

RAPPORT n° 9

FÉVRIER 2021

Observatoire de la politique de défense américaine

La stratégie des États-Unis face aux menaces hybrides

DIDIER GROS – NICOLE VILBOUX

FONDATION
pour la **RECHERCHE**
STRATÉGIQUE

Marché n° 2018 1050 118 198
EJ court 180 005 17 10
notifié le 18 octobre 2018
réunion de lancement :
14 novembre 2018

avec le soutien de la



Liste des abréviations

A2/AD	<i>Anti-Access / Area Denial</i>
ASD SO/LIC	<i>Assistant Secretary of Defense for Special operations and Low Intensity Conflict</i>
CEPC	<i>Civil Emergency Planning Committee</i>
CoE	<i>Center of Excellence</i>
CNAS	<i>Center for New American Security</i>
CSBA	<i>Center for Strategic and Budgetary Assessment</i>
CSIS	<i>Center for Strategic and International Studied</i>
DFE	<i>Dynamic Force Employment</i>
DMO	<i>Distributed Maritime Operations</i>
DNI	<i>Director of National Intelligence</i>
DoD	<i>Department of Defense</i>
GAO	<i>Government Accountability Office</i>
GEC	<i>Global Engagement Center</i>
GOM	<i>Global operating model</i>
IW	<i>Irregular Warfare</i>
JOC	<i>Joint Operating Concept</i>
JOE	<i>Joint Operating Environment</i>
MDO	<i>Multidomain operations</i>
NDAA	<i>National Defense Authorization Act</i>
NDS	<i>National Defense Strategy</i>
NMS	<i>National Military Strategy</i>
NSS	<i>National Security Strategy</i>
OSD	<i>Office of the Secretary of Defense</i>
QDR	<i>Quadrennial Defense Review</i>
SSI	<i>Strategic Studies Institute</i>
TRADOC	<i>Training and Doctrine Command</i>
UE	<i>Union Européenne</i>
USMC	<i>US Marine Corps</i>
USSOCOM	<i>US Special Operations Command</i>

Avertissement

Les propos exprimés dans ce rapport n'engagent que leurs auteurs et ne constituent en aucune manière une position officielle de la Fondation pour la Recherche Stratégique ou du ministère des Armées.

SOMMAIRE

LISTE DES ABRÉVIATIONS

L'ANALYSE AMÉRICAINE DES MENACES « HYBRIDES »	1
RÉSUMÉ	1
INTRODUCTION	3
1. UN CONCEPT QUI ÉVOLUE AVEC LE RÉFÉRENTIEL STRATÉGIQUE AMÉRICAIN	4
1.1. Une notion née avec la « longue guerre » contre des adversaires irréguliers	4
1.2. L'hybridité devient un mode particulier de confrontation interétatique.....	7
2. UNE NOTION ABSORBÉE PAR LES RÉFLEXIONS SUR LA COMPÉTITION EN « ZONE GRISE »	9
2.1. L'hybridité devient l'une des formes ambiguës de conflit	9
2.2. La zone grise s'impose comme l'espace privilégié de confrontation hybride	11
3. DES ACTIVITÉS QUI PRÉSENTENT UN DÉFI MAJEUR POUR LES ÉTATS-UNIS	15
3.1. L'hybridité exploite les failles de la politique de sécurité américaine	16
3.2. Des modalités de compétition privilégiées par les rivaux révisionnistes	18
DES RÉPONSES COUVRANT UN LARGE CHAMP DE « COMPÉTITION STRATÉGIQUE »	21
1. UNE ADAPTATION À LA COMPÉTITION INITIÉE PAR LE DOD	21
1.1. La NDS de 2018 amorce l'élargissement du champ de compétition.....	22
1.2. L'adaptation des forces armées	26
1.2.1. La plupart des Services développent leur contribution à la compétition élargie	26
1.2.2. La dimension interarmées : des opérations tout-domaine intégrées sur l'ensemble du continuum de compétition.....	30
2. À LA RECHERCHE D'UNE STRATÉGIE INTÉGRALE	31
2.1. Des réponses adaptées à la gamme des défis de zone grise	32
2.1.1. Le renforcement de la protection et de la résilience	33
2.1.2. L'élargissement du champ de la dissuasion	34
2.1.3. L'influence	36
2.2. Une nécessaire implication des institutions civiles	36
2.2.1. Les instruments d'influence.....	37
2.2.2. Les domaines économique et financier	38

2.2.3.	Le renseignement.....	40
2.2.4.	Le domaine juridique.....	40
3.	LES MENACES HYBRIDES COMME FACTEUR DE MOBILISATION DES ALLIÉS.....	41
3.1.	La diffusion du concept au sein de l’OTAN.....	41
3.1.1.	Un enjeu intégré à la stratégie de l’Alliance.....	42
3.1.2.	L’articulation des dimensions civile et militaire.....	43
3.2.	L’union européenne et l’appropriation résolue du concept des « menaces hybrides ».....	44
3.2.1.	L’entretien et l’exploitation de la porosité OTAN-UE.....	44
3.2.2.	Les initiatives de l’UE.....	45
	RÉFLEXIONS CONCLUSIVES.....	47
1.	LES DIFFICULTÉS ET ÉCUEILS RENCONTRÉS PAR LES ÉTATS-UNIS.....	47
1.1.	Difficultés liées à la mise en œuvre d’une stratégie intégrée.....	47
1.2.	L’écueil opérationnel : quelle mise en œuvre concrète ?.....	48
1.2.1.	Des postures encore en cours définition.....	48
1.2.2.	L’American Way of War rétif aux exigences de la guerre hybride.....	49
2.	DES VULNÉRABILITÉS À RELATIVISER.....	50
2.1.	L’hybridité, expression contemporaine d’un mimétisme stratégique réincarné ?.....	50
2.2.	Une capacité d’influence toujours considérable.....	52
3.	PERSPECTIVES ET IMPLICATIONS DES STRATÉGIES HYBRIDES AMÉRICAINES.....	53
3.1.	Les dilemmes posés par les États-Unis à leurs principaux adversaires.....	53
3.2.	Des dilemmes stratégiques pour les alliés et partenaires.....	54
ANNEXE 1		
	SCHÉMA D’ÉVOLUTION DES CONCEPTS.....	57
ANNEXE 2		
	EXEMPLES DE DÉFINITION DES ACTIVITÉS HYBRIDES ET DE « ZONE GRISE ».....	58
ANNEXE 3		
	LES ACTIVITÉS HYBRIDES DES RIVAUX.....	60

L'analyse américaine des menaces « hybrides »

Résumé

L'hybridité s'installe dans la réflexion stratégique au milieu de la décennie 2000, dans l'idée de décloisonner les catégories d'enjeux qui se multiplient **avec l'engagement dans les campagnes irrégulières**. Elle entre dans les documents stratégiques et doctrinaux à compter de 2007, **sans pour autant faire l'objet d'une définition institutionnelle**. L'intervention russe dans le conflit ukrainien et l'annexion de la Crimée en 2014 en modifient le périmètre et les implications ; elle devient alors un **mode particulier de confrontation interétatique** et désigne la **confusion croissante entre les modalités de compétition interétatique « légitimes » et les activités hostiles de toute nature destinées à obtenir un gain stratégique sur l'adversaire, sans aller jusqu'à l'affrontement armé direct**.

Parallèlement, la notion de « **zone grise** » émerge et s'impose comme l'espace privilégié de confrontation hybride. Elle se caractérise par « *l'ambiguïté quant à la nature du conflit* », des actions que l'on peine à qualifier de manière objective (elles sont « *perspective-dependent* »), et par un « *certain niveau d'agression* » qui marque le passage de la compétition normale à la « zone grise ».

Quel que soit le nom donné à ces activités, elles sont bel et bien devenues une préoccupation centrale de la communauté stratégique américaine et ont trouvé une **forme de reconnaissance officielle au travers de l'adoption de la « compétition stratégique » comme axe majeur de la politique de sécurité et défense des États-Unis**. Ces activités hybrides constituent un **défi majeur** pour les États-Unis car elles seraient spécifiquement conçues pour **exploiter leurs « vulnérabilités »** (et plus largement celles des États occidentaux) et, en corollaire du point précédent, sont perçues comme les **modes d'action privilégiés par la Russie et la Chine**, les deux puissances révisionnistes les plus dangereuses pour les intérêts américains, si bien qu'il ne s'agit pas seulement d'un débat théorique sur des enjeux potentiels mais aussi d'un discours de mobilisation immédiate.

En réponse, **l'adaptation à la compétition a été initiée par le DoD**, comme l'atteste la *National Defense Strategy* de 2018 qui vient consacrer les travaux conceptuels et doctrinaux des armées, qu'il s'agisse des **MDO – Multi-Domain Operations**, du **GOM – Global Operating Model** ou des opérations tout-domaine intégrées sur l'ensemble du continuum de compétition (**GIO – Globally Integrated Operations**). Mais c'est bien une approche plus globale de type **whole-of-government** voire **whole-of-society** qui est recherchée, sous la forme d'une stratégie inté-

grale. Il s'agit pour les États-Unis d'être capables d'agir de manière coordonnée dans les « espaces » de confrontation ou « domaines contestés » que sont prioritairement **le domaine informationnel, le cyberspace, l'espace, l'économie, et le champ opérationnel militaire**. L'effort porte donc sur les fonctions structurantes que sont **la protection, la dissuasion, l'influence et la coercition**. Pratiquement, il s'agit de mettre en œuvre une gamme complète de moyens et méthodes sur tout le spectre, impliquant ainsi **l'ensemble des institutions civiles**. S'y ajoute la **dimension internationale**, les menaces hybrides devenant un facteur de mobilisation des alliés et partenaires. Dans ce domaine, on aura constaté un certain **prosélytisme américain à l'OTAN** et, par exploitation de la **porosité OTAN-UE**, au sein de cette dernière organisation.

Le déploiement d'une stratégie nationale intégrée se heurte à **plusieurs vulnérabilités et écueils**, de nature bureaucratique parfois, liés aux choix de posture stratégique à assumer (quel déploiement permanent de forces en Europe par exemple), mais aussi, sur le plan militaire, procédant d'une réticence culturelle prononcée aux méthodes de « guerre irrégulière ». Pour autant, *l'hybrid warfare* ne saurait être réduite à l'« arme du pauvre » ou du « faible contre le fort ». Elle est aussi **l'apanage de la puissance américaine** qui, à sa manière, l'emploie sur le continuum de la compétition stratégique, notamment par l'intermédiaire d'une **stratégie d'influence performante** malgré tout sur la scène internationale, comme en témoigne l'appropriation du concept par l'OTAN et l'UE (notions de **résilience** et de **civil preparedness**).

Ainsi, les États-Unis sont en mesure de **poser des dilemmes stratégiques à leurs principaux adversaires**, soit en **mettant eux-mêmes en œuvre des stratégies hybrides**, soit en ravivant une **mobilisation quasi idéologique contre les puissances révisionnistes**, comme semblent l'indiquer les démarches du nouveau président américain vis-à-vis de la Russie et de la Chine. Mais l'Amérique **peut aussi contraindre ses alliés et partenaires**, notamment l'UE, **sur le plan géopolitique** en imposant à terme un choix radical entre le camp occidental et une Chine qui serait l'adversaire systémique voire l'ennemi désigné, **sur le plan économique** par l'exercice de pressions et sanctions juridiques et financières, et **sur le plan stratégique-opérationnel** par l'imposition d'une politique d'attribution collective, d'une conception élargie de la dissuasion (*integrated deterrence*), ou par l'exploitation « inamicale » de vulnérabilités critiques dévoilées.

Introduction

La notion d'hybridité et, en particulier au sein de l'appareil institutionnel américain, ne fait l'objet d'aucune définition nationale claire et partagée. Relevant d'une profusion de termes¹ concurrents ou assimilables, la notion se dilue dans un paysage conceptuel extraordinairement mouvant qui entretient la confusion et rend ainsi toute herméneutique particulièrement difficile.

Ainsi, en 2021, soit une quinzaine d'années après la première apparition puis formalisation du concept d'hybridité, la lecture des publications officielles pourrait nous conduire à le considérer obsolète tant il demeure controversé et semble avoir pris la forme d'un fourre-tout, manipulé par les uns et les autres en fonction d'objectifs parfois politiques voire idéologiques, parfois stratégiques, sans qu'il soit toujours aisé d'en percevoir la cohérence attendue. Ce serait pourtant une erreur, non seulement parce que le concept demeure florissant hors des frontières américaines, mais surtout parce que sa généalogie comme son utilisation actuelle contribuent à éclairer le paysage conceptuel américain et nous permettent d'atteindre à l'essence de la réflexion stratégique en cours.

Il convient donc, dans un premier temps, de démêler l'écheveau des termes, notions et concepts en vigueur au sein de l'appareil institutionnel américain (*hybrid war ; hybrid warfare ; hybrid strategy ; hybrid threat ; hybrid model*), pour ensuite s'interroger sur ce que recouvre spécifiquement l'hybridité aujourd'hui, sur les plans théorique et pratique, et, enfin, en quoi elle nous aide à appréhender la vision stratégique américaine contemporaine.

¹ Dans la mesure où il n'existe pas actuellement de concept formel relatif à l'hybridité, les expressions « concepts » et « notions » seront utilisées indifféremment dans ce rapport.

1. Un concept qui évolue avec le référentiel stratégique américain

1.1. Une notion née avec la « longue guerre » contre des adversaires irréguliers

L'hybridité s'installe dans la réflexion stratégique au milieu de la décennie 2000, dans le mouvement de réforme visant à inscrire durablement les activités irrégulières au cœur de la politique de défense. La notion émerge dans le débat avec l'article du général James Mattis et de Frank Hoffman², ce dernier développant par la suite le cadre de réflexion le plus élaboré sur les formes de combat hybrides (*hybrid warfare*), au travers de nombreuses publications. En parallèle, le concept est étudié lors de la préparation de la *National Defense Strategy* (NDS) de 2005 sous l'impulsion du colonel Nathan Freier, alors à l'OSD, et qui continuera ensuite à développer cette thématique au sein de l'US Army War College³. Même s'il est un peu éclipsé par les travaux sur la contre-insurrection, le sujet connaît un certain succès dans la littérature spécialisée et entre rapidement dans le discours du DoD et des armées, sans jamais toutefois faire l'objet d'une définition institutionnelle⁴.

L'hybridité est d'abord utilisée pour qualifier des formes de confrontation, qui sans être entièrement nouvelles, devraient constituer à l'avenir un danger croissant. Pour Hoffman, les opérations hybrides (*hybrid warfare*) se caractérisent par l'utilisation combinée d'« une gamme complète de modes de combat, incluant les capacités classiques, les tactiques et organisations irrégulières, les actions terroristes dont la violence indiscriminée et la coercition, ainsi que les désordres criminels »⁵. Il s'agit du résultat d'une « convergence » de formes de violence qui ne peuvent plus être envisagées comme des types de conflit séparés, parmi lesquels les armées américaines auraient le loisir de choisir. Il faut en particulier renoncer à la distinction habituelle entre guerre régulière et irrégulière, et s'attendre à ce que les « concurrents utilisent toutes les formes de guerre et de tactiques, parfois simultanément »⁶.

Dans la même logique, le colonel Freier explique que les rédacteurs de la NDS de 2005 envisageaient que les différents types de défis auxquels les États-Unis seraient confrontés « fusionneraient fréquemment [sous forme] hybride complexe », mêlant les menaces irrégulières

² James Mattis, Frank Hoffman, « Future Warfare: The Rise of Hybrid Wars », *Proceedings*, November 2005 – <https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars>

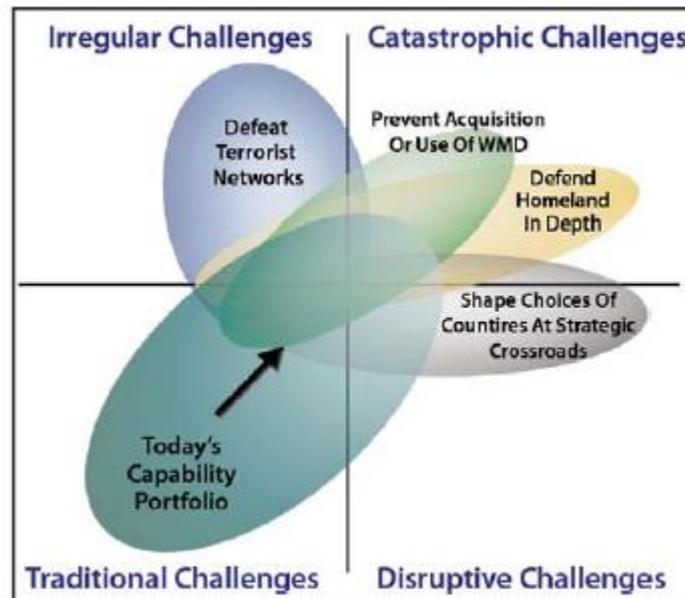
³ Nathan Freier, *Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context*, Carlisle, Strategic Studies Institute, May 2007.

⁴ Le terme « *hybrid* » ne figure pas dans le *DOD Dictionary of Military and Associated Terms* (version de décembre 2020).

⁵ « *a full range of modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts that include indiscriminate violence and coercion, and criminal disorder* » ; Lt-Col. Frank Hoffman, « Hybrid Warfare and Challenges », *Joint Force Quarterly*, Issue 52, 1st quarter 2009, p. 34 – <https://smallwarsjournal.com/documents/jfqhoffman.pdf>

⁶ Ibid.

et catastrophiques, mais se combinant aussi aux « *capacités militaires traditionnelles* » d'adversaires étatiques ou proto-étatiques⁷. Le « quadrant des défis », présenté dans les documents du DoD (NDS puis *Quadrennial Defense Review* (QDR) de 2006), ne mentionnait toutefois pas le domaine hybride.



Source : *Quadrennial Defense Review Report*, US Department of Defense, 2006, p. 19.

La menace de l'hybridité est alors principalement liée à « *la diffusion de l'armement moderne dans le monde, combinée aux leçons tirées par [les] ennemis en Irak et en Afghanistan, [produisant] un degré croissant de létalité dans les conflits contemporains* »⁸. Elle est donc envisagée dans le cadre d'une campagne militaire, où les forces américaines seraient confrontées à « *des adversaires très adaptables et disposant de technologies modernes* ». Or, pour les porteurs du débat, les armées y restent mal préparées. Il s'agit donc de s'assurer que l'expérience durement acquise pendant la « longue guerre » (mais aussi lors de la guerre de 2006 au Liban entre Israël et le Hezbollah) sera prise en compte durablement par l'institution.

L'hybridité est effectivement dans les documents stratégiques et doctrinaux des armées, à commencer par le Département naval, qui l'incorpore dans la Stratégie maritime de 2007⁹, pour décrire la convergence entre menaces régulières et irrégulières provoquée par la combinaison de moyens de combat simples et de haute technologie¹⁰. L'Army intègre à son tour la notion dans le *Capstone Concept* de décembre 2009, puis dans le manuel ADP 3-0, *Unified*

⁷ « *Challenges would often blend into complex hybrids. Not only would irregular and catastrophic challenges merge, but at times, they would also combine with or be underwritten by a state or state-like competitor's traditional military capacity* ». Nathan Freier, *Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context*, op. cit., p. 6.

⁸ Frank G. Hoffman, « Perspectives on the Future Security Environment », Statement before the Subcommittee on Intelligence and Emerging Threats and Capabilities, House Armed Services Committee, U.S. House of Representatives, February 13, 2012, p. 6.

⁹ *A Cooperative Strategy for 21st Century Seapower*, Washington (DC), Department of the Navy, 2007.

¹⁰ Maj. Tim McCulloh, « Theory of Hybrid Conflict », in *Hybrid Warfare*, Report 13-04, McDill AFB, Joint Special Operations University, 2013, p. 9.

Land Operations, d'octobre 2011. Au niveau interarmées, elle apparaît à la fin du *Joint Operating Environment* (JOE) de 2010 : tout en reconnaissant que les « *approches hybrides ne sont pas nouvelles* », les auteurs estiment qu'elles deviennent particulièrement dangereuses du fait de l'intégration de technologies perfectionnées dans des conflits « *prolongés et centrés sur la population* »¹¹.

Bien que l'expression soit couramment employée, un rapport du GAO sur son institutionnalisation au sein du DoD montre en 2010 qu'il n'existe aucune définition commune et que chaque organisation a sa propre conception de l'hybridité¹². À mesure qu'elle se répand, l'utilisation du qualificatif « hybride » s'applique d'ailleurs de manière de plus en plus confuse, à une forme de confrontation (*hybrid warfare/approach*), de conflit (*hybrid war*) ou de menace. Alors que la *National Military Strategy* (NMS) de 2015 mentionne les conflits hybrides, placés sur un « *continuum de conflictualité* » entre les conflits non-étatiques et les conflits interétatiques, les publications de l'Army privilégient l'expression « *hybrid threat* » (et même « *hybrid enemies* » en 2009) pour décrire le même phénomène¹³. De son côté, Frank Hoffman définit simplement les « adversaires hybrides » par leur aptitude à combiner différents modes d'affrontement armé¹⁴.

Reflétant le cadre de réflexion dominant de l'époque, ces adversaires sont généralement assimilés à des organisations non-étatiques capables de se doter de moyens de combat quasi-conventionnels. Le Hezbollah en est l'archétype, faisant l'objet de nombreuses études¹⁵.

Le « modèle » Hezbollah

À partir de 2006, le terme de « guerre hybride » est largement utilisé pour décrire à la fois la nature du conflit et l'acteur libanais. En effet, a alors été mis en évidence le caractère hybride du Hezbollah, à la fois organisation infra-étatique et mouvement terroriste, et organisation armée équipée d'équipements modernes (missiles de type Fajr ou C-802, roquettes de type Khaïbar, drones de type Mirsad, etc.) capable de manœuvrer et de faire face à une force armée adverse conventionnelle de quatrième génération. Plus encore, la manière dont le Hezbollah s'est conduit, associant actions de type asymétrique et manœuvres conventionnelles, a surpris et a sans doute marqué un tournant dans la manière d'évaluer les capacités de ce mouvement. Dès lors, le terme hybride paraissait effectivement judicieux pour qualifier les événements en question qui mêlaient en effet l'étatique et le non-étatique, le conventionnel et le non-conventionnel, l'asymétrie et la symétrie dans le rapport de force, bref une nature, des capacités et un acteur inclassables que la notion d'hybridité, en soulignant le caractère étrange et aberrant au regard des modèles classiques, qualifiait de manière pertinente.

¹¹ *The Operating Environment 2010*, US Joint Forces Command, February 2010, p. 66.

¹² *Hybrid Warfare*, GAO-10-1036R, Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives, September 10, 2010.

¹³ « *The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects* ». Army Doctrine Publication (ADP) 3-0, *Unified Land Operations*, October 2011, p. 4.

¹⁴ « *Any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and battlespace to obtain their political objectives.* ». Lt-Col. Frank Hoffman, « *Hybrid Warfare and Challenges* », op. cit.

¹⁵ Peter Kouretsos, « *A Literature Review – Annex A: Contextualizing Chinese Hybrid Warfare* », in Ross Babbage, *Stealing a March. Case Studies*, Vol. II, Washington (D.C.), CSBA, 2019, p. 2.

Toutefois, l'utilisation d'une approche hybride par des États devient une possibilité de plus en plus prise en compte à la fin de la décennie. L'intervention russe en Géorgie en 2008 est citée par Hoffman comme un premier exemple, mais il s'inquiète plutôt du potentiel de l'Iran à recourir à des méthodes de combat irrégulières en cas de confrontation avec les États-Unis¹⁶.

Au niveau institutionnel, la *Quadrennial Defense Review* de 2010 explique ainsi que les « *approches hybrides* » peuvent aussi bien être utilisées :

- ➔ Par des « *adversaires étatiques utilisant des formes de combat prolongées, recourant potentiellement à des forces auxiliaires* »¹⁷ ;
- ➔ Que par des « *acteurs non-étatiques utilisant des concepts opérationnels et des capacités* » de haute intensité.

La même description figure dans le manuel de l'Army, *Unified Land Operations*, en 2011. Mais la nature des méthodes, comme des objectifs, change avec l'évolution du contexte international.

1.2. L'hybridité devient un mode particulier de confrontation interétatique

L'intervention russe dans le conflit ukrainien et l'annexion de la Crimée en 2014 modifient le périmètre et les implications de l'hybridité. L'attention se porte désormais principalement sur l'utilisation de modes d'action indirects par des États.

