Taxonomie des menaces hybrides

Omniprésente dans les débats politique sur la sécurité, la notion de menace hybride couvre un champ d'attaques variées difficile à appréhender. La présente analyse montre que l'examen ciblé d'une telle situation présuppose une compréhension claire des formes sous-jacentes de conflit hybride.

Par Ivo Capaul

Les pays occidentaux sont de plus en plus exposés à des attaques évoluant dans une zone grise entre guerre et paix. Le déclenchement d'une guerre conventionnelle sur le continent européen a accentué cette tendance. Pour décrire ce phénomène qui a largement contribué à la déstabilisation de la situation de sécurité en Europe, la notion de menace hybride s'impose actuellement. De nombreux cas sont invoqués pour montrer que les différends interétatiques se règlent de plus en plus sous la forme d'un conflit hybride. Ils comprennent par exemple le contrôle des mouvements migratoires irréguliers par la Biélorussie, la théorie diffusée par des acteurs chinois sur les réseaux sociaux selon laquelle le virus du COVID-19 proviendrait d'un laboratoire de recherche de l'armée américaine, la compromission des systèmes d'exploitants d'infrastructures critiques et la fuite orchestrée par les autorités russes d'une téléconférence interceptée entre officiers allemands de haut rang.

Les discours politiques sur la sécurité sont ainsi façonnés par des termes tels qu'une «ère de la guerre hybride» ou une *weaponisation of everything*, pour désigner le fait que tout peut être arsenalisé. Cette évolution n'épargne pas la Suisse: ces dernières années, la notion de «menace hybride» a fait son entrée dans bon nombre de documents sur la politique de sécurité de la Confédération.

L'équipage du « Yi Peng 3 » est soupçonné d'avoir endommagé deux câbles sous-marins en mer Baltique fin 2024. Pouvoir nier les faits est un attribut clé des attaques hybrides. *Mikkel Berg Pedersen / Reuters*

En particulier, l'un des quatre scénarios envisagés par l'armée suisse pour le développement des forces armées repose explicitement sur des formes hybrides de conflits. Le fait que cette notion soit en train de s'institutionnaliser met en évidence la nécessité d'acquérir une compréhension fondamentale de ce que l'on entend par «hybride» et de la manière dont ce concept peut éclairer une situation de menace.

La présente analyse vise à affiner la notion de menace hybride émanant d'un État en vue de créer un consensus minimal sur les éléments de définition à partir de la terminologie existante. Cette approche repose sur l'idée que, pour saisir une situation de menace hybride du point de vue de l'agressé, il faut d'abord comprendre clairement les moyens de guerre hybride utilisés par l'agresseur. Pour ce faire, cette analyse com-

mencera par exposer différentes définitions et réalisera un examen critique de cette notion, avant de présenter une taxonomie permettant de catégoriser les situations de menaces hybrides. Une approche alternative de la question sera proposée, avant de conclure sur le fait qu'un état de menace hybride peut servir de point de départ à l'élaboration d'une stratégie.

Un champ (trop) vaste

Il convient tout d'abord de noter qu'il n'existe pas de définition universellement reconnue d'une menace hybride. Le règlement de la Conduite opérative 17 de l'armée suisse délimite la notion de conflit hybride émanant d'États comme une combinaison d'instruments politiques, économiques, informationnels, humanitaires et paramilitaires visant à atteindre des objectifs stratégiques, dont l'utilisation est généralement irrégulière et dissimulée. L'OTAN définit la *menace hybride* comme «un type de menace qui combine des activités conventionnelles, irrégulières et asymétriques dans le temps et dans l'espace».

La définition de l'UE, qui parle d'un «mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (…) 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», coïncide pour l'essentiel. Le phénomène est décrit de la même manière dans les milieux scientifiques, notamment par E. Reichborn-Kjennerud et P. J. Cullen, qui considèrent la guerre hybride comme une escalade simultanée sur le plan horizontal (extension des actions hostiles à tous les moyens militaires et non militaires de la puissance publique) et sur le plan vertical (intensification, non seulement des actions elles-mêmes, mais aussi de leur coordination dans différents champs d'action).

