et la sécurité intérieure. Bon nombre des défis qui se posent actuellement en matière de paix, de sécurité et de prospérité ont pour origine l'instabilité régnant dans le voisinage immédiat de l'UE et l'évolution des formes de menaces. Dans ses orientations politiques de 2014, le président de la Commission européenne, Jean-Claude Juncker, a insisté sur la nécessité de «travailler à renforcer l'Europe en matière de sécurité et de défense» et de combiner les instruments européens et nationaux d'une manière plus efficace que par le passé. Par la suite, à l'invitation du Conseil des affaires étrangères du 18 mai 2015, la haute représentante, en étroite coopération avec les services de la Commission et l'Agence européenne de défense (AED), et en consultation avec les États membres, a entrepris de présenter ce cadre commun s'accompagnant de propositions qui puissent se traduire en actions pour contribuer à lutter contre les menaces hybrides et renforcer la résilience de l'UE et de ses États membres ainsi que des partenaires[1]. En juin 2015, le Conseil européen a rappelé la nécessité de mobiliser les instruments de l'UE afin de faciliter la lutte contre les menaces hybrides[2].

Bien qu'il existe plusieurs définitions des menaces hybrides et que celles-ci doivent rester adaptables en raison du caractère évolutif desdites menaces, cette notion vise à exprimer le mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (c'est-à-dire diplomatiques, militaires, économiques, technologiques), susceptibles d'être utilisées de façon coordonnée par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs, sans que le seuil d'une guerre déclarée officiellement ne soit dépassé. Généralement, le principal objectif recherché est d'exploiter les vulnérabilités de la cible visée et de créer de l'ambiguïté pour entraver les processus décisionnels. Des campagnes de désinformation massive faisant appel aux médias sociaux pour contrôler le discours politique ou pour radicaliser, recruter et diriger des acteurs agissant par procuration peuvent être des vecteurs de menaces hybrides.

Dans la mesure où la lutte contre les menaces hybrides touche à la sûreté de l'État et à la défense nationale ainsi qu'au maintien de l'ordre public, la responsabilité première incombe aux États membres, la plupart des vulnérabilités nationales étant propres au pays concerné. Cependant, de nombreux États membres de l'UE sont confrontés à des menaces communes, qui peuvent également cibler des réseaux ou des infrastructures transfrontières. On peut réagir plus efficacement à ces menaces par une réponse coordonnée, au niveau de l'UE, faisant appel aux politiques et aux instruments de l'UE,

[1] Conclusions du Conseil sur la politique de sécurité et de défense commune (PSDC), mai 2015 [Consilium 8971/15].
[2] Conclusions du Conseil européen, juin 2015 [EUCO 22/15].

pour s'appuyer sur la solidarité européenne, l'assistance mutuelle et toutes les possibilités offertes par le traité de Lisbonne. Les politiques et instruments de l'UE peuvent jouer et jouent déjà, dans une large mesure, un grand rôle d'apport de valeur ajoutée dans l'amélioration de la connaissance de la situation. Cela contribue à accroître la résilience des États membres, s'agissant de répondre à des menaces communes. L'action extérieure de l'Union proposée au titre du présent cadre repose sur les principes énoncés à l'article 21 du traité sur l'Union européenne (TUE), parmi lesquels figurent la démocratie, l'État de droit, l'universalité et l'indivisibilité des droits de l'homme, et le respect des principes de la charte des Nations unies et du droit international[3].

La présente communication conjointe vise à faciliter une approche globale qui permettra à l'UE, en coordination avec les États membres, de contrer spécifiquement les menaces à caractère hybride, en créant des synergies entre tous les instruments pertinents et en favorisant une coopération étroite entre tous les acteurs concernés[4]. Les actions reposent sur des stratégies et politiques sectorielles existantes qui concourent à une plus grande sécurité. Plus spécifiquement, le programme européen en matière de sécurité[5], la future stratégie globale de l'Union européenne concernant les questions de politique étrangère et de sécurité et le futur plan d'action européen de la défense[6], la stratégie de cybersécurité de l'UE[7], la stratégie pour la sécurité énergétique[8] et la stratégie de sûreté maritime de l'Union européenne[9] sont des outils qui peuvent également contribuer à la lutte contre les menaces hybrides.

Comme l'OTAN s'emploie également à contrer les menaces hybrides et que le Conseil des affaires étrangères a proposé d'intensifier la coopération et la coordination dans ce domaine, certaines des propositions visent à améliorer la coopération UE-OTAN en matière de lutte contre les menaces hybrides.

La réponse proposée s'articule autour des axes suivants: améliorer la connaissance de la situation, renforcer la résilience, et prévenir les crises, y faire face et s'en remettre.

2. RECONNAITRE LE CARACTERE HYBRIDE D'UNE MENACE

Les menaces hybrides visent à exploiter les vulnérabilités d'un pays et ont souvent pour but de saper les valeurs démocratiques et les libertés fondamentales. Dans un premier temps, la haute représentante et la Commission collaboreront avec les États membres en

[3] La charte des droits fondamentaux de l'UE est contraignante pour les institutions et les États membres lorsqu'ils mettent en œuvre le droit de l'Union.
[4] Les éventuelles propositions législatives seront soumises aux exigences de la Commission en matière d'amélioration de la réglementation, conformément aux lignes directrices de la Commission pour une meilleure réglementation [SWD(2015) 111].
[5] COM(2015) 185 final.
[6] À présenter en 2016.
[7] Cadre d'action de l'UE en matière de cyberdéfense [Consilium 15585/14] et communication conjointe intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé», février 2013 [JOIN(2013) 1].
[8] Communication conjointe intitulée «Stratégie européenne pour la sécurité énergétique», mai 2014 [SWD(2014) 330].
[9] Communication conjointe du 6 mars 2014, intitulée «Pour un domaine maritime mondial ouvert et sûr: éléments d'une stratégie de sûreté maritime de l'Union européenne» [JOIN(2014) 9 final].

vue d'améliorer la connaissance de la situation par un suivi et une évaluation des risques auxquels les vulnérabilités de l'UE peuvent être exposées. La Commission est en train de mettre au point des méthodes d'évaluation des risques pour la sécurité afin de contribuer à informer les décideurs et à promouvoir la prise en compte des risques dans l'élaboration des politiques dans des domaines allant de la sûreté aérienne au financement du terrorisme et au blanchiment de capitaux. En outre, il serait judicieux que les États membres réalisent une étude destinée à recenser les domaines vulnérables aux menaces hybrides. L'objectif serait d'établir des indicateurs 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.

