Guerre hybride: distinguer la réalité de la fiction

La «guerre hybride», expression désignant des agressions situées dans la zone grise, en deçà d'une véritable guerre, continue à susciter des craintes. Beaucoup s'attendent à ce que les technologies de l'information révolutionnent cet espace stratégique. Or, les événements qui se sont produits jusqu'ici ne vont pas dans ce sens. Il est donc essentiel de mener une analyse plus systématique des différents instruments utilisés sous ce concept générique.

Par Lennart Maschmeyer

Cela fait près de dix ans que les analystes et les responsables de la défense agitent la perspective d'une «guerre hybride». Cependant, l'ampleur réelle de la menace et les instruments politiques associés à ces rapports de force restent étonnamment flous. Cela n'empêche pas les pays occidentaux de consacrer d'importantes ressources à la question. Cette l'année, l'UE a annoncé la constitution en Moldavie de la première mission entièrement chargée de contrer les «menaces hybrides». Il s'avère donc à la fois urgent et important d'évaluer ces menaces.

La «guerre hybride» telle qu'imaginée par l'IA de Midjourney, octobre 2023.
Conçu par Lennart Maschmeyer et généré à l'aide de Midjourney.

Malheureusement, la notion de «guerre hybride» est particulièrement mal définie. Dans les débats politiques et les milieux universitaires, ce terme générique est essentiellement utilisé pour désigner toute agression ne relevant pas d'une guerre généralisée. La désinformation, le sabotage, la subversion et les cyberopérations entrent notamment dans cette catégorie. La prise de contrôle et l'annexion illégale de la Crimée par la Russie en 2014, le soutien de Moscou aux séparatistes armés dans la région du Donbass en Ukraine (notamment par des soldats sans insigne surnommés les «petits hommes verts») et le déploiement d'une vaste cyber-action ont été perçus comme des preuves de la puissance de ces instruments. Ces activités ont aiguisé l'intérêt des chercheurs. Nombre d'entre eux ont alors considéré que ce type d'agressions de faible intensité incarnait l'avenir de la guerre. Ces arguments et les menaces perçues ont trouvé écho auprès des responsables politiques et les ont incités à modifier leurs stratégies et leurs priorités en matière de défense.

Une révolution technologique?

Les agressions qui ne constituent pas une guerre proprement dite ne sont pas un phénomène nouveau. Cela fait longtemps que les États ont recours à des instruments évoluant dans une «zone grise» entre guerre et paix. Beaucoup pensent que l'utilisation des technologies de l'information renforce l'efficacité de ces agressions hybrides. L'on s'attend plus spécifiquement à ce que les technologies de l'information augmentent la vitesse, l'ampleur et l'intensité des conflits en zone grise par le biais d'opéra-

tions d'influence dans le cyberespace et sur les réseaux sociaux. Les cyberopérations permettent de saboter des infrastructures, de causer des ravages économiques et de perturber les communications dans n'importe quel autre pays en quelques minutes seulement. Quant aux campagnes sur les réseaux sociaux, elles peuvent semer la panique, créer la confusion et influer sur l'opinion publique afin de modifier l'issue d'une élection. Par conséquent, beaucoup pensent que les États auront désormais la possibilité de parvenir à des fins qui, auparavant, étaient hors de portée sans recours à la guerre.

En accord avec cette perception répandue de la menace, les pays ont modifié leurs stratégies et leurs priorités en matière de défense afin de pouvoir contrer les opérations de guerre hybride. En 2015, l'OTAN a placé la lutte contre les «menaces hybrides» au cœur de sa stratégie. L'Alliance définit ces menaces comme un ensemble «d'activités menées ouvertement ou non à l'aide de moyens militaires et de moyens non militaires: désinformation, cyberattaques, pression économique, déploiement de groupes armés irréguliers ou emploi de forces régulières». La récente création d'une mission civile de partenariat de l'UE en Moldavie, dont la priorité est d'assurer la défense contre les menaces hybrides émanant de la Russie, laisse également penser que, malgré l'absence de définition claire, les responsables politiques perçoivent clairement la guerre hybride comme une menace significative. Il n'existe pas de chiffres officiels concernant les budgets alloués à cette question. Cependant, la place qu'elle occupe dans les stratégies et les déclarations officielles indique que les dépenses correspondantes sont probablement conséquentes. Le débat actuel sur l'intégration de la guerre hybride comme quatrième tâche fondamentale incombant à l'OTAN confirme cette orientation. Même la Russie, spécialiste affichée du sujet, a expliqué la hausse de 70 % de ses dépenses militaires en 2023 par la nécessité de contrer la guerre hybride «déclenchée par l'Occident». La Chine, pour sa part, a fait des opérations d'influence, aussi appelées «guerre cognitive» dans le milieu militaire, une composante clé de sa doctrine afin de compenser le manque d'expérience de ses forces en matière de combat armé.