> Il n'existe pas de définition universellement reconnue d'une menace hybride.

Il ressort de ces définitions que la notion comporte une grande part d'abstraction. Elle est devenue un terme fourre-tout de plus en plus vague pour désigner les formes les plus diverses de menaces liées à la conduite non linéaire d'un conflit. Ainsi, une déclaration publique du ministre russe des Affaires étrangères Sergueï Lavrov a été qualifiée de forme de guerre hybride, au même titre que l'occupation puis l'annexion de la Crimée par des soldats russes non identifiés en 2014 (les «petits hommes verts»). L'écart entre ces deux exemples montre que la menace hybride est une notion trop inclusive pour permettre d'effectuer une distinction claire entre différents types de conflits.

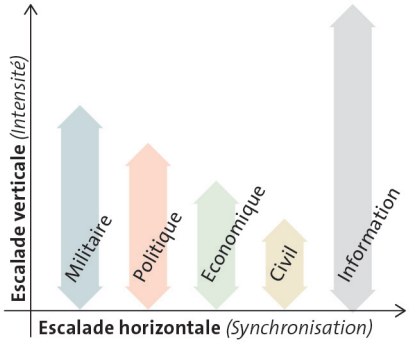
Un autre écueil réside dans le fait que le concept de conflit hybride ne décrit pas un phénomène nouveau, mais constitue simplement une nouvelle manière de désigner une pratique qui s'est développée au fil du temps. La tendance des États à imposer leurs intérêts à d'autres pays par des moyens subversifs et situés en dessous du seuil de guerre est probablement aussi ancienne que les conflits interétatiques en eux-mêmes. On retrouve déjà cette conception de l'art de la guerre dans les écrits de Sun Tzu. Néanmoins, la popularité actuelle de ce terme montre clairement que le conflit hybride est une forme de menace à laquelle les décideurs politiques et militaires des pays occidentaux sont de plus en plus confrontés.

Cet intérêt accru s'explique par deux évolutions majeures. D'une part, la diffusion de nouvelles technologies, telles que les réseaux sociaux, a élargi le champ d'action des mesures de subversion. D'autre part, on constate que les attaques subversives deviennent un instrument de pouvoir intéressant pour les États qui souhaitent rester en dessous du seuil de guerre et ne sont pas en mesure de supporter les coûts potentiels d'une escalade du conflit. Et ce, en particulier dans les situations de destruction mutuelle assurée sur le plan nucléaire. C'est pourquoi des attaques que l'on qualifierait aujourd'hui d'hybrides étaient très répandues pendant la guerre froide (où elles étaient souvent appelées mesures actives ou actions secrètes) et peuvent réapparaître dans le contexte actuel de polarisation géopolitique croissante.

Si la notion de menace hybride constitue une catégorie pertinente dans le discours politique actuel sur la sécurité, ce qui se traduit également par son ancrage croissant dans les documents stratégiques du DDPS, de l'OTAN et de l'UE, il existe un risque qu'elle se transforme en une coquille vide. En effet, si tous les types de conflits interétatiques qui ne sont pas des guerres conventionnelles peuvent être qualifiés d'hybrides, alors il s'agit d'un concept à la fois trop vaste et trop vague pour apporter une contribution significative à la compréhension d'une situation de menace.

Guerre hybride

Basé sur la définition de E. Reichborn-Kjennerud et P. J. Cullen.



