SÉCURITÉ & STRATÉGIE N° 131
Octobre 2017

Institut Royal Supérieur de Défense

La défense contre les « menaces hybrides » : la Belgique et la stratégie euro-atlantique

Estelle Hoorickx

LA DÉFENSE

Octobre 2017

La défense contre les « menaces hybrides » : la Belgique et la stratégie euro-atlantique

Estelle Hoorickx

Institut Royal Supérieur de Défense
Centre d'Etudes de Sécurité et Défense
30 Avenue de la Renaissance
1000 Bruxelles

ISSN 2295-0915

Vos questions, remarques ou commentaires relatifs au présent document peuvent être adressés au :
Directeur du Centre d'Etudes de Sécurité et Défense
Institut Royal Supérieur de Défense
30 Avenue de la Renaissance
1000 Bruxelles
ou par courriel à : +IRSD-CESD-SCVD@mil.be

L'auteure

Le Cdt d'Avi Estelle Hoorickx est attachée de recherche au Centre d'Études de Sécurité et Défense de l'Institut Royal Supérieur de Défense (IRSD). Ses domaines de compétence englobent les développements conceptuels dans l'emploi des capacités de Défense, le terrorisme en Europe et le rôle de la Belgique dans les organisations internationales. Elle effectue un doctorat en histoire sur l'influence de ce pays à l'OTAN pendant la Guerre froide.

Executive Summary

The practices of "hybrid warfare" are seen as a major security challenge by the EU and NATO, wich have been working both separately and cooperatively since 2015 to develop a coherent strategy in the fight against "hybrid campaigns" with the purpose of helping Member States counter this complex threat. The notions of "hybrid threats", or "hybrid warfare" as favored by NATO, are not unanimously supported nor univocally understood by either organization nor, for that matter, within either institution. Even though Belgium has to this day not developed a centralized approach to "hybrid threats", it has addressed the problem through the bias of several bodies responsible for coordinating the country's security policy, no matter the estimated threat level, whether "hybrid" or not. In his latest "Strategic Vision for Defense" issued in June 2016, the Belgian Defense Minister has himself acknowledged the importance of "hybrid warfare".

This study is in two parts. The first part will consider the origins and development of the "hybrid warfare" concept, particularly within the EU and NATO. The second part will explore the various strategies implemented by both organizations as well as Belgium's involvement in the fight against hybrid threats.

Les pratiques de la « *guerre hybride* » sont considérées comme un défi sécuritaire majeur par l'UE et l'OTAN, qui s'attellent depuis 2015 à développer, chacune de leur côté mais en coopérant, une stratégie cohérente dans la lutte contre les « *campagnes hybrides* », afin d'aider les pays membres à contrer cette menace complexe. La notion de « *menaces hybrides* » et celle de « *guerre hybride* », préférée par l'OTAN ne font cependant pas l'unanimité et ne semblent pas toujours signifier la même chose, selon l'organisation et parfois même au sein d'une même institution. À ce jour, il n'existe pas de politique belge centralisée en ce qui concerne la lutte contre les « *menaces hybrides* ». La Belgique dispose néanmoins de différents organismes chargés de coordonner la politique sécuritaire du pays, quel que soit le degré de la menace, qu'elle soit « *hybride* » ou non. Dans sa dernière « *vision stratégique pour la défense* » de juin 2016, le ministre belge de la Défense reconnaît également l'importance de la problématique de la « *guerre hybride* ».

La présente étude comporte deux parties. La première a pour but de mieux discerner comment est né et a évolué le concept de « *guerre hybride* », singulièrement au sein de l'UE et à l'OTAN. La seconde partie analyse la stratégie mise en place par les deux organisations pour lutter contre les menaces hybrides mais également les mesures prises par la Belgique pour participer à cette stratégie.

Table des matières

Liste des abréviations et acronymes

ACOS Ops & Trg	Département d'état-major Opérations et Entraînement
CBRN	Chemical, biological, radiological and nuclear
CERT	Computer Emergency Response Team
CGCCR	Centre Gouvernemental de Coordination et de Crise
CHCRISP	Courrier hebdomadaire du Centre de recherche et d'information socio-politiques
DIMEFIL	Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement
DP	Document parlementaire
EEAS	European External Action Service
ERM	École Royale Militaire
EI	État islamique
EMUE	État-major militaire de l'UE
EU	European Union
(EU) INTCEN	(European Union) Intelligence Analysis Center
FoP	Friends of the Presidency Group
IISS	International Institute for Strategic Studies
IRSD	Institut royal supérieur de défense
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NMSG	Nato Modeling and Simulation Group
NSA	National Security Agency
OCAM	Organe de Coordination pour l'Analyse de la Menace
OTAN	Organisation du traité de l'Atlantique Nord
PACE	Parallel and Coordinated Exercise
PIB	Produit intérieur brut
PESC	Politique étrangère et de sécurité commune
PSC	Political and Security Committee
PSDC	Politique de sécurité et de défense commune
SRI	Sécurité des réseaux et de l'information
TFUE	Traité sur le fonctionnement de l'Union européenne
TUE	Traité sur l'Union européenne
URSS	Union des républiques socialistes soviétiques
RAP	Readiness Action Plan
RDN	Revue Défense Nationale
RFAF	Russian Federation Armed Forces
SEAE	Service européen pour l'action extérieure
SIPRI	Stockholm International Peace Research Institute
STRATCOM	Strategic Communications
UE	Union européenne
VJTF	Very High Readiness Joint Task Force

Introduction

« *Menace hybride ? Vous avez dit menace hybride?* ». On serait en effet tentés d'appliquer la célèbre réplique à un terme qui fait le « *buzz* » aujourd'hui. Georges-Henri Soutou explique le succès actuel de la notion par l'évolution même d'un système international à la fois complexe et « *flou* », engendrant des stratégies qui ne peuvent être en quelque sorte qu'hybrides et répondent à des menaces liées à une certaine dématérialisation des conflits[1]. Selon J-.Ch. Coste, « *ce flou offre l'opportunité à des États, dans le système international actuel, globalement figé par l'équilibre de la dissuasion nucléaire, d'une nouvelle forme de conflictualité, dans laquelle peuvent également intervenir des belligérants privés* »[2].

La présente étude entend traiter des « *menaces hybrides* » ou pratiques de la « *guerre hybride* », considérées, depuis quelques années, comme un défi sécuritaire majeur par l'UE et l'OTAN. Il s'agira à la fois de saisir la complexité sémantique de cette terminologie mais également de comprendre les nouveaux enjeux géopolitiques qui y sont associés. L'implication de la Belgique au sein de l'UE et de l'OTAN pour faire face à ces problématiques constitue un fil rouge important du travail.

Si la « *guerre hybride* » est au cœur de nombreux ouvrages, peu d'entre eux étudient, de façon systématique, l'implication de l'UE et de l'OTAN en la matière. La présente analyse s'appuie sur les positions officielles des deux organisations.

Cette étude comporte deux parties et une conclusion. La première a pour but de discerner comment est né et a évolué le concept de *« guerre hybride* », singulièrement au sein de l'UE et à l'OTAN. Nous verrons à cette occasion, à travers une approche historique fouillée, que cette construction sémantique est loin de faire l'unanimité. La seconde partie analyse la stratégie mise en place par les deux organisations pour lutter contre les menaces hybrides mais également les mesures prises par la Belgique pour participer à cette stratégie. En conclusion, une série de réflexions porteront sur l'utilité d'un recours au *buzz word* de la « *guerre hybride* », pour une redéfinition des stratégies de défense contemporaines et une implication appropriée dans les phénomènes géopolitiques actuels.

[1] G.-H. Soutou, *Éditorial*, dans *Stratégique*, n°111, Paris, 2016, p. 8 ; ID., « La stratégie du flou », dans *Politique Magazine*, n°131, juillet-août 2014.

[2] J-C. Coste, « De la guerre hybride à l'hybridité cyberélectronique », dans *RDN*, mars 2016, p. 23.

Partie 1 : Les « menaces hybrides » : définitions et enjeux

Cette première partie de l'étude a pour but de discerner comment est né et a évolué le concept de *« guerre hybride*», singulièrement au sein de l'UE et à l'OTAN. Nous verrons à cette occasion ce que cette construction sémantique, relativement neuve, engendre comme confusion dans les esprits et pourquoi elle est loin de faire l'unanimité.

La « guerre hybride » : réalité sémantique et géographique

Dans les dictionnaires de référence, le terme « *hybride* » est associé à des registres aussi divers que la biologie, l'agriculture ou la linguistique. L'adjectif renvoie toujours à ce qui est « *composé de deux éléments de nature différente anormalement réunis* »[3]. Dans le langage familier, le terme « *hybride* » peut également être associé à quelque chose « *d'une nature mal définie, vague* »[4]. Ce n'est qu'au début des années 2000 que l'adjectif « *hybride* » est pour la première fois utilisé en association avec un conflit armé.

Deux écoles tentent alors de définir le concept de « *guerre hybride* ». D'une part, l'école « *kinetic kit* », qui n'envisage que l'aspect cinétique de celle-ci, la décrivant comme la combinaison des forces et tactiques militaires régulières[5] et irrégulières[6]. William J. Nemeth est le premier de ce courant de pensée à utiliser, en 2002, le terme de « *guerre hybride* » pour caractériser l' « *insurrection tchétchène* », qu'il décrit comme « *un modèle de guerre hybride* »[7] et « *la forme contemporaine de la guérilla* »[8] dans la mesure où cette guerre « *asymétrique* »[9] constitue une « *continuation de la guerre menée par un 'pré-État' devenu plus efficace vu son emploi de*

---

[3] *Le Petit Robert*, 2007, p. 1256.

[4] *Nouveau Larousse Universel*, 1948, p. 955.

[5] La guerre régulière se caractérise par le recours à un matériel à haute intensité en capital, une armée qui représente un État, contrôlant un territoire, une population et qui défend une ligne de front (E. Tenenbaum, « Guerre hybride : concept stratégique ou confusion sémantique ? », dans *Revue de Défense Nationale (RDN)*, mars 2016, p. 33).

[6] Pour H. Coutau-Bégarie, la guerre est « *irrégulière* » quand elle est « *menée par des combattants sans statut n'appartenant pas à l'armée régulière, c'est-à-dire mise sur pied et entretenue par un pouvoir souverain* » (H. Coutau-Bégarie, « Guerres irrégulières : de quoi parle-t-on ? », dans *Stratégique*, janvier 2009, n° 93-96, p. 15). Dans la guerre irrégulière, le recours à la guérilla, les embuscades mais aussi le terrorisme et la propagande est monnaie courante (E. Tenenbaum, *op. cit.*)

[7] William J. Nemeth, *Future War and Chechnya : a Case for Hybrid Warfare*, thèse, Monterey, 2002, p. v.

[8] *Ibid.*, p. 29. On définit la « *guérilla* » comme des « *opérations militaires et paramilitaires conduites en territoire tenu par l'ennemi, par des forces irrégulières, principalement autochtones* » (*Glossaire OTAN de termes et définitions (anglais-français)*, version 2010 (www.nato.int), p. 2-G-4, [AAP-6 (2010)]).

[9] Pour le colonel Philippe Boone, « *la guerre asymétrique, c'est l'absence de correspondance entre les buts, les objectifs et les moyens des forces belligérantes*». Il s'agit, en d'autres termes, d'un « *conflit qui oppose des combattants dont les forces sont incomparables; où le déséquilibre militaire, sociologique et politique entre les les camps est total; une armée régulière forte contre un mouvement de guérilla à priori faible [ou] une nation contre un mouvement terroriste* » (A. Martin et L. Coriou, « Définir un conflit asymétrique », dans *Le Monde.fr*, 31 mars 2003).

technologies et de méthodes modernes »[10] et son recours à des méthodes non conventionnelles[11]. Issu de la même mouvance, Max Boot considère la récente intervention russe en Crimée comme un exemple de « *guerre hybride* » où ont été déployés armement lourd et forces « *spéciales* » (« *les petits hommes verts* » [12])[13].

D'autre part, l'école dite du « *full spectrum* » ou, selon la terminologie de l'OTAN, du « *DIMEFIL spectrum* »[14], qui rassemble plus d'adhérents que le premier courant intègre dans sa définition de la guerre hybride non seulement les manœuvres cinétiques, ou ce que l'on appelle le « *hard power* » (coercition ou manière forte), mais également les actions non cinétiques, ou « *soft power* » (puissance douce)[15], à laquelle a recours l'*hybrid warfare* afin d'atteindre certains objectifs[16]. La nature de ceux-ci permet de distinguer la « *guerre hybride* » du « *conflit hybride* ». En effet, contrairement à celui de la guerre hybride, le but du « *conflit hybride* » n'est pas de blesser, diminuer ou détruire l'adversaire mais seulement d'influencer le comportement de celui-ci afin qu'il se conforme à la volonté de son adversaire[17]. Dans un « *conflit hybride* », les belligérants n'ont pas recours à des forces armées mais bien à de l'intimidation militaire, des moyens de pression économiques, politiques, diplomatiques ou technologiques[18]. En outre, le recours par l'ennemi à plusieurs des méthodes utilisées dans les guerres et conflits hybrides constitue une « *menace hybride* », dès lors considérée comme « *multidimensionnelle* »[19].

Le général James Mattis et le colonel Frank Hoffman, qui entendent tirer les premiers enseignements du chaos qui s'est emparé de l'Irak[20] et s'inscrivent dans la mouvance du « *full*

---

[10] William J. Nemeth, *Future War and Chechnya: a Case for Hybrid Warfare*, thèse, Monterey, 2002, p. 29.

[11] *Ibid.*, p. 70. La guerre conventionnelle voit s'affronter des armées régulières équipées d'armes de haute technologie. La guerre dite non-conventionnelle se caractérise, quant à elle, par des guérillas menées par des groupes armés irréguliers possédant un armement léger et relevant d'un niveau technologique très limité (L. Henninger, « La 'guerre hybride' : escroquerie intellectuelle ou réinvention de la roue ? », dans *RDN*, mars 2016, p. 51).

[12] Les « *petits hommes verts* », forces spéciales russes sans insignes observées en Crimée, ne permettaient pas une identification correcte, ni la qualification en bonne et due forme d'une agression. Il s'agissait *in fine* de manœuvrer en se servant d'une interprétation du droit international (J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, pp. 19-20 ; E. Tenenbaum, « La manœuvre hybride dans l'art opératif », dans *Stratégique*, n°111, Paris, 2016, p. 52)

[13] Agence européenne de défense, *Hybrid Warfare Threats-Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 novembre 2015 [SCS/P003198], p. 12.

[14] DIMEFIL signifie les fronts diplomatique/politique, de l'information, militaire, économique, financier, du renseignement et juridique.

[15] J. Clech définit le « *soft power* » comme les mesures de coercition commerciales et financières qui ont trait par exemple à la culture, aux médias, aux réseaux sociaux ou à la propagande (J. Clech, « L'hybridité: nouvelles menaces, inflexion stratégique? », dans *RDN*, mars 2016, pp. 12-13).

[16] Agence européenne de défense, *Hybrid Warfare Threats-Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 novembre 2015 [SCS/P003198], p. 9.

[17] I. Mayr-Knoch, N. Mair et J. Mittelstaedt, « Plaidoyer pour une stratégie hybride de l'Union européenne », dans *RDN*, mars 2016, p. 45.

[18] P. Pawlak, *At a glance. Understanding Hybrid Threats, European Parliamentary Research Service*, www.epthinktank.eu, 24 juin 2015.

[19] *Ibid.*

[20] E. Tenenbaum, « La manœuvre hybride dans l'art opératif », dans *Stratégique*, n°111, Paris, 2016, pp. 43-44.

spectrum », définissent la guerre hybride dans un article paru en 2005 dans les *U.S. Naval Institute Proceedings*[21]. Selon eux, la situation américaine en Irak se caractérise à l'époque par « *un état de violence dit post-conflit résultant du vide sécuritaire de la chute du régime baasiste, une guerre civile intercommunautaire et interconfessionnelle, une insurrection contre l'occupant étranger, une activité terroriste internationale, ainsi qu'un risque potentiel de dissémination d'armes de destruction massive* »[22]. Le terme est ensuite repris lors de la guerre d'Israël contre le Hezbollah au Liban en 2006. Israël se révèle en difficulté face à un adversaire qui, tout en restant irrégulier et asymétrique, se montre capable de manœuvrer tactiquement et de conjurer une puissance de feu par des moyens techniques, tels les missiles guidés ou les drones, jusqu'alors utilisés au seul profit d'armées nationales régulières[23].

Plus récemment, la notion d'hybridité a refait surface dans les interventions armées ou non de la Russie en Estonie (2007) [24], en Géorgie (2008)[25] et enfin, en Ukraine (2014)[26]. Lors de la crise russo-ukrainienne, le comportement russe se caractérise, selon certains auteurs, par le recours à une « *guerre de seuil* » permettant de générer des effets stratégiques sans avoir à subir les conséquences d'une opération militaire en bonne et due forme[27]. De tels procédés peuvent profondément déstabiliser la communauté internationale, qui se voit dans l'incapacité de réagir, par la voie militaire notamment[28]. La « *guerre hybride* » englobe ici un certain nombre de pratiques relevant de la stratégie intégrale russe caractérisée par le recours à un ou une combinaison de facteurs ambigus, tels

---

[21] J. N. Mattis et F. Hoffman, « Future Warfare: the Rise of Hybrid Wars », dans *U.S. Naval Institute Proceedings*, novembre 2005, vol. 131, n°11, pp. 18-19.

[22] E. Tenenbaum, « Guerre hybride : concept stratégique ou confusion sémantique ? », dans *Revue de Défense Nationale (RDN)*, mars 2016, p. 32.

[23] *Ibid.*

[24] En avril 2007, l'Estonie est victime d'une série de cyber-attaques sans précédent contre ses sites officiels, ses banques et ses médias, après l'enlèvement dans un jardin public de Tallin d'un mémorial de guerre datant de la période soviétique. (T. Selhorst, « Russia's Perception Warfare. The Development of Gerasimov's Doctrine in Estonia and Georgia and its Application in Ukraine », dans *Militaire Spectator*, n°4, 2016, pp. 154-155).

[25] En août 2008, la Géorgie lance une offensive militaire contre sa province séparatiste d'Ossétie du Sud dont les velléités indépendantistes empoisonnent la vie politique géorgienne depuis quinze ans. La Russie envoie alors chars et artillerie afin de protéger la population de cette région, dont la majorité est en possession d'un passeport russe. Une dizaine de jours après le début des hostilités, un cessez-le-feu est finalement signé. Pendant cette guerre, les Russes auront largement recours à la propagande (« *information warfare* ») et aux attaques cyber sur les principaux serveurs géorgiens (T. Selhorst, *op. cit.*, pp. 155-157).

[26] J-C. Coste, « De la guerre hybride à l'hybridité cyberélectronique », dans *RDN*, mars 2016, p. 19. La crise en Ukraine est une crise diplomatique internationale consécutive à l'occupation la péninsule de Crimée par des troupes pro-russes non identifiées, puis à des mouvements de troupes de l'armée russe près de la frontière ukrainienne, à partir du 27 février 2014, suite à la manifestation pro-européenne « *Euromaïdan* » qui a abouti à la destitution du président ukrainien pro-russe Viktor Ianoukovytch. Le 18 mars 2014, à la suite d'un référendum, le gouvernement russe annonce que la République de Crimée et la ville de Sébastopol deviennent deux nouveaux sujets fédéraux de la Fédération de Russie, ce que conteste la communauté internationale. La crise de Crimée est suivie début avril 2014, par la guerre du Donbass, au sud-est de l'Ukraine, où une insurrection armée séparatiste s'oppose encore à l'heure actuelle au gouvernement central de Kiev. La Russie est accusée de soutenir militairement les insurgés (A. Dumoulin, « Crise russo-ukrainienne. Conséquences sur les politiques de défense de l'OTAN, UE et de défense nationale », dans Sécurité & Stratégie-IRSD, n°125, juin 2016, pp. 3, 6- 8, 15)

[27] J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, p. 20.

[28] *Letter of the Defence Policy Directors of 10 Northem Group Nations to EEAS DSG Maciej Popowsk*i, 17 février 2015.

que la possibilité d'effectuer une invasion de « *petits hommes verts* » sans en subir de conséquences militaires en retour ; le recours russe aux « *proxys* », forces agissant par procuration pour d'autres et soutenues militairement par ceux-ci[29] ; la possibilité d'utiliser les exportations en tant que leviers de pressions politiques ; et plus généralement, l'usage de toutes les ressources de puissance afin de permettre la réalisation des objectifs stratégiques[30]. L'utilisation des armes numériques à des fins de subversion par les Russes en Estonie en 2007, en Géorgie en 2008, et plus récemment en Crimée, est également considérée comme un mode opératoire hybride[31]. En 2009, Frank Hoffman définit la guerre hybride comme la *« capacité de mener une guerre, de façon adaptative, un mixte d'armes conventionnelles[32], de tactiques irrégulières, de terrorisme et de comportements criminels dans l'espace de bataille afin d'atteindre ses objectifs politiques* »[33]. Comme nous le verrons dans les chapitres suivants, cette vision des choses trouvera un certain écho institutionnel auprès de l'UE et de l'OTAN.

D'aucuns considèrent actuellement l'organisation « *État islamique* » (EI) comme un « *acteur hybride* » capable de remporter de vrais succès opératifs[34]. Son expansion territoriale maximale en Syrie et en Irak remonte en effet à 2014[35]. Pour E. Tenenbaum, l'EI recourt à un certain type de manœuvres hybrides qui relèvent de ce que l'on pourrait appeler une « *techno-guérilla* »[36]. Pour J. Henrotin, l'EI constitue en effet « *la forme la plus aboutie de l'ennemi hybride* »[37]. Il est « *l'incarnation du cauchemar (…) : un groupe fondamentalement irrégulier (…) combinant (…) [l'] usage du terrorisme et de la guérilla en tant que modes d'action tactique et [les] technologies modernes. (…) La guerre hybride (…) [à laquelle recourt l'organisation est] une véritable stratégie militaire opérationnelle incluant l'utilisation d'une stratégie d'influence/de guerre psychologique, d'une stratégie des moyens matériels mais aussi humains ; et également l'usage d'une proto-stratégie aérienne, voire d'armes chimiques et biologiques improvisées* »[38]. Selon Stéphane Taillat,

---

[29] L'appui des « *proxys* », singulièrement lors des opérations dans le Donbass, permettait de contourner le droit international afin de saper les bases d'une riposte juridiquement légitime (E. Tenenbaum, « La manœuvre hybride dans l'art opératif », dans *Stratégique*, n°111, Paris, 2016, p. 20). En définitive, la guerre par *proxy* est un « *combat couplé* » qui consiste en l'utilisation simultanée d'une force principale et de forces de guérillas contre un ennemi. On crée ainsi « *une hybridation couplant à la fois des forces conventionnelles et non conventionnelles (concentrées) et non-conventionnelles (dispersées) dans le même temps* » (*Ibid.*, p. 23).