Impact de la « doctrine Gerasimov »

La Russie devient en 2014 le nouveau « modèle » d'adversaire étatique utilisant une approche hybride à la suite de son intervention en Ukraine. Mais pour une partie de la communauté stratégique, il s'agit surtout d'une mise en œuvre d'une véritable « doctrine » de l'hybridité, qui aurait été exposée dans un discours, puis un article de 2013 par le Chef de l'État-Major général des Forces armées russes, le général Gerasimov¹⁸.

Popularisé en Occident par Mark Galeotti, l'article explique que les « *règles de la guerre ont changé* » et que les moyens non militaires jouent un rôle de plus en plus important dans la réalisation des objectifs stratégiques, car la limite entre la paix et la guerre tend à s'estomper. Il constate que l'emploi de mesures politiques, économiques, informationnelles... ajouté à l'utilisation « *masquée* » de forces armées, devient une caractéristique des conflits contemporains, dans lesquels les adversaires recherchent des modes d'action asymétriques exploitant leurs vulnérabilités respectives.

Alors que le général Gerasimov entend décrire implicitement ce qui constitue d'après lui une stratégie occidentale (à l'œuvre en Ukraine ou lors des « *printemps arabes* »), l'approche est qualifiée de « *doctrine* »¹⁹, devenant rapidement une référence de ce que serait la conception russe de la « *guerre non-linéaire* ».

¹⁶ Frank G. Hoffman, « Perspectives on the Future Security Environment », op. cit., pp. 10-11.

¹⁷ 2010 *Quadrennial Defense Review*, US Department of Defense, February 2010, p. 8.

¹⁸ Valerii Gerasimov, « The Value of Science Is in the Foresight », *Military-Industrial Courier*, February 26, 2013. [version originale : « Ценность науки в предвидении », <https://www.vpk-news.ru/articles/14632>]

¹⁹ Mark Galeotti a regretté dans plusieurs publications avoir donné le titre « doctrine Gerasimov » à la traduction américaine de l'article. Mark Galeotti, « I'm Sorry for Creating the 'Gerasimov Doctrine' », *Foreign Policy*, 18 March 2018 – <https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/>.

Pour certains analystes, l'idée de combinaison des modes opératoires réguliers/irréguliers dans une campagne militaire devient moins importante pour caractériser l'hybridité, que la dimension non militaire des activités qui peuvent être utilisées pour s'opposer aux intérêts américains. Ce sont les formes de confrontation clandestines, politiques, économiques ou cyber qui sont mises en avant dans les définitions de la guerre hybride développées après 2014.

Tableau n° 1 : QUELQUES EXEMPLES DE DÉFINITIONS RÉCENTES DE LA « GUERRE HYBRIDE »

Nadia Schadlow 2015	« A blend of military, economic, diplomatic, criminal, and informational means to achieve desired political goals » ²⁰ .
Lauren Speranza, Atlantic Council 2020	« An approach that blends conventional and unconventional, overt and covert, kinetic and non-kinetic, and military and nonmilitary means to undermine a target and achieve the perpetrator's political and strategic goals » ²¹ .
CSIS 2020	« An effort or series of efforts intended to advance one's security objectives at the expense of a rival using means beyond those associated with routine statecraft and short of means associated with direct military conflict. » ²²

Ces définitions sont plutôt des descriptions de modes d'action, dont une grande partie échappe au domaine de la défense. L'hybridité désigne désormais la confusion croissante entre les modalités de compétition interétatique « légitimes » et les activités hostiles de toute nature destinées à obtenir un gain stratégique sur l'adversaire, sans aller jusqu'à l'affrontement armé direct. On retrouve généralement dans le répertoire des actions hybrides les quatre catégories distinguées par Lauren Speranza²³ :

- L'utilisation limitée de la violence sous le seuil de l'affrontement armé ;
- Les attaques cyber et autres atteintes aux infrastructures essentielles ;
- La subversion politique et la coercition économique ;
- Les opérations d'information.

Ces conceptions élargies de l'hybridité tendent à se confondre avec une autre notion apparue plus tardivement, mais qui prend une importance croissante à partir de 2015 : celle de « zone grise ».

²⁰ Nadia Schadlow, « The Problem with Hybrid Warfare », *War on the Rocks*, April 2, 2015.

²¹ Lauren Speranza, *A Strategic Concept for Countering Russian and Chinese Hybrid Threats*, Atlantic Council, July 2020 – <https://www.atlanticcouncil.org/in-depth-research-reports/a-strategic-concept-for-countering-russian-and-chinese-hybrid-threats/>

²² Hijab Sha, Melissa Dalton, *Partners, Not Proxies: Capacity Building in Hybrid Warfare*, CSIS Briefs, May 27, 2020 – <https://www.csis.org/analysis/partners-not-proxies-capacity-building-hybrid-warfare>

²³ Lauren Speranza, *A Strategic Concept for Countering Russian and Chinese Hybrid Threats*, op. cit., p. 3.

2. Une notion absorbée par les réflexions sur la compétition en « zone grise »

Parallèlement à l'évolution de la notion d'hybridité, le débat a en effet suscité l'émergence ou la redécouverte d'autres concepts destinés à décrire des formes de conflictualité « non régulières ». Parmi les expressions les plus utilisées, on retrouve *irregular warfare*, *sharp power*, *active measures*, *political warfare*, *unconventional warfare*... jusqu'à ce que deux termes prennent l'ascendant : *strategic competition* et *gray zone approach* (un schéma synthétisant cette évolution est présenté en annexe 1).

2.1. L'hybridité devient l'une des formes ambiguës de conflit

C'est d'abord dans le cadre de la réflexion sur la guerre irrégulière que s'insère la question de l'hybridité. En dépit des difficultés initiales de définition, l'*irregular warfare* (IW) devient un domaine d'effort majeur du DoD entre 2008 et 2012²⁴. Définie de manière large comme « *une lutte violente entre États et acteurs non étatiques pour la légitimité et l'influence sur les populations concernées* », elle recouvre différents types d'opérations²⁵ ; mais comme la contre-insurrection et le contre-terrorisme occupent alors l'essentiel de l'attention, le thème passe au second plan après 2012, lorsque l'Administration Obama et le DoD entendent sortir des « guerres interminables » et se réorienter sur le haut du spectre de conflictualité. Pour autant, la guerre irrégulière retrouve aujourd'hui un intérêt face aux menaces hybrides (voir deuxième partie), dans un contexte complètement différent.

L'extension du domaine de l'hybridité, désormais mise en œuvre par des États hostiles, a conduit certains analystes à proposer d'autres appellations, en puisant de nouveau dans le répertoire de la Guerre froide. C'est ainsi que la notion de confrontation politique (*political warfare*) est ressuscitée en 2013 par Max Boot²⁶ et Michael Noonan²⁷ pour insister sur les dimensions non militaires de la lutte menée par les adversaires des États-Unis. Fondée sur une définition donnée en 1948 par George Kennan, la notion a un sens très large, englobant « *tous les*

²⁴ Sur l'évolution du concept, voir : « Les concepts liés à la guerre irrégulière : contre-insurrection et stabilisation », in Philippe Gros et alii, *Les nouveaux concepts militaires dans les nouveaux conflits*, FRS/US CREST, Juillet 2010, pp. 149-152.

²⁵ Une Directive du DoD de 2008 y inclut : le contre-terrorisme ; la guerre non conventionnelle (*unconventional warfare*) ; l'aide à la défense interne (*foreign internal defense*, FID) ; la contre-insurrection et les opérations de stabilité. D'autres documents ajoutaient les opérations d'information, les actions civilo-militaires, les activités criminelles...

²⁶ Max Boot, Michael S. Doran, *Political Warfare*, Policy Innovation Memorandum n°3, Council on Foreign Relations, June 2013 – <https://www.cfr.org/report/political-warfare>

²⁷ Michael P. Noonan, « Re-Inventing Political Warfare », *US News & World Report*, August 16, 2013 – <https://www.usnews.com/opinion/blogs/world-report/2013/08/16/political-warfare-in-a-time-of-defense-cuts>

moyens à la disposition d'une nation, hormis la guerre, pour atteindre ses objectifs stratégiques »²⁸. De ce point de vue, seules les intentions hostiles attribuées à un État peuvent permettre de distinguer la « *political warfare* » d'une politique internationale ordinaire²⁹...

L'expression connaît toutefois un succès certain, faisant l'objet de nombreuses publications et études. En 2016, le général Votel et plusieurs autres anciens officiers des Forces spéciales y consacrent un article, expliquant que la « *confrontation politique* » se déploie « *entre la diplomatie et la guerre ouverte* », lorsque ni la conduite normale de la politique, ni le recours à la force classique ne sont des options adéquates³⁰. Un rapport de la Rand de 2018 y inclut les activités de subversion ou de pression économique, les opérations d'influence, le soutien à des forces « *auxiliaires* ». Les auteurs précisent que ces modes d'action doivent servir à « *affaiblir la composition politique ou le processus décisionnel d'un État* »³¹. Selon une étude du CSBA, il s'agit de « *diverses opérations [destinées à] influencer, persuader ou contraindre [des acteurs] à agir de manière conforme avec ses intérêts stratégiques sans recourir à l'emploi effectif de la force* »³².

Malgré l'imprécision qui l'entoure, l'expression est reprise par la Commission d'évaluation de la NDS de 2018³³, mais aussi dans un document doctrinal récent du *Marine Corps*³⁴. Cependant, dans le premier cas, elle constitue un type d'activités hostiles menées dans la « zone grise », alors que pour les *Marines*, elle englobe à l'inverse cet espace de conflictualité (voir infra). Pour d'autres analystes, la *political warfare* décrit les méthodes employées dans la « zone grise », laquelle constitue « *un espace sur le continuum de conflictualité* »³⁵.

La notion de « zone grise » est effectivement celle qui a le plus prospéré dans les travaux des *think tanks*, comme dans le discours institutionnel, et qui sert aujourd'hui à la plupart des analystes à discuter des menaces hybrides.

²⁸ « *Political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives* ». Cité in Kathleen J. McInnis, Martin A. Weiss, *Strategic Competition and Foreign Policy: What is « Political Warfare »?*, In Focus, Congressional Research Service, March 2019, p. 2.

²⁹ Critiquant l'usage du terme, F. Hoffman souligne que cette notion ne relève pas vraiment du domaine de la « guerre » qu'implique le vocable « *warfare* ». Frank Hoffman, « On Not-So-New Warfare: Political Warfare Vs Hybrid Threats », *War on the Rocks*, July 28, 2014 – <https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/>

³⁰ « *Political warfare is played out in that space between diplomacy and open warfare, where traditional statecraft is inadequate or ineffective and large-scale conventional military options are not suitable or are deemed inappropriate for a variety of reasons* ». Joseph L. Votel, Charles T. Cleveland, Charles T. Connett, Will Irwin, « Unconventional Warfare in the Gray Zone », *Joint Force Quarterly*, n°80, 1st Quarter, January 2016 – <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/>

³¹ *The Growing Need to Focus on Modern Political Warfare*, Research Brief, Rand Corporation, 2019, p. 2. La note synthétise un rapport antérieur : Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Raddin, Madeline Magnuson, Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses*, Santa Monica, RAND Corporation, 2018.

³² Ross Babbage, *Stealing a March. Chinese Hybrid Warfare in The Indo-Pacific*, Vol. 1, Washington (D.C.), CSBA, 2019, p. 2.

³³ Eric Edelman, Gary Roughead et al, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission*, Washington (DC), United States Institute of Peace, 2018.

³⁴ MCDP 1-4, *Competing*, Headquarters United States Marine Corps, December 2020, pp. 2-17 – <https://www.marines.mil/Portals/1/Publications/MCDP%201-4.pdf?ver=fGwjmqkxGvv0GPe0mPgqdw%3d%3d>

³⁵ Joseph L. Votel, Charles T. Cleveland, Charles T. Connett, Will Irwin, « Unconventional Warfare in the Gray Zone », op. cit.

2.2. La zone grise s'impose comme l'espace privilégié de confrontation hybride

La notion de défis posés dans une « zone grise ambiguë » était mentionnée dans la QDR de 2010. L'expression « gray zone » est reprise dans l'*Unified Land Operations* de l'Army en 2011 puis dans l'*Operational Environments to 2028* publié par le TRADOC en 2012. Mais ce sont les déclarations du général Votel, alors commandant de l'USSOCOM, devant le Congrès début 2015, qui popularisent l'expression, censée décrire « les conflits qui sortent de la vision traditionnelle paix ou guerre »³⁶. Quelques mois plus tard, l'USSOCOM publie d'ailleurs un Livre blanc exposant sa conception de la zone grise³⁷. Elle se caractérise par « l'ambiguïté quant à la nature du conflit », qui est difficile à placer dans un cadre politique et juridique de temps de paix ou de guerre³⁸. Ces actions sont ainsi difficiles à qualifier de manière objective (elles sont « perspective-dependent »). Cependant les auteurs estiment qu'un « certain niveau d'agression est déterminant » pour marquer le passage de la compétition normale à la « zone grise »³⁹.

Cette approche, qui reste focalisée sur l'emploi limité de la force, est largement étendue par les travaux ultérieurs. Les principales contributions au développement du débat sur la zone grise proviennent à nouveau de Nathan Freier, qui dirige les réflexions du *Strategic Studies Institute* (SSI) de l'Army sur les « gray zone challenges »⁴⁰ et de Michael Mazarr, rattaché à la Rand, mais qui publie une étude de référence pour le SSI en 2015⁴¹. L'expression fait dès lors l'objet de nombreux articles et est reprise par les acteurs institutionnels, du DoD au Département d'État, même si elle ne fait toujours pas l'objet d'une définition officielle.

Son acception reste variable et parfois difficile à distinguer d'autres notions liées à l'hybridité. Un rapport remis en 2017 par un organe consultatif du Département d'État remarque ainsi que la zone grise recouvre des actions qui ont pu être qualifiées de « political warfare », « covert operations », « irregular or guerrilla warfare », « active measures », et autres⁴². Pour de nombreux analystes, les opérations de « zone grise » sont simplement une autre façon de qualifier les confrontations hybrides, entendues au sens large. Mais le plus souvent, elles intègrent aujourd'hui l'hybridité comme une composante dans une forme de conflit dont la caractéristique essentielle est de se situer « entre la paix et la guerre »⁴³.

³⁶ Statement of General Joseph L. Votel, U.S. Army, Commander, United States Special Operations Command, before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, 18 March 2015, p. 7.

³⁷ *The Gray Zone*, White paper, U.S. Special Operations Command, 9 September 2015. Les idées en sont également exposées par le rédacteur dans un article : Philip Kapusta, « The Gray Zone », *Special Warfare*, October–December 2015.

³⁸ Ibid., p. 1.

³⁹ Ibid., p. 3.

⁴⁰ Durant l'été 2015, l'US Army War College lance une étude sur la « compétition en zone grise », sous l'égide de l'*Army Capabilities Integration Center* et du *Joint Staff J-39/Strategic Multi-Layer Assessment Branch*. Nathan Freier (Dir.), *Outplayed: Regaining Strategic Initiative in the Gray Zone*, Carlisle, SSI, US Army War College, June 2016 – <https://apps.dtic.mil/dtic/tr/fulltext/u2/1013807.pdf>

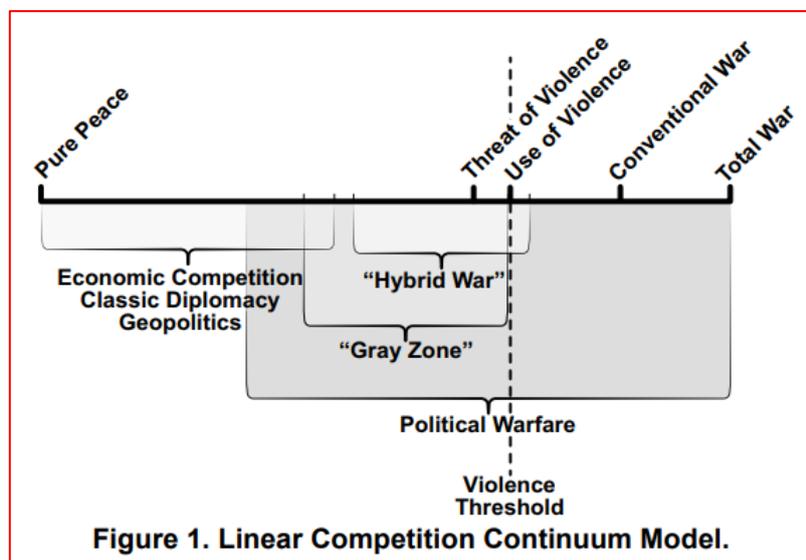
⁴¹ Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Carlisle, Strategic Studies Institute, US Army War College, 2015 – <https://publications.armywarcollege.edu/pubs/2372.pdf>

⁴² International Security Advisory Board, *Report on Gray Zone Conflict*, Washington (D.C.), January 2017, p. 1.

⁴³ Avant même d'utiliser le terme *gray zone*, c'est Nadia Schadlow qui mit l'accent sur l'importance croissante de cet « espace » intermédiaire. « Peace and War: The Space Between », *War on the Rocks*, 18 August 2014.

En 2016, Frank Hoffman souligne ainsi la distinction entre la guerre hybride, qui est un mode de confrontation armée essentiellement caractérisé par « *la fusion de capacités avancées avec la fluidité des tactiques irrégulières* » ; et les activités de « zone grise » qui se situent en-deçà du recours à la violence dans le « *spectre de conflictualité* »⁴⁴.

On retrouve une approche similaire dans le rapport indépendant sur la NDS de 2018. Alors que la Stratégie du DoD n’emploie pas l’expression, la Commission d’évaluation en fait un usage abondant, en considérant les « *agressions de zone crise* » comme des formes de coercition utilisées pour mener la compétition « *dans l’espace entre la paix et la guerre* », alors que « *la guerre hybride [combine] des éléments conventionnels et non conventionnels* »⁴⁵. Cette vision est aussi celle que retient le *Marine Corps* dans le manuel de 2020 consacré à la « compétition »⁴⁶. Cependant, si la « zone grise » englobe la « guerre hybride », elle se distingue de la « *political warfare* », qui peut exister en temps de paix comme de guerre ouverte.



Source : MCDP 1-4, *Competing*, Headquarters United States Marine Corps, December 2020, p. 1-6.

Cette conception particulière reflète bien la diversité d’approches qui persiste dans le débat américain. Le document des *Marines* lui-même finit par considérer que « *la guerre hybride, la guerre de zone grise ou la confrontation politique* » sont des expressions équivalentes, recouvrant « *des activités ouvertes, clandestines et illégales, des tactiques irrégulières, le terrorisme, des comportements criminels [...] pour parvenir à atteindre les objectifs politiques recherchés* »⁴⁷.

On trouve donc aujourd’hui dans les travaux sur le sujet, des auteurs qui traitent les différentes notions de façon équivalente, tandis que certains analystes continuent de qualifier

⁴⁴ Frank Hoffman, « The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War », in Dakota L. Wood, ed., *Index of Military Power*, Washington (D.C.), Heritage Foundation, 2016, p. 29.

⁴⁵ Eric Edelman, Gary Roughead et al, *Providing for the Common Defense*, op. cit., p. viii.

⁴⁶ MCDP 1-4, *Competing*, Headquarters United States Marine Corps, December 2020 – <https://www.marines.mil/Portals/1/Publications/MCDP%201-4.pdf?ver=fGwjmqkxGvv0GPe0mPgdqw%3d%3d>

⁴⁷ Ibid., p. 2-17.

d'approches hybrides ce que d'autres appellent désormais les « activités de zone grise » ; et celles-ci peuvent englober ou non une dimension militaire.

Quelques définitions de la zone grise⁴⁸

M. Mazarr 2015	« <i>Gray zone conflict involves the holistic application of a mosaic of civilization and military tools, short of combat operations, to achieve gradual progress toward political objectives</i> » ⁴⁹
Étude réalisée au profit de l'USSOCOM 2016	« <i>Conceptual space between peace and war, occurring when actors purposefully use multiple elements of power to achieve political-security objectives with activities that are ambiguous or cloud attribution and exceed the threshold of ordinary competition, yet fall below the level of large-scale direct military conflict, and threaten US and allied interests by challenging, undermining, or violating international customs, norms, or laws</i> » ⁵⁰ .
ISAB 2017	« <i>GZ operations [...] involve the use of instruments beyond normal international interactions yet short of overt military force. They occupy a space between normal diplomacy and commercial competition and open military conflict</i> » ⁵¹ .
National Defense Strategy Commission 2018	« <i>The means of gray-zone conflict include everything from strong-arm diplomacy and economic coercion, to media manipulation and cyberattacks, to use of paramilitaries and proxy forces. Singly or in combination, such tactics confound or gradually weaken an adversary's positions or resolve without provoking a military response. Gray-zone conflict is often shrouded in deception or misinformation, making attribution difficult and discouraging a strong response</i> » ⁵² .
Rand 2019	« <i>The gray zone is an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events</i> » ⁵³ .

Pour les experts du CSIS, qui ont largement contribué à populariser le thème de la zone grise, il existe un certain consensus dans la communauté stratégique sur les caractéristiques du « phénomène », ce qui leur permet d'en proposer une définition « de synthèse »⁵⁴ :

« Un effort ou une série d'efforts destiné(es) à atteindre ses objectifs de sécurité au détriment d'un rival en utilisant des moyens dépassant la conduite habituelle de la politique mais sans aller jusqu'aux moyens associés à un conflit direct [...]. En

⁴⁸ Une liste complémentaire est présentée en annexe 2.

⁴⁹ Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, op. cit., p. 64.

⁵⁰ George Popp, Sarah Canna, *The Characterization and Conditions of the Gray Zone*, Boston, NSI Inc., Winter 2016, p. 2.

⁵¹ International Security Advisory Board, *Report on Gray Zone Conflict*, op. cit., p. 1.

⁵² Eric Edelman, Gary Roughead et al, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy*, op. cit., p. 6.

⁵³ Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options*, Santa Monica, RAND Corporation, 2019, p. 8.

⁵⁴ Kathleen H. Hicks, Alice Hunter Friend (Dir.), *By Other Means. Part I: Campaigning in the Gray Zone*, Washington (D.C.), CSIS, July 2019, p. 3.

s’engageant dans une approche de zone grise, un acteur cherche à éviter de franchir le seuil qui conduirait à une guerre ouverte ».

De manière générique, les « instruments » d’action en zone grise, répertoriés par les chercheurs du CSIS⁵⁵, incluent :

- Les opérations d’information, dont la désinformation ;
- La coercition politique ;
- La coercition économique ;
- Les cyber-opérations ;
- Les opérations spatiales ;
- Le soutien à des forces auxiliaires ;
- Les provocations menées par des forces étatiques.

Ces modes d’actions se trouvent chez de nombreux analystes, avec quelques variations⁵⁶. Si certains d’entre eux constituent clairement des activités hostiles, d’autres sont plus difficiles à distinguer de la conduite normale d’une politique extérieure, en-dehors des motivations qui peuvent les animer. Il s’agit là d’un problème soulevé par quelques auteurs, qui s’interrogent sur la pertinence d’un concept spécifique alors qu’il peut être simplement assimilé à une stratégie intégrale⁵⁷. La question a déjà été posée concernant la « guerre hybride », que certains chercheurs considéraient comme une forme ordinaire de guerre interétatique, employant tous les moyens de combat disponibles⁵⁸. Elle vaut aussi pour la notion de *political warfare*, comme on l’a déjà noté.

En 2020, deux professeurs de l’US Naval War College vont plus loin et condamnent sans appel le discours sur l’hybridité et la zone grise, considérant que « *ces termes, [...] devraient être éliminés du lexique stratégique. Ils causent plus de mal que de bien et contribuent à une distorsion de plus en plus dangereuse des concepts de guerre, paix et compétition géopolitique* »⁵⁹.

⁵⁵ Schaus et al., « What Works: Countering Gray Zone Coercion, » CSIS Briefs, July 2018 – https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180716_Schaus_What-Works.pdf?2N5GIQNzTKzXCXELkLmjNOhXI8fyMSq.

⁵⁶ M. Mazarr cite à titre d’exemple : « *use of proxy forces, fifth columns, information warfare, unconventional warfare, economic warfare, economic incentives, cyber harassment, covert operatives, energy diplomacy* ». Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, op. cit., pp. 43-44.

⁵⁷ L’un des plus fervents opposants à la notion de *gray zone* est Adam Elkus, qui en montre les incohérences dans deux articles publiés sur le blog *War on the Rocks* : « 50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense », December 15, 2015 ; « Abandon All Hope, Ye Who Enter Here: You Cannot Save The Gray Zone Concept », December 30, 2015.