Zoom sur les vecteurs d'attaque

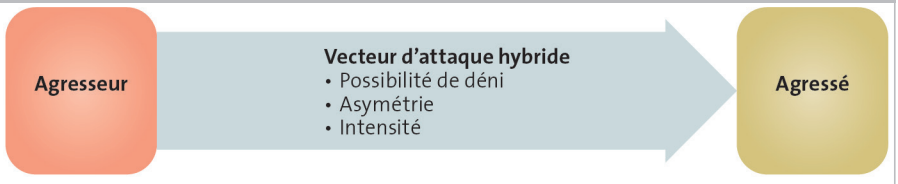
Pour tenter d'éclaircir cette notion diffuse, l'on peut changer de perspective en s'éloignant de la perception de la menace du point de vue de l'entité agressée pour examiner les vecteurs d'attaque émanant d'un agresseur qui relèvent du spectre de la guerre hybride. De telles attaques sont les seuls éléments que l'on peut observer de façon empirique dans le débat sur ce type de conflits. Elles peuvent ainsi servir de point de départ à une analyse inductive d'un risque hybride. Seule l'analyse d'attaques déjà survenues et pouvant être classées comme hybrides peut, en combinaison avec l'extrapolation de possibles agressions à venir, donner un contenu réel à un tableau de menaces hybrides.

Une «attaque» désigne la prise de mesures offensives contre un objectif désigné. Il s'agit d'une action émanant d'un acteur et dirigée contre un autre. Une attaque hybride menée par un État doit donc présenter trois éléments de définition fondamentaux: en premier lieu, un agresseur souhaitant obtenir un effet par le biais de l'action offensive; en deuxième lieu, un agressé (institution étatique, population civile, etc.) sur lequel l'effet doit être obtenu; et en troisième lieu, un vecteur d'attaque hybride. Ce dernier représente la mesure offensive proprement dite et établit un lien entre l'agresseur et l'agressé (voir illustration p. 3).

Les caractéristiques de ce vecteur sont également les éléments qui confèrent à l'at-

taque sa nature *hybride.* Pour être classé comme hybride, le vecteur d'attaque doit avoir trois propriétés: il doit présenter une certaine *possibilité de déni (déni plausible);* être *asymétrique;* et son *intensité* doit être inférieure au seuil de guerre. Ces trois critères, qui sont issus des définitions d'une menace hybride établies par l'armée suisse et l'UE, nécessitent une explication.

Modèle de représentation d'une menace hybride



Source: schéma de l'auteur

La *possibilité de déni* décrit le degré auquel l'État à l'origine de l'agression hybride ou ses dirigeants politiques peuvent nier de manière plausible leur responsabilité. Elle permet alors de réduire les coûts politiques encourus par l'agresseur, car l'agressé est moins susceptible de prendre des mesures de représailles (sous la forme de sanctions, par exemple). C'est pourquoi les attaques hybrides sont souvent menées à l'aide de procédés relevant des services de renseignements, c'est-à-dire de manière cachée (l'auteur reste dissimulé), voire clandestine (l'attaque en elle-même reste dissimulée).

L'*asymétrie* fait référence au champ d'action de l'attaque hybride (réseaux sociaux, sphère économique, société civile, etc.). Un vecteur d'attaque devient asymétrique lorsqu'il est employé dans un champ d'action où l'agressé ne possède pas de dispositifs de défense suffisants. Au fond, cette conception de l'asymétrie consiste à exploiter les forces relatives de l'agresseur par rapport aux faiblesses de l'agressé. La diffusion intentionnelle de désinformation constitue un exemple typique de vecteur d'attaque hybride. Les sociétés démocratiques ouvertes accordent une grande importance à la liberté d'opinion et d'information, ce qui explique pourquoi l'action des États pour lutter contre la désinformation est souvent très limitée.

Enfin, l'*intensité* du vecteur d'attaque est liée au potentiel d'escalade d'une attaque hybride par rapport à un conflit conventionnel. L'intensité de l'effet d'un vecteur d'attaque hybride sur l'agressé est dosée de manière à rester en dessous du seuil de guerre sur l'échelle de l'escalade. Si l'intensité d'une attaque hybride est telle que l'État agressé se voit contraint d'y réagir par des moyens conventionnels avec ses forces armées, le seuil de guerre est alors franchi. Le fait qu'un vecteur d'attaque que l'on pourrait par ailleurs qualifier d'hybride possède également une dimension cinétique constitue un signe qu'une attaque se rapproche du seuil de guerre. Dans un tel cas, on peut parler de conflit dans la *zone grise*.