[30] *Ibid.*, pp. 19-20.

[31] S. Taillat, « Un mode de guerre hybride dissymétrique ? Le cyberspace », dans *Stratégique*, n°111, Paris, 2016, p. 89 ; A. Dumoulin, « Crise russo-ukrainienne. Conséquences sur les politiques de défense de l'OTAN, UE et de défense nationale », dans Sécurité & Stratégie-IRSD, n°125, juin 2016, pp. 6, 15.

[32] Dans la terminologie otanienne, une « arme conventionnelle est une arme qui n'est pas de nature chimique, ni biologique, radiologique ou nucléaire (*Glossaire OTAN de termes et définitions (anglais-français)*, version 2010, p. 2-C-15 (www.nato.int), [AAP-6 (2010)]).

[33] F. Hoffman, « *Hybrid vs. Coumpound War-The Janus Choice: Defining Today's Multifaceted Conflict*», dans *Armed Forces Journal*, octobre 2009.

[34] E. Tenenbaum, « La manœuvre hybride dans l'art opératif », dans Stratégique, n°111, Paris, 2016, p. 56.

[35] *Ibid.*, pp. 56-57.

[36] E. Tenenbaum, « La manœuvre hybride dans l'art opératif », dans Stratégique, n°111, Paris, 2016, p. 57. Christian Malis définit la techno-guérilla comme un mode de guerre qui combine certaines des tactiques classiques de la guérilla et d'autres plus innovantes (*swarming*) et y associe l'usage de technologies avancées comme les drones ou les missiles antichars (Chr. Malis, « Guerre hybride et stratégies de contournement », dans *RDN*, mars 2016, p. 27).

[37] J. Henrotin, « L'État islamique, forme la plus aboutie de l'ennemi hybride ? », dans *DSI* hors série n°40, décembre-janvier 2015.

[38] *Ibid.*, p. 38

la présence active de l'organisation « *État Islamique* » sur les réseaux sociaux afin d'y pratiquer la propagande constitue également un élément important de la manœuvre hybride[39]. D'après Hervé Pierre, « *Daech qui, bien que disposant d'un territoire, d'une population et d'une forme de gouvernement n'est (heureusement) pas reconnu comme un 'État', demeure en conséquence, à défaut d'insertion dans le système international, une organisation 'privée' mais qui excelle dans l'hybridité de posture. Les attentats terroristes commis à l'étranger (…) sur des cibles 'molles' à fort impact médiatico-psychologique sont combinés aux actions d'unités militaires de type conventionnel, opposant, en Syrie comme en Irak, la force à la force* »[40]. [Dans le cas de Daesh], « *le qualificatif d'hybride devient ainsi l'apanage de groupes combattants sociologiquement irréguliers mais en possession de certaines capacités clés considérées comme avancées qui semblaient jusqu'alors l'apanage de stratégies régulières* »[41].

Notons par ailleurs que le recours aux méthodes hybrides ne semble pas être le propre des Russes ou de l'EI. Ainsi, selon l'Agence européenne de défense, les activités chinoises en mer de Chine méridionale représentent un « *usage magistral des composantes non cinétiques de la guerre hybride* »[42]. Désireuse d'occuper une position stratégique importante dans cette région, la Chine y met en œuvre, depuis 2014-2015, sa doctrine des « *trois guerres* » (*Three Warfares*) adoptée en 2003 et « *qui envisage la guerre sous l'angle psychologique, médiatique et légal afin d'atteindre des objectifs stratégiques sans recourir à la guerre cinétique* »[43]. Ainsi, Pékin s'est approprié *de facto* la municipalité de Sansha, nom donné par la Chine en 2012 à l'ensemble des terres émergées dans la zone centrale de la Mer de Chine du Sud. Cet espace maritime est pourtant revendiqué par le Vietnam et Taiwan et ne bénéficie d'aucune reconnaissance juridique[44]. Depuis 2013, la Chine y organise pourtant des voyages touristiques, ce qui attise les tensions dans la région[45]. Cette action se complète par la construction, à grande échelle, de structures portuaires et aéroportuaires basées sur les récifs du centre de la mer de Chine du Sud[46].

D'aucuns prétendent que l'Iran a également recours à certains éléments du spectre de la guerre hybride afin d'accroître son influence au Moyen-Orient. Dès mai 2003, à l'issue de l'opération « *Iraqi Freedom* », l'Iran aurait ainsi infiltré des agents du gouvernement irakien en se cachant parmi les réfugiés irakiens qui retournaient dans leur pays. D'après H. Gardner, cette manière de faire encouragera la Russie à recourir aux « *petits hommes verts* » en Ukraine, « *en révélant comment ceux-ci pouvaient être utilisés comme des outils politiques et militaires efficaces*

---

[39] S. Taillat, « Un mode de guerre hybride dissymétrique ? Le cyberspace », dans *Stratégique*, n°111, Paris, 2016, pp. 89, 95.

[40] H. Pierre, *(Re) penser l'hybridité avec Beaufre*, *Stratégique*, n°111, Paris, 2016, p. 41

[41] E. Tenenbaum, « La manœuvre hybride dans l'art opératif », dans *Stratégique*, n°111, Paris, 2016, p. 46.

[42] Agence européenne de défense, *Hybrid Warfare Threats-Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 novembre 2015 [SCS/P003198], p. 41.

[43] *Ibid.*, p. 31.

[44] En juillet 2016, le tribunal arbitral de la Haye confirme l'existence d'une zone internationale au centre de la mer de Chine du Sud et invalide donc toutes les revendications sur des eaux territoriales dans cette zone. Pékin a cependant déclaré « *la décision des juges nulle et non avenue* » (J.-V. Brisset, « Quand Steve Bannon prédit un conflit en mer de Chine du Sud: le conseiller spécial de Donald Trump est-il un lucide ou un dangereux va-t'en guerre? », dans *Atlantico*, 3 février 2017 (www.atlantico.fr); L. Defranoux, « Dix questions pour comprendre le conflit en mer de Chine méridionale », dans *Libération*, 12 juillet 2016 (www.libération.fr).

[45] F. Lelièvre, « Le tourisme, l'autre arme de Pékin pour conquérir la mer de Chine du Sud, Hongkong », dans www.letemps.ch, 26 mai 2016.

[46] J.-V. Brisset, *op. cit.*

contre leurs voisins respectifs »[47]. Le support militaire et financier de l'Iran aux milices chiites en Irak et du Hezbollah au Liban, ainsi que le recours à des *proxy forces* dans ces pays afin d'y étendre son influence, est également considéré comme une forme de guerre hybride[48]. Hall Gardner associe ici la guerre hybride à une nouvelle forme de « *brinksmanship* » (politique calculée)[49]. L'objectif serait en effet de profiter des lacunes sociales, politiques, économiques et militaires de l'adversaire, dans ce cas-ci Israël et les États-Unis, en utilisant successivement ou simultanément différentes sortes d'attaques ou menaces afin de mettre fin à leur hégémonie dans une région[50].

Si le concept de guerre hybride englobe une vaste réalité géographique et sémantique, il reste cependant largement associé aux méthodes utilisées par la Russie en Ukraine[51]. Le point suivant vise à démontrer que d'aucuns considèrent même la stratégie hybride russe, comme le « *côté obscur de l'approche globale* ».

La stratégie hybride russe, côté obscur de l'approche globale ?

Selon l'Agence européenne de défense, les États membres de l'UE sont particulièrement vulnérables aux variantes non cinétiques des guerres hybrides parce que leurs sociétés et institutions sont décentralisées et démocratiques[52]. Un État autoritaire a en effet davantage de contrôle sur de nombreux instruments d'influence civile, comme l'économie ou les médias, que les états démocratiques, et plus encore l'UE[53]. « *Par ailleurs* », selon I. Mayr-Knoch, *« en démocratie, l'utilisation de certains instruments clandestins est sujet à discussions sur le plan légal et moral ; souci dont ne se préoccupent pas les régimes autoritaires* »[54]. Il est ainsi patent de constater que la convention de Budapest du 23 novembre 2001 sur la cybercriminalité, qui considère celle-ci comme une « *menace pour la démocratie et les États de droit* », n'a toujours pas à ce jour été signée par la Russie[55]. Nombre de gouvernements regardent en effet avec intérêt ces technologies « *qui permettent de porter des coups à leurs adversaires, sans que leur responsabilité juridique puisse être engagée avec certitude* »[56].

Certains considèrent que la « *stratégie hybride*», terme généralement utilisé pour qualifier les méthodes tactiques utilisées par la Russie en Ukraine, serait le « *côté obscur de l'approche*

---

[47] H. Gardner, « Hybrid Warfare: Iranian and Russian Versions of 'Little Green Men' and Contemporary Conflict », dans *Research Paper NATO Defense College*, Rome, n° 123, décembre 2015, p. 6.

[48] United States Army Special Operations Command, *Counter-Unconventional Warfare-White Paper*, 2014, pp. 5, 8 (consultable sur www.publicintelligence.net); C. Macé, « L'Iran, soutien sans faille de Damas », dans *Libération.fr*, 13 décembre 2016.

[49] H. Gardner, *op. cit.*, p. 4.

[50] *Ibid.*, pp. 3-4.

[51] B. Tigner, « An Evolving Threat», dans *Jane's Defence Weekly*, 24 mai 2017, p. 25.

[52] Agence européenne de défense, *Hybrid Warfare Threats-Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 novembre 2015 [SCS/P003198], p. 54

[53] I. Mayr-Knoch, N. Mair et J. Mittelstaedt, « Plaidoyer pour une stratégie hybride de l'Union européenne », dans *Stratégique*, n°111, Paris, 2016, p. 49.

[54] *Ibid.*, p. 47.

[55] N. Arpagian, *Que sais-je? La cybersécurité*, Paris, 2016, p. 19.

[56] *Ibid.*, p. 22.

globale »[57]. Dans ce domaine, comme dans d'autres, tout semble ici surtout une question de point de vue. Ainsi, le Président Poutine aurait justifié l'annexion de la Crimée en 2014 par le précédent du Kosovo, intervention légitime mais à la légalité encore controversée[58]. De l'autre côté, affirme J. Lemaire, « *on a beau assurer que les interventions occidentales sont conditionnées par le respect du droit international, l'interprétation un peu vague du mandat humanitaire autorisant l'intervention en Libye a pu servir de précédent pour l'opération russe en Crimée* »[59].

Quoi qu'il en soit, le concept de « *stratégie hybride* » a émergé au départ dans les états-majors et les *think tanks* occidentaux pour définir les actions russes en Ukraine, dont les buts sont jugés un peu moins avouables que l'approche globale occidentale[60]. Cette dernière consiste, en effet, à « *utiliser l'ensemble des moyens militaires, paramilitaires et non-militaires, à la disposition d'une nation pour atteindre ses objectifs à la lumière de sa conception de l'intérêt national* »[61]. La première stratégie globale de l'UE est adoptée par le Conseil européen en décembre 2013[62] et par l'OTAN dans son « *concept stratégique* » de 1991[63]. Beaucoup considèrent d'ailleurs que la « *stratégie globale* » (« *comprehensive approach* »), appliquée dans le respect du droit international, serait « *la* » solution pour faire face à la guerre hybride[64].

Du point de vue occidental, l'approche globale cherche à répondre à tout un éventail de menaces et défis par un ensemble de moyens appropriés et complémentaires dans le but d'améliorer la sécurité et la stabilité de la société. La stratégie hybride, en revanche, serait pensée pour éroder le pouvoir de l'État et influencer son comportement, avec comme objectif pour l'agresseur de rester en dessous du seuil qui déclencherait une réponse internationale. Ainsi donc, l'ambition russe serait d'attirer des États dans sa sphère d'influence en utilisant des moyens politiques, civils et militaires pour s'assurer qu'ils ne tombent pas sous le joug du bloc euro-atlantique[65]. Pour J. Lemaire, la « *'stratégie hybride' est devenue l'expression fourre-tout pour désigner les éléments de puissance que la Russie a employés en Ukraine. C'est en fait le révélateur de la surcompensation occidentale après des années de manque d'attention vers l'Est, qui aboutit à regrouper toutes les actions de Moscou sous un seul et même label* »[66].

---

[57] S. Biscop, « Hybrid Hysteria », dans *Security Policy Brief* n°64, juin 2015, p. 1; J. Maire, « Stratégie hybride, le côté obscur de l'approche globale ? », dans *RDN*, septembre 2016, p. 1.

[58] B. Durieux (sous la dir.), *La guerre par ceux qui la font : Stratégie et incertitude au XXIe siècle*, Monaco, 2016 (consulté sur https://books.google.be); A. Frachon, « Poutine, la Crimée et le Kosovo, dans *Le Mondre.fr*, 27 mars 2014.

[59] J. Maire, « Stratégie hybride, le côté obscur de l'approche globale ? », dans *RDN*, septembre 2016, p. 2.

[60] *Ibid.*, p. 1.

[61] E. Tenenbaum, « Le piège de la guerre hybride », dans *Focus stratégique* n°63, octobre 2015, p. 36.

[62] Communication conjointe au Parlement européen et au Conseil intitulée « *The EU's Comprehensive Approach to External Conflict and Crises* », 11 décembre 2013 [JOIN (2013) 30 final]. Lors des guerres post-11 septembre, les forces occidentales ont pris conscience qu'elles avaient des difficultés à gérer le volet civil des conflits et ont dès lors adopté une stratégie globale (J. Maire, « Stratégie hybride, le côté obscur de l'approche globale ? », dans *RDN*, septembre 2016, p. 1).

[63] *Le concept stratégique de l'Alliance approuvé par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Rome les 7 et 8 novembre 1991*, Bureau de l'Information et de la Presse de l'OTAN, Bruxelles, novembre 1991, § 24.

[64] United States Army Special Operations Command, *Counter-Unconventional Warfare-White Paper*, 2014, p. 9; J. Clech, « L'hybridité: nouvelles menaces, inflexion stratégique? », dans *RDN*, mars 2016, p. 12.

[65] J. Maire, « Stratégie hybride, le côté obscur de l'approche globale ? », dans *RDN*, septembre 2016, pp. 1-2.

[66] *Ibid.*, p. 3.

En réalité, les documents stratégiques russes ne mentionnent jamais le terme « *hybride* ». La nouvelle version de la « *doctrine militaire de la Russie* » adoptée par le président Vladimir Poutine le 26 décembre 2014 insiste néanmoins sur la nécessité, dans les conflits actuels, de recourir à des « *instruments* » autres que la puissance militaire, à savoir des « *mesures non militaires, politiques, économiques, informationnelles et autres, mises en œuvre avec une large utilisation de la volonté de protester inhérente à la population et des opérations spéciales* »[67]. La Russie aspire à redevenir une puissance qui compte, dans un contexte international où elle doit manœuvrer habilement entre ses aspirations à la grandeur et la réalité d'une économie de plus en plus fragile. L'emploi des stratégies hybrides semble en effet satisfaire ces conditions : les coûts restent supportables, malgré les sanctions internationales éventuelles[68].

La nouvelle doctrine stratégique de la Russie s'inspire largement de l'article publié en février 2013 par le général Valery Gerasimov, chef de la Défense russe. Dans ce document, que d'aucuns appellent la « *doctrine Gerasimov* »[69], le chef de la *Russian Federation Armed Forces* (RFAF) tire les leçons des récentes interventions russes en Estonie (2007) et en Géorgie (2008)[70]. Pour Gerasimov, qui fait allusion dans le début de son analyse aux « *révolutions de couleur* » (« *color revolutions* »[71]) du « *printemps arabe* », « *le rôle des moyens non-militaires pour atteindre les objectifs politiques et stratégiques a augmenté et, dans de nombreux cas, ceux-ci sont devenus plus efficaces que les armes*»[72]. Dans le cœur de son article, qui s'inspire des récentes interventions russes en Europe de l'Est, Gerasimov dresse un tableau détaillé de l'importance des méthodes non militaires pour résoudre les conflits interétatiques, comme par exemple les sanctions économiques, la pression politique et diplomatique, la mise en place d'une opposition politique ou la « *désinformation* »[73]. Selon lui en effet, « *le champ de l'information ouvre de larges possibilités asymétriques pour réduire le potentiel de combat de l'ennemi* »[74].

---

[67] F. d'Alançon, *Russie : la nouvelle doctrine militaire de Poutine*, www.la-croix.com, 27 décembre 2014.

[68] G. Lasconjarias, « Á l'Est du nouveau ? L'OTAN, la Russie et la guere hybride », dans *Stratégique*, n°111, Paris, 2016, p. 115.

[69] T. Selhorst, « Russia's Perception Warfare. The Development of Gerasimov's Doctrine in Estonia and Georgia and its Application in Ukraine », dans *Militaire Spectator*, n°4, 2016, p. 150.

[70] *Ibid.*, p. 148.

[71] Les révolutions de couleur désignent les soulèvements populaires, pour la plupart pacifiques et soutenues par l'Occident, qui ont causé des changements de gouvernement en Afrique du Nord, au Moyen-Orient mais aussi en Eurasie (Géorgie, Ukraine, Kirghizistan et Biélorussie) au début des années 2000 (« The Value of Science ls in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations », dans *Military Review*, janvier-février 2016, pp. 24, 29 ; B. Pétric, « À propos des révolutions de couleur et du soft power américain », Hérodote, vol. 2, n°129, 2008, pp. 7-20). En mai 2014, le ministre de la défense Sergueï Choïgou dénonce ces révolutions de couleur comme facteur de déstabilisation (Sergueï Choïgou, *Discours à la 3e Conférence sur la Sécurité Internationale de Moscou (MCIS)*, 22-23 mai 2014).

[72] « The Value of Science is in the Foresight. New Challenges Demand. Rethinking the Forms and Methods of Carrying out Combat Operations », dans *Military Review*, janvier-février 2016, p. 24.

[73] *Ibid.*, p. 28. La « *désinformation* » consiste, au moyen de campagnes ciblées dans les médias sociaux, à manipuler les informations dans le but de radicaliser des individus, déstabiliser la société et contrôler le discours politique (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* », 6 avril 2016 [JOIN (2016) 18 final], p. 5).

[74] « The Value of Science is in the Foresight. New Challenges Demand. Rethinking the Forms and Methods of Carrying out Combat Operations », dans *Military Review*, janvier-février 2016, p. 27.

Le point suivant de l'étude vise à analyser la complexité sémantique de l'hybridité à travers les textes officiels de l'UE et de l'OTAN mais également à mieux comprendre le rôle joué par la Russie dans la construction de ce concept.

Définitions de l'UE et de l'OTAN

2010-2015 : développement du concept à l'OTAN

Si la notion de guerre hybride, parfois aussi appelée « *guerre non-linéaire* » (*non-linear warfare*)[75], « *guerre hors limites* »[76], « *guerre ambiguë* »[77] , « *guerre de seuil* »[78], ou « *guerre couplée* »[79] (*compound warfare*) suscite le débat depuis une quinzaine d'années, singulièrement dans les milieux académiques, les définitions de l'UE et de l'OTAN en la matière sont assez récentes. En outre, l'OTAN semble privilégier depuis 2014 le terme de « *guerre hybride* » ou de « *pratiques de la guerre hybrides* » à celui de « *menaces hybrides* ». Enfin, si les définitions proposées par l'UE s'inscrivent clairement dans le courant « *full spectrum* » décrit précédemment, celles de l'OTAN se réfèrent, jusqu'à la crise ukrainienne, au courant de l'école cinétique.

Ainsi, l'OTAN définit pour la première fois les « *menaces hybrides* », dans une note d'août 2010, comme « *des menaces posées par des adversaires capables d'utiliser simultanément des moyens conventionnels et non conventionnels de manière adaptative afin d'atteindre leurs objectifs* »[80]. L'apparition du concept à l'OTAN est sans doute liée à la présence dans l'institution du général Mattis, devenu en 2007 commandant pour la transformation et qui cherche alors à anticiper les défis militaires de l'avenir de l'Alliance, dans le contexte des interventions russes en Estonie et

---

[75] H. Gardner, « Hybrid Warfare: Iranian and Russian Versions of 'Little Green Men' and Contemporary Conflict », dans *Research Paper NATO Defense College*, Rome, n° 123, décembre 2015, p. 1.

[76] D'après les colonels chinois Q. Liang et W. Xiangsui, « *Aujourd'hui, (...) le terrain de la guerre a dépassé les domaines terrestre, maritime, aérien, spatial et électronique pour s'étendre aux domaines de la sécurité, de la politique, de l'économie, de la diplomatie, de la culture et même de la psychologie (...)* ». Ces actes hostiles investissent donc de nouveaux domaines qui sortent de la sphère classique de la guerre d'où le titre « *hors limite* » (Q. Liang et W. Xiangsui, *La guerre hors limites*, Paris, 2003, p. 240). Selon Christian Malis, l'ouvrage de ces deux colonels, publié dans leur langue maternelle en 1999, constitue le premier manifeste sur la guerre hybride (Ch. Malis, « Guerre hybride et stratégies de contournement », dans *RDN*, mars 2016, p. 25).

[77] J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, p. 20. La « *guerre ambiguë* » est associée à la question de l' « *attribution* », c'est-à-dire au fait de ne pas pouvoir déterminer l'auteur d'une attaque (Agence européenne de défense, *Hybrid Warfare Threats-Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 novembre 2015 [SCS/P003198], p. 25).