Beaucoup pensent que l'utilisation des technologies de l'information renforce l'efficacité de ces agressions hybrides.

Un bilan décevant

Contrairement aux craintes, cependant, les opérations de guerre hybride enregistrées jusqu'ici affichent un bilan plutôt modeste. La plus grande réussite en la matière serait, de loin, la prise de contrôle de la Crimée par la Russie en 2014. Cependant, les dernières recherches ont conclu que les cyberopérations et les campagnes de désinformation sur les réseaux sociaux n'avaient joué aucun rôle dans cette victoire. En réalité, il s'agissait plutôt d'une opération de subversion traditionnelle sans aucune cybercomposante, impliquant des acteurs téléguidés tels que des groupes religieux marginaux que des agents de Moscou conditionnaient depuis des années. À l'inverse, la cyber-action contre l'Ukraine entreprise ensuite par la Russie n'a pas produit de gains stratégiques mesurables. La révolution technologique attendue dans le déroulement des conflits ne se confirme donc pas.

Au contraire, si la guerre hybride permet aux États d'atteindre des objectifs stratégiques qui étaient hors de portée auparavant sans entrer en guerre, l'analyse logique de la «guerre hybride» menée par la Russie contre l'Ukraine depuis 2014 tend à montrer qu'il s'agit d'un échec puisque Moscou a ensuite lancé une invasion massive en 2022. Cette escalade pourrait s'expliquer par le fait que le Kremlin n'a pas réussi à atteindre ses objectifs stratégiques, notamment le premier d'entre eux qui consistait à faire abandonner à Kyiv sa politique étrangère pro-occidentale. La principale attente des théoriciens de la guerre hybride est ainsi démentie par le conflit même qui a contribué à populariser ce concept. Si la Russie est entrée en guerre, c'est justement parce que l'agression en zone grise a échoué.

On pourrait même soutenir que Moscou ne pouvait pas atteindre ses objectifs stratégiques par la guerre hybride seule. Cela relèguerait la guerre hybride au rang de conflit en zone grise «traditionnel», vidant ainsi le concept de son contenu. La crainte de la guerre hybride reste pourtant très présente. De fait, la théorie russe de la victoire s'appuyait initialement sur des moyens «hybrides» tels que des cellules dormantes, la corruption de fonctionnaires locaux et le recours à des commandos. Or, cette stratégie s'est heurtée à la résistance inattendue de l'Ukraine. L'efficacité de la résistance ukrainienne défie, de surcroît, les craintes que les menaces hybrides affaiblissent la cohésion des sociétés et leur capacité à résister aux agressions sur la durée.

Il serait même possible d'affirmer que l'entêtement de la Russie à poursuivre son agression a renforcé la résilience de l'Ukraine en «formant» notamment ses défenseurs à lutter contre les cyberattaques. Bien sûr, l'Ukraine a également bénéficié d'une grande aide de la part de ses partenaires occidentaux. Cependant, si les ressorts précis de la capacité de résistance ukrainienne restent à étudier en profondeur, force est de constater qu'il n'existe pas de preuve irréfutable de l'efficacité des opérations de guerre hybride. Et cette situation n'est pas propre à l'Ukraine.

En 2007, des groupes de pirates informatiques russes ont mis sur pied une série de cyberattaques visant à perturber le fonctionnement de différentes organisations estoniennes en représailles au retrait d'une statue soviétique dans une ville du pays. À l'époque, l'opération a été décrite comme marquant l'avènement de la cyberguerre et illustrant la gravité de la menace à laquelle les sociétés occidentales étaient exposées. Pourtant, ces attaques n'ont eu que peu d'impact mesurable sur l'économie, les pouvoirs publics ou la société du pays balte. Il aurait donc été plus juste de les considérer comme des nuisances passagères. Au lieu d'affaiblir l'Estonie, l'agression a galvanisé sa résilience et contribué directement à la création par l'OTAN du Centre d'excellence pour la cyberdéfense en coopération à Tallinn, la capitale du pays. Ce centre a considérablement renforcé les cybercapacités de l'État balte, mais également celles de l'Alliance.