La manière dont la Russie a géré le conflit dans la région du Donbass en Ukraine entre 2014 et 2022, au moyen d'unités paramilitaires, de cyberattaques et d'initiatives de désinformation, constitue un exemple de mesures offensives dans la *zone grise*. Il est également intéressant de noter que l'intensité d'un vecteur d'attaque réagit inversement à la possibilité de déni. Plus l'intensité d'un vecteur d'attaque hybride est élevée, moins il est généralement possible de le nier.

Si un vecteur d'attaque présente ces trois caractéristiques, on peut parler d'une attaque hybride au sens de la présente définition. Un État dont les intérêts sont réalistement affectés par de tels vecteurs d'attaque se voit confronté à une situation de menace hybride.

> Seule l'analyse d'attaques déjà survenues et pouvant être classées comme hybrides peut donner un contenu réel à un tableau de menaces hybrides.

Classification des menaces

Un aspect central de cette taxonomie réside dans le fait que les trois critères sur lesquels elle repose ne sont pas des variables binaires. Ils ne sont pas simplement présents ou absents, mais évoluent sur un spectre. L'évaluation du degré d'existence de ces critères permet ainsi de classer les situations de menaces hybrides en trois catégories (voir tableau p.4). La terminologie utilisée dans cette classification correspond à celle de l'UE.

Cette classification peut également permettre de clarifier les responsabilités entre les principaux acteurs étatiques chargés d'assurer la défense contre les attaques dans les trois situations de menaces présentées dans le tableau. Par exemple, la détection des opérations hybrides et la défense contre celles-ci relèvent en premier lieu des services de renseignements. L'armée, quant à elle, ne joue un rôle prépondérant lorsque le seuil de la guerre hybride est dépassé.

Une approche alternative

Une approche alternative pour démêler le concept de menace hybride peut consister à le diviser en une multitude de sous-catégories. Ce procédé ôte à la notion sa force d'expression. Les mesures offensives qualifiées d'hybrides sont ainsi examinées dans le cadre du champ d'action du vecteur d'attaque. Les attaques individuelles ne sont pas considérées comme des phénomènes cohérents et sont donc analysées séparément.

L'avantage de cette approche réside dans la création de catégories plus précises, ce qui permet une analyse plus détaillée des vecteurs d'attaque dans leurs champs d'action respectifs. Mais elle présente également au moins deux inconvénients. Premièrement, de par leur nature, les attaques hybrides ont des effets qui se font sentir sur plusieurs champs d'action superposés. Ainsi, une campagne de désinformation sur Internet se déroule à la fois dans le cyberespace et dans l'espace informationnel. L'étude d'une telle attaque dans un seul champ d'action trouve alors ses limites. Deuxièmement, la notion de conflit hybride tente explicitement de représenter une stratégie intégrative de la part d'un agresseur englobant plusieurs champs d'action.

En divisant le concept de menace hybride en différents sous-domaines, l'on perd précisément son élément central, à savoir l'association à des vecteurs d'attaque permettant d'obtenir un effet sur l'entité agressée. Cette vision intégrative d'un tableau de menace est particulièrement importante pour assurer la défense contre les attaques hybrides, car il sera probablement nécessaire de coordonner les différents instruments politiques de l'État en matière de sécurité. Au niveau stratégique, qui est celui auquel se situe cette analyse, il convient

Catégorisation des menaces hybrides selon les critères de définition du vecteur d'attaque hybride

Désignation	**Possibilité** de déni	**Asymétrie**	**Intensité**	**Exemples**
Ingérence hybride	Élevée: *déni plausible*	Forte asymétrie	En dessous du seuil de guerre	Désinformation via les réseaux sociaux
Opérations hybrides	Modérée: *déni relativement plausible*	Asymétrie	En dessous du seuil de guerre	Sabotage d'infrastructures critiques
Guerre hybride	Faible: *déni non plausible*	Paramilitaire	Conflits dans la «*zone grise*» (proches du seuil de guerre)	Petits hommes verts, création volontaire de mouvements de réfugiés
Guerre conventionnelle	Aucune	Militaire (guerre symétrique)	Seuil de guerre franchi	Invasion totale de l'Ukraine par la Russie depuis 2022