[78] La « *guerre de seuil* » permet de générer des effets stratégiques sans avoir à subir les conséquences d'une opération militaire en bonne et due forme (J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, p. 20).

[79] Selon la terminologie proposée par l'Américain Thomas Huber en 2002, la guerre couplée consiste à combiner une force régulière offensive à une force irrégulière pour déstabiliser l'adversaire. Certains parlent également de « *guerre par procuration* » (*proxy war*) (E. Tenenbaum, « La manœuvre hybride dans l'art opératif », dans *Stratégique*, n°111, Paris, 2016, pp. 49, 51).

[80] Communication conjointe du SHAPE (Grand quartier général des puissances alliées en Europe) et du SACT (Commandant suprême allié Transformation) intitulée *BI-SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*, 25 août, 2010 (consultable sur www.natolibguides.info).

en Géorgie[81]. Notons néanmoins que la Géorgie n'est, contrairement à l'Estonie, ni membre de l'UE, ni de l'OTAN.

Le document intitulé « *OTAN 2020 : une sécurité assurée ; un engagement dynamique* », rédigé par un groupe d'experts à l'occasion du Sommet de l'organisation à Lisbonne en novembre 2010, se borne, quant à lui, à mentionner l'existence des « *variantes hybrides, combinant par exemple la clandestinité d'un groupe terroriste avec la puissance normalement associée à un État-nation- comme les armes de destruction massive (…)* »[82]. Il est étonnant de constater l'absence du terme « *hybride* » dans le dernier « *concept stratégique* » de l'OTAN, rendu public à ce même Sommet[83].

Pour certains experts, la crise ukrainienne de 2014 constitue une rupture stratégique importante de l'ordre international[84]. L'Alliance atlantique dénonce la politique russe dans cette région, vue comme une menace contre la sécurité euro-atlantique, même si l'Ukraine n'est, rappelons-le, ni membre de l'UE, ni de l'OTAN[85]. L'ex-Secrétaire général de l'OTAN, Anders Fogh Rasmussen, affirme en effet que la Russie a des ambitions qui vont au-delà de l'Ukraine et qu'elle pourrait attaquer un État balte afin de tester la solidarité de l'Occident[86]. Les critiques occidentales reposent alors sur la violation de l'intégrité territoriale en Crimée et la déstabilisation de l'est de l'Ukraine mais également sur le non-respect des dispositions du droit international[87]. L'OTAN décide dès lors de geler la coopération dans des projets communs avec la Russie tout en maintenant les consultations à l'échelon des ambassadeurs et des canaux militaires de haut niveau pour éviter les malentendus[88]. Par ailleurs, la crise russo-ukrainienne pousse les pays membres de l'Alliance atlantique et de l'Union européenne à s'engager dans un processus de réassurance militaire et sécuritaire fortement médiatisé : qu'il s'agisse du rappel du contenu de solidarité de l'article 5 du traité OTAN ou de la mise en place de nouveaux quartiers généraux multinationaux, de l'organisation d'exercices et de manœuvres dans les pays d'Europe centrale et orientale ainsi qu'en mer Noire ou de décisions nationales sur de nouvelles acquisitions militaires et d'augmentation relative des budgets de défense[89]. Dans ce contexte de tensions internationales, le texte de la déclaration du sommet du Pays

---

[81] Tenenbaum, « Guerre hybride : concept stratégique ou confusion sémantique ? », dans *RDN*, mars 2016, p. 32.

[82] *OTAN 2020 : une sécurité assurée ; un engagement dynamique. Analyse et recommandations du groupe d'experts pour un nouveau concept stratégique de l'OTAN*, p. 17.

[83] Le concept stratégique de l'OTAN de 2010 est consultable sur www.nato.int.

[84] Interview, par E. Hoorickx, de membres du Secrétariat International de l'OTAN et du Service de l'Action extérieure de l'UE, lors du débat consacré au thème « Défense européenne et OTAN : mariage de raison ? » le 29 mai 2017 au Palais des Académies de Bruxelles.

[85] A. Dumoulin, *Crise russo-ukrainienne. Conséquences sur les politiques de défense OTAN, UE et de défense nationale*, IRSD- Sécurité & Stratégie, n°125, Juin 2016, p. 8.

[86] *Ibid.*, p. 21.

[87] Les critiques occidentales reposaient sur les constats suivants : le non-respect du Mémorandum de Budapest par lequel l'Ukraine abandonnait l'arme nucléaire en échange de la garantie par les États-Unis, le Royaume-Uni …et la Russie de son intégrité territoriale (1994) ; le non-respect du traité russo-ukrainien selon lequel les parties affirment respecter mutuellement leur intégrité territoriale et confirment l'inviolabilité de leurs frontières communes (1997) ; le non-respect du principe de l'inviolabilité des frontières (Acte final d'Helsinki et Acte fondateur OTAN-Russie de 1997). (A. Dumoulin, *op. cit.*, pp. 8, 22).

[88] A. Dumoulin, *op. cit.*, p. 8.

[89] Pour plus de détails sur les dispositions militaires et sécuritaires prises par l'UE et l'OTAN suite à la crise russo-ukrainienne, lire : A. Dumoulin, *op. cit.*, pp. 20-36 ; *Communiqué du Sommet de Varsovie publié par les*

de Galles de 2014 évoque brièvement l'importance pour l'OTAN d'être en mesure de « *faire face efficacement aux défis spécifiques posés par les menaces que présente la guerre hybride, dans le cadre de laquelle un large éventail de mesures militaires, paramilitaires ou civiles, dissimulées ou non, sont mises en œuvre de façon très intégrée* »[90]. Il est intéressant de constater que cette définition se rapproche désormais davantage de la mouvance du « *full spectrum* ». Dès le printemps 2014, Anders Fogh Rasmussen, alors Secrétaire général de l'OTAN, emploie plusieurs fois le terme de guerre hybride pour décrire ce qui paraît être « *un nouvel art de la guerre* » (*a modern kind of warfare*), aux facettes multiples et aux appellations nombreuses[91].

Le texte rédigé par les ministres de la Défense des pays de l'OTAN le 25 juin 2015 encourage une réaction efficace de l'organisation face aux « *menaces hybrides* », sans toutefois en définir la portée, et recommande, sur requête de l'UE[92], une coordination étroite en la matière avec l'Union[93]. L'influence américaine serait-elle à l'origine du flou sémantique qui entoure alors le concept ? Le Département américain de la Défense a en effet récemment déclaré ne pas envisager la publication d'une doctrine de la guerre hybride, arguant du fait que cette catégorie était trop « *diverse* »[94]. Le terme « *hybride* » n'apparaît d'ailleurs dans aucune des trois dernières « *stratégies nationales de sécurité* » des États-Unis (2006, 2010, 2015)[95]. Un document des Forces spéciales américaines de 2014 définit néanmoins la guerre hybride comme « *l'utilisation par un État ou par [un acteur non-étatique] de tous les moyens diplomatiques, informatifs, militaires et économiques disponibles pour déstabiliser un adversaire* »[96]. Selon ce texte, la Russie, l'Iran, la Chine et l'État islamique ont recours aux méthodes hybrides[97].

Peu de temps après les attentats de Paris de novembre 2015, l'OTAN propose une stratégie pour lutter contre « *la guerre hybride* ». Celle-ci repose sur une directive politique de 2015 et un rapport général sur la guerre hybride entériné par les ministres de la défense en juin de la même année. Elle est approuvée par les ministres des Affaires étrangères en décembre 2015 et fait l'objet d'un « *plan de mise en œuvre* » en février 2016. Ce document stratégique offre une définition très précise de la « *guerre hybride* » : celle-ci « *is underpinned by comprehensive hybrid strategies based on a broad, complex, adaptive and often highly integrated combination of conventional and unconventional means, overt and covert activities, by military, paramilitary, irregular and civilian actors, wich are targeted to achieve (geo)political and strategic objectives. They are directed at an adversary's vulnerabilities, focused on complicating decision making and conducted across the full*

---

chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Varsovie les 8 et 9 juillet 2016, § 37.e) et 40.

[90] *Déclaration du sommet du Pays de Galles publiée par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue au pays de Galles les 4 et 5 septembre 2014*, 7 septembre 2014, § 13.

[91] Anders Fogh Rasmussen, *Future NATO*, Londres, 19 juin 2014 (consultable sur www. nato.int).

[92] Agence européenne de défense, *Hybrid Warfare Threats-Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 novembre 2015 [SCS/P003198], p. 22.

[93] *Déclaration des ministres de la Défense des pays de l'OTAN*, 25 juin 2015, §7.

[94] L. Henninger, « La 'guerre hybride' : escroquerie intellectuelle ou réinvention de la roue ? », dans *RDN*, mars 2016, p. 51.

[95] J.J. Andersson et Th. Tardy, « Hybrid: What's in a Name? », dans *Brief Issue* n°32, octobre 2015, p. 2.

[96] United States Army Special Operations Command, *Counter-Unconventional Warfare-White Paper*, 2014, p. 3 (consultable sur www.publicintelligence.net).

[97] *Ibid.*, pp. 3, 4, 29, 32.

DIMEFIL spectrum in order to create ambiguity and denial. Hybrid strategies can be applied by both state and non-state actors, through different models of engagement, wich may vary significantly in sophistication and complexity. Adversaries employing hybrid strategies will seek to remain ambiguous, claim pursuit of legitimate goals and aim to keep their activities below a threshold that results in a coordinated response from the international community. This includes avoiding direct military confrontation, if possible; although the use of overt military action as part of a hybrid strategy cannot be discounted»[98].

Il est intéressant de constater que la définition de l'hybridité s'élargit désormais aux « *acteurs non étatiques* ». Cette nouvelle nuance sémantique permet ainsi d'inclure les organisations terroristes, et singulièrement l'« *État islamique* », comme acteurs « *des pratiques de guerres hybrides* ». Pour l'OTAN, Moscou semble cependant rester l'acteur principal de la guerre hybride. L'« *État islamique* » aurait, en effet, également recours à certaines pratiques hybrides mais sans disposer, comme la Russie, de structures de pouvoir sophistiquées, en ce-compris un réseau diplomatique établi. La complexité des guerres hybrides est telle que seule une approche individualisée permet de comprendre en profondeur la spécificité de la Russie ou de l'État islamique en la matière[99]. La question reste cependant de savoir si l'on peut réellement parler de « *guerre* » avec « *Daesh* ». Dans le jargon juridique, les attaques armées de cette organisation contre les pays de l'OTAN, relèvent en effet davantage d' « *actes terroristes*»[100] dans un état de droit. Par ailleurs, il serait plus opportun de parler de « *conflit armé non international* »[101], voire de « *guerre civile* »[102], en ce qui concerne la lutte armée que mènent l'Irak et la Syrie contre « *l'État islamique* » et à laquelle prend part une coalition internationale, rejointe formellement par l'OTAN en mai 2017[103]. Dans deux lettres adressées au Secrétaire général des Nations Unies et au Président du Conseil de sécurité, les autorités irakiennes ont en effet demandé aux États membres de les assister dans la lutte contre l'EI en leur fournissant notamment un entraînement militaire et une couverture aérienne. Si cette demande d'assistance constitue une base juridique suffisante pour la participation de la

---

[98] Lors de la conférence organisée à Bucarest par le NMSG (*Nato Modeling and Simulation Group*) les 21 et 22 octobre 2016, et intitulée « *Modeling and Simulation for Hybrid Environments* », la définition de la « *guerre hybride* » telle que proposée par l'OTAN en novembre 2015 a été mentionnée. Le contenu de la conférence est disponible sur *https://www.sto.nato.int/publications/.../MP-MSG-143-08P.pdf*

[99] K. Giles, « Conclusion: Is Hybrid Warfare really New? », dans G. Lasconjarias et J. A. Larsen (sous la dir.), *NATO's Reponse to Hybrid Threats*, forum paper 24, NATO Defence College, Rome, 2015, p. 323.

[100] Le « *terrorisme* » signifie « *l'emploi illégal de la force ou de la violence contre les personnes ou des biens, afin de contraindre ou d'intimider les gouvernements ou les sociétés dans le but d'atteindre des objectifs politiques, religieux ou idéologiques* » (*Glossaire OTAN de termes et définitions (anglais-français)*, version 2010 (consultable sur www.nato.int), p. 2-T-5, [AAP-6 (2010)]).

[101] Un « *conflit armé non international* » oppose « *les forces armées [d'un État souverain] [à] des forces armées dissidentes ou des groupes armés organisés qui, sous la conduite d'un commandement responsable, exercent sur une partie [du] territoire [de État souverain susmentionné] un contrôle tel qu'il leur permettent de mener des opérations militaires continues et concertées (…)* » (*Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés non internationaux (protocole II)*, 8 juin 1977, article 1).

[102] Une « *guerre civile* » est un « *conflit armé important et durable qui oppose, sur le territoire d'un État, soit des groupes armés entre eux soit un ou plusieurs groupes armés au pouvoir en place. Pour qu'il y ait guerre civile proprement dite, ces groupes armés doivent être essentiellement composés de citoyens de cet État* ». (*Dictionnaire militaire. Document de travail de l'École Royale militaire et du Centre linguistique*, Bruxelles, 2005, p. 212)

[103] S.n., « L'Otan va rejoindre la coalition anti-EI », dans *Lefigaro.fr*, 24 mai 2017.

coalition en Irak à la lutte contre « *Daesh* », la démarche est bien plus controversée sur le sol syrien[104].

L'OTAN précise par ailleurs que « *the use of hybrid strategies in conflict are not new, but what is new for NATO is the way a wide range of political, civil and military instruments are combined and coherently applied, aiming at particular vulnerabilities of targeted nations and international organizations in order to achieve strategic objectives* »[105]. Il reprend également quelques « *scénarios de guerre hybride modernes* » qui vont au-delà d'une « *simple menace militaire* », à savoir les cyberattaques, les campagnes de propagande et de désinformation ainsi que les pressions politiques et économiques ciblées et coordonnées[106]. Il va donc de soi que les scénarios hybrides peuvent différer d'un conflit à l'autre et que, pris isolément, ils ne sont pas nécessairement illégaux. En revanche, lorsqu'ils sont appliqués ensemble, ils sont davantage susceptibles de menacer un pays allié, voire l'Alliance atlantique tout entière.

Enfin, suite à la demande de l'UE dans sa communication d'avril 2016 de renforcer la coopération avec l'OTAN dans la lutte contre les « *menaces hybrides* », les chefs d'État et de gouvernement rappellent, lors du Sommet de l'OTAN à Varsovie en juillet 2016, avoir « *adopté [en décembre 2015] une stratégie concernant le rôle de l'OTAN dans la lutte contre les pratiques de guerre hybride, qui est actuellement mise en œuvre en coordination avec l'UE* »[107].

Bien que les concepts stratégiques de l'OTAN ne mentionnent pas la problématique de l'hybridité, ils recensent, depuis la fin de la Guerre froide, de nouveaux risques qui menacent la paix et la stabilité euro-atlantiques[108]. Il s'agit notamment du terrorisme, des conflits ethniques, de la rupture des approvisionnements en ressources vitales, de la prolifération des armes de destruction massive, mais également, dans le concept stratégique de 2010, des cyberattaques. Cette problématique est largement médiatisée depuis que l'Estonie et la Géorgie en ont été les victimes quelques années auparavant. Tous les défis sécuritaires recensés dans les concepts stratégiques de l'Alliance englobent en réalité l'ensemble des « *pratiques de la guerre hybride* » reprises dans les autres documents officiels de l'organisation depuis 2010. Ces problématiques appellent des réponses nouvelles, comme le partenariat avec les Nations-Unies, l'Union Européenne et la Russie ou encore la « *gestion de crises* », susceptibles de porter atteinte à la sécurité de l'Alliance[109].

L'OTAN recommande également, depuis la fin de la Guerre froide, de recourir à une « *approche globale* » pour accomplir efficacement ses tâches de sécurité fondamentales[110]. Cette

---

[104] C. Remy, « Quel cadre légal pour la lutte armée contre l'État Islamique ? », e-Note 22-IRSD, 22 septembre 2016 (consultable sur ww.irsd.be).

[105] Voir le contenu de la conférence organisée à Bucarest par le NMSG (*Nato Modeling and Simulation Group*) les 21 et 22 octobre 2016, et intitulée « *Modeling and Simulation for Hybrid Environments* » (texte disponible sur *https://www.sto.nato.int/publications/.../MP-MSG-143-08P.pdf)*

[106] *Ibid.*

[107] *Communiqué du Sommet de Varsovie publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Varsovie les 8 et 9 juillet 2016*, § 37 (i).

[108] Les concepts stratégiques de 1999 et 2010 sont consultables sur http:/www.nato.int/docu/pr/1999/p99-065f.htm et http:/www.nato.int/cps/fr/natohq/topics_56626.htm. Pour le document stratégique de 1991, voir *Le concept stratégique de l'Alliance approuvé par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Rome les 7 et 8 novembre 1991*, Bureau de l'Information et de la Presse de l'OTAN, Bruxelles, novembre 1991.

[109] E. Hoorickx, « Stratégie atlantique et position de la Belgique dans la 'détente' (1954-1972) », dans Stratégique, n°110, décembre 2015, p. 80.

[110] Voir § 24 du concept stratégique de 1991, § 25 du concept stratégique de 1999 et § 21 du concept stratégique de 2010.

stratégie « *reconnaît l'importance des facteurs politiques, économiques, sociaux et environnementaux en plus de l'indispensable dimension de défense* »[111]. En définitive, depuis 1991, l'Alliance atlantique est consciente qu'elle doit aussi pouvoir répondre à des défis sécuritaires non militaires dont les effets pourraient déstabiliser l'organisation tout autant, et parfois même davantage, qu'une attaque militaire conventionnelle.

J. Henrotin se montre cependant critique vis-à-vis de la mise en œuvre de la stratégie [globale] (ou « intégrale »[112]) de l'OTAN qui apparaît trop souvent comme « *séquentielle*»[113]. Il estime en effet que : « *l'organisation [atlantique] comme ses États-membres n'ont jamais été capables de procéder à la concentration des forces militaires, économiques ou politiques nécessaires à la réussite de la stratégie retenue* »[114]. Selon lui, l'OTAN n'a pas été en mesure, aussi bien dans le cas de la contre-insurrection afghane que dans celui de l'Ukraine, de s'adapter conceptuellement et de comprendre la stratégie comme n'étant pas que militaire *stricto sensu*[115]. D'après lui enfin, l'OTAN se focalise de façon excessive sur « *des concepts stratégiques classiques, soit une guerre régulière utilisant un mode d'engagement cinétique au plan de la stratégie militaire générale, inférieur à celui de la stratégie intégrale* »[116].

Hew Strachan rejoint le raisonnement d'Henrotin. Il souligne en effet l'amalgame qui existe à l'OTAN entre « *grand strategy* » (finalités et moyens politiques et militaires à mettre en place sur le long terme) et « *stratégie militaire* » (plans opérationnels prévus pour résoudre des situations spécifiques dans un futur proche)[117]. Il explique cet état de fait par l'influence de la Guerre froide. À cette époque, la zone géographique de la menace était clairement définie, de sorte que la stratégie de l'OTAN pouvait se concevoir à long terme et s'appuyer sur une planification nucléaire[118]. Pour lui, la « *grand strategy* » [de l'OTAN] ne peut plus se reposer sur une planification nucléaire qui ne constitue pas une réponse suffisante aux périls de ce nouveau type, toujours plus nombreux et complexes. Selon Strachan, la « *grand strategy* » [de l'OTAN] doit donc désormais être davantage « *flexible* » et en mesure d'appréhender des situations imprévues (« *contingency* ») ainsi que ce qu'il appelle les « *chocs stratégiques* », c'est-à-dire les nouvelles menaces qui surgissent sur le court terme. [119]. Or, depuis 1991, la garantie suprême de la sécurité des pays membres de l'OTAN continue à être assurée par les forces nucléaires stratégiques de l'Alliance, en particulier celles des États-Unis[120]. Il y a quelques années, la discussion sur la diminution du rôle des armes nucléaires a été abordée à l'OTAN, avec le soutien de Barack Obama qui prônait, dès 2009, un « *monde sans armes nucléaires* ». Mais le sujet a été mis au frigo après le crash du Boeing de Malaysia Airlines au-dessus

---

[111] Voir § 25 du concept stratégique de l'Alliance atlantique de 1999.

[112] J. Henrotin, *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris, 2014, p. 331.

[113] ID., « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, p. 30.

[114] *Ibid.*, p. 28.

[115] *Ibid.*

[116] J. Henrotin, « L'hybridité à l'épreuve des conflits contemporains : le cas russe », dans *RDN*, mars 2016, p. 40.

[117] E. Hoorickx, « Stratégie atlantique et position de la Belgique dans la 'détente' (1954-1972) », dans *Stratégique*, n°110, décembre 2015, p. 81.

[118] *Ibid.*, p. 80.

[119] *Ibid.*, p. 81.

[120] Voir § 55 du concept stratégique de 1991, § 62 du concept stratégique de 1999 et § 18 du concept stratégique de 2010.

de l'Ukraine en juillet 2014…[121]. Lors du sommet OTAN de Varsovie de juillet 2016, il a par ailleurs été rappelé que les forces stratégiques de l'Alliance, en particulier celles des États-Unis constituent la garantie suprême de la sécurité des Alliés[122].

La question des « *menaces hybrides* » et de la stratégie pour y répondre apparaît plus tardivement dans les milieux européens.

Depuis 2015, une problématique au cœur de la politique sécuritaire européenne

Depuis l'entrée en fonction, en novembre 2014, de F. Mogherini à la tête des affaires étrangères et de la politique de sécurité de l'UE, mais également après l'irruption du terrorisme islamiste en Europe et à la suite de la crise ukrainienne, l'UE veut en effet faire de la lutte contre les « *menaces hybrides* » une de ses priorités[123]. Avant cela, la problématique de l'hybridité n'apparaissait pas dans les documents officiels européens. En février 2015, soit un mois après les attentats de *Charlie Hebdo*, les ministres de la défense de l'UE se réunissent de façon informelle à Riga afin de débattre des questions d'actualité et préparer le Conseil européen de la défense de juin 2015. À cette occasion, les ministres discutent de la réaction de l'UE face aux « *menaces hybrides* » et soulignent la nécessité de renforcer la coopération entre l'UE et l'OTAN en la matière[124].