L'ingérence de la Russie dans les élections présidentielles de 2016 aux États-Unis constitue un exemple plausible d'opération de guerre hybride réussie. Moscou a eu recours à une stratégie associant plusieurs instruments: des cyberopérations pour pirater et faire fuiter des e-mails de la Convention nationale démocrate et du directeur de campagne d'Hillary Clinton, John Podesta, de la désinformation sur les réseaux sociaux pour influencer l'électorat et exacerber la polarisation, ainsi que des méthodes traditionnelles de subversion consistant à placer des actifs dans la campagne de Donald Trump et dans l'administration constituée par la suite. La Russie aurait ainsi contribué à la victoire électorale de son candidat favori. Les nombreux titres alarmistes, les avertissements sévères

émanant des responsables politiques et une flopée d'études universitaires recensant de prétendus réseaux de trolls sur les réseaux sociaux laissent penser que cette opération a été une grande réussite. Pourtant, malgré le vif intérêt suscité par l'affaire et les recherches menées sur le sujet, aucun élément probant n'indique que ces activités russes ont eu une incidence mesurable sur l'issue de l'élection. En réalité, une étude récente de l'Université de New York a montré que l'exposition aux opérations d'influence russes via Twitter n'a modifié ni les points de vue, ni les comportements de vote. L'analyse des activités de guerre hybride menées par la Russie ces dix dernières années fait état d'un manque frappant de preuves claires quant à leur efficacité, alors même que leurs limites sont de plus en plus évidentes.

Une analyse plus systématique

Cette situation souligne l'urgence d'analyser de façon plus systématique l'intérêt et le rôle stratégique des divers instruments situés en zone grise et communément regroupés sous le concept de guerre hybride. Dans un premier temps, il apparaît essentiel d'identifier et de distinguer ces différents instruments. En effet, il existe de nombreux types d'opérations et autant d'impacts associés.

Premier instrument notable, les opérations d'influence visant à modifier l'opinion publique et la façon dont les dirigeants politiques sont perçus. L'objectif est de manipuler les processus de décision et les résultats politiques, ainsi que de saborder la confiance et la cohésion au sein de la société. Le sabotage constitue un deuxième instrument. Il consiste à dégrader et endommager des infrastructures et des capacités matérielles. L'objectif est d'affaiblir l'adversaire et de faire pencher le rapport de force en sa propre faveur. Enfin, la subversion constitue un moyen spécifique d'atteindre certains de ces objectifs en infiltrant de manière ciblée des sociétés et des institutions adverses. Les cyberopérations peuvent être considérées comme de nouveaux instruments de subversion. Outre l'influence et le sabotage, la subversion peut également servir des objectifs plus ambitieux tels que le renversement d'un gouvernement, soit par un coup d'État interne, soit par une révolution, armée ou non. Ce levier constitue un instrument de pouvoir particulièrement puissant, car il permet de modifier les préférences sous-jacentes d'un État afin de les mettre en accord avec ses propres intérêts d'une façon bien plus profonde que par la coercition militaire. La révolution armée met d'ailleurs en lumière un quatrième type d'instrument, à savoir l'usage clandestin ou dissimulé de la force. Lors des opérations clandestines, c'est l'activité elle-même qui est secrète. L'opération furtive menée par les États-Unis pour tuer Oussama ben Laden en est une illustration. La dissimulation, quant à elle, consiste à masquer l'identité de l'agresseur, par exemple en déployant des soldats sans insigne tels que les tristement célèbres «petits hommes verts» russes en Crimée.

Une fois l'instrument identifié, il convient de déterminer les objectifs stratégiques plus larges de l'adversaire, puis d'examiner attentivement les éléments démontrant la capacité réelle de cet instrument à servir ces objectifs. Enfin, sur la base de ces éléments, une analyse systématique des conditions pouvant assurer la réussite des différents instruments permet de préciser l'ampleur de la menace.