⁵⁸ Voir par exemple : Antulio Echevarria, *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy*, Carlisle, US Army War College, SSI, April 2016, p. 2 – <https://apps.dtic.mil/dtic/tr/fulltext/u2/1013691.pdf> ; James K. Wither, « Making Sense of Hybrid Warfare », *Connections*, vol. 15, no. 2, 2016, p. 79 – <https://www.jstor.org/stable/pdf/26326441.pdf?refregid=excelsior%3A117443d42eaddb37a643d2f2f361c1e>

⁵⁹ Donald Stoker, Craig Whiteside, « Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking », *Naval War College Review*, Vol. 73, No. 1, Winter 2020, p. 2.

Ils estiment que les activités décrites aujourd’hui comme des manœuvres de zone grise relèvent en fait de deux situations différentes :

- ➔ Soit ce sont des éléments d’une stratégie intégrale (*grand strategy*), similaire à celle que les superpuissances ont menée durant la Guerre froide, mais qui demeurent des activités de temps de paix ;
- ➔ Soit, dans certains cas, ce sont effectivement des actes de guerre, que les autorités refusent d’appeler par leur nom. Ainsi « *ce que la Russie a fait en Ukraine depuis 2014 est la conduite réussie d’une guerre à buts limités, en utilisant à la fois des moyens violents et subversifs* »⁶⁰.

Dans ces conditions, l’idée même de confusion entre les temps de paix et de guerre serait inappropriée, voire dangereuse dans la mesure où elle est susceptible d’entraîner une réponse disproportionnée et d’accréditer la thèse de l’existence d’un état de guerre permanent. Mais cette opinion reste très minoritaire. La plupart des analystes considèrent, comme le réaffirme Nadia Schadlow⁶¹, que la réalité de la compétition internationale n’entre plus dans une vision « *binair*e » où il serait possible de séparer ce qui relève de la compétition pacifique de ce qui constitue une forme de guerre « *sans violence* ». C’est la nature délibérément ambiguë des actions hostiles qui caractérise la zone grise et en fait une forme de conflit particulièrement dangereuse pour les États-Unis.

3. Des activités qui présentent un défi majeur pour les États-Unis

Quel que soit le nom donné aux activités menées sous le seuil du conflit armé ouvert, elles sont bel et bien devenues une préoccupation centrale de la communauté stratégique américaine et ont trouvé une forme de reconnaissance officielle au travers de l’adoption de la « *compétition stratégique* » comme axe majeur de la politique de sécurité et de défense de la présidence Trump.

Dès 2015, Michael Mazarr envisage que « *la zone grise puisse devenir l’arène centrale des rivalités* » des décennies à venir⁶². Nathan Freier partage cette analyse, dans la mesure où la « *nouvelle ère* » de sécurité sera marquée par une « *résistance persistante et organisée* [deliberate] » au statu quo défendu par les États-Unis et leurs alliés. Par ailleurs, le choix de méthodes non régulières restera pertinent puisqu’elles peuvent « *déconcerter* [confound] *les stratégestes américains* » s’ils ne parviennent pas à s’adapter⁶³.

⁶⁰ Ibid., p. 13.

⁶¹ Nadia Schadlow, « It’s a Gray, Gray World », *Naval War College Review*, Vol. 73, No. 3, Summer 2020 – <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8131&context=nwc-review>

⁶² Michael Mazarr, « Struggle in The Gray Zone and World Order », *War on the Rocks*, December 20, 2015 – <https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order/>

⁶³ Nathan Freier, Christopher Compton, Tobin Magsig, « Gray Zone: Why We’re Losing the New Era of National Security », *Defense One*, June 9, 2016 – <https://www.defenseone.com/ideas/2016/06/gray-zone-losing-new-era-national-security-strategy/128957/>

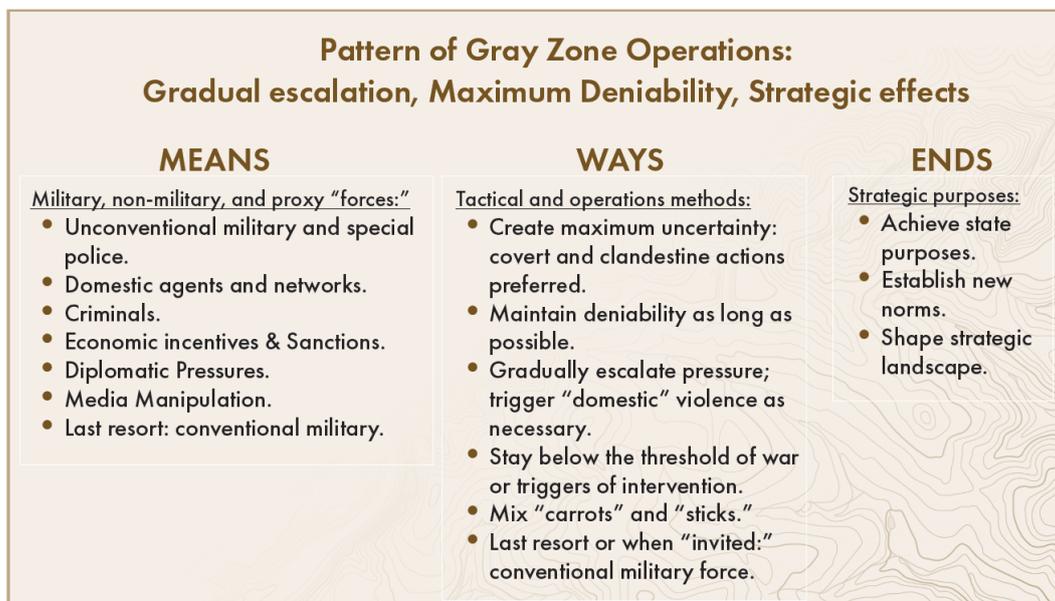
L'importance croissante prise par les menaces hybrides ou de zone grise est en effet liée à deux constats :

- ➔ D'une part, ces phénomènes seraient spécifiquement conçus pour exploiter les « vulnérabilités » des États-Unis (et plus largement des États occidentaux), de sorte qu'il est nécessaire d'y trouver une parade ;
- ➔ D'autre part, et en corollaire du point précédent, ils sont perçus comme les modes d'action privilégiés par les deux puissances révisionnistes les plus dangereuses pour les intérêts américains, si bien qu'il ne s'agit pas seulement d'un débat théorique sur des enjeux potentiels mais aussi d'un discours de mobilisation immédiate.

3.1. L'hybridité exploite les failles de la politique de sécurité américaine

Puisant dans le thème du contournement de la puissance classique, qui avait alimenté les travaux sur les menaces asymétriques à la fin des années 1990, le discours sur l'hybridité postule la recherche par tous les opposants de moyens non-conventionnels destinés à exploiter les vulnérabilités des armées américaines⁶⁴ puis, au-delà, du système politique dans son ensemble. Or, les caractéristiques des menaces de zone grise en font les instruments parfaits pour poursuivre des objectifs hostiles en rendant une réponse américaine particulièrement compliquée.

Plus qu'un ensemble de moyens, les « opérations » de zone grise apparaissent comme une méthode globale de confrontation, fondée sur une double logique de dissimulation et de « patience stratégique ». La démarche est par exemple exposée en 2018 dans une étude de l'Institute for the Study of War, synthétisée dans le schéma suivant.



Source : James M. Dubik, Nic Vincent, *America's Global Competitions: The Gray Zone in Context*, Institute for the Study of War, February 2018, p. 10.

⁶⁴ Cette logique est explicite dans le *Joint Operating Environment* de 2010.

En 2019, une étude de la Rand reprend les principales caractéristiques, déjà identifiées par la plupart des analystes⁶⁵. Les activités de zone grise s’y distinguent ainsi par :

- ➔ Leur nature limitée et ambiguë, destinée à rester sous le seuil justifiant une réponse militaire. Selon Hal Brands, il s’agit d’activités « *coercitives et agressives par nature, mais qui sont délibérément conçues* » pour éviter « *une guerre interétatique ouverte* »⁶⁶ ;
- ➔ Leur mise en œuvre progressive et graduelle, étalée dans le temps, toujours afin d’empêcher une réaction décisive. De ce fait, les « *campagnes de zone grise* » se composent d’une « *longue série de faits accomplis limités* », permettant à leur concepteur d’atteindre ses objectifs « *morceau par morceau* » ;
- ➔ Dans certain cas, leur caractère clandestin, alors que dans d’autres, les actions sont revendiquées, mais justifiées par un discours juridique et politique qui rend leur contestation difficile ;
- ➔ Un calibrage des actions afin d’éviter de mettre en cause les intérêts vitaux des États visés, là encore dans le but d’échapper à une riposte armée.

L’efficacité supposée de cette démarche repose largement sur une « *asymétrie* » entre les possibilités d’action des adversaires dans la zone grise et celles des États-Unis, qui seraient restreints par leur culture et leur système politique. C’est d’abord la traditionnelle « *préférence* » des armées américaines pour les opérations conventionnelles, qui inciterait une nouvelle fois les adversaires à opérer dans la zone grise, pour éviter d’affronter une puissance supérieure⁶⁷.

Ensuite, la distinction habituelle entre temps de guerre et de paix empêcherait les États-Unis de percevoir les activités disparates et déguisées des adversaires comme des éléments d’une stratégie globale⁶⁸, voire d’une guerre totale comparable à la Guerre froide⁶⁹. Cette incapacité à concevoir la compétition comme une confrontation est un obstacle à la mise en place d’une réponse appropriée. Le problème est loin d’être nouveau puisque George Kennan déplorait déjà en 1948 que les États-Unis soient « *handicapés par un attachement populaire* » à la distinction entre paix et guerre, et un refus de reconnaître que les relations internationales sont « *rythmées par une lutte perpétuelle* »⁷⁰. De ce fait, les États-Unis (et leurs alliés) seraient aussi « *beaucoup moins à l’aise* » que leurs rivaux pour mener des actions de zone grise, telle que la « *subversion politique* »⁷¹.

⁶⁵ Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options*, op. cit., pp. 9-10.

⁶⁶ Hal Brands, « Paradoxes of the Gray Zone », Foreign Policy Research Institute, February 5, 2016 – <https://www.fpri.org/article/2016/02/paradoxes-gray-zone/>

⁶⁷ Voir par exemple : Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, op. cit., p. 4.

⁶⁸ Nadia Schadow, « The Problem with Hybrid Warfare », op. cit.

⁶⁹ Christopher Paul, « Confessions of a Hybrid Warfare Skeptic », *Small Wars Journal*, March 3, 2016 – https://small-warsjournal.com/jrn/art/confessions-of-a-hybrid-warfare-skeptic#_edn13

⁷⁰ « *We have been handicapped...by a popular attachment to the concept of a basic difference between peace and war... and by a reluctance to recognize the realities of international relations—the perpetual rhythm of struggle, in and out of war* ». Memorandum *Organizing Political Warfare*, cité in Kathleen J. McInnis, Martin A. Weiss, *Strategic Competition and Foreign Policy: What is « Political Warfare »?*, op. cit., p. 2.

⁷¹ Nadia Schadow, « The Problem with Hybrid Warfare », *War on the Rocks*, op. cit.

Cette limite culturelle se retrouve dans l'organisation des moyens d'action étatique, caractérisée aux États-Unis par une faible intégration et un périmètre plus restreint que dans les régimes « autoritaires », lesquels maîtrisent tous les instruments de puissance. La Commission d'évaluation de la NDS de 2018 constate ainsi que les défis de zone grise se développent souvent « *dans les interstices entre le DoD et les autres ministères et agences, ce qui les rend plus difficiles à traiter* »⁷². La réponse apportée sera ainsi « *soit excessivement militarisée, soit trop contrainte* »⁷³, si les décideurs hésitent à réagir par crainte d'enclencher une escalade qui amènerait à franchir le seuil de la guerre⁷⁴. L'une des particularités de ces actions est d'ailleurs de faire assumer « le risque » du niveau de réaction adéquat aux États-Unis, qui doivent calculer les coûts et dangers de la réponse comme de l'inaction⁷⁵.

Finalement, c'est la société américaine elle-même qui, par son caractère pluraliste et ouvert, présente des points de vulnérabilité. Les rivaux seraient en effet en mesure « *d'exploiter les fissures politiques américaines* » pour influencer les choix stratégiques en leur faveur⁷⁶. Dans ce domaine, c'est particulièrement la Russie qui est mise en cause, puisqu'elle déploierait « *une campagne de désinformation aux États-Unis, pour tenter d'attiser les tensions sociales, raciales et politiques au travers d'enjeux comme Black Lives Matter, la Covid-19, le mouvement Me Too, le contrôle des armes [...] et l'immigration* »⁷⁷. Dans cette lutte avec des régimes autoritaires, les États-Unis et leurs alliés démocratiques sont par nature plus susceptibles d'être affectés par les manipulations de l'information et des règles juridiques (*lawfare*).

La « zone grise » est donc un domaine complexe, où les vulnérabilités américaines sont répétées maximales, de sorte qu'il est communément admis que « *les puissances révisionnistes* » l'utilisent désormais comme le principal champ de « *compétition* »⁷⁸.

3.2. Des modalités de compétition privilégiées par les rivaux révisionnistes

Si la NSS de 2017 ne mentionne pas spécifiquement les notions d'hybridité ou de zone grise, elle place au cœur de la stratégie l'idée d'une « *compétition stratégique* », qui se déroule en partie « *sous le seuil du conflit armé ouvert et aux marges du droit international* »⁷⁹, là où les adversaires mènent des campagnes politiques, économiques et militaires de manière « *calculée pour atteindre un effet maximal sans provoquer de réponse militaire directe* » de Washington.

⁷² Eric Edelman, Gary Roughead et al, *Providing for the Common Defense*, op. cit., p. 9.

⁷³ *The Gray Zone*, op. cit., p. 6.

⁷⁴ Le thème du risque d'escalade est souligné dans : MCDP 1-4, *Competing*, op. cit., p. 2-17. Christopher Paul, « Confessions of a Hybrid Warfare Skeptic », op. cit.

⁷⁵ Ce point est notamment souligné par Nathan Freier, « The Darker Shade of Gray: A New War Unlike Any Other », *Critical Questions*, CSIS, July 27, 2018.

⁷⁶ Ibid.

⁷⁷ Seth G. Jones, « The Future of Competition: U.S. Adversaries and the Growth of Irregular Warfare », *Global Forecast 2021*, CSIS, February 4, 2021.

⁷⁸ James M. Dubik, Nic Vincent, *America's Global Competitions: The Gray Zone in Context*, Institute for the Study of War, February 2018, p. 13.

⁷⁹ « *Adversaries and competitors became adept at operating below the threshold of open military conflict and at the edges of international law* ». *The National Security Strategy of the United States of America*, White House, December 2017, p. 27.

Nadia Schadlow, qui a contribué à l'élaboration du document, réaffirme en 2020 que le concept de zone grise est bien la meilleure manière de décrire les modes d'action privilégiés par les rivaux majeurs. Se référant encore à la « doctrine Gerasimov », elle rappelle que « *la Russie [...] développe des concepts opérationnels utilisant une gamme d'instruments immatériels [non-kinetic] qui restent sous le seuil du conflit conventionnel, afin de produire des effets stratégiques* »⁸⁰. Concernant la Chine, elle se réfère à l'ouvrage récent de David Kilcullen qui expose la manière dont ce pays « *mobilise les multiples dimensions de la puissance nationale au-delà des domaines traditionnellement militaires* », pour atteindre ses objectifs⁸¹. Comme dans le cas russe, les analystes américains trouvent d'ailleurs dans des écrits chinois la confirmation de l'existence d'une conception de la guerre complètement différente de celle des Occidentaux⁸² ; la comparaison entre les influences de Clausewitz et Sun Tzu revient ainsi de manière récurrente dans les publications.

Anthony Cordesman exprime donc début 2021 une opinion largement répandue en affirmant que « *l'essentiel de la compétition militaire avec la Chine et la Russie prendra la forme d'un mélange de zone grise et de guerre hybride* »⁸³. Ces puissances rivales concentrent leurs efforts sur « *les plus bas niveaux d'opérations de zone grise et hybrides, qui comportent bien moins de risques et rendent possible une réelle victoire stratégique* ». Par ailleurs, d'autres auteurs soulignent que ces pays « *auront probablement recours à des tactiques hybrides, avant et pendant toute la durée d'un conflit de haute intensité* »⁸⁴.

Au-delà des discussions terminologiques, les analystes américains ont donc consacré de nombreux travaux à caractériser les approches hybrides ou activités de zone grise en fonction des actions de la Russie et de la Chine⁸⁵ (voir annexe 3). Si elles sont supposées obéir à la même logique, elles présentent néanmoins des spécificités.

Une étude de la Rand identifie ainsi quatre tactiques principales dans les « *campagnes russes de zone grise* »⁸⁶ :

- ➔ Le recours aux campagnes de désinformation destinées à affaiblir les institutions politiques ;

⁸⁰ Nadia Schadlow, « It's a Gray, Gray World », op. cit.

⁸¹ David Kilcullen, *The Dragons and the Snakes. How the Rest Learned to Fight the West*, Oxford, Oxford University Press, 2020. Dans cet ouvrage, il développe la notion de « *liminal warfare* », décrivant les formes de compétition menées « au seuil de la guerre », proposant encore un nouveau terme pour la « guerre hybride ».

⁸² C'est particulièrement le cas de l'ouvrage abondamment cité de Qiao Liang et Wang Xiangsui, *La guerre hors limites*, Rivages, 2004.

⁸³ Anthony Cordesman, *The Biden Transition and U.S. Competition with China and Russia: The Crisis-Driven Need to Change U.S. Strategy*, Washington (D.C.), CSIS, January 2021, p. 10.

⁸⁴ Todd Harrison, Nicholas Harrington, « Bad Idea: Conflating Great Power Competition with High-Intensity Conflict », *Bad Ideas in National Security Series*, Defense 360°, CSIS, December 15, 2020.

⁸⁵ Voir notamment les travaux récents du CSIS : *Chronology of Possible Chinese Gray Area and Hybrid Warfare Operations* (<https://www.csis.org/analysis/chronology-possible-chinese-gray-area-and-hybrid-warfare-operations>) et *Chronology of Possible Russian Gray Area and Hybrid Warfare Operations* (<https://www.csis.org/analysis/chronology-possible-russian-gray-area-and-hybrid-warfare-operations>) ; Heather Conley, et al., « The Kremlin Playbook », CSIS, October 13, 2016. <https://www.csis.org/analysis/kremlin-playbook> ; Raphael S. Cohen, Andrew Radin, *Russia's Hostile Measures in Europe: Understanding the Threat*, Santa Monica, RAND Corporation, 2019 ; Ross Babbage, *Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail*, vol. 1, Washington (DC), CSBA, 2019.

⁸⁶ Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options*, op. cit., p. 43.

- ➔ Les pressions économiques, notamment dans le domaine énergétique, pour obtenir des concessions politiques ;
- ➔ Les démonstrations de force militaires ;
- ➔ Dans certains cas extrêmes, « l'infiltration » de forces russes pour contrôler des zones stratégiques.

Il faudrait y ajouter les « *mesures actives* » mises en œuvre dans les domaines cyber et de l'information, directement contre les États-Unis.

En ce qui concerne la Chine, ses activités hybrides se présentent sous des formes différentes selon les régions concernées :

- ➔ Dans le monde et plus particulièrement en Europe, elle cherche à étendre son influence en comptant principalement sur la « coercition économique », par des investissements massifs ou des relations commerciales déséquilibrées ; et sur les pressions politiques sur les élites⁸⁷, passant par la mobilisation de la diaspora chinoise ou la manipulation de l'information. Ce type d'activité s'est d'ailleurs intensifié et durci depuis la crise de la COVID-19 ;
- ➔ Mais dans la région Indo-Pacifique, où se joue principalement la rivalité avec les États-Unis, les opérations de zone grise sont d'abord les activités navales et mesures destinées à affirmer la présence chinoise dans les eaux disputées de mer de Chine ; elles s'accompagnent des mêmes actions de coercition politique et économique, destinées à rallier des soutiens à Beijing tout en affaiblissant l'influence américaine dans la région.

Finalement, la Chine utilise aussi, de manière globale, des capacités cyber « *parmi les plus sophistiquées* »⁸⁸, y compris contre les États-Unis.

Quoiqu'il y ait des similitudes, les enjeux et problèmes se posent donc de manière différente pour Washington en fonction de l'adversaire qu'il s'agit d'affronter. Cela vaut aussi pour les acteurs révisionnistes de « second ordre », tels que l'Iran, dont les activités hybrides sont davantage du domaine paramilitaire que de la lutte d'influence politique ou économique. Même les « *rogue regimes* » et les organisations terroristes sont toutefois susceptibles de mener des actions hostiles, y compris contre les intérêts américains, dans le domaine cyber qui constitue donc un espace central de la lutte de zone grise.

Si certains analystes soulignent que le choix d'une stratégie appropriée doit donc tenir compte des situations particulières, l'attention aujourd'hui accordée aux menaces « hybrides » favorise plutôt la recherche de solutions génériques.

⁸⁷ Lauren Speranza, *A Strategic Concept for Countering Russian and Chinese Hybrid Threats*, op. cit., p. 7.

⁸⁸ Notamment au travers des actions de l'Unité 61398 de l'Armée. Seth G. Jones, « The Future of Competition: U.S. Adversaries and the Growth of Irregular Warfare », op. cit.

Des réponses couvrant un large champ de « compétition stratégique »

La réponse conceptuelle américaine, procédant d'une démarche inductive par nature foisonnante voire dispersée, s'est depuis traduite par le phénomène assez rare, du passage d'un concept « fourre-tout », déformé par rapport aux prémisses qui l'avaient fondé, au statut de référence internationale partagée par les partenaires et alliés des États-Unis, sans que les institutions américaines elles-mêmes, y compris au sein du Pentagone, ne l'aient validé et n'en aient établi une définition commune.

Là réside le paradoxe de ce concept, qui n'en est pas véritablement un aux États-Unis, mais qui est pourtant à la source des réflexions stratégiques actuelles et continue, de manière subliminale, à exprimer la complexité ambiante et, ainsi, à provoquer la réflexion, l'introspection, l'adaptation et, on le perçoit désormais, la formalisation d'une certaine pensée, non seulement au sein de l'appareil de défense, mais aussi de l'Administration dans son ensemble ; du moins est-ce l'intention. On peut d'ailleurs estimer que l'« hybride » a conduit au renouveau de la réflexion portant sur la notion de stratégie intégrée voire intégrale, en contribuant à fédérer d'autres notions devant lesquelles il s'est finalement effacé, mais dont il a permis le déploiement, sans que soit perdue de vue la dimension éminemment politique et stratégique des fins recherchées.

Les réflexions originelles sur l'hybridité ont ainsi progressivement donné naissance à des directives ou aspirations politico-stratégiques ainsi qu'à des doctrines, au sein de l'appareil de défense et de l'Administration dans son ensemble.

1. Une adaptation à la compétition initiée par le DoD

Ce sont les forces américaines qui, les premières, ont abouti à la mise au point du concept de guerre hybride et ont ainsi contribué, après une parenthèse entre 2010 et 2014, à sa diffusion au-delà des cercles de spécialistes, y compris dans le cadre de leurs relations bilatérales avec les partenaires militaires étrangers⁸⁹. Sur le plan militaire, la réponse américaine s'est construite progressivement, sur les plans conceptuel et doctrinal, au travers de l'application des approches « multi-domaines » (avec leurs variantes, « *cross-domain* / *all-domain* ») à un champ de conflictualité dont l'élargissement a été posé comme principe par la NDS de 2018.

⁸⁹ À titre d'exemple, dès 2015, à l'occasion des réunions d'état-major entre l'armée de Terre française et l'US Army, les représentants de cette dernière débutaient la séance par un exposé complet et précis sur la guerre hybride menée par les Russes en Ukraine.

1.1. La NDS de 2018 amorce l'élargissement du champ de compétition

Bien que ni la guerre hybride, ni la zone grise ne soit mentionnée (au moins dans la version non classifiée), la NDS s'inscrit dans la logique de la NSS et indique clairement que la « *compétition stratégique à long terme avec les puissances majeures* », est désormais la préoccupation prioritaire du DoD⁹⁰. Cette expression, qui ne fait l'objet d'aucune définition précise, décrit néanmoins le phénomène de confrontation hybride : les adversaires utilisent des moyens de coercition relevant de tous les domaines, hormis l'usage direct massif de la force, de façon à atteindre leurs objectifs en « *brouillant les lignes* » entre action civile et militaire⁹¹.