À la suite de cette réunion de Riga, le Service européen pour l'action extérieure (SEAE) définit pour la première fois la « *guerre hybride* » en mai 2015. La situation internationale de l'époque est alors particulièrement préoccupante, singulièrement en Ukraine et en Europe, touchée par des attentats sanglants revendiqués par « *Daesh* ». S'inspirant de la définition de « *guerre hybride* » fournie en 2014 par l'OTAN lors du Sommet du Pays de Galles, l'UE offre davantage d'explications sur les modes opératoires auxquels l'adversaire peut recourir dans le cadre d'une « *guerre hybride* » mais également sur les « *points faibles* » des États membres face aux « *attaques hybrides* ». Le SEAE définit la « *guerre hybride* » comme « *l'utilisation centralisée et contrôlée de diverses tactiques dissimulées ou non, militaires et/ou non militaires. Celles-ci peuvent couvrir des domaines aussi diversifiés que le recours aux services de renseignements, les opérations cyber, la pression économique ou l'usage de forces conventionnelles. (…) [Le but] de l'agresseur est (…) de déstabiliser l'opposant par des méthodes coercitives et subversives, comme le sabotage, la perturbation des moyens des communications et autres services liés notamment à l'énergie. L'agresseur peut agir par l'entremise de groupes d'insurgés proxy ou justifier une agression interétatique sous le couvert d'une 'intervention humanitaire'. Les campagnes massives de désinformation constituent un élément important d'une campagne hybride. Le but ultime est d'influencer, voire de dominer politiquement un pays en ayant recours à une stratégie globale* »[125]. En outre, un aspect important de la guerre hybride est de générer de l'ambiguïté auprès de la population et de la communauté internationale. En effet, l'ambiguïté, c'est-à-dire le problème d'une

---

[121] Interview de R. Huygelen (ambassadeur de Belgique auprès de l'OTAN de 2010 à 2014), par E. Hoorickx le 16 juillet 2015.

[122] *Communiqué du Sommet de Varsovie publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Varsovie les 8 et 9 juillet 2016*, § 53.

[123] Agence européenne de défense, *Hybrid Warfare Threats-Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 novembre 2015 [SCS/P003198], pp. 21-22.

[124] A. Gnëze, « Communiqué de presse. Les ministres de la défense de l'UE réunis à Riga appellent à l'unité dans la lutte contre les menaces qui pèsent sur la sécurité », 19 février 2015 (www. Eu2015.lv)

[125] Agence européenne de défense, *op. cit.*, p. 21.

'attribution' incomplète, empêche une réaction rapide et efficace parce qu'il devient difficile de savoir qui se cache derrière une attaque[126]. Cette réflexion a sans doute contribué à la création d'un nouveau concept, à savoir celui de « *guerre ambiguë* », que bon nombre de chercheurs associent aux récentes interventions de Moscou en Ukraine. Enfin, selon l'Agence de défense européenne, la caractéristique fondamentale de l' « *attaque hybride* » est que celle-ci vise à exploiter les « *vulnérabilités* » d'un État. D'après elle, ces points faibles, tels que la difficulté à mettre en œuvre une communication stratégique efficace ou à protéger des infrastructures critiques, varient selon les pays membres et sont liés aux faiblesses inhérentes à certaines démocraties occidentales structurellement décentralisées[127].

En juin 2015, la haute représentante, qui « *prend [alors] pour acquis la définition (tacite) des menaces hybrides* »[128], demande au Parlement européen et au Conseil d'améliorer les connaissances en la matière et de renforcer la « *résilience* [129] de l'UE ainsi que la coopération avec l'OTAN dans ce domaine[130]. Á l'époque, A. Pawlak, chercheuse au Parlement européen, cite quelques exemples très diversifiés de « *menaces hybrides* ». Il s'agit, selon elle, du terrorisme, de la cybersécurité défaillante, du crime organisé, des contentieux maritimes, des questions spatiales, de la pénurie des ressources ou des « *opérations secrètes* », comme le recours par la Russie à des forces spéciales (« *hommes verts* ») en Ukraine et de la guerre de l'information[131]. Une « *menace hybride* » serait associée, selon cette analyse, à un mode opératoire spécifique, alors même que l'hybridité ne peut qualifier, par définition, qu'une « *combinaison à deux* »[132].

En octobre 2015, l'état-major militaire de l'UE offre également une définition de la « *guerre hybride* » comme « *l'utilisation combinée, centralisée et contrôlée de diverses activités dissimulées ou non, allant des forces conventionnelles à la pression économique ou aux services de renseignements* »[133]. Il ajoute que les campagnes de désinformation et les tactiques coercitives et subversives sont au cœur de la stratégie hybride. En définitive, celle-ci consiste en « *un usage offensif, contre un État, d'une panoplie complète d'instruments (politiques, idéologiques, économiques, informatifs, humanitaires etc.) avec des méthodes conventionnelles ou non* »[134].

Enfin, la communication conjointe de la haute représentante de l'UE pour les affaires étrangères et la politique de sécurité, datée du 6 avril 2016, propose une nouvelle explication des « *menaces hybrides* », qui s'inspire largement des définitions proposées par l'UE puis par l'OTAN en 2015. Selon la communication conjointe, la notion de « *menaces hybrides* » vise à exprimer un

---

[126] Agence européenne de défense, *Hybrid Warfare Threats-Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 novembre 2015 [SCS/P003198], pp. 20, 25-26.

[127] *Ibid.*, p. 54.

[128] *Ibid.*, p. 22.

[129] « La résilience est la « *capacité de résister à une épreuve et de s'en remettre, en en sortant plus fort* » (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* », 6 avril 2016 [JOIN (2016) 18 final], p. 6).

[130] *European Council Conclusions*, 25-26 juin 2015, [EUCO 22/15, § 10 (c)]

[131] P. Pawlak, *At a glance. Understanding Hybrid Threats, European Parliamentary Research Service*, www.epthinktank.eu, 24 juin 2015.

[132] H. Pierre, *(Re)penser l'hybridité avec Beaufre*, *Stratégique*, n°111, Paris, 2016, p. 34.

[133] EU Military Staff, *Draft Food for Thought Paper: Possible EU Military Contributions to Countering Hybrid Threats*, 2 octobre 2015 [EEAS (2015) 1367 REV1], §3.

[134] *Ibid.*

« *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 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* »[135]. Le document précise en outre qu'il existe plusieurs définitions des menaces hybrides et que celles-ci doivent rester « *adaptables* » en raison du caractère évolutif desdites menaces[136].

L'explication sémantique des « *menaces hybrides* » proposée dans la communication conjointe suscite deux réflexions. D'une part, elle laisse à penser qu'une « *menace hybride* » correspond à un mode opératoire spécifique, ce qui est, comme dit précédemment, contradictoire avec la terminologie même de l'hybridité. D'autre part, la définition proposée par l'UE sur les méthodes dites « *non conventionnelles* » ne correspond pas à celle utilisée dans les milieux universitaires. Traditionnellement en effet, la guerre dite non-conventionnelle se caractérise par des guérillas menées par des groupes armés irréguliers possédant un armement léger et relevant d'un niveau technologique très limité. Selon cette terminologie, la diplomatie ou l'économie ne font donc pas partie de la guerre non conventionnelle. Les « *méthodes non conventionnelles* », à laquelle la communication du 6 avril 2016 fait allusion, semblent plutôt assimilées à des modes opératoires non spécifiquement militaires.

Pour contrer les « *menaces hybrides* », l'UE recommande notamment de renforcer la « *résilience* » face aux cyberattaques mais également aux actes terroristes ou criminels[137]. La communication conjointe précise néanmoins que « *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* »[138]. Cette considération laisse donc penser que le terrorisme et la criminalité organisée ne constituent des « *menaces hybrides* » que lorsque les auteurs de tels actes ont recours à la désinformation et à la propagande. Selon un membre de l'EU INTCEN (*European Union Intelligence Analysis Center*), en effet, « *une attaque terroriste ou le crime organisé constituent des menaces hybrides uniquement si on y recourt pour obtenir des résultats politiques qu'on n'obtiendrait pas par la voie militaire [conventionnelle]* »[139]. D'après cette même personne, « *les attentats de Paris de novembre 2015 ne représentent [dès lors] pas une menace hybride, [puisque leurs auteurs n'avaient pas d'autre objectif que de semer la terreur]* »[140]. Pour pouvoir parler de « *menaces hybrides* », il faut qu'il y ait « *non seulement une utilisation de certains outils hybrides mais également une intentionnalité de faire pression sur un État, en obtenant des résultats militaires par des moyens non directement militaires* »[141].

---

[135] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 2.

[136] *Ibid.*

[137] *Ibid.*, pp. 11, 15.

[138] *Ibid.*, p. 15.

[139] Interview réalisée au sein de l'EU INTCEN par E. Hoorickx, le 30 novembre 2016.

[140] *Ibid.*

[141] *Ibid.*

Si les premiers documents stratégiques de l'UE ne mentionnent pas le terme « *hybride* », ils répertorient néanmoins les mêmes menaces sécuritaires que celles reprises dans les « *concepts stratégiques* » de l'OTAN, comme le terrorisme, la criminalité organisée, la prolifération des armes de destruction massive[142] ou, à partir de 2013, la « *dégradation des ressources* » et la cybersécurité[143]. Cette année-là en effet, débute ce qui deviendra l' « *Affaire Snowden* », du nom d'Edward Snowden, ancien informaticien au sein du cabinet Booz Allen Hamilton, sous-traitant de la NSA (*National Security Agency*). Snowden permet à l'époque la mise au jour de l'existence du programme « *Prism* », espionnage à grande échelle conduit depuis 2007 par la NSA, hors du territoire des Etats-Unis[144]. L'hebdomadaire allemand *Der Spiegel* révèle d'ailleurs, dès octobre 2013, que le téléphone mobile personnel d'Angela Merkel est écouté par les grandes oreilles étatsuniennes[145]. Le nouveau concept stratégique de l'UE de 2016, toujours en vigueur actuellement, inclut pour la première fois la problématique des « *menaces hybrides* »[146].

Les menaces hybrides constituent encore actuellement une préoccupation majeure des décideurs politiques. Récemment Guy Verhofstadt, président de l'Alliance des démocrates et des libéraux pour l'Europe, a insisté sur la nécessité pour celle-ci de résister à « *la guerre hybride que Poutine mène contre l'Occident* ». Selon lui, « *à travers les sites de désinformation et les cyberattaques, la Russie cherche [en effet] à saper la confiance des Européens en la démocratie* »[147]. Il fait ici allusion à la cyberopération dont a été accusée la Russie à l'occasion de l'élection présidentielle américaine, au piratage du Bundestag allemand début 2015, à la cyberattaque subie par la Commission européenne en novembre 2016 mais aussi au soutien, financé par la Russie, d'organisations nationalistes d'extrême droite et de mouvements populistes européens, en particulier lors des élections importantes de 2017[148].

En définitive, si les « *menaces hybrides* » sont au cœur de la stratégie de l'UE et de l'OTAN, singulièrement depuis la crise ukrainienne, une certaine confusion sémantique subsiste. La notion de « *guerre hybride* » est d'ailleurs loin de faire l'unanimité. Certains s'interrogent en effet sur la pertinence, l'utilité et les raisons du recours à une telle terminologie.

---

[142] Si la problématique de la prolifération des armes de destruction massive est largement abordée dans le concept stratégique de l'UE de 2003, elle n'est étonnamment pas mentionnée dans celui de 2016 (Note du Haut représentant de l'UE, « Une Europe sûre dans un monde meilleur. Stratégie européenne de sécurité », Bruxelles, 12 décembre 2003, pp. 3-4 ; Communication conjointe au Parlement européen et au Conseil intitulée « *L'approche globale de l'UE à l'égard des crises et conflits extérieurs* »», 11 décembre 2013 [JOIN (2013) 30 final).

[143] Note du Haut représentant de l'UE, « Une Europe sûre dans un monde meilleur. Stratégie européenne de sécurité », Bruxelles, 12 décembre 2003 ; Communication conjointe au Parlement européen et au Conseil intitulée « *L'approche globale de l'UE à l'égard des crises et conflits extérieurs* »», 11 décembre 2013 [JOIN (2013) 30 final], pp. 2, 4 (documents disponibles sur www.eur-lex.europa.eu).

[144] N. Arpagian, *Que sais-je? La cybersécurité*, Paris, 2016, p. 3.

[145] *Ibid.*, p. 4.

[146] Note du Secrétariat général du Conseil de l'Union européenne intitulée « *Une stratégie globale pour la politique étrangère et de sécurité de l'Union européenne* », 28 juin 2016 [approche globale de l'UE décembre 2013 PESC 543, PSDC 395], p. 16.

[147] G. Verhofstadt, « Résistons à la guerre hybride que Poutine mène contre l'Occident », dans *Le Monde*, 2 janvier 2017 (consultable sur www.lemonde.fr).

[148] *Ibid.*

La « guerre hybride» : « escroquerie intellectuelle»[149] ou « occasion de regarder la conflictualité contemporaine en face »[150]?

Le concept de « *guerre hybride* » fait débat[151] et suscite parfois même la polémique. Ainsi, pour certains chercheurs comme Gérard Chaliand, ce terme *« ne nous avance guère pour la compréhension du phénomène. Il s'agit en fait de la guerre irrégulière où se croisent la guérilla, le terrorisme et tous les moyens anciens et nouveaux (notamment à l'échelle des communications et de la drogue)* »[152]. Selon lui également, *« l'invention de mots nouveaux pour désigner un phénomène connu ne fait guère avancer la capacité d'y répondre* »[153]. Laurent Henninger considère même que le débat sur la « *guerre hybride* » procède d'une « *réinvention de la roue* » voire d'une « *escroquerie intellectuelle* »[154]. Pour lui en effet, aucune particularité « *hybride* » n'est réellement nouvelle et surtout ne justifie une nouvelle caractérisation de la guerre, « *car son extension à de nouvelles dimensions, moyens, méthodes, etc., n'en a modifié la nature* »[155]. Et d'ajouter que « *Si changements il y a, ce sont généralement des changements de volume ou éventuellement d'accent mis sur tel ou tel point (…)* »[156]. « *Le problème »,* dit-il, *« c'est que, depuis les années 1950 au moins, on est obnubilé par la classification des guerres et des conflits. (…) [ce qui a] plutôt largement contribué à embrouiller les esprits (…)* »[157]. Pour Henninger, la création d'un vocable nouveau risque en définitive d'introduire beaucoup de confusion dans les esprits militaires ou civils « *qui sont déjà au bord de la surcharge à cet égard* »[158]. De son côté, Tenenbaum met également en garde contre la « *plasticité* »[159] de la notion de « *guerre hybride* ». D'après lui en effet, celle-ci « *renvoie à des réalités tant politico-stratégiques que tactico-opérationnelles et, sans un accord de ceux qui l'emploient sur le sens exact de l'expression, elle risque de mener à bien des incompréhensions, voire à de dangereux quiproquos* »[160].

Pour J. Henrotin, le débat sur la guerre hybride ne procède pas d'une « *escroquerie intellectuelle* », « *du moins, sur [le] versant 'tactique-opératif', dès lors qu'il en est autrement de son versant stratégique* »[161]. Il reconnaît en effet que les différents vecteurs de l'interprétation stratégique de la guerre hybride, à savoir la stratégie intégrale, la guerre par *proxy* et l'usage

---

[149] L. Henninger, « La 'guerre hybride ' : escroquerie intellectuelle ou réinvention de la roue ? », dans *RDN*, mars 2016, p. 51.

[150] J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, p. 31.

[151] J-C. Coste, « De la guerre hybride à l'hybridité cyberélectronique », dans *RDN*, mars 2016, p. 19.

[152] J. Henrotin, *Entretien stratégique avec Gérad Chaliand. Les mutations de la guerre irrégulière*, dans *Stratégique*, n°111, Paris, 2016, p. 141.

[153] *Ibid.*, p. 142.

[154] L. Henninger, « La 'guerre hybride ' : escroquerie intellectuelle ou réinvention de la roue ? », dans *RDN*, mars 2016.

[155] *Ibid.*, p. 53.

[156] *Ibid.*

[157] *Ibid.*, p. 54.

[158] *Ibid.*, p. 53.

[159] E. Tenenbaum, « Le piège de la guerre hybride », dans *Focus stratégique* n°63, octobre 2015, p. 43.

[160] *Ibid.*

[161] J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, p. 17.

d'irréguliers, la guerre de l'information mais également la mobilisation d'une « *rhétorique politique pour se dégager de ses obligations juridiques ou contester leur portée* »[162] sont historiquement classiques, y compris lorsqu'ils sont combinés[163]. Lors de la guerre du Vietnam par exemple, des irréguliers ou « *Vietcong* », étaient directement armés par Hanoï et bénéficiaient *in fine* du soutien de Moscou. Par ailleurs, tout comme l'intervention russe en Ukraine, l'invasion du Koweït en 1990 et la construction d'îles artificielles en mer de Chine méridionale pour faire reconnaître une zone économique exclusive bien plus grande qu'initialement, répondent à une même logique de légitimation de l'action, sur base d'une « *interprétation biaisée du droit international* » voire, éventuellement, d'arguments historiques[164].

La nouveauté serait, selon Henrotin, d'ordre [tactico]-technique[165]. Il considère en effet que « *le concept de guerre hybride sur ses versants tactiques-opératifs rend (…) compte d'une véritable mutation, aux conséquences potentiellement importantes pour les armées occidentales : un saut qualitatif majeur (…). Les organisations suivant les lignes du combat hybride investiraient ainsi le champ des stratégies particulières (aérienne/aérospatiale, navale) ; pourraient être capables de mettre en œuvre des armements chimiques improvisés ; tout en accroissant leur puissance de feu dans le domaine terrestre ; en développant des capacités C51 (Counter Command Control Communications Computers, Intelligence) et une véritable stratégie médiatique leur permettant d'agir à une échelle globale* »[166]. Selon lui, ces évolutions [tactico-opératives] sont rendues possibles par un accès facile aux technologies avancées- en particulier civiles- mais surtout par l'exploitation militaire de ces technologies à travers un processus d'innovation [propre] à l'agilité organisationnelle des irréguliers[167] . Pour Tenenbaum, au vu de la diffusion rapide des armements de précision, « *les combinaisons surprenantes du combat hybride deviendront la norme et le terme même pourrait apparaître comme moins utile d'ici quelques années, dès lors que tous les mouvements irréguliers seront en possession de tels moyens. Rien ne permet donc d'affirmer que ce concept soit promis à un grand avenir*»[168].

Selon Henrotin, « *la massification de la 'dé-identification' des combattants* »[169] [que l'on peut constater dans la guerre hybride] représente également une rupture [tactique] par rapport aux conflits antérieurs. La nouveauté de ce phénomène est à trouver dans l'aspect systématique de l'action et par le volume des forces engagées et non pas dans la question des opérations clandestines, qui n'est historiquement pas neuve[170].

Pour Gérard Chaliand, « *la nouveauté [des conflits actuels] (…) réside (…) dans le domaine intellectuel, dans les savoir-faire et le maniement psychologique de l'adversaire- c'est-à-dire de*

---

[162] J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, p. 26.

[163] *Ibid.*, pp. 26-27.

[164] J. Henrotin, « L'hybridité à l'épreuve des conflits contemporains : le cas russe », dans *RDN*, mars 2016, p. 38.

[165] ID., « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, p. 24.

[166] J. Henrotin., « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, pp. 17-18.

[167] *Ibid.*, p. 18.

[168] E. Tenenbaum, « Le piège de la guerre hybride », dans *Focus stratégique* n°63, octobre 2015, p. 43.

[169] Le concept de *dé-identification* est utilisé pour parler d'un attaquant qui n'est pas clairement identifié (J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, p. 27).

[170] J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *op. cit.*, p. 26.

nous- alors qu'il y a peu de temps, une cinquantaine d'années, ce n'était pas le cas . Jadis, un adversaire ne nous connaissait que fort peu. Aujourd'hui, non seulement il nous connaît, mais il connaît aussi nos points faibles. Le véritable changement est dans les réseaux sociaux »[171]. L'adversaire « *sait avec l'aide indirecte de nos propres média soucieux d'audimat nous manipuler et semer la peur, la psychose* »[172]. I. Mayr-Knoch rejoint G. Chaliand dans son raisonnement. Selon lui en effet, dans la « *guerre hybride* », « *l'intégration des instruments de pression civils aux moyens militaires est cruciale* »[173]. Les opérations hybrides russes en Ukraine orientale ont été impressionnantes en la matière. Il recommande dès lors à l'UE de lancer une « *campagne de conquête des cœurs et des esprits* »[174] dans les États baltes afin que la Russie ne puisse « *répéter sa tactique de division en exploitant les clivages existants entre la minorité russophone et le reste de la société* »[175]. C'est ce que conseille également Tenenbaum. Il encourage en effet à élaborer un vrai « *projet politique* »[176] pour contrer les « *méthodes hybrides* ». Ainsi par exemple, pour éviter qu'une agression extérieure ne s'accompagne d'une insurrection, il convient de combattre celle-ci militairement et surtout politiquement en essayant d'accéder, dans la mesure du possible aux revendications de la population, si celles-ci ne sont pas incompatibles avec nos intérêts fondamentaux. La priorité devra, selon lui, aller à l'élimination des zones de non-droit, le rétablissement d'une présence judiciaire et policière sur tout le territoire mais également la présentation de mesures politiques et sociales venant répondre aux problèmes à l'origine du conflit[177].

En définitive, J. Henrotin considère qu'une focalisation de l'hybridité sur la question russe « *tend à obscurcir la réflexion stratégique* » [178] autour du concept de « *guerre hybride* » et empêche une appréciation saine d'une situation complexe [179] alors que son analyse devrait être « *une occasion de regarder la conflictualité contemporaine en face* » [180]. C'est également ce que pense Henninger qui recommande de ne pas chercher à caractériser par un adjectif unique et réducteur des phénomènes géopolitiques qui devraient, au contraire, être envisagés dans toutes leurs spécificités et complexité[181]. Henrotin affirme ainsi que le succès russe repose bien plus sur les qualités militaires

---

[171] J. Henrotin, *Entretien stratégique avec Gérad Chaliand. Les mutations de la guerre irrégulière*, dans *Stratégique*, n°111, Paris, 2016, p. 141.