<u>Action n° 1</u>: 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.

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

3.1. Cellule de fusion de l'UE contre les menaces hybrides

Il est essentiel que l'UE, en coordination avec ses États membres, ait un niveau suffisant de connaissance de la situation pour détecter tout changement dans l'environnement de sécurité lié à l'activité hybride d'acteurs étatiques et/ou non étatiques. Pour contrer efficacement les menaces hybrides, il importe d'améliorer l'échange d'informations et de promouvoir un partage du renseignement pertinent dans tous les secteurs et entre l'Union européenne, ses États membres et les partenaires.

Une cellule de fusion de l'UE contre les menaces hybrides constituera un point central unique pour l'analyse des menaces hybrides, établi au sein du Centre de situation et du renseignement de l'UE (INTCEN) du Service européen pour l'action extérieure (SEAE). Cette cellule de fusion recevra, analysera et partagera des informations classifiées et de source ouverte spécifiquement relatives aux indicateurs et aux avertissements concernant les menaces hybrides, émanant de différentes parties prenantes au sein du SEAE (y compris les délégations de l'UE), de la Commission (avec les agences de l'UE[10]) et des États membres. En liaison avec les organismes analogues existant au niveau de l'UE[11] et au niveau national, la cellule de fusion étudiera les aspects extérieurs des menaces hybrides pour l'UE et son voisinage, afin d'analyser rapidement les incidents survenant dans ce domaine et d'éclairer les processus de prise de décision stratégique de l'UE, notamment en fournissant des éléments à intégrer dans les évaluations des risques pour la sécurité réalisées au niveau de l'UE. Les résultats analytiques de la cellule de fusion

[10] Conformément à leurs mandats.

[11] Par exemple, le Centre européen de lutte contre la cybercriminalité et le Centre européen de lutte contre le terrorisme d'Europol, Frontex et l'équipe d'intervention en cas d'urgence informatique de l'UE (CERT-UE).

seront traités et utilisés conformément aux règles de l'Union européenne relatives aux informations classifiées et à la protection des données[12]. La cellule travaillera en liaison avec les organismes existants au niveau de l'UE et au niveau national. Les États membres mettront en place des points de contact nationaux qui seront reliés à la cellule de fusion de l'UE contre les menaces hybrides. Le personnel en poste à l'intérieur et à l'extérieur de l'UE (y compris celui des délégations de l'UE et les personnes en opération ou en mission) et dans les États membres devrait également être formé de façon à pouvoir détecter les premiers signes de menaces hybrides.

Action n° 2: création d'une cellule de fusion de l'UE contre les menaces hybrides au sein de la structure existante de l'INTCEN, 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.

3.2. Communication stratégique

Les auteurs de menaces hybrides peuvent se livrer à une désinformation systématique, notamment au moyen de campagnes ciblées dans les médias sociaux, dans le but de radicaliser des individus, de déstabiliser la société et de contrôler le discours politique. La capacité de répondre aux menaces hybrides en recourant à une bonne stratégie de **communication stratégique** revêt une importance essentielle. Apporter des réponses factuelles rapides et mieux sensibiliser l'opinion aux menaces hybrides constituent des facteurs décisifs de renforcement de la résilience sociétale.

La communication stratégique devrait tirer pleinement parti des médias sociaux, ainsi que des médias visuels, audio et en ligne traditionnels. Le SEAE, en s'appuyant sur les activités des task-forces East Stratcom et Arab Stratcom, devrait optimiser le recours à des linguistes maîtrisant d'importantes langues de pays tiers et à des spécialistes des médias sociaux, capables de suivre l'information hors UE et d'assurer une communication ciblée pour réagir à la désinformation. En outre, les États membres devraient mettre au point des mécanismes coordonnés de communication stratégique pour soutenir la mention des sources et lutter contre la désinformation afin de mettre au jour les menaces hybrides.

Action n° 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.

[12] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995.

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

En s'appuyant sur l'expérience de certains États membres et de certaines organisations partenaires[13], un institut multinational ou un réseau d'instituts multinationaux pourrait faire fonction de centre d'excellence pour les menaces hybrides. Un tel centre pourrait se consacrer à des travaux de recherche portant sur les modes de recours à des stratégies hybrides et pourrait favoriser la mise au point de nouveaux concepts et de nouvelles technologies au sein du secteur privé et de l'industrie, afin d'aider les États membres à renforcer leur résilience. Ces travaux de recherche pourraient contribuer à mettre en adéquation les politiques, doctrines et concepts européens et nationaux et à garantir la prise en compte, dans les processus décisionnels, des éléments complexes et ambigus liés aux menaces hybrides. Ce centre mettrait au point des programmes destinés à faire progresser la recherche et des exercices visant à trouver des solutions concrètes aux problèmes actuels posés par les menaces hybrides. Ce centre tirerait sa force de l'expérience acquise par ses participants, de plusieurs nationalités et de différents secteurs, civils et militaires, appartenant au secteur privé et au milieu universitaire.

Ce centre pourrait coopérer étroitement avec les centres d'excellence existants de l'UE[14] et de l'OTAN[15], afin de tirer parti du savoir sur les menaces hybrides qui a été tiré de la cyberdéfense, de la communication stratégique, de la coopération civilo-militaire, de la réponse énergétique et de la réaction aux crises.

<u>Action n° 4</u>: les États membres sont invités à envisager de mettre en place un centre d'excellence pour la «lutte contre les menaces hybrides».

4. ORGANISER LA REPONSE DE L'UE: RENFORCER LA RESILIENCE

La résilience est la capacité de résister à une épreuve et de s'en remettre, en en sortant plus fort. Pour contrer efficacement les menaces hybrides, il y a lieu de se pencher sur les vulnérabilités potentielles des infrastructures clés, des chaînes d'approvisionnement et de la société. Les infrastructures à l'échelle de l'UE peuvent devenir plus résilientes si elles s'appuient sur les politiques et instruments de l'UE.