Des enseignements historiques

Pour les responsables politiques, le premier défi de la lutte contre la guerre hybride consiste à distinguer la réalité de la fiction. Bien entendu, ils doivent se préparer à toute éventualité et examiner tous les scénarios, qu'ils soient passés ou hypothétiques. Cependant, la manière la plus réaliste de prévoir ce qui pourrait se produire à l'avenir est de tirer les enseignements des événements passés. Les résultats concrets des opérations de guerre hybride menées jusqu'ici offrent donc des repères utiles pour contrer les futures menaces. Or, l'analyse des situations passées, y compris d'exemples historiques tels que les opérations secrètes conduites pendant la guerre froide, donne des raisons de se montrer confiant. La crainte d'opérations d'influence et de sabotage n'a rien de nouveau. Au contraire, elle est au cœur des préoccupations des responsables politiques et militaires occidentaux depuis un certain temps déjà. Heureusement, cette crainte n'a pas toujours été justifiée.

Un rapport publié en 1981 par le Département d'État américain sur les «mesures actives» de l'URSS en fournit un exemple instructif. Il indique que l'expertise accumulée au fil des décennies par le KGB dans la mise en place de mesures actives (terme employé à l'époque pour désigner la guerre hybride), associée à l'ouverture des systèmes médiatiques et politiques occidentaux, a créé un environnement propice aux opérations d'influence et de subversion russes. Sur ce fondement, le rapport dresse un tableau pessimiste des menaces qui pesaient alors sur les sociétés occidentales. Pourtant, comme nous le savons, l'URSS s'est effondrée peu de temps après. La situation actuelle est sans doute relativement similaire. Les craintes des responsables politiques et militaires face aux opérations d'influence et de subversion soviétiques pendant la guerre froide reposaient essentiellement sur ce qui pourrait se produire, sans tenir compte des obstacles de taille qui pouvaient empêcher l'URSS d'obtenir les effets escomptés dans la pratique. Il en va de même pour la perception et l'évaluation des menaces concernant les cyberopérations et les campagnes de désinformation sur les réseaux sociaux. Des études récentes montrent que la grande majorité des opérations de subversion visant à renverser des régimes ont été des échecs. En parallèle, les lacunes des cyberopérations sont de plus en plus évidentes. Heureusement, tout ce qui est possible en théorie ne l'est pas en pratique.

> Une analyse plus systématique des divers instruments situés en zone grise, regroupés sous le concept de guerre hybride, est urgente.

Lectures complémentaires

Chiara Libisller, **"'Hybrid Warfare" as an Academic Fashion,"** *Journal of Strategic Studies* 46:4 (2023), pp. 1–23.

Rory Cormac / Richard J. Aldrich, **"Grey Is the New Black: Covert Action and Implausible Deniability,"** *International Affairs* 94:3 (2018), pp. 477–94.

Christopher S. Chivvis, **"Hybrid War: Russian Contemporary Political Warfare,"** *Bulletin of the Atomic Scientists* 73:5 (2017) pp. 316–21.

Arsalan Bilal, **"NATO Review – Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote,"** *NATO Review,* 30.11.2021.

Mark Galeotti, **"Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?,"** *Small Wars & Insurgencies* 27:2 (2016) pp. 282–301.

Lennart Maschmeyer, **"The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations,"** *International Security* 46:2 (2021) pp. 51–90.