[172] *Ibid.*, p. 142.

[173] I. Mayr-Knoch, N. Mair et J. Mittelstaedt, « Plaidoyer pour une stratégie hybride de l'Union européenne », dans *Stratégique*, n°111, Paris, 2016, p. 44.

[174] L'expression « *Hears and Minds* » (cœurs et esprits) ne date pas d'hier. Elle est attribuée, lors de la contre-insurrection en Malaisie en 1951-1954, à Sir Gerald Templer commandant des forces britanniques dans la région. Cette expression désigne « *l'ensemble des activités et des procédés par lesquels un gouvernement, un parti, toute entité politique constituée s'efforce d'infléchir l'état d'esprit de la population* » (F. Géré, Dictionnaire de la désinformation, Paris, 2011).

[175] I. Mayr-Knoch, N. Mair et J. Mittelstaedt, *op. cit.*, p. 50.

[176] E. Tenenbaum, « Le piège de la guerre hybride », dans *Focus stratégique* n°63, octobre 2015, p. 40.

[177] *Ibid.*, pp. 40-41.

[178] J. Henrotin, « L'hybridité à l'épreuve des conflits contemporains : le cas russe », dans *RDN*, mars 2016, p. 37.

[179] ID., « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, p. 29.

[180] *Ibid.*, p. 31.

[181] L. Henninger, « La 'guerre hybride' : escroquerie intellectuelle ou réinvention de la roue ? », dans *RDN*, mars 2016, p. 55.

opératives suivantes (ou « *principes de la guerre* »[182]) : sûreté, surprise[183], concentration des forces, tempo, planification et corrélation des forces, que sur les recours à des moyens hybrides comme la propagande, ou la « *dé-identification* » dont l'article 5 du traité Nord Atlantique n'a que faire. C'est en effet, « *le fait de l'attaque qui détermine si l'Article 5 du traité nord-atlantique est pertinent ; et non le fait que l'attaquant soit clairement identifié ou pas* »[184]. Ainsi, « *une fois engagé dans des opérations, le combattant, identifié ou non, est considéré comme adversaire aux yeux du droit international et est donc une cible parfaitement légitime (…). En ce sens, les inquiétudes que font poindre certains observateurs sur une possible utilisation de ces forces 'dé-identifiées' contre les Pays baltes semblent peu fondées* »[185]. Par conséquent, faire de la Russie un cas exemplaire des opérations hybrides revient à « *s'aveugler sur le caractère des opérations futures en reproduisant les biais auxquels nous sommes vulnérables* »[186]. L'OTAN et l'UE ne se rendraient-ils pas suffisamment compte que l'ennemi actuel est apte à coupler la quantité (ou « *puissance de feu* »[187]) que nous n'avons plus, et la qualité que nous pensons avoir ? Ainsi, dans le cas de la Russie, la part des dépenses consacrées à la Défense n'a cessé d'augmenter entre 2010 et 2015, passant de 12,5% du budget de l'État à 19,7% (et de 2,84% du PIB en 2010 et à 4% en 2014)[188]. L'OTAN reconnaît d'ailleurs que la puissance militaire de la Russie représente un défi fondamental pour l'Alliance[189]. Il est en effet indéniable que l'armée russe connaît ces dernières années une modernisation importante et qu'elle poursuit son réarmement, avec le développement de son complexe militaro-industriel conformément à un plan qui doit s'achever en 2020[190]. D'après le général Hans-Lothar Domröse, ancien commandant des forces interarmées de Brunssum, la Russie dépasse l'OTAN dans le domaine militaire grâce à la modernisation constante de son équipement militaire. Celle-ci a permis à la Russie de développer une haute capacité de combat mais également la maniabilité et la puissance de ses forces armées. À contrario, il constate que les effectifs de l'OTAN ont drastiquement diminué au cours de ces 25 dernières années. Le général conseille d'ailleurs d'entamer des négociations sur le désarmement entre la Russie et l'OTAN afin de rééquilibrer le rapport des forces[191]. La spirale de

---

[182] J. Henrotin, *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris, 2014, p. 141.

[183] André Dumoulin ne partage pas l'affirmation selon laquelle l'OTAN et ses alliés auraient vécu une surprise stratégique avec l'annexion de la Crimée. Selon lui en effet, cette affirmation est difficile à confirmer « *dès l'instant où les systèmes de détection stratégique et satellitaire occidentaux étaient opérationnels ; nonobstant le fait que la Russie a organisé l'annexion en coordonnant des engagements hybrides -terme à la mode-, en donnant visibilité aux forces paramilitaires et autres milices à l'origine incertaine, aboutissant ici à ce que l'opération se termine sans pratiquement aucune victime* » (A. Dumoulin, *Crise russo-ukrainienne. Conséquences sur les politiques de défense OTAN, UE et de défense nationale*, IRSD- Sécurité & Stratégie, n°125, Juin 2016, p. 14).

[184] J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *op. cit.*, p. 27.

[185] *Ibid.*

[186] J. Henrotin, « L'hybridité à l'épreuve des conflits contemporains : le cas russe », dans *RDN*, mars 2016, p. 43.

[187] ID., *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris, 2014, p. 121.

[188] I. Facon, « Que vaut l'armée russe? », dans *Politiques étrangère*, vol. Printemps, n°1, 2016, p. 153.

[189] *Communiqué du Sommet de Varsovie publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Varsovie les 8 et 9 juillet 2016*, § 5.

[190] S. Gilbert, « La modernisation des forces armées russes », projet de rapport général de l'Assemblée parlementaire de l'OTAN [064 STC 15 F], pp.2-3. Pour plus de détails sur les effectifs et les moyens dont dispose l'armée russe, lire : IISS, *The Military Balance 217*, Londres, 2017, pp. 210-223.

[191] Ch. Saarländer, « Deutscher NATO-General warnt vor russischer Militär-überlegenheit», dans *Contra Magazine*, 2 janvier 2016 (consultable sur www.contra.magazin.com). Il n'existe pas de données chiffrées qui

confrontation entre l'OTAN et la Russie de ces dernières années ne favorise pourtant pas des discussions en la matière. Lors des sommets alliés au Pays de Galles en 2014 et à Varsovie en 2016, un véritable programme de réarmement de l'OTAN a même été défini. À Varsovie, l'Alliance atlantique a en outre mis l'accent sur la nécessité de maintenir dans son dispositif aéroterrestre des forces nucléaires tactiques[192]. De son côté, Vladimir Poutine a ordonné le renforcement, dès 2017, de la force nucléaire russe afin que celle-ci soit capable de percer tout bouclier antimissile, comme celui que Washington entend déployer en Europe de l'Est[193]. Notons néanmoins que le budget de défense de la Russie diminue sensiblement depuis 2016 et reste bien inférieur à celui des États-Unis ou de la Chine[194] .

Une puissance comme « *Daesh* » compte quant à elle entre 30 000 et 50 000 combattants[195] et dispose d'armes sophistiquées, ce qui représente un véritable saut quantitatif pour une organisation terroriste[196]. Face à ces nouveaux arsenaux militaires, Henrotin conclut que l'excellence technico-tactique des dispositifs occidentaux ne suffit pas. La tactique n'est en effet rien sans une stratégie à long terme, sans des effectifs suffisants avec un savoir-faire adéquat. De plus, le surengagement des forces occidentales, que ce soit en opérations intérieures ou extérieures, se traduit par des pertes de savoir-faire, au moment où l'adversaire probable en gagne[197]. Pour Henrotin, nous risquons peu à peu de nous retrouver avec des « *nouvelles armées d'ancien régime* »[198], à savoir des forces professionnalisées, techniquement excellentes mais qui pourraient finir par démontrer leur inefficacité, comme celles du cycle historique précédent. Tenenbaum conseille d'adopter un modèle capacitaire adapté à l'évolution et à la diffusion des systèmes d'armes et des tactiques non-

---

reprennent de façon systématique les effectifs militaires mis au service de l'OTAN. L'importante rationalisation des structures de commandement de l'organisation depuis la fin de la Guerre froide permet néanmoins de mieux se rendre compte de la diminution en personnel de l'OTAN.

[192] P. Quilès, « Tensions entre l'OTAN et la Russie: risque de confrontation militaire? », dans *Recherches internationales*, n°108, janvier-mars 2017, pp. 70-72.

[193] S.n., « Russie: Poutine ordonne le renforcement de la force de frappe nucléaire », dans *Le Monde*, 22 décembre 2016 (www.lemonde.fr).

[194] Les dépenses militaires des États-Unis s'élevaient, en 2016, à 611 milliards de dollars, contre 215 milliards de dollars pour la Chine et environ 69,2 milliards de dollars pour la Russie, ce qui la place désormais au troisième rang des plus dépensiers (SIPRI, « Dépenses militaires mondiales : en hausse aux Etats-Unis et en Europe, en baisse dans les pays exportateurs de pétrole » (Communiqué de presse), Stockolm, 24 avril 2017, p. 1).

[195] Données chiffrées issues de O. Saugues, « Rapport d'information sur le Proche et Moyen-Orient », dans *Rapport d'information de l'Assemblée nationale*, n°2666, 18 mars 2015, p. 66. En décembre 2015, le *Soufan Group*, groupe international de consultance stratégique basé à New York, estimait, quant à lui, que l'EI dispose de 27 000 à 31 000 combattants, soit le double du chiffre estimé par ce groupe de consultance en juin 2013 (*SIPRI Yearbook 2016*, Oxford, pp. 28-29).

[196] Al-Qaida aurait compté moins d'un millier de combattants en Afghanistan dans les années 2000. L'ancien ministre français de la défense, Jean-Yves Le Drian estimait en septembre 2014, que « *Daesh*» disposait probablement de « *3000 4x4 Hummer américains récupérés de Mossoul, de 60 000 armes individuelles, de 50 chars lourds, de 150 blindés légers et de materiel antichar*» (O. Saugues, « Rapport d'information sur le Proche et Moyen-Orient », dans *Rapport d'information de l'Assemblée nationale*, n°2666, 18 mars 2015, p. 66). S'il est difficile d'évaluer le stock d'armes dont dispose Daesh actuellement, aucune preuve ne permet d'affirmer que l'organisation terroriste dispose d'armes bactériologiques ou nucléaires (K. Arif, « Rapport d'information sur les moyens de Daesh », dans *Rapport d'information de l'Assemblée nationale*, n°3964, 13 juillet 2016, p. 387).

[197] J. Henrotin, « La guerre hybride comme avertissement stratégique», dans *Stratégique*, n°111, Paris, 2016, pp. 30-31.

[198] *Ibid.*, p. 31.

linéaires[199]. Roland Freudenstein insiste quant à lui sur la nécessité pour l'UE et l'OTAN d'augmenter leurs effectifs en personnel afin de lutter contre les « *menaces hybrides* », singulièrement en matière de désinformation. Selon lui, l'UE ne dispose que d'une dizaine de personnes, et l'OTAN d'à peine du double, pour lutter contre la propagande propagée par Moscou grâce à quelque 500 spécialistes en la matière, aussi appelés « *trolls* ». Or, dit-il, la désinformation utilisée par la Russie est devenue beaucoup plus complexe que pendant la Guerre froide, où « *it was just one big unitary lie ; now it's a complex range of things* »[200].

Pour le colonel E. A. Claessen, ce n'est pas en augmentant l'avance technologique de leurs systèmes d'armement que les pays de l'OTAN arriveront à contrer la stratégie russe. Selon lui en effet, celle-ci est conçue pour neutraliser les avantages que l'OTAN tire de la technologie de pointe. Il est convaincu que « *plutôt que de développer des moyens pour détruire des cibles dites stratégiques avec encore plus de précision et à partir de distances toujours plus grandes, les pays occidentaux devraient développer des capacités dans les domaines de la compréhension, des opérations d'information et d'influence, de l'assistance humanitaire et de la fourniture de services essentiels urbains dans des régions en conflit. C'est le seul moyen d'éviter que l'adversaire ne s'appuie sur le potentiel contestataire de la population pour éterniser ces conflits* ». Et de conclure que « *ceux qui n'investissent que dans les guerres sans contact, s'enliseront partout dans des guerres sans victoire* »[201].

Pour Elie Tenenbaum, l'invention de l'expression « *guerre hybride* », « *concept évasif dont il est souvent difficile de saisir la spécificité* »[202], en dit long sur « *l'appauvrissement de la culture stratégique dans les milieux politiques européens et l'inadaptation des mécanismes de défense collective* »[203]. Selon lui, la « *guerre hybride* » est devenue un « *enjeu de survie bureaucratique pour de nombreux partenaires* » [204], en témoignent la floraison des centres d'excellence de l'OTAN ou des *think tanks* qui traitent cette problématique. D'après ses dires, les membres de ces institutions choisissent parfois même d'altérer le sens du concept pour mieux le faire correspondre à leurs compétences. « *Tous les défis émergents, militaires ou non, sont tout à coup devenus susceptibles d'être désignés comme des 'menaces hybrides' : des cyberattaques aux biotechnologies en passant par le terrorisme (…) et la piraterie maritime* »[205]. Une personnalité importante de l'EU INTCEN émet l'idée personnelle que la guerre hybride est devenue une problématique centrale à l'OTAN. Celle-ci concerne singulièrement la Russie, une puissance qui, toujours selon lui, ne devrait plus seulement être considérée comme ennemie mais aussi comme partenaire[206].

Pour Ch. Malis, la promotion de la notion d'hybridité, qui « *présente une surextension [sémantique] et un caractère biscornu manifeste* », doit être comprise comme un effort politique de reconstruction d'un projet d'entreprise commun pour les pays membres de l'OTAN au moment où sa cohésion, particulièrement en ce qui concerne les relations euro-américaines ou entre certains pays

---

[199] E. Tenenbaum, « Le piège de la guerre hybride », dans *Focus stratégique* n°63, octobre 2015, p. 39.

[200] B. Tigner, « An Evolving Threat », dans *Jane's Defence Weekly*, 24 mai 2017, p. 25.

[201] E. A. Claessen, « La pensée militaire russe : 'guerre sans contact, guerre sans victoire ' », dans RDN, mai 2016, p. 107.

[202] E. Tenenbaum, « La manœuvre hybride dans l'art opératif », dans *Stratégique*, n°111, Paris, 2016, p. 47.

[203] ID., « Le piège de la guerre hybride », dans *Focus stratégique* n°63, octobre 2015, p. 43.

[204] *Ibid.*, p. 35.

[205] *Ibid.*

[206] Interview réalisée au sein de l'EU INTCEN par E. Hoorickx, le 30 novembre 2016.

européens, est secouée par d'inquiétantes dissensions du fait de la situation en Europe de l'Est[207]. Pour Guillaume Lasconjarias également, l'intérêt du concept de « *guerre hybride* » est de redéfinir aujourd'hui et pour le futur proche les stratégies de défense mais également le rôle et l'organisation des architectures de sécurité[208].

D'après lui aussi, « *La popularité du terme [guerre hybride] illustre à merveille l'intérêt d'un concept caméléon qui peut ainsi définir des réalités différentes, qu'il s'agisse de la Russie à l'Est ou d'un groupe non-étatique armé comme Daesh (…). [En définitive,] l'hybridité apparaît rassurante parce qu'elle permet d'inclure tout ce qui est non-conventionnel (…). [Or, comme le rappelle souvent] l'actuel Secrétaire général, Jens Stoltenberg, (…) la première forme de guerre hybride se retrouve avec le cheval de Troie, et (…) il n'y a donc rien que nous n'ayons vu ou rencontré auparavant* »[209]. Pour Lasconjarias néanmoins, « *l'hybridité jette un éclairage accru sur la fragilité des États inclus dans une mondialisation qui les dépasse, et met en lumière la faiblesse des politiques actuelles à réfléchir sur l'ordre du monde, leur place et leur rôle. Il n'est donc pas inintéressant de constater que la réponse aux formes d'hybridité tient souvent en un autre mot-valise : la résilience* »[210]. Le chapitre suivant fera le point sur la stratégie proposée actuellement par l'UE et par l'OTAN pour faire face aux menaces hybrides, notamment en matière de « *résilience* ».

[207] Ch. Malis, « Guerre hybride et stratégies de contournement », dans *RDN*, mars 2016, p. 24.

[208] G. Lasconjarias, « Á l'Est du nouveau ? L'OTAN, la Russie et la guerre hybride », dans *Stratégique*, n°111, Paris, 2016, p. 117.

[209] *Ibid.*, p. 108.

[210] G. Lasconjarias, « À l'Est du nouveau ? L'OTAN, la Russie et la guerre hybride », dans *Stratégique*, n°111, Paris, 2016, p. 117.

Partie 2 : Stratégie euro-atlantique face aux « campagnes hybrides » et implication de la Belgique

Les pratiques de la « *guerre hybride* » sont considérées comme un défi sécuritaire majeur par l'UE comme par l'OTAN, qui s'attellent depuis 2015 à développer, chacune de leur côté, une stratégie cohérente afin d'aider leurs pays membres à lutter contre cette menace complexe. La réponse stratégique proposée par l'UE et l'OTAN, désireuses de coopérer ensemble à la lutte contre les « *campagnes hybrides* », s'articule autour de cinq axes : l'amélioration de la connaissance des « *pratiques hybrides* », le renforcement de la «*résilience*» à celles-ci, l'efficacité de la prévention et de la réponse face à l'attaque hybride (« *Integrated Political Crisis Response* »), et enfin, une meilleure coordination entre les parties dans toutes ces matières, en ce compris la communication stratégique et la cybersécurité[211]. Si les deux organisations s'engagent à soutenir les pays membres dans la lutte contre les « *campagnes hybrides* », elles rappellent que la responsabilité première incombe aux États membres, dans la mesure où la lutte contre les dangers hybrides touche à la sûreté de l'État et à la défense nationale ainsi qu'au maintien de l'ordre public[212]. La présente partie vise à analyser la stratégie mise en place par les deux organisations mais également les mesures prises par la Belgique pour participer au projet.

Reconnaitre les « *campagnes hybrides* » et en déterminer les auteurs

Le premier domaine d'action de l'UE et de l'OTAN concerne la connaissance des « *menaces hybrides* ». Les deux organisations souhaitent en effet être capables de déceler des menaces hybrides prenant forme et de réagir afin qu'une campagne hybride ne dégénère pas en conflit militaire. L'OTAN et l'UE invitent dès lors leurs pays membres à cerner leurs points faibles ou « *vulnérabilités* » face aux risques hybrides[213]. Le Président du Conseil européen a décidé, en juin 2017, de mettre en place un « *groupe des amis de la présidence* » de l'UE (*FoP*), composé d'experts issus de tous les pays de l'UE[214] et mandaté jusque fin juin 2018, afin d'aider

---

[211] Parlement européen, *Countering hybrid threats : EU-NATO cooperation*, mars 2017 (disponible sur www.europarl.europa.eu).

[212] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 2 ; *Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers*, 11 février 2016 (consultable sur www.nato.int).

[213] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 4.

[214] « *Les membres du FoP sont chargés de la coordination du projet de recensement des principales vulnérabilités des pays en matière de menaces hybrides. La plupart d'entre eux sont également les personnes de contact habilitées à représenter les différents États-membres auprès de la cellule de fusion de l'UE* ». Interview téléphonique le 18 août 2017 avec E. Lallemant, représentant permanent de la Belgique auprès de l'UE et personne de contact, pour ce pays, de la cellule de fusion de l'UE contre les menaces hybrides.

les États-membres à la réalisation de ce projet[215]. Début juillet 2017, la nouvelle présidence estonienne du Conseil de l'UE a demandé au *FoP* d'élaborer, pour fin 2017, une « *enquête générique* » qui permettra aux États membres 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* »[216]. Pour ce faire, un formulaire de questions relatives à la connaissance des menaces hybrides et à la capacité de résilience en la matière de chaque pays de l'UE a été distribué aux États-membres. Ces derniers ont été encouragés à répondre au questionnaire en y ajoutant, éventuellement, des données supplémentaires, avant fin septembre 2017. Par la suite, une synthèse des réponses sera rédigée pour constituer la dite « *enquête générique* », en vue de mener des actions ultérieures afin d'améliorer la lutte contre les menaces hybrides. Actuellement, il n'existe pas de politique belge centralisée en matière de lutte contre les « *menaces hybrides* »[217]. Cette terminologie ne semble en outre pas claire pour tous, singulièrement dans les milieux non militaires[218].

Afin d'améliorer la connaissance des « *menaces hybrides* » et de promouvoir l'échange d'informations concernant les menaces hybrides, l'UE encourage la mise en place de centres d'excellence.

La « cellule de fusion » de l'UE et la « Branche Analyse des menaces hybrides » de l'OTAN

La première initiative en la matière remonte à mai 2016. Une « *cellule de fusion de l'UE contre les menaces hybrides* » est alors créée, à Bruxelles, au sein du Centre de situation et du renseignement de l'UE (INTCEN) du Service européen pour l'action extérieure (SEAE). La raison principale de sa création est la crise en Ukraine. Composée de 7 personnes depuis juin 2017, cette cellule reçoit, analyse et partage « *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) et des États membres* »[219]. Une personnalité de l'EU INTCEN souligne néanmoins que « *contrairement à la Guerre froide où les États contrôlaient les informations critiques, ce sont désormais [parfois aussi] les entreprises privées qui en disposent, [ce qui ne facilite pas l'échange de données relatives à l'hybridité]* »[220]. À ce jour, 21 pays de

---

[215] Note de la Présidence du Conseil de l'UE intitulée « Mandate of the Friends of the Presidency Group on the Implementation of Action 1 of the Joint Framework on Countering Hybrid Threats (doc. 7688/16) », 2 juin 2017 [9502/17], p. 3.

[216] Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 4 (voir annexe 2).