4.1. Protéger les infrastructures critiques

Il est important de protéger les infrastructures critiques (par exemple les chaînes d'approvisionnement énergétique et les transports), étant donné qu'une attaque non conventionnelle, par des auteurs de menaces hybrides, sur une «cible vulnérable» pourrait entraîner de graves perturbations de l'économie ou de la société. Pour assurer la protection des infrastructures critiques, le programme européen de protection des infrastructures critiques[16] (EPCIP) prévoit une approche systémique intersectorielle tous

[13] Centres d'excellence de l'OTAN.
[14] Par exemple l'Institut d'études de sécurité de l'Union européenne (IESUE) et les centres d'excellence thématiques de l'UE traitant des questions CBRN.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.
[16] Communication de la Commission sur un programme européen de protection des infrastructures critiques, 12.12.2006, COM(2006) 786 final.

risques, examinant les liens de dépendance et fondée sur la mise en œuvre des activités autour des volets de la prévention, de la préparation et de la réaction. La directive sur les infrastructures critiques européennes[17] établit une procédure de recensement et de désignation des infrastructures critiques européennes (ICE) ainsi qu'une approche commune pour évaluer la nécessité d'améliorer leur protection. Il conviendrait, en particulier, de relancer les travaux entrepris au titre de la directive en vue de renforcer la résilience des infrastructures critiques dans le domaine des transports (par exemple les principaux aéroports et ports de commerce de l'UE). La Commission déterminera s'il y a lieu de mettre au point des outils communs, y compris des indicateurs, destinés à améliorer la résilience des infrastructures critiques contre les menaces hybrides dans tous les secteurs concernés.

<u>Action n° 5</u>: 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.

4.1.1. Réseaux énergétiques

Il est d'une importance capitale, pour l'UE, que la production et la distribution d'électricité ne soient pas perturbées; les pannes de courant importantes pourraient être dommageables. Un élément essentiel de la lutte contre les menaces hybrides consiste à continuer de diversifier les sources d'énergie, les fournisseurs et les itinéraires d'approvisionnement, afin de garantir un approvisionnement en énergie plus sûr et plus résilient. La Commission procède également à des évaluations des risques et de la sûreté («tests de résistance») des centrales électriques de l'UE. Pour veiller à la diversification énergétique, les travaux menés dans le cadre de la stratégie pour l'union de l'énergie s'intensifient: on peut citer, à titre d'exemple, le corridor gazier sud-européen, qui peut permettre d'acheminer en Europe le gaz provenant de la région caspienne, et, dans le nord de l'Europe, la mise en place de nœuds d'approvisionnement en gaz liquide fonctionnant avec de multiples fournisseurs. C'est l'exemple à suivre en Europe centrale et orientale, comme dans la zone méditerranéenne, où un nœud gazier est en cours de construction[18]. Le développement du marché du gaz naturel liquéfié contribuera lui aussi positivement à la réalisation de cet objectif.

Pour ce qui est des matières et installations nucléaires, la Commission soutient l'élaboration et l'adoption des normes de sûreté les plus élevées, ce qui a pour effet de renforcer la résilience. La Commission encourage une transposition et une mise en œuvre cohérentes de la directive sur la sûreté nucléaire[19], qui fixe des règles pour la prévention

[17] Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JO L 345 du 23.12.2008).
[18] Sur les progrès réalisés jusqu'à présent, voir l'État de l'Union de l'énergie 2015 [COM(2015) 572 final].
[19] Directive 2009/71/Euratom du Conseil du 25 juin 2009 établissant un cadre communautaire pour la sûreté nucléaire des installations nucléaires, modifiée par la directive 2014/87/Euratom du Conseil du 8 juillet 2014.

des accidents et l'atténuation des conséquences des accidents, et des dispositions de la directive sur les normes de base[20], relative à la coopération internationale en matière de préparation aux situations d'urgence et d'intervention d'urgence, notamment entre États membres voisins et avec les pays voisins.

Action n° 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.

4.1.2 Transports et sécurité de la chaîne d'approvisionnement

Les transports sont essentiels au fonctionnement de l'Union. Les attaques hybrides contre des infrastructures de transport (comme les aéroports, les infrastructures routières, les ports et les chemins de fer) peuvent avoir de graves conséquences, entraînant des perturbations des chaînes de déplacement et d'approvisionnement. Dans la mise en œuvre de la législation relative à la sûreté aérienne et maritime[21], la Commission procède à des inspections régulières[22] et, par ses travaux en matière de sûreté des transports terrestres, entend faire face aux menaces hybrides émergentes. À cet égard, un cadre de l'UE est en cours de discussion au titre du règlement révisé sur la sûreté aérienne[23], dans le contexte de la stratégie de l'aviation pour l'Europe[24]. Par ailleurs, les menaces pesant sur la sûreté maritime sont examinées dans le cadre de la stratégie de sûreté maritime de l'Union européenne et du plan d'action accompagnant celle-ci[25]. Ce dernier permet à l'UE et à ses États membres de relever de manière globale les défis qui se posent en matière de sûreté maritime, y compris la lutte contre les menaces hybrides, dans le cadre d'une coopération intersectorielle entre acteurs civils et militaires visant à protéger les infrastructures critiques maritimes, la chaîne d'approvisionnement mondiale, les

[20] Directive 2013/59/Euratom du Conseil du 5 décembre 2013 fixant les normes de base relatives à la protection sanitaire contre les dangers résultant de l'exposition aux rayonnements ionisants et abrogeant les directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom et 2003/122/Euratom.

[21] Règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002; règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile; directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports; règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires.

[22] Conformément au droit de l'UE, la Commission est tenue de procéder à des inspections afin de veiller à la mise en œuvre correcte, par les États membres, des exigences en matière de sûreté aérienne et maritime. Cela inclut des inspections auprès de l'autorité compétente de l'État membre, ainsi que dans les ports et les aéroports, chez les transporteurs aériens, dans les navires et auprès des entités appliquant des mesures de sûreté. Les inspections de la Commission visent à garantir que les normes de l'UE sont pleinement mises en œuvre par les États membres.

[23] Règlement (UE) 2016/4 de la Commission du 5 janvier 2016 modifiant le règlement (CE) n° 216/2008 du Parlement européen et du Conseil en ce qui concerne les exigences essentielles en matière de protection de l'environnement; règlement (CE) n° 216/2008 du Parlement européen et du Conseil du 20 février 2008 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence européenne de la sécurité aérienne.

[24] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions - Une stratégie de l'aviation pour l'Europe [COM(2015) 598 final du 7.12.2015].

[25] En décembre 2014, le Conseil a adopté un plan d'action destiné à mettre en œuvre la stratégie de sûreté maritime de l'Union européenne (http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf).

échanges maritimes et les ressources énergétiques et naturelles maritimes. On veille également à la sécurité de la chaîne d'approvisionnement internationale dans le cadre de la stratégie et du plan d'action de l'Union européenne sur la gestion des risques en matière douanière[26].