Le principal rédacteur de la NDS, Elbridge Colby, précise par la suite que la menace posée par les puissances rivales est multiforme ; elle inclut les « *activités de zone grise* », que Beijing et Moscou entendent combiner avec leurs réseaux A2/AD, leurs forces de manœuvre et leurs capacités stratégiques, dans une « *théorie de la victoire* » intégrée⁹². Face à cela, la priorité de la NDS est certes de consolider la dissuasion par la restauration des capacités de combat de haute intensité, mais aussi d'empêcher la Chine ou la Russie d'atteindre leurs buts sous le seuil de l'affrontement ouvert en créant le fameux « fait accompli ».

La stratégie de défense comporte donc un axe d'extension de l'espace de compétition (« *expanding the competitive space* »), dont la signification est loin d'être claire⁹³, mais qui indique la volonté du Département de jouer un rôle au-delà des opérations de combat. C'est dans cette logique que peut aussi s'inscrire le développement d'un « *Global Operating Model* » (GOM), présenté par Colby comme un nouveau « *paradigme* » de conduite de la guerre (*war-fighting*)⁹⁴ et qui organise la posture et l'emploi des forces pour gagner la compétition et si nécessaire l'affrontement armé. Le dispositif interarmées s'articule désormais en quatre strates (*layers*)⁹⁵ :

- ➔ Les forces de contact (« *contact layer* »), qui assurent en temps normal la présence à l'extérieur auprès des partenaires et participent ainsi à la lutte d'influence qui se joue dans la « zone grise » ;
- ➔ Les forces d'arrêt (« *blunt layer* »), qui sont destinées à amortir le premier choc d'une agression, pour la stopper et priver l'adversaire de la réalisation rapide de ses objectifs ;
- ➔ Les forces de renfort (« *surge layer* »), principalement des forces expéditionnaires, basées aux États-Unis (CONUS) ou sur d'autres théâtres, qui seraient engagées pour « *gagner la guerre* » ;

⁹⁰ *Summary of the 2018 National Defense Strategy*, US Department of Defense, January 2018, p. 4.

⁹¹ *Ibid.*, p. 2.

⁹² Elbridge Colby, *Addressing China and Russia's Emergence as Great Power Competitors and the Implementation of the National Defense Strategy*, Testimony before the Senate Armed Services Committee, January 2019, p. 3.

⁹³ La Commission indépendante souligne que cet objectif n'est pas précisément défini. Eric Edelman, Gary Roughead et al, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy*, op. cit., p. 19.

⁹⁴ Elbridge Colby, *Addressing China and Russia's Emergence as Great Power Competitors*, op. cit., p. 8.

⁹⁵ *Summary of the 2018 National Defense Strategy*, op. cit., p. 7.

- ➔ Les forces demeurant aux États-Unis, qui assurent la défense du territoire en toutes circonstances (« *homeland layer* »).

Les activités menées « au contact » consistent principalement à renforcer les capacités des alliés, à collecter du renseignement et empêcher les adversaires, à la fois, d'exercer une « *domination du champ des perceptions* » et d'obtenir des gains limités par surprise⁹⁶.

Toutefois, la NDS insiste sur le fait que la compétition stratégique requiert « *une parfaite intégration de multiples instruments de la puissance nationale* », de sorte que la défense n'en constitue qu'un élément. Comme le souligne Elbridge Colby, le combat classique reste au centre des priorités du DoD, ce qui implique que « *les forces interarmées doivent aussi effectuer moins de « *shaping* » et autres activités secondaires* »⁹⁷.

La focalisation sur la restauration des capacités de dissuasion classique est défendue par quelques experts. Des analystes du CNAS estiment ainsi que le DoD ne doit s'impliquer qu'avec modération dans la « zone grise », au travers d'activités de renseignement, de coopération de sécurité ou d'opérations d'information, mais que l'accent doit rester mis sur la réponse à l'enjeu de sécurité le plus important, à savoir l'affrontement de haute intensité⁹⁸.

Cette opinion est toutefois largement dissonante dans le discours actuel de la communauté stratégique. Les experts chargés par le Congrès d'évaluer la NDS se sont montrés sceptiques quant à la traduction concrète des orientations affichées. Ils estimaient en 2018 que le DoD n'avait pas « *de plan pour l'emporter dans les compétitions de zone grise* » et ils ne voyaient pas d'éléments témoignant d'efforts substantiels dans ce domaine⁹⁹. Si la critique vaut plus largement pour l'ensemble du gouvernement, la Commission demandait au DoD de développer « *des stratégies plausibles et des concepts opérationnels* » pour gagner « *sous le seuil de la guerre* »¹⁰⁰.

Deux ans plus tard, une majorité d'analystes continue de penser que le DoD « *doit encore adapter sa réflexion, ses procédures, sans parler de ses priorités budgétaires et d'équipement* » pour répondre aux besoins de la compétition¹⁰¹. Chacun insiste certes sur un aspect différent à développer, mais tous estiment que l'accent reste mis sur la préparation « *du pire scénario de guerre [plutôt] que sur les formes plus larges de compétition civile et militaire* » auxquelles les États-Unis doivent pouvoir répondre¹⁰². Ainsi, Anthony Cordesman appelle la nouvelle Administration à « *recentrer la stratégie militaire [...] pour donner aux conflits hybrides et de zone*

⁹⁶ Elbridge Colby, *Addressing China and Russia's Emergence as Great Power Competitors*, op. cit., p. 8.

⁹⁷ Ibid.

⁹⁸ Jim Mitre, Andre Gellerman, « Defining DoD's Role in Gray Zone Competition », Washington (D.C.), CNAS, August 24, 2020 – <https://www.cnas.org/publications/commentary/defining-dods-role-in-gray-zone-competition>

⁹⁹ Eric Edelman, Gary Roughead et al, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission*, op. cit., p. 19.

¹⁰⁰ Ibid., p. 27.

¹⁰¹ Thomas G. Mahnken, *Selective Disclosure: A Strategic Approach to Long-Term Competition*, Washington (D.C.), CSBA, 2020, p. 1.

¹⁰² Anthony Cordesman, *The Biden Transition and U.S. Competition with China and Russia: The Crisis-Driven Need to Change U.S. Strategy*, op. cit., p. 2.

grise au moins la même, voire une priorité plus élevée », que celle qui est donnée à la guerre de haute intensité¹⁰³.

Dans ce contexte, le Pentagone entendait sans doute manifester son intérêt réel pour la compétition et « combler une lacune »¹⁰⁴, en publiant, deux ans après la NDS, une annexe consacrée à la guerre irrégulière¹⁰⁵. Le retour de ce thème peut sembler surprenant puisqu'il avait émergé dans un cadre complètement différent et était associé à la contre-insurrection et au contre-terrorisme. Mais pour certains experts de ces questions, le domaine large de la guerre irrégulière peut aussi couvrir l'utilisation par des États de modes de confrontation « non traditionnels », visant principalement la volonté et la capacité d'action politique de l'adversaire¹⁰⁶. Les activités « hybrides » de la Russie et la Chine seraient en fait des formes de guerre irrégulière.

Le document du DoD propose donc une définition de l'*irregular warfare* (IW) raccourcie et modifiée par rapport à celle de 2010, en supprimant notamment le qualificatif « violent » pour caractériser la « *lutte entre États et acteurs non étatiques pour influencer les populations et affecter la légitimité* »¹⁰⁷. Elle regroupe toujours l'*Unconventional Warfare* (UW), les opérations de stabilisation, d'aide à la défense interne (*Foreign Internal Defense*, FID), de contre-terrorisme et de contre-insurrection, mais il faut y ajouter les activités liées aux domaines de l'information opérationnelle, du cyber, de la finance, du ciblage de réseaux, de la coopération de sécurité et de la coopération civilo-militaire. Dans le cadre de la menace représentée principalement par la Russie, la Chine et l'Iran, sont mises en exergue les activités suivantes : désinformation, ruse, sabotage, guerre économique, recours à des supplétifs (*proxies*), activités de guérilla et opérations clandestines.

Dès lors, partant du constat que les États-Unis ont trop souvent été réactifs et prompts à « oublier » selon un cycle « *boom and bust* »¹⁰⁸, il est jugé impératif qu'ils soient en mesure de conduire eux-mêmes des activités dites irrégulières avec efficacité. Cela implique notamment de prendre l'initiative et de sortir d'une approche strictement réactive : l'un des auteurs du document souligne que le DoD doit s'efforcer de « *dicter les termes de la compétition* » en utilisant des méthodes « *proactives, dynamiques et non-orthodoxes* »¹⁰⁹. L'Annexe affiche

¹⁰³ Ibid., p. 13.

¹⁰⁴ C'est ainsi que le présente l'un des concepteurs du document, qui était *Irregular Warfare Team Chief* au sein du bureau de l'*Under Secretary of Defense for Policy*. Kevin Bilms, « The Defense Department just published a Summary of the National Defense Strategy's Irregular Warfare Annex. Here's why it's so Significant », Modern War Institute, October 2, 2020 – <https://mwi.usma.edu/the-defense-department-just-published-a-summary-of-the-national-defense-strategys-irregular-warfare-annex-heres-why-its-so-significant/>

¹⁰⁵ *Summary of the Irregular Warfare Annex to the National Defense Strategy*, US Department of Defense, 2020 – <https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF>

¹⁰⁶ Voir notamment : David H. Ucko, Thomas A. Marks, *Crafting Strategy for Irregular Warfare*, Washington (D.C.), National Defense University Press, July 2020 – <https://ndupress.ndu.edu/Portals/68/Documents/strat-mono-graph/crafting-strategy-for-iw.pdf?ver=2020-07-02-111410-093>

¹⁰⁷ *Summary of the Irregular Warfare Annex to the National Defense Strategy*, op. cit., p. 2.

¹⁰⁸ Ibid., p. 1.

¹⁰⁹ Kevin Bilms, « The Defense Department Just Published a Summary of the National Defense Strategy's Irregular Warfare Annex », op. cit.

d'ailleurs clairement l'objectif de trouver « *des manières innovantes de perturber, contrer et prévenir* » les actions coercitives et subversives¹¹⁰.

Le document appelle donc à l'institutionnalisation du concept, à son appropriation par l'ensemble des forces armées – et pas seulement les forces spéciales – et au développement et à l'emploi de capacités irrégulières (notamment par la supériorité technologique en matière d'intelligence artificielle et de physique quantique).

La revalorisation institutionnelle de l'IW se traduit en novembre 2020 dans un Mémoire modifiant la position hiérarchique de l'*Assistant Secretary of Defense SO/LIC*, qui devient un conseiller direct du Secrétaire à la défense¹¹¹. Son Bureau est réorganisé, avec en particulier la transformation du *Combating Terrorism Technical Support Office* en *Irregular Warfare Technical Support Directorate*, témoignant de la volonté de l'OSD de sortir d'une vision du rôle des Forces spéciales centrée sur la lutte contre le terrorisme¹¹².

Le document insiste aussi sur la nécessaire implication de l'interministériel (lien explicite entre l'IW et l'*Unified Action*) ainsi que des pays alliés et partenaires, puisqu'il s'agit pour les États-Unis de « *promouvoir leurs intérêts nationaux au travers et grâce à [by, with, and through] leur réseau* » international.

Certes, le « retour » de l'IW est circonscrit à la sphère de la défense américaine et aux opérations militaires et peut s'expliquer par le fait qu'il s'agit là d'un concept connu, même s'il n'a cessé d'évoluer et a toujours été l'objet de débats internes, dont la mise en exergue est peut-être aussi le moyen d'englober les problématiques hybrides et de zone grise. Quoi qu'il en soit, il mérite l'attention car il introduit ou préconise des évolutions notables en lien direct avec la notion d'hybridité :

- La conduite assumée d'opérations irrégulières contre des États, et pas seulement des entités non étatiques, dans le cadre de la compétition stratégique globale ;
- L'appel à une approche inter-agence intégrée dans la durée¹¹³ ;
- L'exploitation voire l'orientation des compétences des pays alliés et partenaires, ainsi que le recours à des supplétifs, selon une approche très pragmatique également assumée, et une logique d'économie de moyens, ce afin de bénéficier d'un avantage stratégique face aux adversaires (cas de l'Europe vis-à-vis de la Russie par exemple).

¹¹⁰ *Summary of the Irregular Warfare Annex to the National Defense Strategy*, op. cit., p. 7.

¹¹¹ Conformément à la volonté du Congrès, ses compétences sont désormais équivalentes à celles d'un *Under Secretary* (USD). Voir : *Analyse organique du Département de la défense*, Note 8 de l'Observatoire de la politique de défense, FRS, décembre 2020.

¹¹² Jason Criss Howk, « From Counterterrorism to Irregular Warfare: What Does That Mean? », *Clearance Jobs*, January 15, 2021 – <https://news.clearancejobs.com/2021/01/15/from-counterterrorism-to-irregular-warfare-what-does-that-mean/>

¹¹³ Les réflexions initiales sur la guerre hybride aboutissaient déjà, en 2005-2009, à insister sur l'importance d'une telle approche. L'hybridité est constamment liée dans le discours américain à la recherche d'une réponse nationale interagence... qui ne semble jamais être pleinement mise en œuvre.

1.2. L'adaptation des forces armées

Si la réponse aux menaces dans la zone grise doit logiquement dépasser le domaine militaire, les armées y ont toutefois un rôle important à jouer, à condition qu'elles s'adaptent aux différentes modalités de la compétition. Parallèlement à la reconstitution des capacités de combat de haute intensité, les *Services* entendent donc montrer que leur contribution peut couvrir tout le « continuum de conflictualité ».

1.2.1. La plupart des Services développent leur contribution à la compétition élargie

Si le concept d'hybridité a été originellement porté et introduit au sein des instances de réflexion doctrinale des armées par des officiers de l'USMC, notamment F. Hoffman avec l'appui du général Mattis¹¹⁴, c'est principalement à l'US Army que l'on doit, une dizaine d'années plus tard, à la suite des opérations russes en Ukraine, le renouveau de la réflexion dans ce domaine.

Les débats des années 2000 sur la « guerre hybride », bien qu'assourdis par la priorité donnée ensuite aux opérations de contre-insurrection en Irak et en Afghanistan, avaient suffisamment marqué le milieu de la défense pour qu'à l'occasion de cet événement catalyseur que fut l'annexion de la Crimée et la mise sous contrôle d'une partie de l'Est ukrainien, l'US Army y voie l'expression d'une évolution, sinon d'une rupture, dans le caractère de la guerre¹¹⁵.

Le général Mark Milley¹¹⁶ profita ainsi de la tenue annuelle de l'AUSA¹¹⁷, en octobre 2015, pour livrer, devant l'ensemble du leadership de l'US Army et des représentants de la plupart des chefs d'état-major des armées de Terre des pays alliés et partenaires, sa vision du contexte stratégique et du rôle de l'Army pour les années voire décennies à venir. À la lumière des événements de l'année précédente et des menaces hybrides alors identifiées, le général Milley fonda son argumentaire sur les prémisses suivantes :

- ➔ Le retour de la compétition stratégique et de la logique du rapport de force, en particulier du fait d'une Russie résurgente ;
- ➔ La matérialisation de cette compétition selon des modalités et par le recours à des instruments nouveaux, complexes et innovants dont cherchait à rendre compte la notion de « guerre hybride » ;
- ➔ Le changement subséquent du caractère de la guerre dont il convenait de prendre la mesure au plus vite.

¹¹⁴ Le Lieutenant General Mattis, alors *Allied Command Transformation Commander*, contribua ainsi à la diffusion du concept au sein de l'OTAN dès 2007.

¹¹⁵ Initiation des travaux par le général Odierno, alors chef d'état-major de l'US Army, qui, après avoir été Commandant des forces américaines en Irak de 2010 à 2011, avait avec lucidité perçu les évolutions en cours et la phase de transition dans laquelle entraient les armées américaines.

¹¹⁶ Chief of Staff of the Army – CSA, à compter du mois d'août 2015, actuellement *Chairman of the Joint Chiefs of Staff* (depuis 2019).

¹¹⁷ Association of the US Army : il s'agit du rassemblement annuel de tous les décideurs de l'US Army, des industriels (salon d'armement), des membres du gouvernement et des autorités du Pentagone, ainsi que des représentants des différents homologues étrangers du CSA. Les autres *Services* procèdent de même.

Le lien était ainsi établi entre le nouveau contexte stratégique, les menaces dites hybrides et ce qui allait devenir le cheval de bataille doctrinal de l'US Army, la *Multi-Domain Battle* (MDB). Par-là, l'Army visait deux objectifs : se replacer au centre du jeu interarmées en réaffirmant son rôle essentiel malgré l'épuisement consécutif aux années de contre-insurrection, et légitimer celui-ci dans le cadre d'une future bataille – à l'image de l'*Air-Land Battle* des années 1980 – dont les composantes seraient désormais l'ensemble des domaines¹¹⁸, dans chacun desquels et au croisement desquels elle aurait un rôle majeur à jouer.

La MDB évolua rapidement pour se transformer en MDO¹¹⁹, après des échanges avec d'une part le Marine Corps¹²⁰, d'autre part, le DoD dans son ensemble, et notamment l'US Air Force qui, la première, a introduit ces termes de multidomaine (opérations « *cross-domain* » au tournant de la décennie puis multidomaines vers 2014-2015)¹²¹. La notion de MDO élargissait l'acceptation trop tactique du terme « *battle* » pour mieux exprimer non seulement la complexité des enjeux, mais aussi celle des actions à conduire, dans un cadre intrinsèquement interarmées, et si possible inter-agences.

Le concept présenté par le TRADOC fin 2018 explique que « *les forces de l'Army, en tant qu'élément de la force interarmées, mènent des opérations multidomaines pour l'emporter dans la compétition ; si nécessaire, elles pénètrent et désintègrent les systèmes ennemis de déni d'accès et d'interdiction de zone et exploitent la liberté de manœuvre qui en résulte pour atteindre les objectifs stratégiques (gagner) et forcer un retour à la compétition en des termes favorables* ». On note que les idées traditionnelles de victoire et de retour à la paix n'apparaissent plus, témoignant d'une part de la conviction que la « compétition » est désormais l'état normal permanent des relations internationales et que, d'autre part, la recherche d'une victoire décisive est hors de propos pour des enjeux limités et si on entend éviter une escalade nucléaire.

Surtout, les opérations multidomaines, dans l'acceptation de l'Army, ne s'appliquent pas seulement dans le cadre d'une confrontation armée, mais sur le cycle complet de la compétition. Elles prendront donc des formes différentes selon la situation :

- De préférence, il s'agira de mener une « *compétition efficace pour dissuader l'escalade* » et empêcher l'adversaire d'atteindre ses objectifs ;
- Si cela ne suffit pas, l'emploi des forces doit rapidement « *interdire à l'adversaire de réaliser ses objectifs* » et créer un avantage relatif, permettant de trouver une solution politique ;
- Finalement, si aucun des belligérants n'obtient de succès rapide, il faut pouvoir « *vaincre l'ennemi dans une guerre prolongée* »¹²².

¹¹⁸ Terre, Air, Mer, Cyber, Espace, milieu sous-marin.

¹¹⁹ TRADOC Pamphlet 525-3-1, *The US Army in Multi-Domain Operations 2028*, December 2018.

¹²⁰ Associé d'emblée, grâce à sa nature de force expéditionnaire et à ses travaux antérieurs fondateurs en matière d'hybridité.

¹²¹ Voir Philippe Gros, Vincent Turret, « La synergie multidomaine », FRS, Note de l'observatoire des conflits futurs, juillet 2019 – <https://www.frstrategie.org/programmes/observatoire-des-conflits-futurs/synergie-multidomaine-2019>.

¹²² TRADOC Pamphlet 525-3-1, *The US Army in Multi-Domain Operations 2028*, op. cit., p. 24.

Sous le seuil du conflit, les armées contribuent à la lutte contre les efforts d'intimidation de l'adversaire. L'Army doit « *s'engager activement* » dans les domaines cyber et de l'information (« *information environment operations* »), mais aussi par le soutien à des partenaires confrontés à des menaces irrégulières. Dans la mesure où l'enjeu majeur est d'assurer la cohésion des alliances, les exercices et activités de coopération de sécurité constituent aussi un moyen de renforcer la crédibilité de l'engagement américain et de la dissuasion.

Ces préoccupations sont partagées par le Département naval, qui est particulièrement concerné par les activités hybrides de la Chine, mais aussi de l'Iran. La stratégie des forces navales (*Navy/Marine Corps/Coast Guard*), présentée fin 2020, explique ainsi que la synchronisation des capacités et compétences des trois *Services* offre une « *puissance navale intégrée tout-domaine* » (*Integrated All-Domain Naval Power*), renforçant leur contribution traditionnelle à l'action interarmées, dans la compétition comme dans le combat. Il est surtout intéressant de noter la volonté « *d'opérer de manière plus déterminée [assertively] pour l'emporter dans la compétition de routine* », afin de défendre l'ordre international et de dissuader les rivaux de recourir à l'agression directe¹²³. Les forces navales envisagent donc d'avoir à mener des opérations « *fermes et convaincantes pour s'opposer au comportement malveillant* » des adversaires, en acceptant « *un risque tactique calculé* »¹²⁴. Au-delà, c'est toujours par l'aptitude « *à rendre le combat ingagnable pour eux* », que s'exerce l'effet dissuasif majeur¹²⁵.

On relèvera que le Département naval entend hiérarchiser ses efforts, de sorte que les opérations et la posture seront focalisées sur la réponse aux activités chinoises, dans la zone Indo-Pacifique et dans le monde. Cette orientation se retrouve clairement aussi dans les directives données en 2020 par le Commandant du Marine Corps, le général Berger, pour engager une restructuration fondamentale du *Service*.

L'un des objectifs de la réforme est de répondre à l'insuffisance des moyens « *disruptifs et moins létaux adaptés à la lutte contre les activités malveillantes des acteurs menant des stratégies de 'zone grise'* »¹²⁶. Dans cette perspective l'USMC doit développer les capacités qui lui procureront un « *avantage asymétrique* »¹²⁷ dans cet espace de confrontation privilégié par les rivaux majeurs. Cela devrait accroître son « *aptitude à mener la compétition directement, continuellement et mondialement, par des moyens acceptables par les Américains et conformes au droit* »¹²⁸. La prise en compte de ce champ d'action se traduit aussi par la publication fin 2020 d'un manuel consacré à la « *compétition* ». Il vise à orienter la réflexion et la conduite des *Marines* dans ce contexte particulier et exposer la manière dont ils « *contribuent à gagner*

¹²³ « *Operate more assertively to prevail in day-to-day competition* ». *Advantage at Sea*, US Department of the Navy, December 2020, p. 2.

¹²⁴ *Ibid.*, p. 9.

¹²⁵ *Ibid.*, p. 10.

¹²⁶ *Force Design 2030*, US Marine Corps, March 2020, p. 2.

¹²⁷ *Ibid.*, p. 12. Les réformes doivent également permettre de consolider la dissuasion classique, de mettre en œuvre les concepts opérationnels en vigueur (DMO, EABO, LOCE) et de conduire de véritables opérations distribuées.

¹²⁸ Gen. David H. Berger, « *The Case for Change* », *Marine Corps Gazette*, June 2020, p. 11 – <https://mca-marines.org/wp-content/uploads/The-Case-for-Change.pdf>

les compétitions de la Nation, y compris celles qui se situent sous le seuil de la violence »¹²⁹. Le document retient deux rôles pour les armées¹³⁰ :

- ➔ Elles contribuent aux « *stratégies d'attraction* », visant à inciter ou persuader les autres d'agir de manière favorable aux États-Unis, ce qui passe notamment par la coopération militaire ;
- ➔ Et elles sont évidemment des instruments de coercition, sous une forme de contrainte (*compellence*) ou de dissuasion (*deterrence*).

Le manuel, qui n'entre pas à proprement parler dans la doctrine du Corps, expose principalement des conceptions générales, destinées à exposer la vision de la compétition. S'il témoigne de la volonté du *Service* d'intégrer les nouvelles préoccupations stratégiques, on doit constater que les changements structurels et d'équipement entrepris par le général Berger restent déterminés par les impératifs d'un engagement de haute intensité avec la Chine. De même, les concepts existants (en particulier l'*Expeditionary Advanced Based operations* – EABO) sont jugés aussi pertinents pour « *gagner la compétition sous le seuil du conflit* », que pour assurer une dissuasion par interdiction crédible¹³¹. Il n'y a donc pas lieu de concevoir des réponses spécifiques pour la compétition.