[217] K. Haegens, *'Hybrid Warfare". Een onderzoek naar de Belgische militaire capaciteiten om deze vorm van oorlogvoering te bestrijden*, ERM, Bruxelles, 28 avril 2017, pp. 36, 39; témoignages récoltés par E. Hoorickx en 2016 et 2017 auprès de fonctionnaires belges issus de ministères liés à la sécurité. Ceux-ci ont préféré rester anonymes.

[218] Témoignages récoltés par E. Hoorickx en 2016 et 2017 auprès de divers acteurs militaires, ou non, qui occupent des postes-clés dans des institutions fédérales belges liées à la sécurité.

[219] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 4.

[220] Interview réalisée au sein de l'EU INTCEN par E. Hoorickx, le 30 novembre 2016.

l'UE, dont la Belgique[221], ont fourni à la cellule de fusion des points de contact nationaux « *chargés de coopérer et d'entretenir une communication sécurisée* »[222] avec la cellule de fusion de l'UE. La cellule reçoit des renseignements relatifs à ces dangers sur une base volontaire. Elle suit entre autres la Russie et les « *outils hybrides* » que celle-ci utilise, à savoir le cyber et la propagande. Faute de moyens budgétaires suffisants, la cellule ne couvre cependant pas toutes les menaces hybrides développées par d'autres pays. Elle ne s'occupe pas des questions terroristes, qui sont du ressort de la division « *contre-terrorisme* » issue de la cellule « *Politique de sécurité et de prévention des conflits* » de la SEAE[223]. Depuis janvier 2017, la cellule rédige un périodique (*Hybrid Bulletin*) qui analyse les menaces hybrides actuelles. Ce document est distribué au sein des institutions et organes de l'UE ainsi qu'aux points de contact nationaux[224].

Jusqu'au printemps 2017, l'OTAN ne disposait pas d'une cellule équivalente à celle de l'UE en matière d'analyse et de partage d'informations sur les « *menaces hybrides* ». L'Alliance pouvait néanmoins déjà compter sur un grand nombre de centres d'excellence qui traitent des problèmes liés à la guerre hybride, comme la cyberdéfense ou la désinformation[225]. Par ailleurs, elle vient de mettre en place une « *Branche Analyse des menaces hybrides* », équivalent de la « *cellule de fusion de l'UE contre les menaces hybrides* ». Cette nouvelle structure otanienne devrait faciliter l'échange d'informations entre les deux institutions[226].

Le centre européen de lutte contre les menaces hybrides d'Helsinki

Par ailleurs, et conformément à une des recommandations de la communication conjointe d'avril 2016, un « *Centre européen de lutte contre les menaces hybrides* » a été inauguré le 11

---

[221] La Belgique a fourni, en janvier 2017, le nom de deux personnes de contact avec la cellule de fusion de l'UE contre les menaces hybrides. Ces personnes travaillent respectivement au Centre Gouvernemental de Coordination et de Crise (CGCCR) et à la représentation permanente de la Belgique auprès de l'UE.

[222] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 5.

[223] Interview réalisée au sein de l'EU INTCEN par E. Hoorickx, le 30 novembre 2016.

[224] Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 5.

[225] L'OTAN dispose depuis 2007, d'un centre d'excellence interarmées pour la défense CBRN en République tchèque (Vyskov) ; depuis 2008, d'un centre d'excellence pour la cyberdéfense en Estonie (Tallinn) ; depuis 2012, d'un centre d'excellence pour la sécurité énergétique établi en Lituanie (Vilnius) et depuis 2015, d'un centre d'excellence pour la communication stratégique (STRATCOM) localisé en Lettonie (Riga) qui a pour mission de renforcer la sécurité de l'information et de protéger l'espace public des alliés contre la désinformation (voir www.nato.int). L'UE dispose, quant à elle, d'un institut d'études de sécurité (2002) et, depuis 2010, de centres d'excellence thématiques traitant des questions CBRN (2010) (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* », 6 avril 2016 [JOIN (2016) 18 final], p. 6 ; R. Trapp, « The EU's CBRN Centres of Excellence Initiative after Six Years », dans *Non-proliferation Papers*, février 2017, p. 1 (www.sipri.org)).

[226] S.n., *Rapport d'étape sur les suites données à l'ensemble de propositions entériné le 6 décembre 2016 par le Conseil de l'Atlantique Nord et le Conseil de l'Union européenne*, 14 juin 2017, p. 3 (disponible sur www.nato.int) ; Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 5.

avril 2017 à Helsinki. Ce projet finlandais, à vocation « *multinationale et multidisciplinaire* »[227] vise à améliorer la connaissance en matière de menaces hybrides afin de mieux les contrer[228]. Il est prévu que ce centre coopère étroitement avec des experts gouvernementaux et non gouvernementaux mais également avec les centres d'excellence de l'UE et de l'OTAN. Ses premiers projets de recherche seront lancés en automne 2017, notamment la rédaction d'un livre sur les menaces hybrides. En outre, le centre envisage d'élaborer une doctrine mais également de proposer une formation et d'organiser des exercices « *visant à améliorer les capacités individuelles des participants, ainsi que l'interopérabilité entre les participants, l'UE et l'OTAN pour lutter contre les menaces hybrides* »[229]. Bien que l'UE ne soit pas signataire du protocole d'accord sur l'établissement du centre, Federica Mogherini a accordé un « *soutien total* » à la Finlande pour la création de celui-ci[230]. Elle encourage d'ailleurs une « *relation de travail étroite* » entre ce centre et la cellule de fusion de l'UE contre les menaces hybrides[231].

D'ici la fin de l'année 2017, le centre de recherche d'Helsinki devrait pouvoir compter sur dix personnes travaillant à temps plein et en réseau avec des experts de tous les États participant au projet. Aujourd'hui, le protocole d'accord de celui-ci a été signé par neuf pays: États-Unis, France, Grande-Bretagne, Pologne, Finlande, Suède, Lettonie, Lituanie, Norvège et Espagne[232]. Contrairement à la cellule de fusion européenne, le centre d'Helsinki compte donc, parmi ses membres, des États qui ne font pas partie de l'UE ou de l'OTAN. Or, comme mentionné par B. Tigner, selon un haut responsable de l'OTAN, il est « *souvent plus facile d'obtenir des informations des pays partenaires que de ses propres alliés* »[233]. En outre, d'après un expert du contre-espionnage, « *les gouvernements nationaux n'aiment pas révéler aux autres [pays alliés] leurs points faibles* », en particulier dans le domaine de la cybersécurité[234]. La création du centre d'excellence d'Helsinki permet ainsi d'élargir la réflexion à l'OTAN, où la question de la guerre hybride fait débat. En effet, si celle-ci est largement associée aux actions menées par les Russes et l' « *État islamique* », les priorités des États-membres de l'Alliance atlantique divergent souvent. Ainsi, d'après R. Huygelen, ambassadeur de Belgique auprès de l'OTAN de 2010 à 2014, les pays baltes, la Pologne, la Roumanie ou la Tchéquie veulent pouvoir continuer à faire face à la menace russe tandis que les pays du Sud de l'Europe sont géographiquement plus concernés par les conflits qui se déroulent en Afrique ou le combat contre l' « *État islamique* »[235].

---

[227] N. Gros-Verheyde, « Le premier centre d'excellence européen, sur les menaces hybrides, ouvre ses portes à Helsinki », dans *bruxelles2.eu*, 19 avril 2017.

[228] S.n., *EU Welcomes Establishment of the Finnish Centre of Excellence for Countering Hybrid Threats*, Bruxelles, www. eeas.europa.eu, 11 avril 2017

[229] N. Gros-Verheyde, *op. cit.*

[230] N. Gros-Verheyde, *op. cit.*; *Speech by Minister Soini at the Signing of the Memorandum of Understanding Establishing the European Centre of Excellence for Countering Hybrid Threats*, 11 avril 2017 (consultable sur www.formin.finland.fi).

[231] N. Gros-Verheyde, « Le premier centre d'excellence européen, sur les menaces hybrides, ouvre ses portes à Helsinki », dans *bruxelles2.eu*, 19 avril 2017.

[232] *Ibid.* ; S.n, « Helsinki : un lieu contre les 'menaces hybrides' », dans *Le Figaro.fr*, 11 avril 2017.

[233] B. Tigner, « An Evolving Threat», dans *Jane's Defence Weekly*, 24 mai 2017, p. 26.

[234] *Ibid.*, p. 29.

[235] Interview de R. Huygelen par E. Hoorickx le 16 juillet 2015.

Pour créer leur centre d'excellence, les Finlandais se sont inspirés du concept suédois de « *défense totale* »[236], réactivé en décembre 2015 par la Suède pour faire face au danger russe. Les Finlandais et les Suédois constituent, d'après une personnalité importante de l'EU INTCEN, la «*Ivy League européenne dans la lutte contre les menaces hybrides* »[237], singulièrement dans le domaine de la cybersécurité. Lors de l'inauguration du centre d'excellence à Helsinki, Timo Soini, ministre finlandais des Affaires étrangères a souligné que *« les menaces hybrides et les tactiques hybrides sont devenues l'un des défis de sécurité les plus importants pour la sécurité en Europe (…) [et notamment en] Finlande, (…) elle aussi une cible d'influence hybride (…) dans le domaine de la cybernétique [par exemple]* »[238]. Il a également insisté sur l'utilisation d'éléments hybrides dans les crises récentes : « *Au cours de la crise migratoire actuelle, nous avons vu des éléments d'influence hybride tant par les acteurs étatiques que par les acteurs non étatiques [sic]. La direction des flux de migration peuvent être utilisés comme méthode de pression politique. Et les auteurs d'actes hybrides tentent de radicaliser les membres vulnérables de la société en tant qu'acteurs indirects* »[239].

Penchons-nous dès lors sur un concept-clé de la lutte contre les menaces hybrides, à savoir la « *résilience* », ou capacité à résister et à sortir renforcés des « *campagnes hybrides* »[240]. Depuis quelques années, ce terme est devenu très à la mode dans les milieux internationaux. Il fait l'objet en 2012 d'une communication de la Commission européenne relative aux problèmes des famines qui touchent alors le Sahel et la Corne de l'Afrique[241]. Si la notion ne figure pas dans la stratégie européenne de 2003, ni dans le document qui en améliore la mise en œuvre en 2008, elle fait son apparition dans une note stratégique de l'UE en 2013 et est mentionnée sur presque toutes les pages du deuxième document stratégique de l'UE, paru en 2016[242]. Le terme n'apparaît en revanche dans aucun concept stratégique de l'OTAN mais est mentionné pour la première fois

---

[236] Pendant la Guerre froide, la Suède, officiellement neutre, avait conçu un vaste dispositif d'urgence de « *défense totale* » impliquant civils et militaires en cas d'incident majeur avec l'URSS (S.n., « Suède : le retour de la 'défense totale' », dans *Lettre d'informations stratégiques et de défense online*, www.ttu.fr, 28 juillet 2016 ; *Suède: les municipalités doivent se préparer à la guerre à la demande du gouvernement*, www.rt.com, 14 décembre 2016).

[237] Interview réalisée au sein de l'EU INTCEN par E. Hoorickx, le 30 novembre 2016.

[238] N. Gros-Verheyde, « Le premier centre d'excellence européen, sur les menaces hybrides, ouvre ses portes à Helsinki », dans *bruxelles2.eu*, 19 avril 2017.

[239] *Ibid.*

[240] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 6.

[241] Commission européenne, *Communication from the Commission to the European Parliament and the Council. The EU Approach to Resilience: Learning from Food Security Crises*, 3 octobre 2012 [COM (2012) 586 final].

[242] Note du Haut représentant de l'UE, « Une Europe sûre dans un monde meilleur. Stratégie européenne de sécurité », Bruxelles, 12 décembre 2003; S.n., Rapport sur la mise en œuvre de la stratégie européenne et de sécurité. Assurer la sécurité dans un monde en mutation, Bruxelles, 11 décembre 2008 [S407/08] ; Communication conjointe au Parlement européen et au Conseil intitulée « *L'approche globale de l'UE à l'égard des crises et conflits extérieurs* »», 11 décembre 2013 [JOIN (2013) 30 final) ; Note du Secrétariat général du Conseil de l'Union européenne intitulée « *Une stratégie globale pour la politique étrangère et de sécurité de l'Union européenne* », 28 juin 2016 [approche globale de l'UE décembre 2013 PESC 543, PSDC 395], p. 3, 6-7, 11, 16, 18, 19, 20-22, 27, 29, 37, 39, 41.

dans le texte de la déclaration du sommet du Pays de Galles de 2014[243]. Depuis lors, la « *résilience* » apparaît régulièrement dans les documents relatifs aux « *menaces hybrides* »[244].

La « résilience » aux « pratiques de la guerre hybrides»

L'UE et l'OTAN s'engagent à aider leurs pays membres à améliorer leur « *résilience* », comme la leur propre, face aux « *pratiques de la guerre hybride* » non spécifiquement militaires, à savoir le sabotage, les cyberattaques, la propagande, la désinformation ou les attaques CBRN. Pour contrer efficacement celles-ci, les deux organisations recommandent à leurs pays membres de protéger leurs « *vulnérabilités potentielles* ». L'OTAN et l'UE relèvent ainsi un nombre important de « *points faibles* » potentiels, à savoir la protection des infrastructures critiques (transports, centrales électriques ou installations nucléaires et spatiales), la préparation aux incidents ou attaques CBRN, la cyberdéfense, la lutte contre le terrorisme ou la faculté de mettre en œuvre une « *communication stratégique* » efficace[245]. Celle-ci consiste, en cas de « *désinformation systématique* » d'un adversaire, à pouvoir « *apporter des réponses factuelles et mieux sensibiliser l'opinion aux menaces hybrides* »[246]. Elle doit être cohérente et efficace avant et pendant un conflit hybride. Pour l'aider dans cette tâche, l'UE dispose, depuis 2015, de deux « *task-forces* » : « *East Stratcom* » pour les questions liées à la Russie et « *Arab Stratcom* », pour les problématiques du Moyen-Orient[247]. L'OTAN est aidée, quant à elle, par son centre d'excellence pour la communication stratégique localisé à Riga, depuis 2015. En juillet 2017, l'UE a en outre annoncé « *le lancement prochain d'un nouveau site web (#EUvsdisinformation) doté d'un outil de recherche en ligne [qui] améliorera sensiblement l'accès des utilisateurs* »[248] et permettra une mise en garde contre les campagnes de désinformation.

La Belgique est attentive à améliorer sa propre « *résilience* », même si celle-ci ne s'inscrit pas dans un projet spécifique de lutte contre les « *menaces hybrides* ». Dans son dernier accord gouvernemental, le Premier ministre préconise néanmoins une *« approche coordonnée de la sécurité* », où le politique et les services publics doivent collaborer de manière efficiente,

---

[243] *Déclaration du sommet du Pays de Galles publiée par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue au pays de Galles les 4 et 5 septembre 2014*, 7 septembre 2014, § 72-73.

[244] Lors de la table ronde organisée à Bruxelles par le Parlement européen le 16 novembre 2016 et intitulée « *NATO-EU Cooperation after de Warsaw Summit : Countering Hybrid Warfare* », le terme « *résilience* » était sur toutes les lèvres des personnalités de l'UE et de l'OTAN participant au débat. Cette conférence réunissait différents experts, décideurs politiques, fonctionnaires et représentants de l'industrie afin de faire le point sur le contenu du Sommet de l'OTAN à Varsovie et sur les projets de l'UE et de l'OTAN en matière de lutte contre les menaces hybrides.

[245] 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* », 6 avril 2016 [JOIN (2016) 18 final], pp. 6-18.

[246] *Ibid.*, p. 5.

[247] *Ibid.*

[248] Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 5.

singulièrement dans la lutte contre la radicalisation, le terrorisme et les cyberattaques[249]. À ce jour, différents arrêtés royaux ont d'ailleurs été signés afin de favoriser la protection des infrastructures critiques de la Belgique. Ainsi, par exemple, un nouvel arrêté royal a été signé, en février 2016, pour améliorer la sécurité et la protection des infrastructures critiques dans le secteur du transport ferroviaire[250]. En mai 2017, la Commission européenne a organisé un atelier sur les menaces hybrides pesant sur les infrastructures critiques. Presque tous les États-membres mais également des gestionnaires d'infrastructures critiques, la cellule de fusion de l'UE et l'OTAN, en qualité d'observateur, ont pris part à l'exercice. La Commission consultera de nouveau les parties prenantes à l'automne, afin d'adopter des indicateurs destinés à améliorer la protection et la résilience des infrastructures critiques contre les menaces hybrides avant la fin 2017[251]. La Belgique dispose par ailleurs d'une stratégie de cybersécurité qui vise notamment à « *une protection et une sécurisation optimales des infrastructures et systèmes publics critiques contre la cybermenace* »[252]. Le « *Centre Cybersécurité Belgique* » a néanmoins pointé du doigt des manquements en matière de « *cyber sécurité nucléaire* »[253]. Avant la fin 2017, les États membres devront avoir transposé la « *directive sur la sûreté nucléaire européenne* »[254]à leur propre législation. La société anonyme Engie-Electrabel a également rédigé son propre « *Plan de sûreté nucléaire 2016-2020* »[255]. Le « *Plan national de sécurité 2016-2019* » de la police fédérale met également en évidence l'importance de la lutte contre le terrorisme, l'extrémisme violent, la criminalité organisée et la « *cybercriminalité* »[256]. Le gouvernement belge fait aussi de la lutte contre « *Daesh* » une de ses priorités. Celle-ci se traduit dans des domaines très divers, comme le renforcement de la coopération entre l'Intérieur et la Justice, la traque au financement des réseaux terroristes, la protection de la population et des infrastructures, en sollicitant la Défense mais également en développant un programme de déradicalisation[257]. En outre, fin juin 2017, et à la demande de la Commission européenne, tous les États membres, se sont vus contraints de transposer la quatrième directive antiblanchiment de l'UE afin de lutter contre le financement du terrorisme[258].

---

[249] *Accord de gouvernement de la Belgique,* 9 octobre 2014, pp. 131, 143, 147 (consultable sur www.premier.be).

[250] « Arrêté royal du 19 février 2016 relatif à la sécurité et la protection des infrastructures critiques, pour le secteur du Transport, sous-secteur du transport ferroviaire », dans *Moniteur belge*, 7 avril 2016, pp. 23017-23023.

[251] Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 7.

[252] *Cyber Security Strategy Belgium*, 23 novembre 2012, p. 7 (consultable sur www.enisa.europa.eu).

[253] D.P, *Rapport d'audition sur la cybersécurité des centrales nucléaires en Belgique*, Chambre des représentants, 20 janvier 2017, p. 6.

[254] Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 8.

[255] Ph. Van Troeye, *Plan de sûreté nucléaire 2016-2020 d'Electrabel*, s.d. (consultable sur www.culturesurete.be).

[256] G. Bomal (sous la dir.), *Plan national de sécurité de la police fédérale 2016-2019*, s.d.

[257] D. Leroy, «La Belgique et Daesh: état des lieux, dans *Revue militaire belge*, » n°14, juillet 2017, p. 67.

[258] Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 14.

En janvier 2017, une doctrine de « *communication stratégique* » a été développée par ACOS Ops&Trg. Celle-ci souligne l'importance d'une proactivité plutôt que d'une réactivité face à la désinformation[259]. Il existe d'ailleurs, au sein de la Défense, une réelle volonté d'élargir ce projet aux autres instances politiques belges afin qu'une politique nationale en la matière puisse être mise en place[260]. D'aucuns regrettent en effet qu'il n'existe pas de réelle stratégie contre les campagnes de désinformation russes[261]. Lorsqu'en octobre 2016, Moscou accuse la Belgique d'avoir participé à des bombardements responsables de la mort de civils aux environs d'Alep, le Ministère des Affaires étrangères dément catégoriquement les faits en regrettant « *vivement qu'aucune consultation préalable n'ait eu lieu en vue d'établir les faits, avant que ces accusations ne soient rendues publiques* » [262]. Selon certains, cet incident tenait de « *l'écran de fumée au moment où la communauté internationale [envisageait] des sanctions contre les Syriens et les Russes pour les bombardements massifs et indiscriminés des positions rebelles à Alep* »[263].

Si l'UE et l'OTAN font preuve de bonnes intentions en matière de « *résilience* » et sont décidées à utiliser les « *politiques et instruments* »[264] existants, il semble que ce soit la cybersécurité qui fasse, à ce jour, l'objet du suivi le plus important. Ainsi, la directive de sécurité des réseaux et de l'information (SRI) de l'UE, adoptée le 6 juillet 2016, fixe de nouvelles obligations en matière de cybersécurité aux États membres et à certaines entreprises afin de créer un cyber environnement fiable au sein de l'UE[265]. Il est prévu que la Belgique revoie pour mai 2018, sa cyberstratégie à la lumière de cette directive. La mission sera chapeautée par le « *centre pour la cybersécurité Belgique* »[266]. La cybersécurité constitue une priorité du gouvernement belge, singulièrement afin de « *garantir une sécurisation et une protection optimales des infrastructures critiques* »[267]. Depuis 2009, la Belgique dispose en outre d'une « *équipe d'intervention d'urgence en sécurité informatique* » (ou « CERT-*Computer Emergency Response Team* »[268]) qui peut, en cas d'urgence informatique, coopérer avec « *l'équipe d'intervention*

---

[259] BEL MoD, *Strategic Communications*, ACOT-COD-STRATCOM-DCOJ-001-DRC2/DRC2, Ed 001/Rev 000,

[260] K. Haegens, *'Hybrid Warfare". Een onderzoek naar de Belgische militaire capaciteiten om deze vorm van oorlogvoering te bestrijden*, ERM, Bruxelles, 28 avril 2017, p. 37.

[261] *Ibid.*

[262] S.n., *Bombardement en Syrie: la Russie accuse toujours la Belgique, mais les numéros d'avions ne correspondent pas*, www.rtbf.be, 20 octobre 2016.

[263] *Ibid.*

[264] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 3.

[265] « Directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information », dans l'Union, dans le *Journal officiel de l'Union européenne*, 19 juillet 2016.