<u>Action n° 7</u>: 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 ainsi que de la stratégie et du plan d'action de l'UE sur la gestion des risques en matière douanière, 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.

4.1.3 Espace

Les menaces hybrides pourraient cibler les infrastructures spatiales, avec des conséquences multisectorielles. L'UE a établi un cadre de soutien à la surveillance de l'espace et au suivi des objets en orbite[27] destiné à mettre en réseau les moyens détenus par les États membres pour fournir des services de surveillance de l'espace et de suivi des objets en orbite[28] aux utilisateurs identifiés (États membres, institutions de l'UE, propriétaires et opérateurs de véhicules spatiaux, et autorités chargées de la protection civile). Dans le contexte de la future stratégie spatiale pour l'Europe, la Commission se penchera sur la poursuite de sa mise en place, afin de surveiller les menaces hybrides pesant sur les infrastructures spatiales.

Les communications par satellite sont des ressources essentielles pour la gestion des crises, la réaction aux catastrophes, ainsi la surveillance policière, côtière et des frontières. Elles constituent l'ossature d'infrastructures de grande envergure telles que les systèmes de transport ou spatiaux ou les systèmes d'aéronefs télépilotés. À la suite de l'invitation lancée par le Conseil européen concernant la préparation de la prochaine génération de télécommunications gouvernementales par satellite, la Commission, en coopération avec l'Agence européenne de défense, est en train d'évaluer les possibilités de centraliser la demande, dans le contexte de la future stratégie spatiale et du futur plan d'action européen de la défense.

Bon nombre d'infrastructures critiques ont besoin d'une information de temps exacte pour synchroniser leurs réseaux (énergie et télécommunications, par exemple) ou horodater les transactions (marchés financiers, par exemple). Le fait d'être tributaire du seul signal de synchronisation temporelle du système mondial de navigation par satellite

[26] Communication de la Commission au Parlement européen, au Conseil et au Comité économique et social européen relative à la stratégie et au plan d'action de l'UE sur la gestion des risques en matière douanière: faire face aux risques, renforcer la sécurité de la chaîne d'approvisionnement et faciliter le commerce [COM(2014) 527 final].

[27] Voir la décision 541/2014 du Parlement européen et du Conseil.

[28] Tels que le déclenchement d'alertes visant à éviter les collisions au cours de la phase d'exploitation en orbite ainsi que le déclenchement d'alertes relatives aux destructions ou collisions ainsi qu'aux rentrées risquées d'objets spatiaux dans l'atmosphère terrestre.

n’assure pas la résilience requise pour contrer les menaces hybrides. Galileo, le système mondial de navigation par satellite européen, offrirait une deuxième source temporelle fiable.

<u>Action n° 8</u>: dans le contexte de la future stratégie spatiale et du futur 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.

4.2. Les capacités de défense

Les capacités de défense doivent être renforcées afin d'améliorer la résilience de l’UE face aux menaces hybrides. Il est important de déterminer les principaux domaines pertinents sur le plan des capacités, tels que la surveillance et la reconnaissance. L'Agence européenne de défense pourrait jouer un rôle clé dans le développement des capacités militaires aux fins de la lutte contre les menaces hybrides (en raccourcissant les cycles de développement des capacités de défense, en investissant dans des technologies, systèmes et prototypes ou en ouvrant les entreprises de défense aux technologies commerciales innovantes, par exemple). Les actions pouvant être mises en œuvre pourraient être examinées dans le cadre du futur plan d’action européen de la défense.

<u>Action n° 9</u>: 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.

4.3. Protéger la santé publique et la sécurité alimentaire

La santé de la population pourrait être mise en péril par la manipulation de maladies transmissibles ou la contamination des denrées alimentaires, des sols, de l'air et de l’eau potable par des agents chimiques, biologiques, radiologiques et nucléaires (CBRN). En outre, la propagation délibérée de maladies animales ou végétales pourrait nuire gravement à la sécurité alimentaire de l’Union et avoir des répercussions économiques et sociales majeures dans des secteurs essentiels de la chaîne alimentaire de l’UE. Les structures existantes de l’UE en matière de sécurité sanitaire, de protection de l'environnement et de sûreté alimentaire peuvent être utilisées pour répondre aux menaces hybrides résultant de telles pratiques.

Conformément à la réglementation de l'UE en matière de menaces transfrontières sur la santé[29], les mécanismes existants coordonnent la capacité de réaction aux menaces transfrontières graves sur la santé en associant les États membres, les agences de l'UE et les comités scientifiques[30] par l'intermédiaire du système d'alerte précoce et de réaction. Le comité de sécurité sanitaire, qui coordonne la réaction des États membres face aux menaces, pourrait servir de point de contact pour les vulnérabilités en matière de santé publique[31] afin de permettre la prise en compte des menaces hybrides (et, en particulier, du bioterrorisme) dans les orientations en matière de communication de crise et les exercices de renforcement des capacités (simulation de crise) menés avec les États membres. Dans le domaine de la sûreté alimentaire, le système d'alerte rapide pour les denrées alimentaires et les aliments pour animaux (RASFF) et le système commun de gestion des risques (SCGR) en matière douanière permettent aux autorités compétentes d'échanger des informations relatives à l'analyse de risque en vue de la surveillance des risques sanitaires liés aux denrées alimentaires contaminées. En ce qui concerne la santé animale et végétale, le réexamen du cadre juridique de l'UE[32] permettra d'ajouter de nouveaux éléments à la panoplie d'outils existante[33] en vue d'une meilleure préparation aux menaces hybrides.

Action n° 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.

4.4. La cybersécurité

L'UE profite pleinement de sa société interconnectée et numérisée. Des cyberattaques risqueraient de perturber les services numériques sur l'ensemble de son territoire. De telles attaques pourraient être utilisées par les auteurs de menaces hybrides. Il importe de renforcer la résilience des systèmes de communication et d'information en Europe afin de soutenir le marché numérique unique. La stratégie de cybersécurité de l'UE et le programme européen en matière de sécurité définissent le cadre stratégique global des initiatives de l'UE dans les domaines de la cybersécurité et de la cybercriminalité. L'UE