Finalement, alors que le domaine de l'IW est *a priori* celui des Forces spéciales, leur contribution à la compétition hybride nécessite pourtant une évolution, dans la mesure où depuis 20 ans, leur rôle s'est réduit aux opérations de contre-terrorisme. Il faudrait donc qu'elles « réapprennent » la gamme de leurs activités traditionnelles, et notamment la dimension de « *political warfare* »¹³². Cette réorientation dépendra en grande partie de l'impulsion qui sera donnée par le prochain responsable des opérations spéciales à l'OSD : l'élévation du poste d'*Assistant Secretary of Defense* (ASD) au rang d'*Under Secretary* serait un signe de l'attention accordée à cet instrument, de même que la nomination rapide d'un titulaire à ce poste, qui n'était occupé que par des « intérimaires » depuis 2019. Lors de son audition de confirmation devant le Sénat, Lloyd Austin a manifesté sa volonté de mettre en œuvre les réformes prévues par le Congrès pour accroître les compétences et moyens de l'*ASD for Special Operations/Low Intensity Conflict*.

¹²⁹ MCDP 1-4, *Competing*, op. cit, p. 1-1.

¹³⁰ Ibid., pp. 2-9 – 2-12.

¹³¹ J. Noel Williams, « Force Design », *Marine Corps Gazette*, July 2020, p. 17 – <https://mca-marines.org/wp-content/uploads/Force-Design.pdf>

¹³² Kaley Scholl, « The use of US special operation forces in great power competition: Imposing costs on adversarial gray zone operations », *Military Times*, December 15, 2020 – <https://www.militarytimes.com/opinion/commentary/2020/12/15/the-use-of-us-special-operation-forces-in-great-power-competition-imposing-costs-on-adversarial-gray-zone-operations/>

1.2.2. La dimension interarmées : des opérations tout-domaine intégrées sur l'ensemble du continuum de compétition

Le *Joint Staff* a publié le 22 octobre 2018 une mise à jour de la Joint Publication 3-0, *Joint Operations*¹³³, document de référence pour la conduite des opérations interarmées. Y est confirmée la pertinence de quelques notions relatives à l'évolution de l'environnement stratégique et des menaces, en particulier :

- ➔ Le « *Conflict continuum* » ou continuum de la conflictualité, dans le temps et l'espace, prenant en compte l'effacement de la distinction des temps de paix et de guerre ;
- ➔ L'évolution du caractère de la conflictualité¹³⁴, en raison notamment du caractère transrégional, multidomains et multifonctions (multi-capacitaires)¹³⁵ des menaces ;
- ➔ Par voie de conséquence, l'insistance sur le concept de *Unified Action*¹³⁶.

Le document reste toutefois relativement classique, dans sa présentation du rôle des forces interarmées, alors qu'une autre publication (*Joint Concept for Integrated Campaigning*), de mars 2018, propose une révision de la conception du spectre de conflictualité, mettant l'accent sur l'abolition de la séparation entre paix et guerre. Cette idée fait ensuite l'objet d'une *Joint Doctrine Note 1-19*¹³⁷, qui décrit un « *continuum de compétition* », où la politique des acteurs associe en permanence, selon les enjeux, des éléments de coopération, de « *compétition sous le niveau du conflit armé* » et de confrontation armée. Dans cet environnement, qui est en fait celui qui existait pendant la Guerre froide, la mise en œuvre des opérations interarmées tout-domaine (*Joint All-domain operations – JADO*) se traduit par un ensemble d'activités, synthétisées dans un schéma récent de l'US Air Force¹³⁸ :

JADO Across the Competition Continuum	
Continuum region	Joint all-domain operations, activities, and investments
Cooperation	<ul style="list-style-type: none"> ✦ Improve materiel and non-materiel partner nation interoperability. ✦ Obtain and maintain air and cyberspace domain access enabling global reach and rapid projection of military power. ✦ Establish cooperative sharing agreements improving mutual support in crisis response.
Competition	<ul style="list-style-type: none"> ✦ Incorporate all-domain approaches into flexible deterrent options. ✦ Expose and counter malign influence. ✦ Maintain freedom of access and maneuver in the global commons.
Conflict	<ul style="list-style-type: none"> ✦ Gaining information advantage. ✦ Projecting global combat power. ✦ Synchronizing action in, from, or through all domains to gain and maintain theater access. ✦ Overmatching adversary forces at decisive points. ✦ Preserve combat capability to conduct future operations

¹³³ JP 3-0, *Joint Operations*, Incorporating Change 1, Washington (D.C.), Joint Chiefs of Staff, 22 October 2018 – https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf

¹³⁴ Ibid. « Transregional, Multidomain, and Multifunctional (TMM) in nature ».

¹³⁵ Déploiement potentiellement concomitant de capacités allant du conventionnel à l'information, des forces spéciales au cyber.

¹³⁶ JP 3-0, *Joint Operations*, op. cit. Figure 1-3, Page I-9.

¹³⁷ JDN 1-19, *Competition Continuum*, Washington (D.C.), Joint Chiefs of Staff, June 2019.

¹³⁸ Annex 3-99, *Department of the Air Force's Role in Joint All-Domain Operations*, October 8, 2020 – https://www.dctrine.af.mil/Portals/61/documents/Annex_3-99/3-99-D01-JADO-Introduction.pdf

Poursuivant la logique d'intégration globale des opérations (*Globally integrated operations*), mantra du *Joint Staff* depuis une décennie, il s'agit toujours de développer l'aptitude des forces à traiter des menaces inter-domaines, de portée globale, dans le cadre d'une pensée stratégique émancipée des contraintes géographiques de niveau régional. Mais le *Joint Concept for Integrated Campaigning* de mars 2018 entend poser les bases d'une nouvelle manière de concevoir des campagnes menées sur tout le spectre de compétition, de manière continue, évolutive et intégrée, ce qui implique aussi la synchronisation avec les agents non-militaires¹³⁹. Tous les documents doctrinaux affirment en effet avec constance que les forces interarmées ne sont que l'un des instruments de la puissance nationale, lesquels « *devraient opérer ensemble comme un tout interdépendant et intégré* [an interrelated and integrated whole] »¹⁴⁰.

L'objectif du *Joint Staff* est donc de rechercher un avantage décrit comme asymétrique par la conception et la conduite d'opérations globales intégrées, interarmées, tout-domaine, interarmes et interalliées. Il s'agit, dans un espace de compétition considérablement élargi, de s'imposer sur l'ensemble du continuum de la compétition, et de développer une défense commune avec alliés et partenaires par le bénéfice de capacités complémentaires.

Aujourd'hui la plupart des documents stratégiques¹⁴¹ produits par les différents *Services* ou par l'interarmées et la défense en général, se réfèrent aux notions de « *multi-domain* » puis, de « *all-domain* » et d'intégration, en référence aux enseignements tirés de l'étude des conflits récents et à l'impératif d'intégration gouvernementale (« *whole-of-government* », voire « *whole-of-society* » désormais) induit par leur caractère intrinsèquement combinatoire. Lors de son audition de confirmation devant le Sénat, le nouveau Secrétaire à la défense rappelle ainsi que « *pour de nombreux aspects de la guerre hybride, le Département de la défense ne peut réussir sans les efforts unifiés et intégrés de [ses] partenaires interministériels et des alliés, particulièrement concernant la diplomatie, le développement, l'information et le renseignement* »¹⁴².

2. À la recherche d'une stratégie intégrale

Alors que l'ensemble des publications du DoD insiste sur l'importance de la coordination inter-agences, il n'existe pas à ce jour de véritable stratégie gouvernementale, formalisée, de lutte contre les menaces hybrides ou tout type d'activité dite de « zone grise ». La communauté stratégique ne cesse de le déplorer et de faire des recommandations destinées à rattraper ce retard.

Pour autant, les réflexions en cours et les initiatives prises, en interne comme à l'échelle internationale, permettent de discerner les orientations en cours et les tendances qui pour-

¹³⁹ *Joint Concept for Integrated Campaigning*, The Joint Staff, March 2018, p. 11 – https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257

¹⁴⁰ *Ibid.*, p. 3.

¹⁴¹ A titre d'exemple : DNI, *World Threat Assessment*, (« *cut across all domains* »), 29 janvier 2019 ; *Homeland Threat Assessment*, DHS, 6 octobre 2020 ; *Maritime Strategy-Advantage at Sea*, Department of the Navy, (« *Integrated all-domain naval power* »), 17 décembre 2020. Ces documents font référence au « All-Domain » et à l'intégration.

¹⁴² Senate Armed Services Committee, *Advance Policy Questions for Lloyd J. Austin, Nominee for Appointment to be Secretary of Defense*, January 2021, p. 39.

raient se matérialiser à court ou moyen terme dans ce domaine. Celles-ci sont d'ailleurs partiellement reflétées dans la NSS de 2017 par exemple, en des formulations laissant entrevoir les raisonnements sous-jacents qui, rapportés à la nature et à l'objet des menaces hybrides, permettent de dessiner l'économie de la réponse américaine à ce défi.

2.1. Des réponses adaptées à la gamme des défis de zone grise

L'appel constant à la revitalisation du concept de stratégie intégrée, voire intégrale, s'appuie d'abord sur une large reconnaissance des vulnérabilités nationales dans le cadre d'une vision holistique :

- ➔ Sur le plan politique, ce sont les divisions et polarisation politiques internes dont l'exploitation par les puissances « hostiles », via notamment des opérations d'influence et de « guerre informationnelle », pourrait porter atteinte à la légitimité des institutions démocratiques et au fonctionnement de l'État ;
- ➔ Sur le plan sociétal, les tensions voire fractures socio-politiques et socio-économiques apparaissent comme autant de points faibles dont la persistance voire l'instrumentalisation contribueraient à saper les fondements de la cohésion nationale ;
- ➔ Sur le plan des infrastructures critiques, de toute nature, on souligne toujours la fragilité des réseaux (énergie, information, cyber, etc.), des opérateurs d'intérêts vitaux, etc. ;
- ➔ Sur le plan diplomatico-militaire, c'est l'érosion du « leadership » américain due à la fois à une « fatigue » nationale à la suite des guerres de contre-insurrection et à une politique d'influence globale agressivement et résolument concurrencée ; c'est aussi le contournement de la suprématie militaire conventionnelle.

À partir de ces constats, on assiste à la construction d'une ébauche de réponse unifiée qui obéit moins à une direction politique claire qu'à l'appropriation par les différents acteurs d'un référentiel commun. Comme on l'observe souvent dans le débat stratégique américain, l'accumulation des diverses contributions, institutionnelles ou non, aboutit à produire un discours normatif servant de guide à l'action nationale, avant de se diffuser à l'ensemble du monde occidental. Cette vision commune des enjeux de l'hybridité se caractérise par les éléments suivants :

- ➔ L'identification de domaines d'action prioritaires, régulièrement cités comme nouveaux « espaces » de confrontation ou « domaines contestés » :
 - ⇒ Le domaine informationnel ;
 - ⇒ Le cyberspace ;
 - ⇒ L'espace ;
 - ⇒ L'économie ;
 - ⇒ Le champ opérationnel militaire, déjà abordé.
- ➔ L'importance accordée à la coopération internationale ;

- ➔ L'adaptation des fonctions structurantes que sont :
 - ⇒ La protection, devant mettre l'accent sur les capacités d'anticipation-alerte (renseignement), mais aussi de résilience / « *preparedness* » ;
 - ⇒ La dissuasion ;
 - ⇒ L'influence ;
 - ⇒ La coercition.

Chacune de ces fonctions est amenée à évoluer pour répondre à un spectre élargi de menaces caractérisées par l'ambiguïté.

2.1.1. Le renforcement de la protection et de la résilience

Ce domaine est d'abord celui du *Department of Homeland Security* (DHS), dont le rôle dans la compétition stratégique s'affirme fin 2020, au travers de la publication d'un premier *Homeland Threat Assessment*, présentant un éventail élargi de préoccupations ; puis d'un rapport plus spécifique, exposant le Plan d'action stratégique du Département pour contrer les menaces chinoises, dans quatre domaines¹⁴³ :

- ➔ L'immigration illégale, qui est un instrument d'accès aux technologies de pointe et à l'information sensible. Les contrôles doivent ainsi être renforcés, en particulier sur les étudiants et chercheurs chinois demandant des visas, mais aussi sur les réseaux facilitant l'entrée et le séjour de citoyens chinois aux États-Unis ;
- ➔ L'économie et les échanges commerciaux (voir infra) ;
- ➔ La cybersécurité et la protection des infrastructures critiques ;
- ➔ Ainsi que la sécurité des approches et du domaine maritime, principalement au travers des *Coast Guard*.

Pour de nombreux experts, la résilience de la société américaine face aux tentatives de manipulation et d'exploitation des divisions internes est un enjeu majeur. Si cela commence par la restauration de la confiance dans les institutions et les responsables politiques, il s'agit évidemment d'un sujet sur lequel la capacité d'action des autorités est limitée et rarement consensuelle. Mais, dans la lutte d'influence mondiale, il est également important d'aider « *les amis, partenaires et alliés à résister à la guerre politique menée par [les] adversaires communs, en développant la résilience des institutions politiques et de la population* »¹⁴⁴.

¹⁴³ *DHS Strategic Action Plan to Counter the Threat Posed by the People's Republic of China*, US Department of Homeland Security, January 2021, pp. 6-8 – https://www.dhs.gov/sites/default/files/publications/21_0112_plcy_dhs-china-sap.pdf

¹⁴⁴ David Maxwell, « Resistance and Resilience in Asia – Political Warfare of Revisionist and Rogue Powers », Remarks delivered for the SOCPAC Conference on Resistance and Resilience in Asia, Monterey, February 4-6, 2020 – <https://ipdefenseforum.com/2020/02/special-forces-talk-resilience-and-regional-competition/>

2.1.2. L'élargissement du champ de la dissuasion

Les travaux sur la zone grise alimentent l'idée selon laquelle l'environnement stratégique de compétition appelle un renouveau de la conception de la dissuasion. Des études en ce sens sont entreprises dès 2015 par l'*Army Special Operations command*, qui propose alors l'adoption d'une « *Comprehensive Deterrence* », définie comme « *la prévention d'actions adverses par l'existence ou l'utilisation proactive de capacités crédibles, physiques, cognitives ou morales, destinées à augmenter le coût perçu par l'adversaire à un niveau de risque inacceptable par rapport au bénéfice attendu* »¹⁴⁵. Ces réflexions n'ont toutefois pas connu de suites institutionnelles et ont été supplantées par la notion de dissuasion inter-domaines (*cross-domain deterrence*). Alors qu'elle ne s'applique pas précisément aux menaces hybrides lorsqu'elle émerge à la fin de la présidence Bush¹⁴⁶, celles-ci sont incluses à partir de 2015, d'abord pour prendre en compte les défis du domaine cyber. Les *Cross-Domain Deterrence Seminars* organisés annuellement par le Lawrence Livermore National Laboratory depuis 2014 (jusqu'en novembre 2018) témoignent ainsi d'une évolution vers la recherche d'une « dissuasion intégrée », également capable de traiter les différents modes d'action « de zone grise », de la Russie et de la Chine en particulier¹⁴⁷. Dans cette approche, il s'agit non seulement de combiner l'ensemble des moyens offensifs/défensifs, nucléaires/conventionnels, cinétiques/non-cinétiques, mais aussi nationaux avec ceux des alliés, ce qui conduit ses promoteurs à souligner l'ampleur de la tâche et les freins à surmonter pour y parvenir.

Si elle soulève plus d'interrogations que de réponses¹⁴⁸, la viabilité d'une stratégie de dissuasion dans la zone grise est abordée dans la plupart des travaux sur le sujet, faisant ressortir certains éléments « consensuels ». D'abord, l'aptitude à dissuader des actions hostiles est actuellement jugée insuffisante et doit être améliorée selon une double logique :

- ➔ D'une part, empêcher le passage des activités hostiles de toute nature (y compris par l'usage de moyens militaires) à l'agression armée directe. Pour cela, les États-Unis doivent entretenir leur aptitude à l'emporter dans une confrontation classique, ce qui justifie les efforts accomplis pour adapter les forces à une guerre de haute intensité ;
- ➔ D'autre part, cette supériorité militaire étant l'une des causes du recours des adversaires aux méthodes « hybrides », il faut pouvoir décourager la poursuite de ces modes d'action de façon qu'ils ne permettent pas à leur auteur d'atteindre ses objectifs.

¹⁴⁵ *Comprehensive Deterrence White Paper*, US Army Special Operations Command, April 2016, p. 9 – <https://www.soc.mil/Files/ComprehensiveDeterrenceWhitePaper.pdf>

¹⁴⁶ Dans la logique d'évolution de la dissuasion américaine entérinée par la *Nuclear Posture Review* de 2008, la « *cross-domain deterrence* » envisageait initialement l'intégration des éléments classiques, spatiaux, cyber, de défense antimissile avec la triade nucléaire, pour couvrir tout le spectre des menaces potentielles sur les intérêts nationaux. Voir : James Scouras, Edward Smyth, Thomas Mahnken, *Cross-Domain Deterrence In Us–China Strategy*, The Johns Hopkins University Applied Physics Laboratory, (2014) 2017 – <https://www.jhuapl.edu/Content/documents/CrossDomainWeb.pdf>

¹⁴⁷ Voir notamment les rapports des séminaires de 2016 (https://cgsr.llnl.gov/content/assets/docs/CDD_Report_Nov_2016_FINAL.pdf) et 2017 (<https://wmdcenter.ndu.edu/Portals/97/Documents/Publications/ISD%20Workshop%20AAR%20FINAL%20for%20DISTRO.pdf?ver=2017-08-29-121014-033>).

¹⁴⁸ Voir par exemple les différents thèmes de discussion recensés in "*Compete, Deter, and Win*" in a *Trans-Regional Perspective: On Meeting the New Challenges of Extended Deterrence*, Center for Global Security Research, Lawrence Livermore National Laboratory, February 2019 – https://cgsr.llnl.gov/content/assets/docs/ED_Bibliography_FEB2019_Final.pdf

Cette dimension de la dissuasion est celle qui soulève le plus d'intérêt et d'interrogations dans le débat actuel. De manière générale, elle devrait s'appuyer sur une combinaison de modes d'action dans laquelle l'instrument militaire n'aurait qu'un rôle limité (principalement à la démonstration de force), aux côtés des instruments économique, diplomatique (y compris la « diplomatie publique »), cyber et d'action clandestine (renseignement et opérations). Il s'agit donc de concevoir une stratégie intégrale¹⁴⁹ servant à l'une ou l'autre des deux grandes options génériques de dissuasion, adaptées au nouveau contexte :

- ➔ L'interdiction des activités de zone grise, par des actions entravant ou répondant directement à celles que mettent en œuvre les adversaires, dans le domaine concerné. Cela requiert d'abord de manifester une volonté ferme de défendre ses intérêts et de ne pas céder à l'intimidation ;
- ➔ La punition, consistant à « faire payer » (*cost imposition*) à l'adversaire le prix de ses agissements, de différentes manières :
 - ⇒ En s'attaquant à sa réputation internationale, ce qui implique de révéler ses activités « masquées » et d'en exposer le caractère contestable, au regard des règles et normes établies ;
 - ⇒ En cherchant à affaiblir directement sa légitimité interne, par des campagnes visant à discréditer le gouvernement auprès de la population¹⁵⁰ ; par le soutien à des organisations d'opposants ;
 - ⇒ En mettant en œuvre une campagne correctement calibrée de sanctions économiques, sans hésiter à recourir aussi à des mesures commerciales (depuis les accords commerciaux jusqu'aux taxes et contrôles douaniers renforcés) et financières (contrôle de la dette), du même type que celles qu'utilisent les adversaires (et singulièrement la Chine).

Cette gamme de réponses doit certes s'adapter à l'adversaire et ne peut apporter de solution immédiate et décisive. Mais elle offre la possibilité de résoudre le dilemme perçu entre l'inaction ou l'escalade, le passage à l'affrontement armé étant considéré comme un « échec de la dissuasion ».

Toutefois, l'une des difficultés pour les États-Unis réside toujours dans la mise en œuvre d'une dissuasion « élargie » (*extended deterrence*), car la plupart des menaces « hybrides » pèsent d'abord sur des alliés ou partenaires. Il conviendrait donc de coordonner les stratégies, pour éviter de présenter des failles exploitables par l'adversaire, ce qui complexifie encore le développement d'une approche multidimensionnelle. En outre, le caractère ambigu propre à ce type de menace ne facilite pas la définition commune des enjeux, des risques, ni des options politiquement acceptables. Cette question se pose par exemple en ce qui concerne l'aptitude de l'alliance nippo-américaine à traiter les ingérences chinoises dans les îles Senkaku¹⁵¹.

¹⁴⁹ On retrouve par exemple cette idée appliquée à deux cas différents : Michael C. McCarthy, Matthew A. Moyer, Brett H. Venable, *Deterring Russia in the Gray Zone*, Carlisle, SSI, US Army War College, March 2019 ; Michael Eisenstadt, *Operating in the Gray Zone: Countering Iran's Asymmetric Way of War*, Policy Focus, n° 162, The Washington Institute for Near East Policy, January 2020.

¹⁵⁰ Voir par exemple : Elisabeth Braw, « The West is surprisingly well-equipped for gray-zone deterrence », *Defense One*, October 28, 2020.

¹⁵¹ Scott W. Harold, Yoshiaki Nakagawa, Junichi Fukuda et alii, *The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains*, Santa Monica, Rand, 2017 – https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF379/RAND_CF379.pdf

2.1.3. L'influence

La conception actuelle de la compétition de zone grise en fait avant tout une lutte d'influence. Selon Cordesman, elle consiste pour une grande part à « agir [shaping] sur le comportement d'autres pays et acteurs non-étatiques par un mélange complexe d'actions aux niveaux civil et militaire »¹⁵². Nathan Freier estime même que « l'influence stratégique » est une dimension « prééminente » parmi tous les domaines contestés, parce que c'est dans le champ des perceptions que se déterminent les choix et décisions qui affectent la sécurité nationale¹⁵³.

La NSS en fait fort logiquement un pilier de la stratégie américaine à l'échelle de la planète, et l'envisage de manière holistique, avec pour champs d'application tous les domaines possibles, grâce à des compétences renouvelées et renforcées, et ciblant l'ensemble des acteurs, quelle que soit leur nature, qu'il s'agisse de puissances hostiles ou partenaires.

2.2. Une nécessaire implication des institutions civiles

La présupposition sur laquelle reposent les démarches en cours peut être exprimée en ces termes : si l'on ne pense pas hybride, on ne peut ni identifier, ni comprendre les menaces en question, encore moins les anticiper, ni même y réagir à temps. Sur le plan politique, il s'agit là de la confirmation de l'intérêt d'une approche dite « *whole-of-government* », qui n'est aucunement nouvelle puisqu'elle est d'une certaine manière le pendant américain du concept de « *comprehensive approach* » européen et fut au cœur de la stratégie de contre-insurrection américaine menée en Irak et en Afghanistan, avec les résultats mitigés que l'on sait. Mais il y a désormais volonté d'aller beaucoup plus loin car l'application d'une telle approche n'est plus uniquement localisée sur un théâtre mais géopolitique, puisqu'elle est appelée à répondre à une menace multiforme qui a pour cible non pas les forces armées américaines en tant que telles – même si, bien évidemment, elles sont concernées – mais la société en général, au travers de ses vulnérabilités, exploitées à des fins de déstabilisation dans la durée par la puissance hostile.

Sur le plan pratique – et pédagogique –, celle-ci se traduit par le recours à l'acronyme DIFEMIL¹⁵⁴, qui succède ainsi au DIME¹⁵⁵, et recouvre donc l'ensemble des domaines et acteurs potentiellement impliqués, attestant par-là de l'élargissement du concept de « *whole-of-government* ». Il s'agit, d'une part, de mettre en place des structures nouvelles afin de contrer le jeu adverse, avec un effort particulier sur le plan de la diplomatie d'influence. L'exemple le plus emblématique de ces ajustements concerne le *Global Engagement Center* (GEC), rattaché au Département d'État, dont la mission consiste principalement à lutter contre la désinformation et la propagande, y compris en soutien des pays alliés et partenaires.

D'autre part, on vise l'activation de méthodes innovantes par les différents ministères concernés, dès le temps de paix, consistant à contrer les actions hostiles, à dissuader, à anticiper

¹⁵² Anthony Cordesman, *The Biden Transition and U.S. Competition with China and Russia: The Crisis-Driven Need to Change U.S. Strategy*, op. cit., p. 16.

¹⁵³ Nathan Freier, « The Darker Shade of Gray: A New War unlike any Other », op. cit.

¹⁵⁴ DIFEMIL : *Diplomatic, Information, Financial, Economic, Military, Intelligence, Legal*.