[266] A. Dammekens, *Cybersécurité- la directive européenne impose aux entreprises l'obligation de notifier les cyberincidents*, 12 juillet 2016 (consultable sur www.vbo-feb.be). Le « *Centre pour la Cybersécurité Belgique* », créé en octobre 2014 et relevant de l'autorité du Premier ministre, est chargé d'élaborer une stratégie de cybersécurité pour la Belgique, d'assurer la gestion de crise en cas de cyberincidents, en coopération avec le Centre de coordination et de crise du gouvernement, de rendre des avis sur la politique à suivre et de prendre des initiatives afin de conseiller et de protéger les entreprises, les consommateurs et les pouvoirs publics (*Accord de gouvernement de la Belgique*, 9 octobre 2014, p. 148 ; www.ccb.belgium.be).

[267] *Accord de gouvernement de la Belgique*, 9 octobre 2014, p. 148.

[268] Le « CERT » de la Belgique dépend du « *Centre pour la Cybersécurité Belgique* » et a une double mission : d'une part, coordonner la gestion et la réponse aux incidents d'ampleur nationale auprès d'opérateurs

interinstitutionnelle de l'UE » (CERT-EU)[269]. Notons enfin, la création, en février 2017, du « *centre européen pour la cybersécurité dans l'aviation* », qui coopère aussi avec le CERT-EU[270].

La problématique de « *cyberdéfense* » est également au cœur des préoccupations de l'OTAN. L'Alliance atlantique dispose d'ailleurs, depuis 2008, d'un centre d'excellence pour la cyberdéfense situé à Tallinn, en Estonie. Celui-ci mène des exercices mais également des activités de recherche et de formation dans des domaines techniques, juridiques et stratégiques liés à la cybersécurité[271]. Depuis janvier 2017, la Belgique participe également aux activités du centre, aux côtés de seize autres pays de l'Alliance atlantique[272]. Lors du sommet de Varsovie de juillet 2016, l'Alliance atlantique a en outre affirmé reconnaître *« le cyberespace en tant que domaine d'opérations dans lequel l'OTAN doit se défendre aussi efficacement qu'elle le fait dans les airs, sur terre et en mer* »[273]. Elle s'est alors engagée à « *faire de l'amélioration des moyens de cyberdéfense de [ses] infrastructures et réseaux nationaux une priorité* »[274]. Début décembre 2016, l'UE et l'OTAN ont approuvé un certain nombre de mesures de coopération, en matière de cybersécurité, relatives à l'échange d'information, la formation et la participation à des exercices communs[275]. En février 2017, les ministres de la défense de l'OTAN ont entériné un « *plan d'action révisé pour la cyberdéfense* » et une « *feuille de route pour le traitement du cyberespace en tant que domaine d'opérations* », afin d'améliorer l'aptitude des Alliés à travailler ensemble, à développer leur capacités cyber et partager des informations. Enfin, l'OTAN et l'UE commencent à intégrer les « *cyberattaques*» dans leurs exercices annuels de « *gestion de crises* » qui ont désormais lieu dans un environnement fictif de menaces hybrides. Le premier entraînement impliquant les deux organisations, toujours dans un scénario d'attaque hybride, aura lieu en septembre- octobre 2017. Au cours de cet exercice, intitulé « *PACE17* » (*Parallel and Coordinated Exercise*), l'ennemi aura non seulement recours à des « c*yberattaques* » contre les infrastructures critiques de son adversaire mais également à de la propagande[276]. Dans ces différents exercices auxquels participe la Belgique, la « *communication stratégique* » joue également un rôle important.

---

d'infrastructures critiques ou de services essentiels ; et d'autre part, faire office de niche d'information en matière de cybersécurité (http://www.ccb.belgium.be/fr/node/79).

[269] Le CERT-EU, opérationnelle depuis septembre 2012, veille à la cybersécurité des institutions européennes et collabore également avec différents CERT des États-membres (https://cert.europa.eu/cert/plainedition/en/cert_about.html).

[270] Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 9.

[271] https://ccdcoe.org/about-us.html.

[272] S.n., *La Belgique a rejoint le centre d'excellence de l'Otan pour la défense cybernétique,* www. rtbf.be, 26 avril 2016.

[273] *Communiqué du Sommet de Varsovie publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Varsovie les 8 et 9 juillet 2016*, § 70.

[274] *Ibid.*, § 71.

[275] Parlement européen, *Countering hybrid threats : EU-NATO cooperation*, mars 2017 (disponible sur www.europarl.europa.eu).

[276] P Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], pp. 18-19.

L'efficacité de la prévention et de la réponse à offrir en cas d'attaque hybride

L'efficacité de la prévention et de la réponse face à une attaque hybride constitue le cinquième axe de la stratégie proposée par l'UE et l'OTAN. Lorsque l'auteur d'une attaque hybride est démasqué, les deux organisations ont alors pour objectif d'écarter la menace. De par leur essence même et les capacités dont elles disposent, la réaction des organisations ne sera cependant pas la même.

Stratégie de l'OTAN

La volonté de l'OTAN d'être en mesure de répondre rapidement et fermement aux nouveaux défis de sécurité émanant de l'est et du sud s'inscrit dans la lignée du « *plan d'action réactivité* » (RAP-*Readiness Action Plan*) lancé par l'OTAN lors du Sommet du pays de Galles en 2014 et réaffirmé au Sommet de Varsovie en 2016. Ce plan constitue le plus important renforcement de la défense collective de l'OTAN depuis la Guerre froide[277]. En cas d'attaque hybride d'un pays allié, le Conseil pourrait invoquer l'article 5 du traité de Washington, comme il le ferait en cas d'agression armée[278].

Depuis 2016, la Belgique prend part aux deux volets du « *plan d'action réactivité* ». Elle contribue d'une part, aux « *mesures d'assurance* » de ce projet, destinées à rassurer les populations d'Europe centrale et orientale par le renforcement de la défense de leur pays[279]. Dans ce cadre, l'armée belge participe à la « *mission de renforcement de la police de l'air* » de l'organisation (*Enhanced Air Policing Mission*) et à des opérations de déminage dans la mer Baltique[280]. D'autre part, elle contribue aux « *mesures d'adaptation* » de la RAP destinées à permettre à l'Alliance d'être davantage en mesure de « *réagir de manière rapide et décisive à des crises soudaines* »[281]. L'armée belge met ainsi des effectifs et des moyens de ses trois composantes à disposition de la nouvelle « *force opérationnelle interarmées à très haut niveau de préparation* » (VJTF-*Very high readiness Joint Task Force*), capable de se déployer dans des délais très courts pour « *répondre aux défis qui se posent, en particulier à la périphérie du territoire des pays de l'OTAN* »[282].

Un « *plan de mise en œuvre* » de la stratégie otanienne en matière de lutte contre la guerre hybride a été rédigé en février 2016. Le but est d'améliorer sa capacité à contrer les pratiques de la guerre hybride mais également la résilience des pays membres de l'Alliance. Certains pays ont réaffirmé leur volonté de s'engager militairement dans la lutte contre les menaces hybrides. Ainsi par exemple, le ministère de la Défense des Pays-Bas a publié une note où il déclare l'importance que peuvent jouer les forces armées pour « *anticiper* » mais également contrer les campagnes hybrides. Elles constituent non seulement un moyen important de « *dissuasion* » mais également de « *protection* » des infrastructures vitales[283]. Dans sa dernière « *vision stratégique pour la*

---

[277] S.n., *Le plan d'action « réactivité »*, 1 mars 2017. Article disponible sur www.nato.int.

[278] S.n., « Les attaques hybrides provoqueront une réponse militaire collective de l'OTAN », dans www.rt.com, 1e décembre 2015.

[279] S.n., *Le plan d'action « réactivité »*, 1 mars 2017. Article disponible sur www.nato.int.

[280] S. Vandeput, *Communiqué de presse du 2 décembre 2016 sur les opérations 2017*, consultable sur www.vandeput.belgium.be.

[281] S.n., *Le plan d'action « réactivité»*, 1 mars 2017. Article disponible sur www.nato.int.

[282] *Déclaration du Sommet du Pays de Galles*, 5 septembre 2014, § 8 (www.nato.int).

[283] K. Haegens, *'Hybrid Warfare". Een onderzoek naar de Belgische militaire capaciteiten om deze vorm van oorlogvoering te bestrijden*, ERM, Bruxelles, 28 avril 2017, p. 35.

défense » de juin 2016, le ministre belge de la Défense reconnaît également l'importance de la problématique de la « *guerre hybride* » qu'il définit comme une guerre qui « *combine des moyens et des méthodes militaires et non militaires afin de déstabiliser des pays* »[284]. Il est par ailleurs conscient que « *des services de renseignements performants sont un premier maillon essentiel pour identifier rapidement les menaces hybrides et les comprendre, afin de pouvoir réagir rapidement pour anticiper une escalade (…)* »[285] et que « *Écarter les menaces hybrides nécessite aussi un renforcement de la 'comprehensive approach' et donc l'utilisation de tous les éléments de pouvoir pour soutenir la stabilité et la sécurité* »[286]. Il souligne enfin l'importance du renforcement de la cybercapacité militaire de la Belgique afin de pouvoir répondre aux besoins de la défense collective[287].

Il est intéressant de constater que, depuis 2015, le Ministère de défense nationale de la Lituanie distribue à ses concitoyens un manuel explicatif et de conseils en cas d'attaques ou de situations d'urgence. Le document explique par exemple comment faire face en cas d'agression CBRN ou comment reconnaître les *« petits hommes verts* »…[288] D'aucuns considèrent en effet que les États baltes redoutent que le scénario ukrainien ne touche leurs propres pays. Ces anciennes républiques de l'URSS comptent en effet d'importantes minorités russes et craignent l'émergence de mouvements séparatistes appuyés par Moscou[289]. Notons également qu'entre 2009 et 2016, parmi les pays membres de l'OTAN, outre la Roumanie et la Pologne, seuls les pays baltes ont augmenté la part du PIB attribuée aux dépenses de défense[290]. Celle-ci avoisine 1,5% et dépasse même, en ce qui concerne l'Estonie et de la Pologne, la directive OTAN des 2%[291].

Stratégie de l'UE

Pour être en mesure de réagir rapidement aux « *événements déclenchés par les menaces hybrides* »[292], la haute représentante préconise, quant à elle, trois actions spécifiques. Il s'agit, tout d'abord, d'examiner l'applicabilité et les implications pratiques des dispositions juridiques dont dispose l'UE pour faire face aux « *menaces hybrides* ». La représentante permanente rappelle que « *si plusieurs menaces hybrides constituent une agression armée*[293] *contre un État membre de*

---

[284] BEL MoD, *La vision stratégique pour la Défense*, Bruxelles, 29 juin 2016, p. 28.

[285] *Ibid,* p. 42.

[286] *Ibid.*, p. 42.

[287] *Ibid.*, p. 53.

[288] Ministère de la défense nationale de Lituanie, *Prepare to Survive Emergencies and War: a Cheerful Take on Serious Recommendations,* Vilnius, 2015.

[289] S.n., « La menace russe pèse sur les pays baltes », dans *la-croix.com*, 3 mars 2015.

[290] Selon la terminologie définie par l'OTAN, le concept de « *dépense de défense* » englobe tous les paiements effectués pour la défense dans son sens large. Dans le cas de la Belgique, sont considérées comme dépenses de défense, le budget de la défense nationale et les pensions militaires et civiles du personnel de la Défense - dépendant du ministère des Pensions (Ph. Manigart, *L'évolution des dépenses militaires en Belgique depuis 1900*, CHCRISP n°1009, Bruxelles, 30 septembre 1983, p. 4 ; R. Flamant et P.-J. Parrein, *La vision stratégique pour la défense*, 29 juin 2016, p. 74).

[291] *Les dépenses de défense des pays de l'OTAN (2009-2016)*, 13 mars 2017, p. 2 [communiqué PR/CP (2017) 045] (www.nato.int)

[292] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 18.

[293] La résolution 3314 des Nations Unies du 14 décembre 1974 définit une « *agression* » comme *« l'emploi de la force armée par un État contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre*

l'UE, [la clause d'assistance mutuelle de] l'article 42, paragraphe 7 du TUE [Traité sur l'Union européenne][294] *pourrait être invoqué[e] afin d'apporter une réponse appropriée en temps utile* »[295]. En effet, « *compte tenu des ambiguïtés liées aux actions hybrides, l'applicabilité possible en dernier ressort de la clause de solidarité, [décrite dans l'article 222 TFUE (Traité sur le fonctionnement de l'Union européenne) et relative aux attaques terroristes ou catastrophes naturelle ou d'origine humaine dont un pays de l'UE pourrait être victime]*[296]*, devrait faire l'objet d'une évaluation de la Commission et de la haute représentante, dans leurs domaines respectifs de compétence, si un des États membres fait l'objet de menaces hybrides importantes* »[297].

Ainsi par exemple, après les attentats de Paris de novembre 2015, le président de la république française a préféré invoquer l'article 42§7 TUE plutôt que l'article 222 TFUE qui semblait pourtant rédigé pour cette occasion tragique. Si la clause d'assistance mutuelle de l'article 42§7 TUE peut ne pas totalement correspondre à la situation, notamment en raison des débats ancestraux qui déchirent la communauté internationale sur la notion « *d'agression armée* », le choix de la France s'explique pour différentes raisons politiques et juridiques[298]. Une des raisons importantes du choix français est que l'article 222 TFUE ne concerne qu'une assistance internationale sur le territoire des États-membres, ce que ne désirait pas la république[299]. Au contraire, en invoquant la clause de l'article 42§7 TUE plutôt que l'article 222 TFUE ou encore l'article 5 de l'OTAN qui consacre le principe de défense collective, la France

---

État, ou de toute autre manière incompatible avec la Charte des Nations Unies (…) » (article premier de la résolution 3314 de l'Assemblée générale des Nations Unies du 14 décembre 1974).

[294] Comme dit dans article 42§7 du traité sur le fonctionnement de l'Union européenne: « *Au cas où un État membre serait l'objet d'une agression armée sur son territoire, les autres États membres lui doivent aide et assistance par tous les moyens en leur pouvoir, conformément à l'article 51 de la charte des Nations unies. Cela n'affecte pas le caractère spécifique de la politique de sécurité et de défense de certains États membres. Les engagements et la coopération dans ce domaine demeurent conformes aux engagements souscrits au sein de l'Organisation du traité de l'Atlantique Nord, qui reste, pour les États qui en sont membres, le fondement de leur défense collective et l'instance de sa mise en œuvre* » (« Traité sur l'Union européenne (version consolidée) », disponible sur www.eur-lex.europa.eu).

[295] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 19.

[296] L'article 222 du traité sur le fonctionnement de l'Union européenne dispose que « *l'Union et ses États-membres agissent conjointement dans un esprit de solidarité si un État-membre est l'objet d'une attaque terroriste ou la victime d'une catastrophe naturelle ou d'origine humaine. L'Union mobilise tous les instruments à sa disposition, y compris les moyens militaires mis à sa disposition par les États-membres, pour (…) porter assistance à un État membre sur son territoire, à la demande de ses autorités politiques (…)* » (« Traité sur le fonctionnement de l'Union européenne (version consolidée) », disponible sur www.eur-lex.europa.eu). L'UE définit les infractions terroristes comme des « *actes intentionnels (…) qui, par leur nature ou leur contexte, peuvent porter gravement atteinte à un pays ou à une organisation internationale lorsque l'auteur les commet dans le but de gravement intimider une population ou contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque ou gravement déstabiliser ou détruire les structures fondamentales politiques, constitutionnelles, économiques ou sociales d'un pays ou une organisation internationale (…)* » (article premier de la *Décision cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme*, disponible sur www.eur-lex.europa.eu).

[297] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 19.

[298] F. Gouttefarde, « L'invocation de l'article 42§7 TUE : la solidarité militaire européenne contre le terrorisme », dans *RDN*, mars 2016, pp. 68-69. D'après F. Gouttefarde, les actes terroristes ne constituent pas un crime d'agression, celui-ci supposant l'existence de deux États souverains reconnus par la communauté internationale, dont l'un serait agresseur et l'autre victime (*Ibid.*, p. 72).

[299] *Ibid.*, p. 73.

pouvait garder le contrôle de sa souveraineté et notamment de sa politique extérieure tout en cherchant à renforcer l'engagement des Européens dans les opérations internationales de lutte contre le terrorisme et permettre ainsi d'alléger le dispositif français[300].

Ensuite, afin d'améliorer une réaction rapide et efficace en cas d'attaque hybride, un protocole opérationnel commun entre les États membres, la Commission et la haute représentante, et établi par la Commission européenne, précise, depuis juillet 2016, le rôle de chaque institution de l'Union et de chaque acteur dans les procédures à appliquer en cas de campagne hybride, depuis la première phase d'identification jusqu'à la phase finale d'attaque[301]. Le document sera testé à l'automne 2017, dans le cadre de l'exercice « *PACE17* » dirigé par l'OTAN et auquel participera l'UE[302]. Le but de la manœuvre est de tester les divers mécanismes et les capacités d'interaction de l'UE afin « *d'accélérer la prise de décision lorsque l'ambiguïté créée par une menace hybride nuit à la clarté* »[303].

Enfin, la haute représentante encourage les États membres à s'interroger sur les capacités d'action militaire à mettre en œuvre dans la lutte contre les menaces hybrides, dans le cadre de la politique de sécurité et de défense commune (PSDC)[304]. La Commission européenne affirme d'ailleurs que « *les priorités en termes de capacités visant à renforcer la résilience face aux menaces hybrides recensées par les États membres pourraient (…) être admissibles à une aide au titre de Fonds européen de la défense dès 2019* »[305]. L'Agence européenne de défense collabore, par différentes études, à la réflexion sur la mise en œuvre de nouvelles capacités d'action militaires pour lutter contre les menaces hybrides. Ainsi par exemple, une analyse est prévue pour 2018, sur le rôle des forces militaires dans la lutte contre les minidrones, susceptibles d'être utilisés contre les infrastructures critiques[306]. En outre, différentes réunions ont été organisées par l'État-major militaire de l'UE (EMUE) mais également par les directeurs généraux de la politique de défense de l'UE. De ces discussions auxquelles la Belgique a participé, il ressort que la contribution militaire relative aux « *menaces hybrides* » sera relativement limitée, ne nécessitera pas la mise en place de capacités militaires spécifiques et sera en tout cas subordonnée à l'approche civilo-politique. Les « *menaces hybrides* » ont néanmoins un impact sur les priorités, concepts et doctrines militaires[307].

---

[300] F. Gouttefarde, « L'invocation de l'article 42§7 TUE : la solidarité militaire européenne contre le terrorisme », dans *RDN*, mars 2016, pp. 73, 76.

[301] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 19 (voir annexe 1).

[302] Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 18.

[303] *Ibid.*, p. 19.

[304] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 19.

[305] Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 10.

[306] *Ibid.*

[307] « *Workshop on the EU Military Contribution to Countering Hybrid Threats. 13/14 Dec 2016, Lisbon* », document non publié; *EU Defence Policy Directors Meeting*, Bruxelles, 5 mai 2017, document non publié.

Par ailleurs, selon les représentants des pays membres présents aux réunions, la coopération interdépartementale et les structures nationales existantes devraient suffire pour faire face aux « *menaces hybrides* » [308]. La Belgique dispose ainsi de différents organismes chargés de coordonner la politique sécuritaire du pays, quel que soit le degré de la menace. Il s'agit du Conseil National de Sécurité, responsable d'établir et de coordonner la politique générale du renseignement et de la sécurité du pays[309], du Centre Gouvernemental de Coordination et de Crise (CGCCR) qui garantit, 24 heures sur 24, la collecte et la diffusion aux instances compétentes de « *toutes les informations urgentes de toute nature* »[310] et de l'Organe de Coordination pour l'Analyse de la Menace (OCAM) chargé d'effectuer des évaluations stratégiques et ponctuelles sur les menaces terroristes et extrémistes à l'encontre de la Belgique[311]. Différents « *plans d'urgence* » existent en Belgique pour améliorer la coordination des actions des instances responsables[312].

L'UE et l'OTAN désirent améliorer leur capacité et celle de leurs pays membres à réagir aux « *campagnes hybrides* ». Pour ce faire, les deux organisations préconisent de renforcer leur coopération en la matière.

La coopération entre l'UE et l'OTAN

L'UE et l'OTAN entendent davantage coopérer pour répondre plus efficacement aux « *menaces hybrides* ». Dès mai 2015, l'UE en manifeste le souhait et l'OTAN répond favorablement à cette demande quelques mois plus tard[313]. Les deux organisations « *partagent [en effet] les mêmes valeurs et sont confrontées à des défis similaires* »[314]. Elles souhaitent dès lors

---

[308] « *Workshop on the EU Military Contribution to Countering Hybrid Threats. 13/14 Dec 2016, Lisbon* », document non publié; *EU Defence Policy Directors Meeting*, Bruxelles, 5 mai 2017, document non publié.

[309] Créé en février 2015, le Conseil National de Sécurité établit la politique générale du renseignement et de la sécurité, en assure la coordination, et détermine les priorités des services de renseignement et de la sécurité. Il est également compétent pour la coordination de la lutte contre le financement du terrorisme et de la prolifération des armes de destruction massive. Il définit en outre la politique en matière de protection des informations sensibles. Le Conseil National de Sécurité est présidé par le Premier ministre et comprend les ministres ayant dans leurs attributions la Justice, la Défense, l'Intérieur et les Affaires étrangères et les Vice-Premiers ministres qui n'ont pas ces matières dans leurs compétences (www.premier.be).

[310] Créé en 1986, le Centre Gouvernemental de Coordination et de Crise (CGCCR) garantit une permanence ininterrompue, 24 heures sur 24 et 7 jours sur 7, pour la collecte, l'analyse et la diffusion aux instances compétentes de toutes « *les informations urgentes de toute nature* ». Il s'agit notamment des actualités relatives au terrorisme, aux cyber-incidents, à la santé publique, aux accidents ferroviaires, aux catastrophes naturelles ou au nucléaire (www.crisiscentrum.be).

[311] Créé en 2006, l'Organe de Coordination pour l'Analyse de la Menace (OCAM) est chargé d'effectuer des évaluations stratégiques et ponctuelles sur les menaces terroristes et extrémistes à l'encontre de la Belgique. Il établit ainsi « *l'échelle de la menace* » à partir d'informations glanées auprès de plusieurs organes comme la Sûreté de l'État les polices locales et fédérale et divers SPF (www.centredecrise.be).