[29] Décision n° 1082/2013/UE du Parlement européen et du Conseil du 22 octobre 2013 relative aux menaces transfrontières graves sur la santé et abrogeant la décision n° 2119/98/CE, JO L 293 du 5.11.2013, p. 1.
[30] Décision C(2015) 5383 de la Commission du 7 août 2015 établissant des comités scientifiques dans le domaine de la sécurité des consommateurs, de la santé publique et de l'environnement.
[31] Conformément à la décision n° 1082/2013/UE du Parlement européen et du Conseil du 22 octobre 2013 relative aux menaces transfrontières graves sur la santé et abrogeant la décision n° 2119/98/CE, JO L 293 du 5.11.2013, p. 1.
[32] Règlement (UE) 2016/429 du Parlement européen et du Conseil du 9 mars 2016 relatif aux maladies animales transmissibles et modifiant et abrogeant certains actes dans le domaine de la santé animale («législation sur la santé animale»), JO L 84 du 31.3.2016, p. 1. En ce qui concerne le règlement du Parlement européen et du Conseil relatif aux mesures de protection contre les organismes nuisibles aux végétaux («législation sur la santé des végétaux»), le Parlement européen et le Conseil sont parvenus à un accord politique sur le texte dudit règlement le 16 décembre 2015.
[33] Au nombre de ces outils figurent notamment les banques de vaccins de l'UE, un système électronique sophistiqué d'information sur les maladies des animaux et une obligation renforcée concernant les mesures mises en place par les laboratoires et d'autres entités s'occupant des agents pathogènes.

contribue activement au renforcement de la sensibilisation, des mécanismes de coopération et des réponses apportées dans le cadre des résultats escomptés de la stratégie en matière de cybersécurité. La proposition de directive relative à la sécurité des réseaux et de l'information[34], en particulier, apporte une réponse aux risques en matière de cybersécurité encourus par un large éventail de prestataires de services essentiels dans les domaines de l'énergie, des transports, des finances et de la santé. Il convient que ces prestataires, de même que les prestataires de services numériques clés (comme l'informatique en nuage, par exemple) prennent des mesures de sécurité adéquates et rapportent les incidents graves aux autorités nationales, en signalant d'éventuelles caractéristiques hybrides. Dès leur adoption par les colégislateurs, la transposition et la mise en œuvre effectives de la directive devraient permettre le développement des capacités en matière de cybersécurité dans l'ensemble des États membres, grâce à une coopération accrue dans ce domaine au moyen de l'échange d'informations et de bonnes pratiques sur la lutte contre les menaces hybrides. La directive prévoit notamment la mise en place d'un réseau de 28 équipes nationales de réaction aux incidents touchant la sécurité informatique (Computer Security Incident Response Teams - CSIRT) et d'une équipe d'intervention de l'UE en cas d'urgence informatique[35] à des fins de coopération opérationnelle sur une base volontaire.

Afin d'encourager la coopération entre les secteurs public et privé et des approches de la cybersécurité à l'échelle de l'UE, la Commission a mis sur pied la plateforme SRI, qui propose des orientations concernant les bonnes pratiques en matière de gestion des risques. Alors que les États membres fixent les exigences de sécurité et définissent les modalités de la notification des incidents de portée nationale, la Commission encourage un degré élevé de convergence entre les approches suivies sur le plan de la gestion des risques, fondées notamment sur le réseau de coopération et l'Agence européenne chargée de la sécurité des réseaux et de l'information («ENISA»).

<u>Action n° 11</u>: 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 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.

[34] Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information (SRI) dans l'Union, présentée par la Commission le 7 février 2013 - COM(2013) 48 final. Un accord politique a été trouvé par le Conseil de l'UE et le Parlement européen sur cette proposition de directive, et la directive devrait être adoptée prochainement.

[35] Computer Emergency Response Team (CERT-EU) (équipe d'intervention interinstitutionnelle de l'UE en cas d'urgence informatique).

4.4.1. L'industrie

La dépendance croissante à l'égard de l'informatique en nuage et des mégadonnées a conduit à une vulnérabilité accrue face aux menaces hybrides. La stratégie pour le marché unique numérique prévoit un partenariat public-privé contractuel en matière de cybersécurité[36], qui sera axé sur la recherche et l'innovation et permettra à l'Union de conserver un degré élevé de capacité technologique dans ce domaine. Le partenariat public-privé contractuel permettra d'instaurer un climat de confiance entre les différents acteurs du marché et de développer des synergies entre l'offre et la demande. Alors que ce partenariat et les mesures qui l'accompagnent porteront essentiellement sur des produits et des services de cybersécurité dans le domaine civil, les résultats de ces initiatives devraient permettre aux utilisateurs de technologies d'être également mieux protégés contre les menaces hybrides.

Action n° 12: 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.

4.4.2. L'énergie

L'émergence de la domotique et des appareils intelligents, le développement des réseaux intelligents et la numérisation de plus en plus importante du système énergétique se traduisent également par une vulnérabilité accrue aux cyberattaques. La stratégie européenne pour la sécurité énergétique[37] et la stratégie de l'Union pour la sécurité énergétique[38] privilégient une approche «tous risques» intégrant la résilience face aux menaces hybrides. Le réseau thématique sur la protection des infrastructures énergétiques critiques favorise la collaboration entre les opérateurs du secteur énergétique (pétrole, gaz, électricité). La Commission a lancé une plateforme en ligne en vue de l'analyse et du partage d'informations sur les menaces et les incidents[39]. Elle procède également, conjointement avec les parties prenantes[40], à l'élaboration d'une stratégie globale pour le secteur énergétique en ce qui concerne la cybersécurité des opérations liées aux réseaux intelligents, dans le but de réduire les vulnérabilités. Alors que les marchés de l'électricité sont de plus en plus intégrés, les règles et procédures en matière de traitement des situations de crise ont toujours une dimension nationale. Nous devons veiller à ce que les États membres coopèrent les uns avec les autres pour ce qui est de la préparation aux risques, ainsi que de la prévention et de l'atténuation de ceux-ci, et à ce que tous les acteurs concernés s'appuient sur un ensemble commun de règles.

[36] Dont le lancement est prévu à la mi-2016.
[37] Communication de la Commission au Parlement européen et au Conseil intitulée «Stratégie européenne pour la sécurité énergétique», COM(2014) 330 final.
[38] Communication intitulée «Cadre stratégique pour une Union de l'énergie résiliente, dotée d'une politique clairvoyante en matière de changement climatique» - COM(2015) 80 final.
[39] Incident and Threat Information Sharing EU Centre - ITIS.
[40] Dans le cadre de la plateforme «Energy Expert CyberSecurity Platform (EECSP)».

<u>Action n° 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.