¹⁵⁵ DIME : *Diplomacy, Information, Military, Economy*.

parfois, dont les caractéristiques, dans la lettre comme dans l'esprit, correspondent en tous points à la définition de l'hybridité¹⁵⁶. Figurent ci-dessous quelques exemples des initiatives prises.

2.2.1. Les instruments d'influence

L'action diplomatique américaine est évidemment globale, permanente, et particulièrement dynamique. Paradoxalement, si l'on se réfère à la rhétorique utilisée par les autorités américaines au cours des dernières années, on est frappé par le peu de crédit qu'elles accordent à leur propre rayonnement, et, par-delà la posture victimaire parfois adoptée, par la fragilité intrinsèque qu'elles attribuent au système de gouvernement démocratique et, par voie de conséquence, à l'exercice de la puissance américaine, en contradiction flagrante avec l'énergie déployée, les moyens consacrés, et le credo américain. Car l'activité diplomatique américaine dans son acception la plus large, qui met au cœur de son action la promotion des alliances dont elle est si riche, n'a jamais véritablement faibli, nonobstant le discours du président Trump, et demeure une constante de l'implication américaine dans le monde. Il y a donc là un double discours qui s'est développé à l'occasion de la vulgarisation des menaces hybrides désormais présentées comme visant à la déstabilisation des sociétés démocratiques par des puissances hostiles autoritaires (Chine, Russie, Iran, Corée du Nord). La meilleure preuve, et la plus flagrante, en est sans doute l'immense succès rencontré par les États-Unis dans l'exportation du concept de « menaces hybrides », aussi bien au sein de l'OTAN que de l'UE. L'hybridité y est consacrée et de nombreuses mesures ont été prises, et continuent de l'être, afin de lutter contre ces menaces (voir infra), prioritairement face à la Russie, et de manière croissante face à la Chine. Il s'agit là d'une réussite indéniable de la diplomatie américaine, dont on constate depuis l'élection à la présidence de Joe Biden qu'elle fera l'objet de tous les efforts.

Combinée à la diplomatie classique, l'utilisation stratégique de l'information est également un aspect central de la lutte contre les actions hybrides menées par les puissances hostiles. Dans ce domaine, négligé après la fin de la Guerre froide, puis redécouvert à l'occasion de « la guerre des idées » contre les organisations djihadistes, les États-Unis ne sont pas restés inactifs, bien au contraire. La transposition dans le cadre de la compétition de zone grise commence dès l'Administration Obama, pour lutter contre l'activisme russe. Elle avait ainsi introduit un dispositif dans le cadre du vote du *National Defense Authorization Act* de 2016 qui donnera naissance au *Global Engagement Center*¹⁵⁷.

Entité inter-agence rattachée au Département d'État, sa mission première est de « définir, diriger, synchroniser, intégrer et coordonner les efforts du gouvernement fédéral pour identifier, comprendre, révéler et contrer les efforts de propagande et de désinformation des États et acteurs non-étatiques étrangers, destinés à affaiblir ou influencer les politiques, la sécurité ou la stabilité des États-Unis, de leurs alliés et partenaires ». À noter, pour l'année fiscale 2019, l'expression du besoin budgétaire au profit du GEC s'élevait à 55,4 millions \$, en nette aug-

¹⁵⁶ In *Understanding Russian « Hybrid Warfare »*, Testimony by Christopher S. Chivvis, presented before the House Armed Services Committee, 22 mars 2017. M. Chivvis conclut son allocution en reconnaissant que « du point de vue de la Russie, les stratégies américaine et otanienne sont de nature hybride ».

¹⁵⁷ Le *Global Engagement Center* a été créé à la suite du vote du *Countering Foreign Propaganda and Disinformation Act* présenté au Congrès le 10 mai 2016. La loi s'intitulait initialement : « *Countering Information Warfare Act* ».

mentation (36 millions \$ en 2017), pour appuyer la campagne contre ISIS et les efforts conduits pour discréditer les opérations de propagande et de désinformation menées par des États et acteurs non étatiques étrangers¹⁵⁸.

Il s'agit là d'un effort de communication stratégique, dont l'objectif vise à contrer les campagnes de désinformation, et dont on trouve un modèle similaire au Royaume-Uni¹⁵⁹. On a, depuis, souvent peiné à prendre la mesure de ces initiatives américaines en raison de la situation de crise intérieure que le pays connaît. Pourtant, le GEC, qui n'est jamais que l'instrument officiel d'un appareil de communication stratégique plus vaste, est particulièrement actif, aux États-Unis comme à l'étranger. Selon les dires de M. Jonathan Henick, *Deputy Coordinator*, il conduit notamment des activités relevant des opérations d'information, du renseignement, et des opérations psychologiques, et est par ailleurs en contact étroit avec les GAFAM, avec lesquels il semble jouer un double jeu, à la fois embarrassé par leur pouvoir croissant et leur autonomisation (problématique de la définition et du contrôle des algorithmes), et rassuré par leur efficacité dans leur contribution au rayonnement américain, y compris sur le plan strictement économique¹⁶⁰.

2.2.2. Les domaines économique et financier

Dans ce domaine, l'Amérique est en situation de domination telle qu'elle est en mesure de déployer une gamme d'instruments de contrôle et de répression sur l'ensemble de la planète, y compris au détriment de ses propres alliés. L'arme des sanctions, contre des individus, des entités diverses (entreprises, banques, etc.), et des États, est devenue emblématique de l'étendue de la puissance américaine¹⁶¹. L'extraterritorialité du droit américain, ne serait-ce que par son aspect dissuasif¹⁶², confère à ce pays un avantage décisif dont il use et abuse parfois, et correspond en tous points, par son usage, à la qualification de menace hybride, puisqu'elle peut ainsi contribuer à la déstabilisation économique et physique des cibles visées, dans la durée, et en retirer des avantages significatifs en matière de compétition stratégique.

Sur le plan économique, la lutte pour la suprématie mondiale fait rage. Les années Trump ont marqué un tournant, non pas tant sur le fond – la compétition économique est une réalité

¹⁵⁸ [FY 2019 CBJ A1 for SharePoint editing \(state.gov\)](#)

¹⁵⁹ A l'occasion d'une présentation par les autorités britanniques compétentes de leur dispositif national dans ce domaine, faite à une délégation interministérielle française (MEAE-MINARM-SGDSN), en novembre 2019.

¹⁶⁰ « *The State Department considers that the big platforms have a positive influence abroad, and that their business model is a valuable contribution to our nation's strength* ». Propos tenus par le directeur du GEC reçu le 20 mars 2019 au SGDSN, qui a par ailleurs fait état du souhait américain de pouvoir agir de manière plus multilatérale, c'est-à-dire d'avoir directement accès aux entreprises et universités françaises concernées par la problématique de la désinformation.

¹⁶¹ Le choc du 11-Septembre a conduit au renforcement d'un certain nombre de dispositifs notamment sur le plan financier. Les mesures prises à l'époque pour mieux contrôler les transactions internationales des groupes terroristes ont ensuite été largement utilisées pour exercer un contrôle durci sur l'ensemble des transactions internationales en dollars. Parmi les dispositifs consolidés, on citera l'organisme interministériel CFIUS (*Committee on Foreign Investment in the United States*), lui-même renforcé par les dispositions du FIRRMA (*Foreign Investment Risk Review Modernization Act*) du 13 août 2018, le *Foreign Corrupt Practices Act* (FCPA, 1977), et le CAATSA (*Countering America's Adversaries Through Sanctions Act*, 2017) qui cible en particulier la Russie et dont les effets sur l'appareil militaire de ce pays, notamment dans le domaine des hautes technologies, a des effets contraignants extrêmement marqués.

¹⁶² La controverse persiste quant à la nature extraterritoriale du droit américain et la réalité de l'exercice du principe de présomption contre l'extraterritorialité propre au droit américain.

depuis toujours et l'arme économique a de tout temps été maniée avec une efficacité redoutable par les États-Unis, y compris au détriment de leurs plus proches alliés dans certains secteurs clés –, mais sur la forme, avec l'adoption désinhibée d'une approche éminemment transactionnelle des relations bilatérales. Face à la montée en puissance chinoise, la question est désormais ouverte de savoir jusqu'où les États-Unis seront prêts à aller en matière de compétition, c'est-à-dire de degré de prise en compte du multilatéralisme et donc des intérêts de leurs propres alliés, parfois concurrents. La posture américaine, sous le mandat Trump, a donné un avant-goût des conséquences économiques et commerciales pour les alliés et partenaires de l'engagement dans une rivalité systémique ; sera-t-elle démentie ?

On notera ensuite que la préservation de la « *sécurité économique et commerciale* » est désormais l'une des missions du DHS, que le Département entend mieux codifier et institutionnaliser¹⁶³. Il prévoit notamment de produire un *Annual Assessment of the Economic Security of the Homeland*, pour évaluer les menaces et envisager les réponses appropriées. Dès à présent, le DHS entend s'attaquer à la menace chinoise :

- ➔ En intensifiant la lutte contre les contrefaçons, contre l'importation aux États-Unis de produits issus du travail forcé ou du détournement de propriété intellectuelle ;
- ➔ En surveillant de manière systématique les activités des entreprises liées au Parti communiste, dans les régions sensibles du monde ;
- ➔ Ou en menant des campagnes de sensibilisation du public et des opérateurs privés américains à l'égard des « *méthodes prédatrices* » de la Chine.

La transformation explicite des enjeux économiques en question de sécurité nationale affecte aussi les relations avec les partenaires, qui sont priés d'entrer dans cette logique. Ainsi, via l'OTAN et surtout l'UE, a récemment été introduite, dans le catalogue des menaces hybrides, l'utilisation par des puissances hostiles, principalement la Chine en l'occurrence, des investissements directs à l'étranger (IDE). Ceux-ci sont considérés comme une arme subversive et de sape des économies ciblées, contre laquelle il faut désormais collectivement œuvrer, en partageant notamment les informations en possession de chacun des États, mais aussi en renforçant les contrôles nationaux et en donnant l'avantage aux « concurrents amis ». L'entrisme américain est notable à l'OTAN et, par sympathie, au sein de l'UE sur ces questions économiques, et plus particulièrement des IDE ; on ne saurait raisonnablement y voir une simple mesure de précaution – certes réelle et légitime – car il y a là un point d'entrée pour la puissance américaine et une possibilité de consolidation de sa propre supériorité, par le dilemme stratégique qu'elle suscite, i.e., le choix entre un « abandon » à la Chine malveillante et un « ralliement » à la bienveillante Amérique¹⁶⁴. Dans ce domaine, la mise en œuvre d'un contrôle renforcé des IDE est souhaitée par la plupart des puissances concernées, la France en premier lieu. Pour autant, plus que le principe, c'est la mécanique visée qui peut poser problème car elle résulterait ainsi d'une subversion des principes au profit d'une pratique – au nom de l'hostilité des stratégies hybrides – potentiellement compromettante et porteuse de vulnérabilités.

¹⁶³ DHS *Strategic Action Plan to Counter the Threat Posed by the People's Republic of China*, op. cit., p. 19.

¹⁶⁴ L'activisme américain ciblant les secteurs sensibles des nouvelles technologies en particulier, sous la forme d'actions combinées de renseignement, d'investissement et de pression juridique, est une réalité bien connue de nos entreprises et de nos services qui n'a rien à envier à la concurrence.

2.2.3. Le renseignement

Commençons par rappeler que, dans la culture anglo-saxonne, l'« *intelligence* » est avant tout un instrument d'influence à finalité politique. S'agissant du sujet qui nous intéresse, la lutte contre les menaces hybrides, on notera que les États-Unis ont, à l'occasion de la publication par le DNI de leur évaluation mondiale de la menace en 2019¹⁶⁵, retenu comme principale caractéristique du nouvel environnement sa dimension multidomaines (« *cut across all domains* ») et son ciblage des valeurs portées par les sociétés (démocratiques) visées. Plus particulièrement, le DNI recommande de faire effort dans les domaines de la lutte contre les menaces cyber (en appelant à une politique d'attribution plus volontariste pour atténuer ce qui constitue aujourd'hui une vulnérabilité), de la lutte contre les opérations d'influence en ligne et les ingérences électorales, et de la lutte contre la prolifération des armes de destruction massive, en particulier chimiques. Bien qu'il ne soit pas fait mention du terme hybride, on relève à la lecture du document que les préoccupations des services de renseignement portent pratiquement sur des champs couverts par les menaces dites hybrides, telles que définies dans les enceintes internationales. Plus largement d'ailleurs, le DNI intègre les menaces contre la société américaine, endogènes comme extérieures, en conformité avec les préoccupations exprimées par les autorités diplomatiques et militaires américaines au sein de l'OTAN, justifiant ainsi une nouvelle approche défensive, dite « *whole-of-society* ».

2.2.4. Le domaine juridique

Dans ce domaine, les États-Unis sont depuis longtemps en pointe et leurs compétences en matière de *lawfare*¹⁶⁶ ne sont plus à démontrer ; aujourd'hui, elles satisfont d'ailleurs pleinement aux critères de définition d'une menace hybride.

Le *lawfare* s'inscrit dans ce que certains experts qualifient de phase juridique de la mondialisation. Dans le contexte de concurrence croissante entre systèmes juridiques (États-Unis, Chine, Union européenne), la diffusion du droit constituerait ainsi pour le pays concerné un outil d'influence et requerrait la mise en œuvre d'une stratégie de *lawfare* afin de consolider ses positions. Cette situation se double de l'émergence d'espaces non encore régulés (espaces juridiques déterritorialisés, domaines numérique et cyber, absence d'un encadrement juridique des ressources spatiales par des opérateurs privés, etc.) dont le contrôle par le droit est un enjeu majeur pour les États-Unis et leurs concurrents. La stratégie mise en œuvre par les États-Unis est essentiellement de nature normative, par le biais de la législation nationale de portée extraterritoriale, dont l'exemple emblématique est la législation relative aux sanctions. Son déploiement est, dans certains cas, typique d'un recours aux « manœuvres » dites hybrides, lorsqu'il vise par exemple à affaiblir des concurrents. Ainsi les sanctions massives imposées à des établissements bancaires, y compris de pays alliés, ou sanctions internationales,

¹⁶⁵ La communauté du renseignement a publié le 29 janvier 2019 le « Worldwide Threat Assessment » qui répertorie l'ensemble des menaces auxquelles les États-Unis doivent faire face en en procurant une analyse et en formulant des recommandations et des priorités d'action.

¹⁶⁶ Par analogie avec le terme « *warfare* », traduit par « guerre judiciaire », « guerre juridique », « guerre par le droit » ou encore « droit comme outil de puissance ». Le *lawfare* peut être compris soit comme l'« usage stratégique du droit par un acteur du système international, dans le but de faire avancer une cause ou de bénéficier d'un avantage sur ses adversaires », soit comme le « détournement et l'abus du droit à des fins politiques et militaires ». Ces éléments de définition ont été établis par les services du MEAE.

contre la Russie ou l’Iran notamment. Dans ce dernier cas, les pays européens, dont la France, ont dû renoncer à toute activité économique bilatérale¹⁶⁷.

3. Les menaces hybrides comme facteur de mobilisation des alliés

Plus que tout autre concept récent, et en lien avec la diffusion de la notion de « zone grise », celui de « menaces hybrides » a été depuis 2014 un vecteur d’influence stratégique majeur pour les États-Unis sur la scène internationale, et est ainsi devenu l’élément central de leur vision de la compétition stratégique.

3.1. La diffusion du concept au sein de l’OTAN

Dès le Sommet du Pays de Galles en 2014, l’OTAN, dans son communiqué final¹⁶⁸, précisait au point 13 qu’elle était déterminée à lutter contre les menaces hybrides (« *hybrid warfare threats* ») conçues comme : « *les mesures militaires – ouvertes et clandestines –, paramilitaires et civiles mises en œuvre selon des dispositions à haut degré d’intégration* », et qu’elle porterait son effort à la fois sur la communication stratégique (campagne d’influence permanente) et sur son partenariat avec l’Union Européenne (UE), sur l’ensemble du spectre de la dite lutte.

La lecture du rapport annuel 2019 de l’OTAN¹⁶⁹ nous permet de constater que les notions d’hybridité et de zone grise sont considérées comme équivalentes et aisément interchangeables, en fonction des thématiques abordées. Ces activités hostiles sont ainsi principalement caractérisées par le fait qu’elles contribuent à rendre floue voire obsolète la distinction classique entre les temps de paix et de guerre, et qu’elles visent à déstabiliser et affaiblir les pays cibles.

On constate ainsi qu’indépendamment de l’influence américaine en son sein, réelle et productive, l’OTAN, en tant qu’organisation dotée de nombreux organes dédiés à la préparation de l’avenir, et par un processus de dépassement du simple agrégat des contributions individuelles de ses États membres, a elle-même directement contribué à la théorisation de l’hybridité pour en faire un champ nouveau de compétence. Ainsi, par l’éventail des travaux conceptuels et doctrinaux plus ou moins englobants, conjugué à l’arsenal en constante évolution des mesures préconisées, l’OTAN s’est imposée comme théoricien et acteur de premier plan dans le domaine de la lutte contre les menaces hybrides, avec comme objectif majeur de renforcer sa légitimité dans le nouveau contexte stratégique international.

¹⁶⁷ En 2018, en raison des sanctions économiques imposées par les États-Unis, et des menaces de représailles afférentes, les groupes français Total et PSA ont dû se retirer du marché iranien, le deuxième en volume à l’étranger pour PSA.

¹⁶⁸ [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, 05-Sep.-2014](#)

¹⁶⁹ OTAN, Rapport Annuel 2019, p. 29 : « *Defending against Hybrid Threats* ».

3.1.1. Un enjeu intégré à la stratégie de l'Alliance

Bien que l'OTAN reconnaisse dans ses communiqués et documents officiels la responsabilité première des nations dans la lutte contre les menaces hybrides, elle préconise néanmoins, pour celles-ci comme pour elle-même, plusieurs actions.

Au niveau national, le développement d'une approche intergouvernementale du problème est préconisé, en fonction des capacités de chaque nation, et dans la plus étroite coopération entre elles, les pays les plus fragiles étant appelés à solliciter le concours des pays alliés ou de l'OTAN directement¹⁷⁰.

Au niveau collectif, on note d'abord le soutien américain à l'adoption de la notion de « *modern deterrence* »¹⁷¹, placée au cœur de son dispositif de lutte contre les menaces hybrides par le Royaume-Uni notamment. Il s'agit de prendre un ensemble de mesures qui puissent :

- Décourager (acception française du terme « *deterrence* » non appliqué au domaine nucléaire) les activités hostiles dans les domaines suivants, en particulier : cyber, économie, espace ;
- Accroître le niveau de coopération de l'OTAN avec l'UE, en particulier dans les domaines de la communication stratégique, de la politique énergétique, de la mobilité militaire, et de la coopération civilo-militaire ;
- Faciliter le développement d'un système d'attribution collective des attaques cyber et de coordination de la réponse¹⁷² ;
- Contribuer au développement de plans dans le cadre d'une défense nationale intégrée, à l'image de ce que sont capables de produire, selon l'OTAN, les États scandinaves cités en référence, en renforçant notamment la protection des infrastructures critiques, civiles et militaires.

Finalement, l'Alliance encourage la mise en œuvre de différentes stratégies visant à :

- Améliorer la résilience des pays membres dans l'ensemble des secteurs potentiellement visés par les activités hybrides ;
- Améliorer les dispositifs de renseignement et en particulier les systèmes d'alerte (*early warning*) ;
- Développer les capacités défensives dans le domaine cyber (mesures de protection, etc.) ;
- Encourager la coopération avec les partenaires internationaux, en particulier avec l'UE.

¹⁷⁰ À l'exemple des unités de lutte contre la menace cyber, dont l'une a été déployée en 2019 au Monténégro. Bien que l'action constituât avant tout une opération de communication stratégique, il n'en est pas moins significatif qu'elle fût conduite par l'OTAN, non pas l'UE.

¹⁷¹ Cette notion apparaît en fait dès la fin de la Première Guerre mondiale, et a récemment été reprise par le Royaume-Uni. Le RUSI a notamment développé les travaux sur ce sujet depuis 2018. Voir par exemple : Elisabeth Braw, « Modern Deterrence: Preparing for the Age of Grey-Zone Warfare », RUSI, Vol. 38, n°10, November/December 2018 – https://rusi.org/sites/default/files/20181105_newsbrief_vol38_no10_braw_web.pdf

¹⁷² Clairement, au vu du poids et des compétences des États-Unis, il s'agirait en fait pour la majorité des États membres d'accepter de se reposer sur le renseignement américain ou anglo-saxon pour définir la politique d'attribution, donc d'accepter une totale inféodation, avec les risques politiques encourus.

3.1.2. L'articulation des dimensions civile et militaire

L'institutionnalisation de l'hybridité au sein de l'OTAN s'est finalement traduite par une inflexion majeure, soit la « civilianisation » du concept originel de « guerre hybride » et son exportation dans le champ de la dimension civile de la sécurité, inflexion désormais formalisée par le recours aux termes, générique, de résilience et, spécifique, de « *civil preparedness* ».

Pour l'OTAN, ce depuis 2016, un effort particulier est impératif dans ce domaine, compris comme le renforcement des États et des sociétés face au caractère déstabilisateur et subversif de la menace. La résilience est ainsi assimilée à ce que l'OTAN appelle la « *civil preparedness* » et se matérialise par un effort considérable, sous influence des États-Unis, très efficacement relayés par le Royaume-Uni, de réorganisation et de re-priorisation des instances de l'OTAN, au travers du renforcement de ses compétences « civiles ». Cette véritable offensive s'est d'ailleurs traduite par la réunion inédite des responsables de la sécurité nationale des pays membres en mai 2019¹⁷³ pour traiter des menaces hybrides, y compris dans leur composante civile. Elle s'est aussi, dans la durée, de manière presque subreptice mais particulièrement efficace en termes d'influence, concrétisée par la revitalisation et la réorientation des travaux du Comité des plans d'urgence dans le domaine civil (CEPC)¹⁷⁴, souvent jugés secondaires par les États membres en général, et la France en particulier¹⁷⁵. Cette évolution est potentiellement majeure car elle assigne une véritable mission de sécurité non militaire à l'OTAN et, par le biais de la coopération institutionnalisée avec l'UE, sur laquelle nous reviendrons, accroît progressivement le champ de compétences de l'Alliance et lui confère des prérogatives élargies dans le domaine de la sécurité, empiétant clairement sur les compétences « naturelles » de l'UE¹⁷⁶.

Sur le plan militaire¹⁷⁷, il s'agit d'encourager les appareils de défense des États membres à développer leurs capacités et leur disponibilité opérationnelles, à davantage recourir à leurs forces spéciales, à améliorer leurs compétences dans le domaine de l'information opérationnelle (et pour cela s'appuyer sur l'OTAN) et, enfin, à opérer un changement d'état d'esprit pour mieux prendre en compte la réalité et la complexité de ces menaces qui appellent de nouvelles réponses et de nouvelles méthodes. Par ailleurs, prenant en compte le fait que les

¹⁷³ Réunion à Bruxelles le 28 mai 2019 des Conseillers à la sécurité nationale ou de leurs représentants (le SGDSN pour la France) imposée par le Secrétaire général de l'OTAN sous pression américaine, ce malgré les réticences réaffirmées de plusieurs pays, en particulier de la France. Cette réunion fut présentée comme exceptionnelle, mais il est raisonnable de penser qu'elle aura créé un précédent qui confèrera une plus grande légitimité à l'avenir aux initiatives otaniennes dans ce domaine.

¹⁷⁴ Le CEPC est le principal organe consultatif de l'OTAN pour la protection des populations civiles et l'utilisation des ressources civiles à l'appui des objectifs de l'OTAN.

¹⁷⁵ Pourtant, l'on sait très bien que la norme est aussi le produit de l'usage répété dans le temps de procédures, eussent-elles été à l'origine préconisées par un organe consultatif.

¹⁷⁶ En s'appuyant notamment sur l'article 4 du Traité qui stipule la consultation dès qu'un État partie estime sa sécurité menacée.

¹⁷⁷ À titre d'exemple, les déclarations du général Scaparrotti le 17 janvier 2018, en introduction de la 178^{ème} session du Comité militaire : « *Today's strategic context is different than when we made the last NCS change; a resurgence of Russia as a strategic competitor, growing unrest and instability in Africa and the Middle East as well as terrorism is reshaping our strategic environment. This security environment is compounded by the rapid growth and proliferation of new technologies; technologies that can be acquired by both state and non-state actors. This underscores the need to adapt to today's evolving threats. Our ability to respond requires different approaches, and different capabilities* ».

menaces hybrides comportent une dimension militaire essentielle, l'OTAN a décidé, dès 2016, d'adapter son plan de dissuasion et de défense¹⁷⁸ (révision en 2021).