Des motifs d'optimisme

En outre, certains éléments montrent clairement que les opérations d'influence peuvent susciter des retours de bâton non souhaités. Les experts comparent les opérations de subversion, d'influence et de désinformation à l'injection d'un virus dans le système sanguin de l'ennemi. Or, comme pour un vrai virus, il existe un risque réel de propagation hors de la société ciblée. Les archives Mitrokhine (un recueil de notes sur les opérations du KGB dévoilé par l'ancien agent Vassili Mitrokhine lorsqu'il a fait défection) font état d'une paranoïa croissante parmi les dirigeants du KGB pendant la guerre froide concernant d'éventuels traîtres dans les rangs de l'organisation et montrent les efforts et les moyens financiers croissants déployés pour les traquer et les punir. Ces efforts ont fini par entraver la mission principale du KGB, qui était d'affaiblir les États-Unis. Il existe ainsi de nombreux exemples de situations où les dirigeants du KGB, et par extension les dirigeants de l'URSS, ont cru à leur propre propagande et pris des décisions politiques aux conséquences néfastes. La décision d'envahir la Tchécoslovaquie en 1968 en est une illustration. Les dirigeants de l'URSS pensaient une contre-révolution imminente et s'attendaient à ce que l'opinion publique soutienne massivement leur intervention – deux éléments qui n'existaient que dans la propagande soviétique. Cette occupation censée être temporaire a alors dû perdurer jusqu'à la fin de la guerre froide. L'invasion de l'Ukraine par la Russie, dont les troupes s'attendaient à «libérer» le pays avec le soutien de l'opinion publique, rappelle cette situation. De fait, les analystes s'accordent de plus en plus à dire que Vladimir Poutine, qui a limogé de son administration tous ceux ne faisant pas preuve d'une loyauté absolue, a été mal informé et a eu tendance à croire la propagande russe. Sans accès au Kremlin, cela reste difficile à prouver.

De manière peut-être contrintuitive, les systèmes fermés et autocratiques peuvent s'avérer plus vulnérables aux retours de bâton et aux dysfonctionnements que les systèmes ouverts et démocratiques. Si l'ouverture des systèmes démocratiques facilite les opérations d'influence, la cohabitation d'une multitude de sources d'information et de récits concurrents au sein de la sphère publique offre la possibilité de déminer et de contrer la désinformation. Pour cela, il faut bien sûr que l'écosystème médiatique fonctionne correctement – ce que la polarisation rend de plus en plus compliqué. Dans les systèmes autocratiques fermés, les sources d'information alternatives et les récits concurrents sont généralement bien moins nombreux. De tels systèmes sont donc très susceptibles de tomber dans le piège des campagnes de manipulation et de désinformation qu'ils orchestrent eux-mêmes. Ces différences structurelles présentent des forces et des faiblesses dont il faut tenir compte. L'analyse tend à montrer que les systèmes démocratiques ont un avantage relatif, ce qui devrait être source d'optimisme dans la lutte contre la désinformation et les opérations d'influence.

> Les systèmes fermés et autocratiques peuvent s'avérer plus vulnérables aux retours de bâton et aux dysfonctionnements que les systèmes ouverts et démocratiques.

Même si la guerre hybride est moins efficace qu'on le pense généralement, elle constitue néanmoins une menace de taille. Il convient donc de ne pas l'ignorer. Au contraire, l'élaboration de contre-stratégies efficaces nécessite une analyse plus systématique des instruments employés et des moyens de les neutraliser. D'une part, cela implique de reconnaître la place que continuent d'occuper les opérations d'influence, de sabotage et de subversion traditionnelles (c'est-à-dire non soutenues par les technologies) et de hiérarchiser les réponses en conséquence. D'autre part, il est également essentiel de tenir compte de l'héritage stratégique des instruments de zone grise associés à la guerre hybride. Ces instruments ne sont pas aussi nouveaux qu'ils en ont l'air. Il peut donc s'avérer utile de s'appuyer sur les stratégies de contre-espionnage passées et les enseignements qui en ont été tirés. Dans ce contexte, il est notamment important de prendre en compte la logique de la tromperie et son intérêt aussi bien offensif que défensif. L'un des principaux défis à relever réside dans le fait que les campagnes intégrées, qui se composent d'un éventail d'instruments de zone grise (aussi bien traditionnels que cyber) nécessiteront une réponse intégrée qui doit dépasser les silos institutionnels et doctrinaux actuels.

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

Lennart Maschmeyer est Senior Researcher au Center for Security Studies (CSS) à l'ETH de Zurich ou il travaille sur le cyber conflit, les politiques de pouvoir et la subversion.

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.

Éditrice: Névine Schepers
Relecture: Névine Schepers
Layout et graphiques: Miriam Dahinden-Ganzoni

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

Parus précédemment:

Le rôle des structures d'appui à la médiation No 331
Le maintien de la paix des Nations Unies No 330
La planification de la Bundeswehr No 329
La gestion des coûts liés aux catastrophes No 328
L'Asie centrale et la rivalité entre grandes puissances No 327
Promesses et paradoxes de la diplomatie scientifique No 326

ISSN: 2296-0228; DOI: 10.3929/ethz-b-000639170