4.4.3. Garantir des systèmes financiers sains

L'économie de l'UE a besoin d'un système financier et de paiement sûr pour fonctionner. Il est essentiel de protéger le système financier et ses infrastructures contre les cyberattaques, quelles que soient les motivations ou la nature des auteurs de celles-ci. Pour faire face aux menaces hybrides à l'égard des services financiers de l'UE, le secteur doit comprendre la menace, avoir testé ses propres défenses et disposer de la technologie nécessaire pour se protéger des attaques. L'échange d'informations sur les menaces entre les acteurs du marché financier ainsi qu'avec les autorités compétentes et les principaux prestataires de services ou leurs clients est par conséquent fondamental. Cet échange doit cependant être sûr et respecter les exigences en matière de protection des données. Dans le droit fil des travaux menés dans des enceintes internationales, et notamment des travaux du G7 dans ce secteur, la Commission s'efforcera de déterminer les éléments qui entravent le partage approprié d'informations sur les menaces et proposera des solutions. Il est important de garantir des contrôles réguliers et une amélioration des protocoles en vue de protéger les entreprises et les infrastructures concernées, y compris l'amélioration constante des technologies permettant de renforcer la sécurité.

<u>Action n° 14</u>: la Commission, en collaboration avec l'ENISA[41], 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.

4.4.4. Transports

Les systèmes de transport (ferroviaire, routier, aérien, maritime) modernes s'appuient sur des systèmes d'information qui sont vulnérables aux cyberattaques. Comme ces systèmes ont une dimension transfrontière, l'UE a un rôle particulier à jouer en la matière. La Commission, en coordination avec les États membres, continuera d'analyser les cybermenaces et risques liés à des interférences illicites avec les systèmes de transport. Elle procède actuellement à l'élaboration d'une feuille de route sur la cybersécurité dans le secteur aéronautique, en collaboration avec l'Agence européenne de la sécurité aérienne (AESA)[42]. Les cybermenaces pesant sur la sûreté maritime sont également

[41] Agence européenne chargée de la sécurité des réseaux et de l'information.

[42] Le nouveau règlement AESA fait actuellement l'objet de discussions entre le Parlement européen et le Conseil, à la suite de la proposition présentée par la Commission en décembre 2015. Proposition de règlement du Parlement européen et du Conseil concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de la sécurité aérienne de l'Union européenne, et abrogeant le

examinées dans le cadre de la stratégie de sûreté maritime de l'Union européenne (SSMUE) et du plan d'action accompagnant celle-ci.

<u>Action n° 15</u>: 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.

4.5. Cibler le financement des menaces hybrides

Les auteurs de menaces hybrides ont besoin de fonds pour pouvoir poursuivre leurs actions. Ces fonds peuvent être utilisés pour soutenir des groupes terroristes ou des formes de déstabilisation plus subtiles, telles que le soutien de groupes de pression et de partis politiques marginaux. L'UE a intensifié ses efforts contre le financement de la criminalité et du terrorisme, ainsi que le prévoit le programme européen en matière de sécurité, au moyen notamment du plan d'action[43]. Dans ce contexte, le nouveau cadre européen de lutte contre le blanchiment de capitaux renforce la lutte contre le financement du terrorisme et le blanchiment d'argent, facilite le travail des cellules nationales de renseignement financier (CRF) en vue de la détection et du suivi des virements suspects et permet des échanges d'information, tout en garantissant la traçabilité des transferts de fonds dans l'Union européenne. Il pourrait donc également contribuer à la lutte contre les menaces hybrides. Dans le cadre des instruments de la PESC, des mesures restrictives adaptées et efficaces pourraient être envisagées aux fins de la lutte contre les menaces hybrides.

<u>Action n° 16</u>: 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.

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

Bien que les actes terroristes et l'extrémisme violent ne présentent pas en soi de caractère hybride, les auteurs de menaces hybrides peuvent cibler et recruter des personnes vulnérables dans la société, et les radicaliser en utilisant les moyens de communication modernes (notamment les médias sociaux sur l'internet et les groupes agissant par procuration) et en ayant recours à de la propagande.

Dans le cadre de la stratégie pour un marché unique numérique, la Commission analyse actuellement la nécessité d'élaborer de nouvelles mesures contre les contenus à caractère extrémiste sur l'internet en tenant pleinement compte de leur incidence sur le droit fondamental à la liberté d'expression et d'information, notamment des procédures strictes

règlement (CE) n° 216/2008 du Parlement européen et du Conseil - COM(2015) 613 final, 2015/0277 (COD).

[43] Communication de la Commission au Parlement européen et au Conseil relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme - COM(2016) 50 final.

pour le retrait de contenus illicites en épargnant les contenus licites («notification et action») ainsi qu'une responsabilité et une vigilance accrues de la part des intermédiaires dans la gestion de leurs réseaux et systèmes. Ces mesures viendraient compléter la démarche volontaire mise en place actuellement, qui consiste pour les entreprises actives dans le domaine de l'internet et des médias sociaux, en particulier dans le cadre du forum de l'Union sur l'internet et en collaboration avec l'unité de signalement des contenus sur l'internet au sein d'Europol, à retirer rapidement la propagande terroriste.

Dans le cadre du programme européen en matière de sécurité, la lutte contre la radicalisation passe par l'échange d'expériences et la promotion de bonnes pratiques, notamment par la coopération dans les pays tiers. L'équipe de conseil en communication stratégique sur la Syrie vise à renforcer la mise au point et la diffusion d'autres messages pour contrer la propagande terroriste. Le réseau de sensibilisation à la radicalisation soutient les États membres et les praticiens qui sont en contact avec des personnes radicalisées (notamment les combattants terroristes étrangers) ou considérées comme vulnérables à la radicalisation. Ce réseau organise des activités de formation et fournit des conseils. Il proposera une aide aux pays tiers prioritaires disposés à coopérer. La Commission favorise également la coopération judiciaire entre les acteurs de la justice pénale, y compris Eurojust, pour combattre le terrorisme et la radicalisation dans les États membres, notamment en ce qui concerne le traitement à réserver aux combattants terroristes étrangers et aux combattants de retour dans leur pays d'origine.

En complément des actions dans le cadre de son **action extérieure** décrites ci-dessus, l'UE contribue à la lutte contre l'extrémisme violent, notamment par un dialogue et une communication sur le plan extérieur, par de la prévention (lutte contre la radicalisation et le financement du terrorisme), ainsi que par des mesures visant à s'attaquer aux facteurs économiques, politiques et sociétaux qui permettent aux groupes terroristes de se développer.