Pour mémoire, dans son édition de 2016, la posture de l'OTAN s'articulait autour des cinq axes suivants :

- ➔ Le renforcement de la présence avancée (EFP) en Europe de l'Est, l'idée étant de consolider l'aspect dissuasif de la posture de force de l'OTAN afin de prévenir la politique du fait accompli par la Russie dont on a vu qu'il s'agissait, dans la vision américaine, d'une des caractéristiques majeures de la guerre hybride et de la stratégie russe ;
- ➔ Le renforcement des défenses cyber ;
- ➔ La lutte contre les menaces hybrides, en particulier le développement de la résilience et de la « *civil preparedness* » ;
- ➔ L'amélioration de la synergie entre les capacités ISR interalliées ;
- ➔ La mise en œuvre du *Readiness Action Plan*¹⁷⁹ (RAP).

Le prochain DDP devrait se caractériser par une approche globale structurée autour de la préparation du secteur civil et des forces nationales, du renforcement de la défense cyber et antimissile, et de la consolidation des forces conventionnelles et militaires. Trois axes d'effort sont mis en avant :

- ➔ La cohésion : face à la multiplication et diversification des menaces, il faut appeler à l'unité et à la cohésion interne ;
- ➔ Les capacités : plus qu'un conflit majeur, ce sont bien les vulnérabilités des États membres et les actions adverses en périphérie (A2/AD) qui sont à craindre. Dès lors, les efforts devraient porter sur le renforcement de l'EFP, l'amélioration des capacités ISR et du partage du renseignement, mais aussi de la disponibilité opérationnelle et de la réactivité des forces comme des centres de commandement ;
- ➔ La communication stratégique, qui pourrait mettre l'accent sur le refus de l'escalade nucléaire telle qu'assumée par la doctrine russe ; l'augmentation des dépenses militaires ; et la consolidation des partenariats internationaux.

3.2. L'union européenne et l'appropriation résolue du concept des « menaces hybrides »

3.2.1. L'entretien et l'exploitation de la porosité OTAN-UE

Dès 2014 et le Sommet du pays de Galles, l'OTAN a clairement fait de sa relation avec l'UE une priorité dans le domaine de la lutte contre les menaces hybrides. Depuis, les consultations et échanges entre les deux organisations se sont multipliés et ont notamment débouché sur la

¹⁷⁸ La posture de dissuasion et de défense de l'OTAN est en cours de révision actuellement. Il est prévu que soit couvert l'ensemble des domaines, notamment le cyber, l'espace, mais aussi les menaces hybrides, tout comme, évidemment, les menaces plus conventionnelles. La notion de *deterrence* serait ainsi considérablement élargie.

¹⁷⁹ Le *Readiness Action Plan* a été approuvé par les États membres à l'occasion du Sommet de septembre 2014. Il vise à accroître la réactivité des forces et structures de commandement, en particulier face à la Russie, après les événements de Crimée.

mise sur pied en 2017 du Centre d'excellence (CoE) européen pour la lutte contre les menaces hybrides¹⁸⁰, implanté à Helsinki. Adoubé par l'OTAN et l'UE, ce centre profite de son statut original et d'une certaine autonomie pour servir de pont entre les deux organisations, mais aussi, et surtout – ce dont la France ne s'est que tardivement rendu compte –, de relais d'influence des pays moteurs dans le domaine concerné, principalement les États-Unis et le Royaume-Uni. Ces deux États sont particulièrement actifs et ont d'emblée chacun pris en charge une des directions du Centre, avec l'Allemagne, afin d'orienter la réflexion qui y est conduite et de contribuer ainsi à la vulgarisation du concept d'hybridité dans son acception la plus large,¹⁸¹ et à sa prise en compte par l'ensemble des parties prenantes. Désormais, tout en maintenant une posture antirusse assumée, et soutenue par les États baltes et la Pologne en particulier, ils élargissent le champ d'application des menaces hybrides à la Chine, rival stratégique des États-Unis.

Le CoE n'est certes qu'un organe consultatif et un centre de recherche ; pour autant, au quotidien, il est actif dans la diffusion des réflexions et objectifs américains et britanniques, reprenant à son compte certains des travaux officiels de ces pays. Aujourd'hui, deux axes d'effort sont mis en avant dont les conséquences potentielles pour la France ne sont certainement pas à négliger : le focus croissant sur la Chine et l'élargissement du domaine de la lutte à la dimension civile, en écho à la *civil preparedness* de l'OTAN, et en parallèle de la réforme entreprise du CEPC sous impulsion américaine. La rhétorique, la diffusion de concepts, la sémantique, autant que l'orientation des travaux et les domaines ou pays étudiés, font partie de la stratégie d'influence poursuivie par les États-Unis au sein du Centre, et par voie de conséquence, au sein de l'OTAN et de l'UE.

3.2.2. Les initiatives de l'UE

On ne peut qu'être impressionné par la rapidité avec laquelle l'Union européenne a fait sien ce concept, érigé au rang de priorité et aujourd'hui traité par toutes les composantes institutionnelles, soit la Commission, le Service européen d'action extérieure (SEAE)¹⁸², mais aussi le Conseil, par l'intermédiaire du Groupe ERCHT¹⁸³.

À partir de la « définition » otanienne de la guerre hybride, l'UE a elle-même défini les menaces hybrides en ces termes :

« Le mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (c'est-à-dire diplomatiques, militaires, économiques, tech-

¹⁸⁰ La France compte depuis le printemps 2020 un représentant intégré au centre et siège au Conseil d'administration, représentée par le SGDSN.

¹⁸¹ Au sein du CoE, l'hybridité est un véritable concept « fourre-tout », et la liste des domaines ou sujets qu'il englobe, s'allonge et se diversifie d'année en année, comme ont pu le constater le SGDSN et la DGRIS.

¹⁸² Au sein du Service européen d'action extérieure (SEAE), le travail d'analyse des risques est effectué par l'INT-CEN, le centre de renseignement et de situation de l'Union, à partir de « sources ouvertes » et d'analyses des services de renseignements des États membres. Depuis 2016, une cellule dédiée aux menaces hybrides a été mise sur pied, la Cellule de fusion hybride (*Hybrid Fusion Cell*).

¹⁸³ Il s'agit, au niveau du Conseil, d'un Groupe de travail horizontal institué en 2019, consacré à la lutte contre les menaces hybrides : le « groupe de travail horizontal pour améliorer la résilience et lutter contre les menaces hybrides (*Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats*) ».

nologiques), 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 ».

L'Union s'est ainsi dotée dès 2016 d'un Cadre commun en matière de lutte contre les menaces hybrides, comprenant vingt-deux mesures opérationnelles, et complété en 2018 par un plan pour « *accroître la résilience et renforcer la capacité à répondre aux menaces hybrides*¹⁸⁴ ». S'y ajoute, en 2020, la mise en place au Parlement européen d'une Commission spéciale sur « *l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation* ».

Pour aller plus loin, l'UE a confié au Centre commun de recherche de la Commission européenne (*Joint Research Center of the European Commission*) et au Centre d'excellence d'Hel-sinki la mission d'élaborer un modèle conceptuel¹⁸⁵ qui puisse servir de référence dans la façon de caractériser les menaces hybrides. Ce document, diffusé en interne fin 2019, identifie quatre piliers : les acteurs (avec leurs objectifs stratégiques), les domaines, les instruments et les phases (durée, contrôle du risque d'escalade, etc.) dont la combinaison et la persistance, associées à la manipulation des seuils de détection, à l'activation des mécanismes de réponse et d'attribution, et à l'ambiguïté et l'exploitation des vulnérabilités des systèmes démocratiques constituent le ciment, le lien qui confère à ces variables la nature d'une menace hybride.

Ce modèle conceptuel, s'il a le mérite d'explorer en profondeur les différentes composantes de l'hybridité et d'essayer d'apporter une compréhension commune à l'objet d'étude, n'en demeure pas moins un outil dont la plasticité est susceptible d'instrumentalisation, notamment parce qu'il décrit de manière holistique les domaines d'action. Dès lors, toute action conduite dans quelque domaine que ce soit et jugée hostile, ne serait-ce que parce qu'elle émane d'un adversaire putatif, peut être considérée comme relevant de l'hybridité. En conséquence, c'est d'une certaine manière un état de conflit permanent que ce modèle conceptuel cautionne. Les conséquences politiques et stratégiques sont potentiellement lourdes.

¹⁸⁴ <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52016JC0018>: « *Cadre commun en matière de lutte contre les menaces hybrides* » ; <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018JC0016> : « *Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides* ».

¹⁸⁵ Commission européenne, JRC Technical Reports, « *The Landscape of Hybrid Threats: A Conceptual Model* », 20 décembre 2019, à l'attention du *Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats*.

Réflexions conclusives

Si le discours sur les menaces hybrides a entraîné une multiplication des initiatives et prises de position américaines pour tenter d'y apporter une réponse globale, ces efforts se heurtent à des limites et contraintes liées au fonctionnement même de leur système politique. De nombreux observateurs le déplorent d'ailleurs et y voient une faiblesse majeure. Il convient pourtant de relativiser les vulnérabilités des États-Unis, en considérant qu'ils disposent d'un certain nombre d'atouts dans la compétition de zone grise.

1. Les difficultés et écueils rencontrés par les États-Unis

1.1. Difficultés liées à la mise en œuvre d'une stratégie intégrée

Sur le plan bureaucratique, le déploiement d'une stratégie nationale intégrée demeure à ce jour une intention, généralement partagée, mais sans doute hors de portée au vu de la complexité d'une telle machinerie, de la persistance de tensions et divergences en matière d'analyse politique interne, et de l'existence de rivalités, structurelles et culturelles, entre grandes « agences ». L'Amérique, même si elle est en phase d'adaptation et toujours en proie au doute quant à ses possibilités d'action dans un monde en pleine évolution, n'a pas renié ses grands objectifs qui découlent d'une vision de son rôle et de sa place dans le monde empreinte d'un universalisme qui lui est consubstantiel. Là où le bât blesse, c'est dans la mise en œuvre concrète, au sein d'une administration pléthorique, au rythme des changements incessants de leadership, d'une véritable stratégie intégrée, c'est-à-dire d'une combinaison, d'une articulation et d'une coordination de multiples stratégies spécifiques couvrant l'ensemble des domaines d'action.

Sur le plan géostratégique, les manœuvres possibles face aux menaces hybrides, en raison même de la nature de ces dernières et de l'envergure de la compétition stratégique en cours dans un monde globalisé, soulèvent des dilemmes internes voire des contradictions et incohérences significatifs. Deux problématiques nous paraissent devoir être relevées :

- ➔ Celle de la stratégie en matière de géoéconomie : comment, en effet, concilier les exigences d'une réponse complète aux menaces hybrides et assumer une confrontation géostratégique avec la Chine, dans un système libéral dont les corporations « championnes » américaines font une part significative de leur chiffre d'affaires avec ou via le compétiteur majeur ? comment impliquer l'instrument économique dans un contexte d'interdépendance prononcée, alors que les chaînes de valeur

qui en sont les artères sont éclatées ?¹⁸⁶ comment donc, engager une lutte de manière crédible, y compris sur les valeurs, en s'affranchissant des grands principes du libre-échange sur lesquels la mondialisation prônée par les États-Unis a été construite ?

- ➔ Le dilemme de la rivalité systémique et du respect des souverainetés : comment, tout en s'engageant dans une rivalité systémique, concilier l'exercice d'un leadership revendiqué et présenté comme une loi historique, la mobilisation des alliances, en particulier de l'OTAN, face à la Russie et à la Chine, et le respect des souverainetés particulières des alliés dont les visions stratégiques et les intérêts présentent, chez certains dont la France, des divergences notables¹⁸⁷ ? comment gérer l'extrême complexité de la situation géostratégique mondiale que l'on ne peut objectivement réduire à l'équation du premier degré de la Guerre froide sans piétiner le principe de souveraineté et heurter voire affaiblir ses propres alliés¹⁸⁸ ?

Sur le plan militaire, et plus largement de la défense, le concept d'*Unified Action* est la transposition de la notion de stratégie intégrée dans la conduite des opérations interarmées. S'il n'est pas illusoire en soi, il est très difficile à mettre en œuvre sur le plan pratique. C'est ce qu'a d'ailleurs révélé la conduite des opérations de contre-insurrection passées, au cours desquelles le poids du DoD fut tel que c'est ce seul ministère, sous l'autorité de la présidence, qui joua le rôle de coordonnateur et remplit lui-même, en s'en offrant les moyens, une partie non négligeable des missions censées être conduites par l'inter-agence dans son ensemble.

1.2. L'écueil opérationnel : quelle mise en œuvre concrète ?

1.2.1. Des postures encore en cours définition

Les concepts du *Joint Staff* et des différents *Services* ont leur vertu et semblent avoir trouvé suffisamment de points de convergence et un niveau de cohérence et de maturité tel qu'ils rendent crédible l'adaptation des forces armées en cours. Pour autant, le défi est immense, d'autant que persistent des interrogations de nature politique sur la stratégie à adopter, face à la Russie en Europe, ou à la Chine en Asie du Sud-Est, qui se concrétisent par l'ambiguïté des décisions, lorsqu'elles sont prises, et, par voie de conséquence, par les difficultés de mise en œuvre que rencontrent les armées, sur le terrain. Un exemple emblématique en est sans

¹⁸⁶ Henry Kissinger, *World Order*, New York, Penguin Press, 2014, pp. 232-233 : c'est après avoir identifié ce dilemme et posé qu'aucune des deux puissances n'était en mesure d'exercer seule le rôle de « leader » du monde tel qu'auparavant assumé par les États-Unis au sortir immédiat de la Guerre froide, qu'il conclut à la nécessaire recherche d'une combinaison entre un équilibre des pouvoirs et un concept de partenariat.

¹⁸⁷ Ainsi que l'atteste l'entretien au SGDSN, le 21 septembre 2018, avec Mr. Christopher T. Robinson, U.S. Department of State, Bureau of European and Eurasian Affairs, Deputy Assistant Secretary. Ce dernier, après avoir prôné une politique d'attribution collective systématique face à l'ennemi russe et vanté les efforts d'influence de son pays à l'UE, a fait part de son incompréhension face à l'idée d'une architecture de sécurité européenne.

¹⁸⁸ Cette question a été abordée à l'occasion d'un entretien avec Jake Sullivan, désormais *National Security Advisor*, au SGDSN, en février 2020. Prenant en compte les remarques de ses interlocuteurs sur le caractère parfois dévastateur, en particulier dans la perspective d'une rivalité systémique avec la Chine, de la « guerre économique » entre les grands groupes et États américains et leurs homologues européens, Jake Sullivan eut cette réponse déconcertante de franchise : « Yes, you've got a point, I never thought of it that way ».

doute celui du dilemme stratégique auquel est confrontée l'US Army dans le choix de sa posture en Europe¹⁸⁹. Face à la complexité de la menace, incluant notamment la dimension hybride, et des enjeux, une étude commanditée par l'état-major du Secrétaire à l'Army (voir le rapport 7 de cet Observatoire, sur les structures de force) a identifié trois approches stratégiques possibles¹⁹⁰ et recommandé d'investir dans une « *Multidomain Alliance* » qui mette l'accent sur le développement des capacités satisfaisant aux impératifs des MDO, dans un cadre interarmées et multinational. L'horizon envisagé est 2028, et le débat n'est pas tranché.

1.2.2. *L'American Way of War rétif aux exigences de la guerre hybride*

Lorsque le général Votel, alors SOCOM Commander, publia le Livre blanc sur la « zone grise » en 2015, il ne se contenta pas de décrire une nouvelle réalité comportant des enjeux majeurs en matière de sécurité nationale ; il fit également une proposition très forte, voire provocatrice, consistant à préconiser la constitution de deux forces armées américaines, l'une traditionnelle et conventionnelle, l'autre dédiée à la lutte contre les activités en zone grise, formée bien évidemment à partir des forces spéciales¹⁹¹. Par-delà les rivalités internes entre *Services*, il nous semble qu'une mesure aussi audacieuse procédait d'une compréhension intime de la réticence culturelle des forces américaines à ce qui n'est ni conventionnel, ni régulier, ni de haute intensité, bref à ce que l'on englobe dans le « *Other Than War* ». Cette réticence est profonde ; elle s'est exprimée fortement tout au long des années 2000, au plus fort des opérations de contre-insurrection, au point qu'à l'époque le Secrétaire à la défense Robert Gates avait dû sévir pour que l'armée américaine s'adaptât¹⁹². *L'American Way of War*, que la zone grise et les menaces hybrides testent et défient, est enracinée et ne sera pas aisément révisée. Le général Votel savait que le simple fait de promouvoir une approche fondée sur la dualité, la réversibilité ou l'adaptabilité est loin d'être chose évidente – elle ne l'est jamais – pour les États-Unis, moins encore que pour d'autres armées à vocation plus expéditionnaire. Au sein de l'US Army, les généraux Perkins et McMaster l'avaient d'ailleurs identifié dès 2015, lors des travaux sur la MDB puis la MDO, au cours desquels ils s'intéressèrent de très près au modèle expéditionnaire français dans sa dimension « culturelle ». Le véritable défi opérationnel que pose l'hybridité aux armées américaines est fondamentalement celui de l'incertitude, combinaison de l'imprévisibilité, de l'opacité, de la polymorphie, et du risque.

¹⁸⁹ *Striking the Balance. US Army Force Posture in Europe in 2028*, US Army War College, Strategic Studies Institute.

¹⁹⁰ Ibid. Ces trois approches sont : « *Privilege dynamic force employment* », « *privilege global competition* », « *privilege armed conflict* ».

¹⁹¹ *The Gray Zone*, op. cit., p. 9 : « *War and the gray zone share some characteristics, but the fundamentally different approaches required to do both well necessitate specialization. As many senior strategists have suggested, there should be two broad categories of U.S. military forces. Category One forces should focus on conventional warfare and be powerful enough to defeat potential adversary state militaries such as North Korean. Category Two forces would focus on being able to act in the gray zone. They would feature smaller, more agile and deployable units. The two sets of forces would not necessarily be mutually exclusive, and they could support each other as needed. However, their manning, training and equipping would look quite different* ».

¹⁹² Robert Gates avait pu dénoncer, à sa manière, le syndrome d'une armée « trop riche », privilégiant sur le plan matériel la recherche de l'« *exquisite* » au détriment du « juste nécessaire ». L'épisode de l'équipement des forces américaines en véhicules MRAP en fut un exemple emblématique.

2. Des vulnérabilités à relativiser

En dépit de la posture défensive et parfois victimaire affichée, l'étude de la nature, des conditions et des modalités de la réponse américaine au défi de la « guerre hybride » et, plus largement, des menaces hybrides, laisse entrevoir une dimension nettement plus volontariste de l'action de la première puissance mondiale, sur les plans conceptuel et opérationnel. Cela conduit à s'interroger sur l'éventuel rôle des États-Unis dans le développement de l'*hybrid warfare* et, aujourd'hui et dans une perspective de court-moyen terme, sur la manœuvre stratégique qu'ils conduisent dans ce domaine.

Par son statut et sa puissance, l'Amérique n'a-t-elle pas elle-même contribué à l'émergence de ce que l'on nomme aujourd'hui l'*hybrid warfare*, à des fins de préservation de l'ordre établi et de satisfaction de ses intérêts et de ses valeurs ? L'Amérique, en cherchant à façonner le monde¹⁹³, n'a-t-elle pas « fait de l'hybride » sans le savoir ? Les États-Unis n'ont-ils pas, sans le vouloir, contribué à l'émergence du phénomène que certains adversaires, en particulier la Russie, qu'il ne s'agit aucunement de dédouaner, ont, eux, porté à un autre niveau, celui de la « guerre hybride », conceptualisée et opérationnalisée, pensée et conduite en violation du droit international, dans une démarche de confrontation stratégique résolue non exclusive du recours à la force ?

L'« *hybrid warfare* » ne saurait être réduite à l'arme du pauvre ou du faible face au fort. Elle est aussi la matérialisation d'un *modus operandi* plus ou moins performant entretenu et développé par toute puissance engagée dans une compétition stratégique. Dans le cas des États-Unis, elle permet d'agir au service du grand objectif qu'est le maintien d'un équilibre des forces qui leur soit favorable dans chacune des aires régionales où s'exprime cette compétition. D'une certaine manière, l'« *hybrid warfare* » peut être considérée comme l'instrument achevé du *smart power* ; elle peut aussi, pour ce qui concerne les États-Unis, constituer une composante de la troisième *Offset Strategy*¹⁹⁴.

2.1. L'hybridité, expression contemporaine d'un mimétisme stratégique réincarné ?

Dans l'équation de l'*hybrid warfare*, commençons par distinguer la composante strictement militaire de l'ensemble plus vaste que constitue le déploiement des menaces hybrides dans tous les domaines de la compétition stratégique.

¹⁹³ Que cette ambition s'exprime par un universalisme droit-de-l'homme ou par une politique néoconservatrice occidentaliste. Le « *shaping* », dont une des modalités est le « *regime change* », est au cœur de la réflexion stratégique américaine, en particulier depuis la fin de la Seconde Guerre mondiale. On aura d'ailleurs noté qu'Anthony H. Cordesman en fait un des piliers de l'adaptation stratégique qu'il préconise.

¹⁹⁴ Toute stratégie dite de compensation doit être comprise comme la recherche, par l'innovation opérationnelle, organisationnelle et technologique, d'un avantage asymétrique face à tout adversaire, censé certes assurer la prévalence en cas de conflit armé de haute intensité, mais avant tout de dissuader toute entreprise hostile grâce à la supériorité incontestable ainsi acquise. Après la première *offset strategy* des années 1950-60 (restauration de l'avantage par l'armement nucléaire) et la deuxième des années 1970-80, (*guided munitions et stand-off battle*), les États-Unis ont officiellement lancé leurs travaux dédiés à une troisième *offset strategy*, sous la direction d'Ash Carter, Secrétaire à la défense, et de son adjoint, Bob Work.

Sur le plan militaire, les États-Unis ont tôt identifié les changements en cours en matière de conduite de la guerre, ou du moins leur potentiel d'évolution, et ont mené des travaux conceptuels dès le début des années 2000, d'une manière certes confuse au point de faire se dissoudre la notion d'hybridité elle-même¹⁹⁵, mais suffisamment pertinente pour faire école. Toutefois, c'est bien l'adversaire russe qui, par la mise en œuvre d'une stratégie *a posteriori* qualifiée d'hybride, ce dès 2008 en Géorgie, a progressivement bouleversé le paysage classique de l'affrontement stratégique et remis en question bien des principes établis. Le véritable révélateur fut toutefois le choc de 2014 qui provoqua une forme de retour à un phénomène de rivalité mimétique¹⁹⁶ entre les deux puissances. Les armées américaines ont ainsi érigé les travaux russes en doctrine de la « guerre hybride », la fameuse doctrine Gerasimov, matérialisant ainsi et légitimant du même coup leur propre analyse de l'évolution de l'environnement stratégique. Ainsi, ce qu'il s'est passé depuis 2014 sur le « front hybride » peut nous amener à interroger la rhétorique des deux puissances concernées et, en particulier, le schéma à tendance victimaire mis en avant à des degrés divers par les États-Unis comme par la Russie ; une logique mimétique fut bien à l'œuvre. On soulignera toutefois que la position de la Némésis russe, hybride ou pas, était effectivement fondée sur une remise en cause de l'ordre établi, fût-ce en violation des principes du droit international et du droit des conflits armés.

Quant à la manœuvre hybride plus globale, on ne peut que constater que les États-Unis en ont été des protagonistes de premier plan depuis la fin de la Seconde guerre mondiale, au travers notamment de leur diplomatie d'influence, de leur stratégie de lutte dans le domaine informationnel, mais aussi grâce à leur avance technique et technologique.

Ainsi, la combinaison des moyens, la diversité des méthodes, l'exploitation des vulnérabilités adverses, quels que soient les domaines, n'introduisent pas de nouveauté radicale, d'autant qu'elles ont été pratiquées, avec une certaine efficacité d'ailleurs, par les États-Unis dans le passé. La rupture, ou du moins l'inflexion notable, provient du fait que les États-Unis, comme les puissances démocratiques occidentales en général, se sentent pris de cours et quelque peu dépourvus face à l'ampleur et à l'opérationnalisation méthodique et créative, à la faveur des nouvelles technologies, du concept, et que l'ordre international dont ils sont le garant est de nouveau menacé, cette fois-ci de manière plus subversive et complexe, rendant toute forme de réaction et de réponse potentiellement délicate à conduire et à assumer.