Source: Tableau de l'auteur basé sur la terminologie de M. Wigell, H. Mikkola et T. Juntunen.

donc de rejeter la fragmentation de la notion de menace hybride en fonction de ses champs d'action. C'est le caractère intégré du concept qui doit primer. Au niveau de la défense opérationnelle contre les dangers, en revanche, une subdivision des menaces en fonction des différents champs d'action peut s'avérer tout à fait judicieuse, car elle permet de déterminer quelle institution étatique est responsable de la mise en œuvre des contre-mesures.

La présente analyse propose de prendre en compte les trois critères que sont la *possibilité de déni, l'asymétrie* et *l'intensité* pour caractériser les attaques hybrides.

Vers l'élaboration de stratégies

La notion de menace hybride est omniprésente dans le débat politique sur la sécurité, car ce terme générique couvre un champ d'attaques variées difficile à appréhender. En parallèle, cette situation a pour effet d'élargir toujours plus le périmètre de définition du concept, ce qui empêche d'effectuer une distinction claire entre les différents tableaux. Une solution à ce problème peut consister à définir une telle menace en s'appuyant sur les propriétés abstraites des vecteurs d'attaque qui peuvent être considérés comme «hybrides».

Pour pouvoir effectuer une telle classification, la présente analyse propose, en se fondant sur les terminologies de l'armée suisse, de l'OTAN et de l'UE, de prendre en compte les trois critères que sont la *possibilité de déni, l'asymétrie et l'intensité*. Leurs caractéristiques peuvent servir de cadre de référence pour élaborer un tableau des situations de menaces hybrides. En outre, cette approche aide à ancrer l'évaluation d'une telle menace dans la réalité empirique. Pour compléter l'évaluation selon cette méthode, il faudrait également analyser les objectifs concrets poursuivis par l'agresseur lors d'une attaque hybride. La présente analyse ne s'est pas penchée sur cet aspect.

Pour conclure, il convient de souligner que la notion de menace hybride constitue un guide pour mieux appréhender et catégoriser une situation observable de manière empirique. En revanche, cette notion ne livre pas de stratégie sur la manière dont les instruments étatiques peuvent être employés pour réagir à des menaces hybrides du point de vue de l'agressé. Il s'agirait d'une étape ultérieure qui nécessiterait probablement une approche intégrative à l'échelle du gouvernement ou de la société (*whole-of-government* ou *whole-of-society*). Pour pouvoir formuler une telle stratégie, il faut au préalable parvenir à une compréhension claire de la menace hybride concrètement présente.

Voir le site thématique du CSS pour en savoir plus sur les doctrines militaires et les acquisitions d'armements.

Ivo Capaul est Researcher au sein de l'équipe «Defense Policy and Armaments Acquisition» au Center for Security Studies (CSS) à l'ETH de Zurich.

Les **analyses de politique de sécurité** du CSS sont publiées par le Center for Security Studies (CSS) de l'ETH de Zürich. Le CSS est un centre de compétence en matière de politique de sécurité suisse et internationale. Deux analyses paraissent chaque mois en allemand, français et anglais.

Éditeur: Lucas Renaud
Révision linguistique: Névine Schepers, Ivo Capaul
Layout et graphiques: Miriam Dahinden-Ganzoni

Feedback et commentaires: css.info@sipo.gess.ethz.ch
Plus d'éditions et abonnement: www.css.ethz.ch/cssanalysen

Parus précédemment:

La confiance dans les gouvernements en temps de crise No 351
État du débat sur la neutralité de la Suisse No 350
La Géorgie à la croisée des chemins No 349
L'évolution des partenariats de l'UE et de l'OTAN No 348
L'approche japonaise de la promotion de la paix No 347
La médiation comme entreprise d'État en Türkiye No 346

ISSN: 2296-0228; DOI: 10.3929/ethz-b-000711100