Action n° 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.***

4.7. Renforcer la coopération avec les pays tiers

Comme souligné dans le programme européen en matière de sécurité, l'UE a mis davantage l'accent sur le renforcement des capacités dans le domaine de la sécurité dans les ***pays partenaires***, notamment en exploitant le lien entre sécurité et développement et en renforçant la dimension «sécurité» de la nouvelle politique européenne de voisinage[44]. Ces actions peuvent également contribuer à promouvoir la résilience des partenaires aux actions hybrides.

[44] Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, intitulée «Réexamen de la politique européenne de voisinage», [JOIN(2015) 50 final du 18.11.2015].

La Commission entend intensifier davantage l'échange d'informations opérationnelles et stratégiques avec les pays concernés par l'élargissement et les pays du partenariat oriental et du voisinage méridional, dans la mesure nécessaire pour lutter contre la criminalité organisée, le terrorisme, la migration irrégulière et le trafic d'armes légères. En matière de lutte contre le terrorisme, l'UE renforce sa coopération avec les pays tiers en mettant en place des dialogues et des plans d'action améliorés en matière de sécurité.

Les instruments de financement de l'action extérieure de l'UE visent à mettre sur pied des institutions opérationnelles et responsables dans les pays tiers[45], ce qui est une condition indispensable pour pouvoir répondre de manière efficace aux menaces pour la sécurité et favoriser la résilience. Dans ce contexte, la réforme du secteur de la sécurité et le renforcement des capacités en matière de sécurité et de développement[46] constituent des outils essentiels. Dans le cadre de l'instrument contribuant à la stabilité et à la paix[47], la Commission a mis en œuvre des actions destinées à renforcer la cyber-résilience et les capacités de ses partenaires à déceler et à se défendre contre les cyberattaques et la cybercriminalité, ce qui peut être utile à la lutte contre les menaces hybrides dans les pays tiers. L'UE finance des activités de renforcement des capacités dans les pays partenaires afin d'atténuer les risques pour la sécurité liés aux questions CBRN[48].

Enfin, dans un esprit d'approche globale de la gestion des crises, les États membres pourraient déployer les outils et les missions de la politique de sécurité et de défense commune (PSDC), indépendamment ou en complément des instruments de l'UE, pour aider les partenaires à renforcer leurs capacités. Les actions suivantes pourraient être envisagées: i) appui des communications stratégiques, ii) soutien consultatif des ministères clés exposés aux menaces hybrides, iii) aide supplémentaire à la gestion des frontières en cas d'urgence. D'autres synergies pourraient être envisagées entre les instruments de la PSDC et les acteurs dans les domaines de la sécurité, des douanes et de la justice, notamment les agences compétentes de l'UE[49], Interpol et la Force de gendarmerie européenne, conformément à leurs mandats.

---

[45] Idem; communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, intitulée «La stratégie d'élargissement de l'UE» [COM(2015) 611 final du 10.11.2015]; communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, intitulée «Accroître l'impact de la politique de développement de l'UE: un programme pour le changement» [COM(2011) 637 final du 13.10.2011].

[46] Communication conjointe intitulée «Renforcer les capacités pour favoriser la sécurité et le développement - Donner à nos partenaires les moyens de prévenir et de gérer les crises [JOIN(2015) 17 final].

[47] Règlement (UE) n° 230/2014 du Parlement européen et du Conseil du 11 mars 2014 instituant un instrument contribuant à la stabilité et à la paix (JO L 77 du 15.3.2014, p. 1).

[48] Parmi les domaines couverts figurent le contrôle des frontières, la gestion des crises, la première intervention, les trafics illicites, le contrôle des exportations de biens à double usage, la surveillance et le contrôle des maladies, la criminalistique nucléaire, le rétablissement après incident et la protection des installations à haut risque. Les bonnes pratiques acquises grâce aux outils mis au point dans le cadre du plan d'action de l'UE dans le domaine CBRN, par exemple le centre européen de formation à la sécurité nucléaire et la participation de l'Union au groupe de travail international sur la surveillance des frontières, peuvent être partagées avec les pays tiers.

[49] EUROPOL, FRONTEX, CEPOL, EUROJUST.

<u>Action n° 18</u>: 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.

5. PREVENIR LES CRISES, Y FAIRE FACE ET S'EN REMETTRE

Comme indiqué au point 3.1, la cellule de fusion de l'UE contre les menaces hybrides proposée par l'Union a pour mission d'analyser les indicateurs pertinents afin de prévenir les menaces hybrides, d'y répondre et d'en informer les décideurs de l'UE. S'il est possible de compenser les lacunes par des politiques à long terme aux niveaux national et de l'UE, il demeure essentiel à court terme de renforcer les capacités des États membres et de l'Union afin de prévenir les menaces hybrides, d'y faire face et de s'en remettre à bref délai et de manière concertée.

Une réaction rapide aux événements déclenchés par les menaces hybrides est primordiale. À cet égard, le renforcement des actions nationales de protection civile et des capacités du centre européen de coordination des interventions d'urgence[50] pourrait constituer un mécanisme efficace de réaction aux aspects des menaces hybrides nécessitant une intervention sur le plan de la protection civile. Cela pourrait se faire en coordination avec d'autres mécanismes de réaction et systèmes d'alerte précoce de l'UE, en particulier la salle de veille du SEAE en ce qui concerne les aspects relatifs à la sécurité extérieure et le centre stratégique d'analyse et de réaction pour ce qui est de la sécurité intérieure.

La clause de solidarité (article 222 du TFUE) permet une action de l'Union et de ses États membres si un État membre est l'objet d'une attaque terroriste ou la victime d'une catastrophe naturelle ou d'origine humaine. Les dispositions d'application de l'action mise en œuvre par l'Union pour aider l'État membre sont régies par la décision 2014/415/UE du Conseil[51]. Les modalités de coordination au sein du Conseil devraient se fonder sur le dispositif intégré de l'UE pour une réaction au niveau politique dans les situations de crise[52]. Ces modalités prévoient que la Commission et la haute représentante, dans leurs domaines respectifs de compétence, recensent les instruments pertinents de l'Union et soumettent au Conseil des propositions de décisions sur des mesures exceptionnelles.

L'article 222 du TFUE concerne également les situations impliquant une assistance directe par un ou plusieurs États membres à un État membre en cas d'attaque terroriste ou de catastrophe. La décision 2014/415/UE du Conseil ne s'applique pas à ces situations.