[312] *Arrêté royal relative au plans d'urgence et d'intervention*, 16 février 2006; *Arrêté royal portant fixation du plan d'urgence national relatif à l'approche d'une prise d'otage terroriste ou d'un attentat terroriste*, 1 mai 2016.

[313] Agence européenne de défense, *Hybrid Warfare Threats-Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 novembre 2015 [SCS/P003198], pp. 21-22.

[314] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 20.

développer une connaissance commune des risques hybrides, mettre en œuvre une communication stratégique cohérente avant et pendant un conflit hybride [315] mais également collaborer dans le domaine de la cybersécurité et la « *prévention et gestion de crises* »[316]. La haute représentante précise néanmoins qu'une interaction plus étroite entre l`UE et l'OTAN doit se faire « *dans le respect de l'autonomie décisionnelle et des règles relatives à la protection des données de chaque organisation* »[317].

D'après un témoignage personnel récolté auprès de l'INTCEN, l'échange d'informations relatives aux menaces hybrides entre l'UE et l'OTAN n'est pas encore suffisant et devrait être amélioré. En effet, les procédures légales de transmission de l'information sont assez lourdes et « *L'OTAN est un système très procédural contrairement à l'UE qui produit davantage de documents consensuels et qui fonctionne de façon plus fluide* »[318].

En décembre 2016, le Conseil de l'UE s'est déclaré satisfait du communiqué du Sommet de Varsovie de juillet 2016, parce qu'il « *imprime un nouvel élan et confère une nouvelle teneur à la coopération entre l'UE et l'OTAN dans les domaines de la lutte contre les menaces hybrides (...)* »[319]. En juillet 2017, la Commission européenne a évalué la communication conjointe d'avril 2016, intitulée « *Cadre commun en matière de lutte contre les menaces hybrides : une réponse de l'Union européenne* ». Il ressort de cette analyse que les efforts conjugués de l'UE et l'OTAN, entrepris au cours de l'année 2017, « *ont produit des résultats substantiels* »[320]. Outre une coopération dans le domaine de la recherche et de la technologie en matière de cyberdéfense entre l'UE et l'OTAN, le rapport mentionne ainsi les avancées suivantes : une interaction entre la « *cellule de fusion* » de l'UE et la « *Branche Analyse des menaces hybrides* » de l'OTAN ; l'organisation, en octobre 2017, du premier exercice commun (PACE17) entre les deux organisations, en vue de « *tester leur réaction à un scénario de menace hybride* » et leur participation commune à des sessions d'information mutuelle en matière de résilience aux menaces hybrides. Le prochain rapport d'étape sur la coopération entre l'UE et l'OTAN proposera des pistes pour élargir leur coopération en la matière[321].

---

[315] Agence européenne de défense, *Hybrid Warfare Threats-Implications for European Capability Development. Strategic Context Report: Relevance of Hybrid Threats for European Security*, 30 novembre 2015 [SCS/P003198], p. 22.

[316] 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* », 6 avril 2016 [JOIN (2016) 18 final], p. 20.

[317] *Ibid.*

[318] Interview réalisée au sein de l'EU INTCEN par E. Hoorickx, le 30 novembre 2016.

[319] *Conclusions du Conseil sur la mise en œuvre de la déclaration commune du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du Traité de l'Atlantique Nord*, 6 décembre 2016 [PESC 1004, PSDC 699, COPS 378, POLMIL 147, EUMC 146], p. 2.

[320] Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final], p. 20.

[321] *Ibid.*, pp. 19-20.

Conclusions et recommandations[322]

Les constats

Menaces, conflits et guerres hybrides

Si le recours aux méthodes hybrides est aussi ancien que la guerre, le concept de « *guerre hybride* » ou de « *menaces hybrides* » englobe, depuis peu, une vaste réalité sémantique, où l'adversaire peut aussi faire appel à du « *hard power* », conventionnel ou non, qu'à du « *soft power* ». Selon certains, l'engagement d'actions cinétiques ne constitue pas une condition *sine qua non* de la stratégie hybride. C'est d'ailleurs ce qui différentie le « *conflit hybride* » de la « *guerre hybride* », notion utilisée pour la première fois dans le cadre d'un conflit armé afin de qualifier l'insurrection tchétchène.

Dans les milieux scientifiques, les pratiques de la guerre hybride sont associées à des acteurs très divers. Néanmoins, force est de constater que la Russie occupe une place de premier plan dans les débats relatifs à cette problématique. D'aucuns considèrent même la stratégie hybride russe, comme le « *côté obscur de l'approche globale* ».

La notion de « *menaces hybrides* » et celle de « *guerre hybride* », préférée par l'OTAN depuis 2014, sont des terminologies qui évoluent avec le temps, au gré de la situation internationale. Les premières définitions fournies par l'Alliance atlantique apparaissent dans le contexte des interventions de la Russie dans ses anciennes républiques socialistes, à savoir l'Estonie, la Géorgie et l'Ukraine. Dans un premier temps, le concept de « *menaces hybrides* » concerne l'utilisation simultanée de moyens conventionnels et non conventionnels. Ensuite, quand éclate la crise russo-ukrainienne, la « *guerre hybride* » désigne la mise en œuvre, très intégrée, de moyens militaires et non militaires afin de déstabiliser un adversaire. L'UE dévoile sa première définition de la « *guerre hybride* » en mai 2015, après que la France ait fait l'objet d'attaques terroristes particulièrement sanglantes. Si cette définition s'inspire largement de celle de l'OTAN, elle offre davantage de détails sur les modes opératoires de la « *guerre hybride* » ou « *guerre ambiguë* », à savoir les cyberattaques, la désinformation, le sabotage ou la « *guerre par procuration* ». L'« *attaque hybride* » vise à exploiter les « *vulnérabilités* » des États et à empêcher une réponse coordonnée de la communauté internationale. Quelques mois plus tard, l'OTAN développe sa première stratégie afin de lutter contre les « *pratiques de la guerre hybride* », dans laquelle les acteurs sont désormais « *étatiques* » ou « *non étatiques* ». L'« *État islamique* » aurait, en effet, également recours à certaines pratiques hybrides mais sans disposer, comme la Russie, de structures de pouvoir sophistiquées, en ce-compris un réseau diplomatique établi. La complexité des guerres hybrides est telle que seule une approche individualisée permet de comprendre en profondeur la spécificité de la Russie ou de l'État islamique en la matière. Reste par ailleurs à déterminer s'il est opportun de qualifier de « *guerre* » les actes terroristes perpétrés par Daesh.

Au sein de l'UE en tout cas, le terme de « *menace(s) hybride(s)* » est préféré à celui de « *guerre hybride* » utilisé à l'OTAN, ce qui peut susciter une certaine confusion sémantique. Par ailleurs, la terminologie utilisée ne semble pas signifier la même chose dans les milieux civils et militaires de l'UE. Au sein de l'état-major militaire européen, la notion de « *menace hybride* » décrit l'utilisation combinée des « *pratiques de la guerre hybride* » et est donc employée comme un synonyme de la « *guerre hybride* ». Dans les milieux civils par contre, le concept de « *menaces*

[322] Les conclusions de cette étude feront prochainement l'objet d'un article intitulé : « Quelle stratégie euro-atlantique face aux 'menaces hybrides' ? », dans *Revue Défense Nationale*. (E. Hoorickx)

hybrides » semble directement associé à des domaines aussi divers que le sabotage, les cyberattaques, la propagande, la désinformation ou les attaques CBRN. Une « *menace hybride* » correspondrait donc ici à un mode opératoire spécifique, ce qui est contradictoire avec la signification même de l' « *hybridité* » qui ne peut qualifier, par définition, qu'une combinaison à deux. Néanmoins - et ceci rend la question encore plus épineuse - pour que ces « *menaces* » soient considérées comme « *hybrides* », elles doivent être combinées entre elles et utilisées afin d'atteindre certains objectifs politiques précis. En outre, l'apparition du concept de « *résilience* » contribue encore davantage à complexifier la notion. En effet, lorsque l'UE recommande aux États membres de contrer les « *menaces hybrides* », elle les encourage en réalité à atténuer leurs « *vulnérabilités potentielles* » dans la lutte contre le terrorisme ou la criminalité organisée par exemple. Le pas est dès alors vite franchi pour renvoyer les « *menaces hybrides* » aux « *points faibles* » des États. En tout cas, force est de constater que la notion d'hybridité n'est pas comprise de la même façon par tous.

Il n'est par conséquent pas étonnant que la notion de « *guerre hybride* » ne fasse pas l'unanimité. D'aucuns remettent en cause l'utilité d'une telle terminologie « *fourre-tout* », souvent associée à un autre mot-valise, celui de la « *résilience* », et parlent même d'une « *réinvention de la roue* », au service de la bureaucratie otanienne. D'un point de vue stratégique, cette posture se défend. La stratégie intégrale, la guerre par procuration ou la guerre de l'information sont en effet historiquement classiques, même lorsque ces éléments sont intégrés dans une même opération. De plus, les défis sécuritaires recensés dans les documents stratégiques de l'OTAN dès 1991, et de l'UE dès 2003, englobent toutes les « *pratiques de la guerre hybride* » ou « *menaces hybrides* » reprises dans les communiqués officiels des deux organisations depuis le début des années 2010. Seule la problématique de la cybersécurité apparaît plus récemment comme nouveau défi stratégique, à savoir en 2010 à l'OTAN et en 2013 pour l'UE.

Si nouveauté il y a, elle est donc à chercher sur le versant tactique-opératif de la « *guerre hybride* ». Le danger cyber, la massification de la « *dé-identification* » des combattants lors de la crise russo-ukrainienne ou l'appropriation, par un ennemi irrégulier comme « *Daesh* », de technologies avancées devenues ergonomiques, en sont des exemples probants.

Cinq axes pour une réponse stratégique

Les pratiques de la « *guerre hybride* » sont considérées comme un défi sécuritaire majeur par l'UE et l'OTAN, qui s'attellent depuis 2015 à développer, chacune de leur côté mais en coopérant, une stratégie cohérente dans la lutte contre les « *campagnes hybrides* », afin d'aider les pays membres à contrer cette menace complexe. La réponse stratégique proposée par l'UE et l'OTAN s'articule autour de cinq axes : l'amélioration de la connaissance des « *pratiques hybrides* », le renforcement de la «*résilience*» à celles-ci, l'efficacité de la prévention et de la réponse face à l'attaque hybride (« *Integrated Political Crisis Response* »), et enfin, une meilleure coordination entre les parties dans toutes ces matières, en ce compris la communication stratégique et la cybersécurité. Si les deux organisations s'engagent à soutenir les pays membres dans la lutte contre les « *campagnes hybrides* », elles rappellent que la responsabilité première incombe aux États membres. Elles sont également décidées à utiliser les « *politiques et instruments* » existants pour faire face à cette problématique.

L'UE et l'OTAN prennent des mesures concrètes pour lutter contre les « *pratiques de la guerre hybride* ». Tout d'abord, pour mieux étudier celles-ci, l'UE dispose, depuis mai 2016, d'une cellule chargée de centraliser et partager les informations liées à la problématique. Depuis le printemps 2017, l'OTAN possède une cellule équivalente, ce qui devrait faciliter l'échange d'informations avec l'UE. Ensuite, la cyberdéfense constitue une priorité en matière de « *résilience* ». Les États ont reçu des recommandations strictes de l'UE pour rédiger leur stratégie de cybersécurité. Par ailleurs, l'OTAN et l'UE commencent à intégrer la problématique des « *cyberattaques* » dans leurs exercices communs ou non. Depuis peu, la vulnérabilité des

infrastructures critiques et la propagande sont également incluses dans les scénarios des entraînements.

Enfin, pour réagir de manière rapide et décisive à une éventuelle « *campagne hybride* », l'Alliance peut compter sur le « *plan d'action réactivité* » (RAP) lancé en 2014. Depuis juillet 2016, l'UE dispose, quant à elle, d'un protocole opérationnel, commun entre les États membres, la Commission et la haute représentante, qui précise le rôle de chaque institution de l'Union européenne et de chaque acteur dans les procédures à appliquer en cas de campagne hybride, depuis la première phase d'identification jusqu'à la phase finale d'attaque. L'applicabilité et les implications pratiques des dispositions juridiques de l'UE et l'OTAN pour faire face aux menaces hybrides font l'objet de discussions importantes. En outre, dans le cas de l'UE, la contribution militaire est relativement limitée, ne nécessite pas la mise en place de capacités militaires spécifiques et est en tout cas subordonnée à l'approche politique. Les « *menaces hybrides* » ont néanmoins un impact sur les priorités, concepts et doctrines militaires. Par ailleurs, au niveau national, la coopération interdépartementale et les structures nationales existantes devraient suffire pour répondre aux « *campagnes hybrides* ».

La politique belge de lutte contre les menaces hybrides

La Belgique investit beaucoup dans sa cybersécurité et se dote des instruments nécessaires pour améliorer sa résilience et répondre aux recommandations de l'UE et de l'OTAN dans ce domaine. La lutte contre la radicalisation, le terrorisme et la protection des infrastructures critiques font également partie des priorités sécuritaires de l'État belge. À ce jour, il n'existe pas de politique belge centralisée en ce qui concerne la lutte contre les « *menaces hybrides* ». La Belgique dispose néanmoins de différents organismes chargés de coordonner la politique sécuritaire du pays, quel que soit le degré de la menace, qu'elle soit « *hybride* » ou non. En outre, le ministère de la Défense, qui considère la « *guerre hybride* » comme un défi de premier ordre, participe activement au « *plan d'action réactivité* » (RAP) de l'OTAN.

Les recommandations

Adopter une terminologie commune

Si l'UE et l'OTAN estiment nécessaire de disposer d'une terminologie spécifique pour définir des attaques qui recourent à des moyens militaires ou non pour exploiter les « *vulnérabilités* » des États et empêcher ainsi une réponse coordonnée de son adversaire, il est urgent qu'ils parlent le même langage, singulièrement s'ils veulent pouvoir coopérer efficacement. À cet égard, il apparaît que le terme « *guerre hybride* » prête moins à confusion que celui de « *menace(s) hybride(s)* ».

Regarder la conflictualité contemporaine en face

Plutôt que de se focaliser sur un terme caméléon, qui sème souvent le trouble dans les esprits, l'UE et l'OTAN devraient utilement regarder la conflictualité contemporaine en face, à savoir que l'ennemi actuel est apte à coupler la quantité que nous n'avons plus et la qualité que nous pensons toujours avoir. L'émergence du *buzz word* de la « *guerre hybride* » peut dès lors être l'occasion de redéfinir les stratégies de défense contemporaines et d'envisager les phénomènes géopolitiques dans toutes leurs spécificités et complexité. En effet, le surengagement des forces occidentales, que ce soit en opérations intérieures ou extérieures, se traduit par des pertes de savoir-faire, au moment où l'adversaire probable en gagne. L'excellence technico-tactique des dispositifs occidentaux ne suffit

plus. Il convient dès lors d'élaborer une stratégie à long terme et de mobiliser des effectifs suffisants dotés d'un savoir-faire adéquat. Dans ce contexte, il serait judicieux de considérer avec attention et de répondre adéquatement aux questions suivantes : la Russie représente-t-elle réellement une menace pour l'UE ou pour l'OTAN ? Moscou a-t-elle l'intention d'attaquer, militairement et/ou cybernétiquement un État balte afin de tester la solidarité de l'Occident, et singulièrement de l'OTAN ? Si oui, les forces occidentales sont-elles suffisamment puissantes, équipées et maniables pour réagir efficacement et de manière coordonnée? Si non, la Russie peut-elle être considérée comme un partenaire, singulièrement dans la lutte contre le terrorisme ? L'organisation « *État islamique* », de son côté, est-elle en mesure de mettre à mal nos infrastructures critiques, notamment par le recours au cyberterrorisme ? Si oui, comment améliorer notre capacité à déceler les auteurs des cyberattaques ? Serait-il possible de nous rendre moins dépendants des réseaux informatiques ?

Répondre efficacement à la propagande

Comment répondre efficacement à la propagande? Ne conviendrait-il pas d'augmenter les effectifs de l'UE et l'OTAN afin d'être en mesure de réagir efficacement face à la désinformation devenue un phénomène très complexe? La coopération civilo-militaire est-elle suffisante en la matière? Ainsi par exemple, pour éviter qu'une agression extérieure ne s'accompagne d'une insurrection, ne conviendrait-il pas, sans pour autant négliger l'intervention militaire, de prêter une meilleure attention aux revendications politiques et sociales de la population, si celles-ci ne sont pas incompatibles avec nos intérêts fondamentaux?

Impliquer toujours davantage la Belgique dans les centres d'excellence européens

Les travaux de la « *cellule de fusion de l'UE* », de la « *Branche Analyse des menaces hybrides* » de l'OTAN et du « *centre européen de lutte contre les menaces hybrides* » d'Helsinki peuvent aider, d'une part, à déceler les « *menaces hybrides* » en gestation et d'autre part, à en déterminer l'origine afin de réagir de manière telle qu'une campagne hybride ne dégénère pas en conflit militaire mais soit endiguée et atténuée avant toute escalade. Le budget consacré par l'UE à la lutte contre le danger hybride pourrait néanmoins être revu à la hausse dans le but de permettre la surveillance d'un nombre plus important de pays ayant recours aux pratiques de la guerre hybride. D'autres centres d'excellence comme celui spécialisé dans la cyberdéfense, et localisé à Tallinn en Estonie, ont également un rôle important à jouer. L'implication de la Belgique dans ces différents organismes lui permet de rester un partenaire crédible de l'UE et de l'OTAN, alors que l'environnement de l'Europe a fondamentalement changé à la suite de la crise ukrainienne et de l'instabilité sur le flanc sud. À cet égard, on ne peut qu'encourager l'État belge à rejoindre les pays signataires du protocole d'accord sur le projet de centre de recherche d'Helsinki.

Enfin, la Belgique pourrait utilement développer une politique centralisée qui prenne en compte ses intérêts vitaux, ses vulnérabilités et les réponses globales à apporter face aux campagnes hybrides.

Annexes

Annexe 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* » (6 avril 2016)

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, 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. RECONNAÎTRE LE CARACTÈRE 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 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.

Action n° 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.

3.ORGANISER LA RÉPONSE DE L'UE : AMÉLIORER 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 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.

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.

Action n° 4: 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 RÉPONSE DE L'UE : RENFORCER LA RÉSILIENCE

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 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.

Action n° 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.

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 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 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].

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 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 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.

Action n° 8: 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.

Action n° 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.

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 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»).

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 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.

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.

Action n° 13: 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.

Action n° 14: 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 examinées dans le cadre de la stratégie de sûreté maritime de l'Union européenne (SSMUE) et du plan d'action accompagnant celle-ci.

Action n° 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.

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.

Action n° 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.

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 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.

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.

Action n° 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.

5.PRÉVENIR 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. 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 COOPÉRATION 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.

Action n° 22: 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.

Notes:

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].

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].

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).

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

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.

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.

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 (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 ; 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; .

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. http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf 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 ().

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.

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.

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).

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)».

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 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.

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].

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.

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/

Annexe 2 : Commission européenne, *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'* (19 juillet 2017)

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 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 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 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 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 nº 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, 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 nº 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, 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.

Action nº 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.

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.

Action nº 13: 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.

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] .

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 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.

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 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 n° 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.

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

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.

Action nº 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.

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.

Action nº 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.

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

Action nº 22: 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.

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.

Notes:

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.

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

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.

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.

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

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).

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).

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/studieshttps://bookshop.europa.eu/en/evaluation-of-risk-assessment-capacity-at-the-level-of-member-states-authorities-performing-coast-guard-functions-in-order-to-identify-commonalities-and-ways-to-enhance-interoperability-and-cooperation-in-this-field-across-eu-pbEA0417344/?CatalogCategoryID=JRWep2OwmH0AAAFEQf8mwjCM.

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 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

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.

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..

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.

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

Éléments de bibliographie

La bibliographie est intégrée dans les notes de bas de page. Les ouvrages repris ci-dessous ont été particulièrement utiles à l'auteure pour mener à bien son étude.

Travaux de référence

- J. Henrotin, *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris, 2014.
- Revue Défense Nationale, *Penser la guerre… hybride?,* mars 2016.
- Revue Stratégique n°111, *Hybridité et Guerre hybride*, mai 2016.

Documents OTAN

- Communication conjointe du SHAPE (Grand quartier général des puissances alliées en Europe) et du SACT (Commandant suprême allié Transformation) intitulée *BI-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*, 25 août, 2010 (consultable sur www.natolibguides.info).
- *Déclaration du sommet du Pays de Galles publiée par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue au pays de Galles les 4 et 5 septembre 2014*, 7 septembre 2014.
- *Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the North Atlantic Council at the Level of Defence Ministers*, 11 février 2016 (consultable sur www.nato.int);
- *Communiqué du Sommet de Varsovie publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Varsovie les 8 et 9 juillet 2016.*

Documents UE

- Agence européenne de défense, *Hybrid Warfare threats-implications for european capability development. Strategic context report: relevance of hybrid threats for European security*, 30 novembre 2015 [SCS/P003198].
- EU Military Staff, *Draft Food for Thought Paper: Possible EU Military Contributions to Countering Hybrid Threats*, 2 octobre 2015 [EEAS (2015) 1367 REV1].

- 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* », 6 avril 2016 [JOIN (2016) 18 final].
- Parlement européen, *Countering hybrid threats : EU-NATO cooperation*, mars 2017 (disponible sur www.europarl.europa.eu).
- Note de la Présidence du Conseil de l'UE intitulée « Mandate of the Friends of the Presidency Group on the Implementation of Action 1 of the Joint Framework on Countering Hybrid Threats (doc. 7688/16) », 2 juin 2017 [9502/17].
- Commission européenne, *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'*, Bruxelles, 19 juillet 2017, [JOIN (2017) 30 final].

Institut Royal Supérieur de Défense
Centre d'Etudes de Sécurité et Défense
30 Avenue de la Renaissance
1000 Bruxelles