¹⁹⁵ En particulier dans les années 2006-2010, à l'occasion des débats sur la guerre régulière et irrégulière, ou encore sur les opérations de contre-insurrection.

¹⁹⁶ On pourra se référer aux travaux de René Girard dans ce domaine, notamment à ses considérations sur la relation franco-allemande et sa théorie de la montée aux extrêmes au cours du XX^e siècle, telles que développées dans René Girard, *Achever Clausewitz*, Flammarion, 2011. Girard y explicite sa thèse du désir mimétique ou désir d'appropriation comme dépassement du désir hégélien de reconnaissance (Chapitre II, p. 72-73).

2.2. Une capacité d'influence toujours considérable

La plupart des observateurs admettent que l'occidentalisme¹⁹⁷, dont le fer de lance est sans nul doute le messianisme démocratique porté par l'Amérique, est désavoué. Le « camp occidental » souffre aujourd'hui, d'abord de ses excès passés – la deuxième guerre d'Irak notamment¹⁹⁸ – et surtout d'une crise interne que vivent nombre de sociétés, sur fond de crise de la mondialisation.

Pour autant, la diplomatie d'influence américaine reste un outil exceptionnellement performant. Les États-Unis sont en effet parvenus à prendre la mesure de leurs adversaires et à mobiliser leur propre camp. Face à une Russie résurgente déployant des stratégies hybrides assumées, les États-Unis n'ont-ils pas œuvré avec efficacité à la mobilisation du camp occidental ? puis, très récemment, en s'engageant dans une rivalité systémique, avec la Chine, n'ont-ils pas malgré tout réorienté les débats (au sein de l'OTAN par exemple) et exercé pleinement leur leadership en fonction de leurs intérêts avant tout ? Certes, la présidence Trump a semé le doute quant à la solidité des alliances et à la crédibilité du partenaire américain. Pour autant, l'Amérique que l'on dit en retrait et vacillante, a su imposer à la plupart de ses alliés et partenaires sa vision géostratégique, malgré la rhétorique « trumpienne »¹⁹⁹, et réintroduire progressivement des éléments d'une lutte en cours ou à venir de nature quasi-idéologique²⁰⁰. L'Amérique n'a-t-elle pas sonné, face à la menace grandissante et à la remise en question de la dichotomie paix-guerre, la mobilisation générale que l'OTAN, par exemple, exprime au travers du renouveau de la défense collective ? Cette mobilisation ne couvre-t-elle pas l'ensemble des domaines de la « lutte », lesquels correspondent d'ailleurs à l'arsenal des menaces dites hybrides qui auront été un vecteur puissant, parce qu'à la fois holistique et subtil, de cette entreprise, soit qu'elle fût subie, initiée, ou cautionnée par les États-Unis ?

La vision de l'hybridité comme forme achevée du *smart power* prend ainsi tout son sens. Si, par une ironie cruelle, les États-Unis, qui l'ont conceptualisé, et pratiqué, de manière essentiellement pragmatique, mais surtout en position de force, face à des adversaires alors convalescents, diminués, ou encore immatures, en subissent désormais les effets, il n'en reste pas moins qu'il s'agit d'une donnée de leur puissance, relativement aisément remobilisable, tant leur arsenal est complet et leur savoir-faire, à condition de quelques ajustements, rodé.

¹⁹⁷ Hubert Védrine, « Le danger de l'occidentalisme », entretien, *Revue internationale et stratégique*, N° 75, 2009/3, pp. 135-140.

¹⁹⁸ Comme l'a noté Alexandra de Hoop Scheffer, *Hamlet en Irak*, CNRS Éditions, mars 2007 : le soft-power américain a été considérablement et durablement terni par la guerre en Irak.

¹⁹⁹ Car la rhétorique « trumpienne », aussi déstabilisante fût-elle pour les alliés et, parfois, pour l'Administration américaine, n'a pas toujours été suivie à la lettre, comme l'atteste le rôle qu'a tenu le Secrétaire à la défense Mattis, ou encore l'étroite coopération opérationnelle entretenue en Europe de l'Est (*Enhanced Forward Presence*) ou avec la France au Sahel par exemple.

²⁰⁰ Les récentes déclarations du nouveau président américain sont explicites et comportent systématiquement une référence de nature idéologique à la morale comme fondement de l'action des États-Unis face à l'hostilité russe et chinoise.

3. Perspectives et implications des stratégies hybrides américaines

3.1. Les dilemmes posés par les États-Unis à leurs principaux adversaires

Essayons d'identifier la manière dont les États-Unis pourraient à leur tour défier leurs adversaires dans le domaine qui nous intéresse et leur poser ainsi un ou des dilemmes de nature stratégique. Deux grandes options semblent envisageables.

D'une part, la dissuasion par le pari du « perdant-perdant » : il s'agirait pour les États-Unis de retourner l'avantage asymétrique créé par leurs adversaires contre ces derniers en acceptant de livrer bataille de manière hybride, c'est-à-dire de faire leurs les « nouvelles règles du jeu ». En procédant ainsi, et nonobstant les difficultés d'ordre opérationnel, capacitaire, ou encore juridique voire éthique qui y sont associées, les États-Unis pourraient espérer éroder voire annuler cet avantage puisque celui-ci trouve sa raison d'être et sa force dans son opposition à un adversaire conventionnel obéissant aux lois et principes du droit international. C'est donc peut-être en embrassant le défi ainsi posé par leurs adversaires que les États-Unis leur présenteraient le plus redoutable dilemme.

Une telle approche, dont on voit bien qu'elle est d'ores et déjà en partie mise en œuvre dans certains domaines (le cyber à l'évidence), présente toutefois un risque politico-stratégique majeur puisqu'elle implique d'accepter que la loi du plus fort, cette fois dans un contexte de dérégulation et d'« anarchisation » de l'ordre international, finisse par s'imposer. Jusqu'où aller et que sacrifier, donc, pour l'emporter ?

D'autre part, un nouvel effort de mobilisation idéologique peut être lancé. D'une certaine manière, ce qui constituait par le passé l'éventail des activités plus ou moins hostiles menées en permanence par les nations dans le cadre de la compétition stratégique dont on voulait croire qu'elle avait disparu, est aujourd'hui qualifié d'activités hybrides ou de zone grise, mêlant les dimensions militaire et civile²⁰¹. Dès lors, par leurs revendications, les adversaires des États-Unis, la Russie – menace-étalon ainsi désignée en 2016²⁰² – mais surtout la Chine – *near-peer competitor* – pourraient conduire ces derniers à s'engager de nouveau dans une bataille d'idées et de valeurs, reproduisant ainsi des schémas passés. Le président Biden a d'ores et déjà évoqué l'idée d'une conférence des démocraties²⁰³, dont on perçoit bien la logique sous-jacente. Une telle initiative ne s'adresse d'ailleurs pas seulement aux puissances rivales ; elle pose en soi un dilemme stratégique aux partenaires et alliés des États-Unis puisqu'il pourrait s'agir *in fine* d'accepter une dépendance politico-stratégique, à l'image de ce qui se produisit lors de la Guerre froide. Cette perspective siéra à certains alliés et en contraindra d'autres, dont la France, si l'on s'en réfère à la stratégie de défense et de dissuasion exposée en février 2020 par le président Macron.

²⁰¹ Aux États-Unis comme au Royaume-Uni, il devient explicite que la notion de menace hybride a été assimilée à celle d'activité hostile.

²⁰² La Russie est devenue pour les États-Unis la « *Pacing Threat* », telle que décrite par le général J. Dunford, alors *Chairman of the Joint Chiefs of Staff*, à l'occasion notamment d'une allocution au salon de l'AUSA, Washington, D.C., octobre 2016.

²⁰³ Le président Biden a annoncé dès avant son élection son intention d'organiser un Sommet des démocraties, le *Global Democracy Summit*.

Sur le plan politico-stratégique, les États-Unis sont en mesure de perturber le jeu de leurs adversaires en recourant à certaines initiatives majeures, parmi lesquelles :

- ➔ La consolidation des alliances dans les zones stratégiques : sur fond de mobilisation politique voire idéologique, les États-Unis pourraient en fait disposer d'une plus grande latitude face aux « agressions hostiles » pour remobiliser leur camp voire, au besoin, procéder à une forme de chantage, du moins de pression, sur leurs potentiels partenaires afin de les dissuader de coopérer avec leurs adversaires. Pour cela, il faudra bien évidemment être capable de concurrencer l'activisme chinois en particulier – notamment sur le plan économique –, mais la dégradation de l'image de la Chine et son comportement agressif pourraient ainsi grandement servir l'Amérique, en dépit de ses propres errements.
- ➔ Le recours à une politique d'attribution collective (« *name and shame* ») systématique et désinhibée face à toute menace de nature subversive, dont l'objectif serait de faire encourir un risque réputationnel majeur aux puissances rivales, notamment la Chine, au moment où cette dernière s'efforce de convaincre voire de séduire. Il s'agirait ainsi de renforcer le potentiel de dissuasion et de prendre l'ascendant sur le plan de la communication stratégique.

Sur le plan « stratégique-opérationnel » : il paraît raisonnable d'envisager que les États-Unis poursuivent et intensifient leurs démarches et activités dans les domaines suivants :

- ➔ L'opérationnalisation du concept de « *modern deterrence* », visant à la mobilisation de tous les secteurs des sociétés potentiellement ciblés par des actes hostiles, afin d'atteindre un degré suffisant de résilience sociétale. Il s'agit donc d'une entreprise de renforcement des capacités, civiles (*civil preparedness*) comme militaires, des différents États, selon des normes et standards que la partie américaine contribuera activement à définir voire imposer.
- ➔ Le déploiement d'un arsenal hybride plus offensif articulé autour de trois axes d'effort que sont les domaines cybernétique, économique et financier, et juridique. La réponse à la guerre hybride est en construction côté américain (GIO, MDO, etc.). La réponse à l'éventail des menaces de zone grise est, elle, plus complexe à mettre en œuvre. Il semble toutefois probable que les États-Unis usent de leur supériorité dans certains domaines pour attaquer les vulnérabilités adverses, ou compenser certaines de leurs difficultés dans d'autres domaines. Il est donc probable qu'ils continueront à user voire abuser de leurs armes stratégiques redoutables que sont leur dynamisme technologique et scientifique (intelligence artificielle, quantique, robotique, etc.), leur avantage asymétrique structurel qu'est le dollar (monnaie de réserve internationale, contrôle des flux financiers internationaux en dollars, etc.) et l'extraterritorialité de leur droit.

3.2. Des dilemmes stratégiques pour les alliés et partenaires

Tout autant que la stratégie ciblant les puissances rivales, l'attitude de l'Amérique vis-à-vis de ses propres alliés et partenaires importe au plus haut point tant elle recèle des opportunités et des risques, dans l'ensemble des domaines couverts par les menaces hybrides.

Sur le plan politique, le focus croissant sur la Chine pourrait devenir source de dilemme pour de nombreux pays puisqu'il invitera tôt ou tard, en cas d'avènement d'une nouvelle bipolarité, à faire un choix stratégique entre Chine et États-Unis²⁰⁴, aux ramifications multiples et aux conséquences, notamment économiques, particulièrement lourdes pour les pays concernés. Certes l'activisme chinois est l'objet de préoccupations croissantes de la part des alliés de Washington ; mais les États-Unis sont néanmoins parvenus à faire partager leur propre analyse de la situation, en particulier le danger représenté par les menaces hybrides et autres activités de zone grise, au point d'orienter l'OTAN vers la préparation d'une rivalité systémique avec la Chine²⁰⁵. Une telle « mutualisation » d'une conception nationale mérite sans doute débat.

Sur le plan économique et financier, le dollar, en tant que monnaie de réserve internationale, est l'arme économique – et politique – absolue pour les États-Unis. Le contrôle ainsi exercé sur les transactions internationales en dollars, conjugué à l'extraterritorialité du droit américain, placeront les alliés et partenaires devant des dilemmes à la fois politiques et économiques récurrents en mettant en balance la relation stratégique bilatérale concernée avec des gains économiques ou financiers ponctuels. Selon les circonstances et les intérêts en jeu, une forme de chantage, comme par le passé, pourrait ainsi être exercée sur certains partenaires. Bien évidemment, cet outil, puissant, sera sans doute à manier avec perspicacité afin de ne pas mettre en péril, par contrecoup, la cohésion indispensable entre alliés.

Sur le plan stratégique-opérationnel, les considérations supra se déclineront dans les différents domaines couverts par les menaces hybrides, variant selon les pays, les enjeux et intérêts concernés, et les priorités de l'administration américaine. Ainsi se posera sans doute fréquemment la question pour les pays partenaires du dévoilement de leurs vulnérabilités. Prenons deux exemples : les infrastructures critiques et l'économie.

- S'agissant des infrastructures critiques, l'on comprendra aisément que, nonobstant la nécessaire adaptation des structures par la prise en compte de la menace, les échanges induits entre partenaires impliquent le potentiel dévoilement de données sensibles relevant souvent de la sécurité nationale, et dont l'exploitation à des fins concurrentielles, par les partenaires étatiques comme par certaines grandes entreprises rivales, présenterait un risque majeur pour la souveraineté nationale notamment. Il s'agira donc de trouver un équilibre entre souveraineté, protection du secret et sécurité nationale, et nécessaire coopération et assistance mutuelle.
- Il en va de même dans le domaine économique, où la prise en compte par le concept des menaces hybrides de la dimension économique et, plus particulièrement, de la « menace » posée par les IDE émanant de puissances hostiles, en l'occurrence principalement la Chine, pose là aussi un problème majeur pour toute nation engagée dans une compétition économique féroce. Une forme de transparence sur les situations vécues au plan national, et les échanges afférents d'informations et

²⁰⁴ Cette idée, et ce risque, ont été très clairement exprimés par E. Macron dans son discours sur la stratégie de défense et de dissuasion, 7 février 2020.

²⁰⁵ On peut là encore citer René Girard qui, dans son ouvrage *Achever Clausewitz*, p. 91, écrit : « ...les Chinois, qui ont une vieille culture militaire, ont théorisé depuis trois mille ans le fait qu'il faut utiliser la force de l'adversaire pour mieux la retourner. Les Chinois subissent donc moins l'attraction du modèle occidental, qu'ils ne l'imitent pour triompher de lui ».

de données contribueraient sans doute à rendre vulnérable le pays concerné à une concurrence redoublée doublée d'une pression politique partisane.

Ainsi, à partir de leur propre conception de l'hybridité, les États-Unis apportent des réponses de plus en plus complètes et ciblées aux défis rencontrés et laissent entrevoir les contours d'une évolution nettement confrontationnelle de leur posture géostratégique face, en particulier, à la Russie et à la Chine. Cet état d'esprit et ces dispositions présentent pour la France les principaux enjeux suivants :

- ➔ Un enjeu de positionnement, qui consiste à définir notre vision stratégique et les grands objectifs qui doivent servir nos propres intérêts afin de clarifier et d'assumer notre posture vis-à-vis de notre allié américain ;
- ➔ Un enjeu d'influence, qui consiste à mettre en œuvre une stratégie volontariste dans ce domaine afin de faire entendre notre propre conception des problématiques associées à l'hybridité, et d'être en mesure d'influer sur les débats et éventuelles décisions prises, notamment dans les enceintes internationales prioritaires pour nous que sont l'OTAN et l'UE ;
- ➔ Un enjeu de coopération, qui consiste à identifier les voies d'une action conjointe et mutuellement bénéfique, sur les plans stratégique et opérationnel, pour faire face aux défis communs posés par certaines des stratégies hybrides adverses ;
- ➔ Un enjeu de préservation, qui consiste, par une approche holistique, à renforcer nos dispositifs et capacités d'action dans l'ensemble des domaines stratégiques offrant de potentielles vulnérabilités face au déploiement de stratégies hybrides agressives, d'où qu'elles émanent.

Annexe 2

EXEMPLES DE DÉFINITION DES ACTIVITÉS HYBRIDES ET DE « ZONE GRISE »

Source	Hybride	Zone grise
F. Hoffman	« A full range of modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts that include indiscriminate violence and coercion, and criminal disorder » ²⁰⁶ .	« Term captures deliberate multidimensional activities by a state actor just below the threshold of aggressive use of military forces. In such conflicts, adversaries employ an integrated suite of national and subnational instruments of power in an ambiguous war to gain specified strategic objectives without crossing the threshold of overt conflict. » « Gray zone or ambiguous conflicts, ... involve conflict activity short of violence. Hybrid threats ably combine various modes of fighting in time and space, with attendant violence in the middle of the conflict spectrum. » ²⁰⁷
N. Freier		« The gray zone is the awkward and uncomfortable space between traditional conceptions of war and peace » ²⁰⁸ . « Gray zone threats share three characteristics. The first is hybridity: they combine methods and strategic effects. Second, they menace U.S. defense and military convention because they do not conform neatly to a linear spectrum of conflict or equally linear military campaign models. Finally, they disrupt strategic risk calculations by presenting a paralyzing choice between high-risk action and equally high-risk inaction ».
J. Dubik, N. Vincent		« The gray zone is commonly understood as the hostile or adversarial interactions among competing actors below the threshold of conventional war and above the threshold of peaceful competition » ²⁰⁹ .
AEI	« Russia considers hybrid warfare a form of conflict which includes strategic uses of economic, diplomatic, and influence operations, along with the use of military forces and espionage. By contrast, the U.S. thinks of hybrid warfare as actions or tactics used before a conventional war. While the U.S. thinks it is managing pre-conflict aggression, Russia	« Known as gray-zone aggression, these nonmilitary attacks take place in the gray area between war and peace. Tactics range from cyberattacks and disinformation to subversive business practices and intimidation, and civil society is a frequent target » ²¹¹ .

²⁰⁶ Lt-Col. Frank Hoffman, « Hybrid Warfare and Challenges », *Joint Force Quarterly*, Issue 52, 1st quarter 2009, p. 34.

²⁰⁷ Frank Hoffman, « The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War », in *Index of Military Power*, Heritage Foundation, 2016.

²⁰⁸ Nathan Freier, Christopher Compton, Tobin Magsig, « Gray Zone: Why We're Losing the New Era of National Security », *Defense One*, June 9, 2016 – <https://www.defenseone.com/ideas/2016/06/gray-zone-losing-new-era-national-security-strategy/128957/>

²⁰⁹ James M. Dubik, Nic Vincent, *America's Global Competitions: The Gray Zone in Context*, Institute for the Study of War, February 2018, p. 9.

²¹¹ Gray-zone aggression: Countering a growing national security threat, Web Event, AEI, November 10, 2020 – <https://www.aei.org/events/gray-zone-aggression-countering-a-growing-national-security-threat/> Voir également : Grayzone and Non-Kinetic Threats: A Primer, AEI, October 2020 – <https://www.aei.org/wp-content/uploads/2020/10/Elisabeth-Braw-Grayzone-Non-Kinetic-Threats-Primer.pdf?x88519>

	already considers itself in the midst of a strategic battle disguised as competitive aggression » ²¹⁰ .	
Atlantic Council	« An approach that blends conventional and unconventional, overt and covert, kinetic and non-kinetic, and military and nonmilitary means to undermine a target and achieve the perpetrator’s political and strategic goals » ²¹² . « Hybrid threats ... include four key categories: low-level use of force; cyberattacks; economic and political coercion and subversion; and information war » ²¹³ .	
CSBA	« Diverse military and/or paramilitary operations undertaken to secure priority strategic interests following authorization to use kinetic force either from the outset or in the event that deployed units are forcibly challenged by rival military and/or paramilitary forces. » ²¹⁴	
CSIS	« An effort or series of efforts intended to advance one’s security objectives at the expense of a rival using means beyond those associated with routine statecraft and short of means associated with direct military conflict. » ²¹⁵	« The toolkit for coercion below the level of direct warfare includes information operations, political coercion, economic coercion, cyber operations, proxy support, and provocation by state-controlled Forces. » ²¹⁶
CNAS		« The state between war and peace, where actors (state and non-state) seek to defeat their opponents without extensive or sustained military activity » ²¹⁷

²¹⁰ « Putin is winning Russia’s hybrid war against America », *National Review*, December 9, 2020 – <https://www.aei.org/op-eds/putin-is-winning-russias-hybrid-war-against-america/>

²¹² Lauren Speranza, *A Strategic Concept for Countering Russian and Chinese Hybrid Threats*, Atlantic Council, July 2020 – <https://www.atlanticcouncil.org/in-depth-research-reports/a-strategic-concept-for-countering-russian-and-chinese-hybrid-threats/>

²¹³ Franklin D. Kramer, Lauren M. Speranza, *Meeting the Russian hybrid challenge*, Atlantic Council, May 2017 – <https://www.atlanticcouncil.org/in-depth-research-reports/report/meeting-the-russian-hybrid-challenge/>

²¹⁴ Ross Babbage, *Stealing a March. Chinese Hybrid Warfare in the Indo-Pacific: Issues and Options for Allied Defense Planners*, Vol. 1, CSBA, 2019, p. 2 – https://csbaonline.org/uploads/documents/Stealing_a_March_Final.pdf

²¹⁵ Hijab Sha, Melissa Dalton, *Partners, Not Proxies: Capacity Building in Hybrid Warfare*, CSIS Briefs, May 27, 2020 – <https://www.csis.org/analysis/partners-not-proxies-capacity-building-hybrid-warfare>

²¹⁶ *Gray Zone Project*, CSIS – <https://www.csis.org/grayzone>

²¹⁷ Nicholas Heras, « Gray Zones in the Middle East », CNAS, September 18, 2017 – <https://www.cnas.org/publications/reports/gray-zones-in-the-middle-east>

Annexe 3 LES ACTIVITÉS HYBRIDES DES RIVAUX

Le tableau ci-dessous présente quelques exemples d'actions dites hybrides ou de zone grise, décrites dans différents travaux américains. Ils sont classés en fonction des principales catégories retenues par la Rand dans l'étude de Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options*, 2019.

	Russie	Chine
Domaine militaire		
Utilisation / soutien de forces auxiliaires	Transfert d'équipement militaire aux séparatistes d'Abkhazie et d'Ossétie du sud avant la guerre de Géorgie en 2008. In 2018, Russian mercenaries trained Serbian Honour, a separatist paramilitary organization in Serbia	Utilisation de forces navales paramilitaires (garde-côtes, milices) dans les eaux contestées de mer de Chine.
Intimidation	Exercice militaire de juillet 2008 à proximité de la frontière géorgienne. Manœuvres aériennes dangereuses et violations de l'espace aérien. Manœuvres de proximité réalisées par un satellite d'inspection auprès d'un satellite militaire américain.	Déploiement massif de forces à la frontière avec le Vietnam lors de l'incident de Haiyang Shiyou 981 en 2014. Incursions dans l'espace aérien japonais, notamment autour des îles Senkaku en août 2016. Manœuvres de suivi ou d'interception de navires ou appareils militaires américains opérant en mer de Chine orientale.
Domaine de l'information	1,4 million de <i>tweets</i> lancés par des <i>bots</i> pour influencer la campagne présidentielle américaine de 2016.	Campagne d'influence pour obtenir le ralliement aux revendications chinoises. Augmentation du nombre de media contrôlés par le PCC. Operations du <i>Chinese United Front Work Department</i> et d'autres agences du PCC au sein d'universités, de médias et d'ONG australiens.
Domaine cyber	Attaque simultanée de réseaux bancaires, gouvernementaux et médiatiques en Estonie en 2007. Attaque des sites internet du gouvernement allemand en Janvier 2015, à l'arrivée du Premier ministre ukrainien à Berlin.	Cyber intrusions contre le Japon et les Philippines lors de la crise de l'atoll de Scarborough. Vol de propriété intellectuelle aux États-Unis et en Europe.
Domaine légal	Attribution de la nationalité russe aux minorités russophones pour alimenter le séparatisme.	Déclaration unilatérale d'une zone de défense aérienne (<i>Air Defense Identification Zone – ADIZ</i>) en mer de Chine orientale en 2013. Création d'un centre international de droit maritime pour légitimer les revendications territoriales chinoises.

<p>Domaine économique</p>	<p>Sanctions. Interruption des livraisons d'énergie.</p>	<p>Utilisation d'agents économiques contrôlés par l'État pour développer la présence dans les zones contestées (construction, exploitation). Utilisation du commerce, de l'aide ou des sanctions pour influencer l'attitude des pays concernés par les revendications. Attribution de prêts massifs à des pays vulnérables qui ne pourront les rembourser.</p>
<p>Domaine politique</p>	<p>Manipulation des minorités. Financement de mouvements politiques favorables à la Russie (prêt accordé au Front national en 2014). Assassinat d'opposants.</p>	