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_fr.
[51] Décision 2014/415/UE du Conseil concernant les modalités de mise en œuvre par l'Union de la clause de solidarité (JO L 192 du 1.7.2014, p. 53).
[52] http://www.consilium.europa.eu/fr/documents-publications/publications/2014/eu-ipcr/

Compte tenu des ambiguïtés liées aux actions hybrides, l'applicabilité possible en dernier ressort de la clause de solidarité devrait faire l'objet d'une évaluation de la Commission et de la haute représentante, dans leurs domaines respectifs de compétence, si un État membre de l'UE fait l'objet de menaces hybrides importantes.

Contrairement à l'article 222 du TFUE, si plusieurs menaces hybrides sérieuses constituent une agression armée contre un État membre de l'UE, l'article 42, paragraphe 7, du TUE pourrait être invoqué afin d'apporter une réponse appropriée en temps utile. L'apparition de menaces hybrides graves et de grande ampleur peut également nécessiter une coopération et une coordination renforcées avec l'OTAN.

Lors de la préparation de leurs forces, les États membres sont encouragés à prendre en compte les menaces hybrides potentielles. Pour être en mesure de prendre des décisions rapides et efficaces en cas d'attaque hybride, les États membres doivent procéder à des exercices réguliers, au niveau tant opérationnel que politique, afin de mesurer les capacités de décision aux niveaux national et multinational. L'objectif serait de disposer d'un protocole opérationnel commun entre les États membres, la Commission et la haute représentante, définissant des procédures efficaces à appliquer en cas de menace hybride, depuis la première phase d'identification jusqu'à la phase finale d'attaque, et de préciser le rôle de chaque institution de l'Union et de chaque acteur dans le processus.

En tant que volet important de l'engagement dans le cadre de la PSDC, il pourrait être envisagé de mettre en place: a) une formation civile et militaire, b) des missions d'encadrement et de conseil destinées à améliorer les capacités de sécurité et de défense d'un État menacé, c) des plans d'urgence pour identifier les signes de menaces hybrides et renforcer les capacités d'alerte rapide, d) un appui à la gestion des contrôles aux frontières en cas d'urgence, e) un soutien dans des domaines spécifiques tels que l'atténuation du risque CBRN et l'évacuation des non-combattants.

Action n° 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.

Action n° 20: 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.

Action n° 21: 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.

6. RENFORCER LA COOPERATION AVEC L'OTAN

Les menaces hybrides constituent un défi non seulement pour l'UE, mais aussi pour les autres grandes organisations partenaires, notamment l'Organisation des Nations unies (ONU), l'Organisation pour la sécurité et la coopération en Europe (OSCE), et en particulier l'OTAN. Une réaction efficace exige un dialogue et une coordination au niveau tant politique qu'opérationnel entre les organisations. Une interaction plus étroite entre l'UE et l'OTAN permettrait aux deux organisations de mieux se préparer et répondre efficacement aux menaces hybrides, de façon complémentaire et par un soutien mutuel, sur la base du principe d'inclusion et dans le respect de l'autonomie décisionnelle et des règles relatives à la protection des données de chaque organisation.

Les deux organisations partagent les mêmes valeurs et sont confrontées à des défis similaires. Les États membres de l'UE et les alliés de l'OTAN attendent de leurs organisations respectives qu'elles les soutiennent et agissent rapidement, avec détermination et de manière coordonnée en cas de crise ou, idéalement, à titre préventif avant que la crise ne survienne. Plusieurs domaines ont été répertoriés en vue d'une coopération et d'une coordination plus étroites avec l'OTAN, notamment la connaissance de la situation, les communications stratégiques, la cybersécurité et la prévention et la gestion des crises. Le dialogue informel en cours entre l'UE et l'OTAN sur les menaces hybrides devrait être renforcé afin de synchroniser les actions des deux organisations dans ce domaine.

Il est important, pour la complémentarité des réponses UE/OTAN, que les deux organisations aient une connaissance commune de la situation avant et pendant la crise. Le partage régulier d'analyses et d'enseignements tirés pourrait y contribuer, de même que des contacts directs entre la cellule de fusion contre les menaces hybrides de l'UE et celle de l'OTAN. Il est tout aussi important de renforcer la connaissance mutuelle des procédures respectives de gestion des crises pour garantir des réactions rapides et efficaces. La résilience pourrait être améliorée en veillant à la complémentarité entre les normes fixées pour les éléments critiques de leurs infrastructures, ainsi que par une collaboration étroite en matière de communications stratégiques et de cyberdéfense. Des exercices conjoints pleinement inclusifs, au niveau tant politique que technique, contribueraient à rendre plus efficaces les capacités décisionnelles respectives des deux organisations. La recherche de possibilités d'actions de formation complémentaires permettrait d'atteindre un niveau comparable d'expertise dans des domaines critiques.

<u>Action n° 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.

7. CONCLUSIONS

La présente communication décrit dans les grandes lignes des actions conçues pour contribuer à la lutte contre les menaces hybrides et au renforcement de la résilience aux niveaux national, de l'UE et des partenaires. L'accent étant mis sur **l'amélioration de la connaissance de la situation**, il est proposé de mettre en place des mécanismes spécifiques pour l'échange d'informations avec les États membres et de coordonner les capacités de l'UE en matière de communications stratégiques. Des actions sont présentées en vue de **renforcer la résilience** dans des domaines tels que la cybersécurité, les infrastructures critiques, la protection du système financier contre les utilisations illicites et la lutte contre l'extrémisme violent et la radicalisation. Dans chacun de ces domaines, la mise en œuvre des stratégies convenues d'un commun accord par l'UE et les États membres et l'application intégrale par ces derniers de la législation en vigueur constitueront une première étape essentielle des efforts à fournir. D'autres actions plus concrètes sont également présentées dans le prolongement de ces efforts.

Pour **prévenir les menaces hybrides, y faire face et s'en remettre**, il est proposé d'étudier la possibilité d'appliquer la clause de solidarité prévue à l'article 222 du TFUE (et précisée dans la décision correspondante) et l'article 42, paragraphe 7, du TUE en cas d'attaque hybride grave et de grande ampleur. Les capacités en termes de prise de décisions stratégiques pourraient être améliorées par la mise en place d'un protocole opérationnel commun.

Enfin, il est proposé de **renforcer la coopération et la coordination entre l'UE et l'OTAN** dans un effort commun de lutte contre les menaces hybrides.

Pour la mise en œuvre de ce cadre commun, la haute représentante et la Commission s'engagent à mobiliser les instruments de l'UE dont elles disposent respectivement dans ce domaine. Il est important que l'UE œuvre conjointement avec les États membres à la réduction des risques associés aux éventuelles menaces hybrides que font peser les acteurs étatiques et non étatiques.