diploweb.com La revue géopolitique
ISSN : 2111-4307

Les menaces hybrides : quels enjeux pour nos démocraties ?

mercredi 24 janvier 2024,par Estelle HOORICKX

Citer cet article / To cite this version :
Estelle HOORICKX, **Les menaces hybrides : quels enjeux pour nos démocraties ?**, *Diploweb.com : la revue géopolitique, 24 janvier 2024.*

Hum... Vous semblez apprécier le DIPLOWEB.COM. Nous vous en remercions et vous invitons à participer à sa construction.

Le DIPLOWEB.COM est LE media géopolitique indépendant en accès gratuit, fondé en l'an 2000. Nous vous proposons de participer concrètement à cette réalisation francophone de qualité, lu dans 190 pays. Comment faire ? Nous vous invitons à verser un "pourboire" (tip) à votre convenance via le site **https://fr.tipeee.com/diploweb** . Vous pouvez aussi rédiger un chèque à l'ordre du DIPLOWEB.COM et l'adresser à Diploweb.com, Pierre Verluise, 1 avenue Lamartine, 94300, Vincennes, France. Ou bien encore faire un virement bancaire en demandant un RIB à l'adresse expertise.geopolitique@gmail.com.

Avec 5 000€ par mois, nous pouvons couvrir nos principaux frais de fonctionnement et dégager le temps nécessaire à nos principaux responsables pour qu'ils continuent à travailler sur le DIPLOWEB.COM.
Avec 8 000€ par mois, nous pouvons lancer de nouveaux projets (contenus, événements), voire l'optimisation de la maquette du site web du DIPLOWEB.COM.

Les menaces hybrides : de quoi parle-t-on ? Quels sont les outils hybrides de plus en plus nombreux et diversifiés qui nous menacent ? Quels sont les principaux acteurs des attaques hybrides ? Estelle Hoorickx fait œuvre utile en précisant les concepts, les stratégies et les moyens utilisés pour nuire aux démocraties en les polarisant à outrance. Les défis sont considérables. Seul un effort durable et conjugué de l'UE et des autres démocraties, impliquant l'ensemble des sociétés civiles, peut produire des effets bénéfiques sur le long terme.

Ce document s'inspire de l'analyse personnelle présentée par l'autrice aux membres de la direction générale de la sécurité et de la protection du Parlement européen (DG SAFE) le 7 décembre 2023, à l'occasion de son dixième anniversaire. Il est publié en anglais sous le titre "*Hybrid Threats : What are the Challenges for our Democracies ?*" dans l'IRSD e-Note 54, janvier 2024. Le lien est indiqué en pied de page.

QUELLES sont les principales menaces hybrides auxquelles nous devons faire face aujourd'hui et vis-à-vis desquelles nous devrons nous prémunir demain pour préserver nos démocraties ? Question cruciale à laquelle il est pourtant difficile de répondre. Ne vaudrait-il d'ailleurs pas mieux parler d'attaques hybrides plutôt que de « menaces hybrides » ? Dans le contexte actuel – où les conflits sont de plus en plus dématérialisés –, les attaques hybrides sont en effet devenues continues, sans que nous en ayons nécessairement conscience. Comme le souligne très justement Nathalie Loiseau, députée française au Parlement européen, il est en effet « difficile de savoir où s'arrête la paix quand la guerre de l'information fait rage en permanence ». [1] En d'autres termes, et sans vouloir être alarmiste, nous sommes toutes et tous, potentiellement, en guerre. Une cyberattaque ou une campagne de désinformation peut en effet avoir des conséquences létales.

Estelle Hoorickx
Air force Senior Captain (OF-3) Estelle Hoorickx, PhD is a research fellow at the Centre for Security and Defence Studies (CSDS), within the Belgian Ministry of Defence.
Commandante d'aviation, PhD Estelle Hoorickx est chercheuse au Centre d'études de sécurité et défense (CESD) du ministère de la Défense belge.

Depuis une dizaine d'années, les « attaques hybrides » à l'encontre de nos pays occidentaux se sont intensifiées mais également diversifiées. Des « acteurs étrangers, malveillants et autoritaires, étatiques ou non, parmi lesquels la Russie et la Chine » [2], recourent à ces pratiques pour nuire à l'Union européenne (UE) et à ses États membres, saper la confiance de

l'opinion publique dans les institutions gouvernementales, empêcher le débat démocratique, attaquer nos valeurs fondamentales et exacerber la polarisation sociale. [3] Nos démocraties – caractérisés par un accès à une information pluraliste, ouverte et largement diffusée – sont particulièrement **vulnérables aux campagnes de désinformation mais également aux tentatives d'ingérences étrangères**.

Le mythe de la fin de l'histoire qui annonçait le triomphe de la démocratie libérale après l'effondrement du bloc soviétique fait définitivement partie du passé. En 2023, seuls 8 % de la population mondiale vivent dans une démocratie pleine et entière. [4] La brève « pax americana » a bel et bien vécu et entérine le retour d'un nouveau bras de fer non plus entre l'Est et l'Ouest mais plus largement entre « l'Ouest » et le « reste » de la planète, selon la formule de la géopoliticienne Angela Stent. [5] En témoignent les récents événements en Ukraine mais également en Israël, qui révèlent une fois encore la perte d'influence des pays occidentaux sur les enjeux de gouvernance internationale. [6] L'Occident conserve néanmoins un certain attrait auprès des populations non occidentales, ce qui déplaît fortement à certains régimes autoritaires en quête de puissance. [7]

Avant d'analyser plus en détails les menaces hybrides et les enjeux qui y sont liés, il convient de faire un petit rappel historique et sémantique sur la réalité de ces menaces dont on parle de plus en plus mais qui restent souvent mal comprises. **Avec les années, le terme « hybride » a en effet évolué** et s'est quelque peu éloigné de sa signification originelle. Certains estiment même que cette notion a tendance à devenir une terminologie « fourre-tout ». [8] Il est vrai que le concept est finalement « presque aussi ambigu que les situations qu'il veut décrire sont incertaines ». [9]

Les menaces hybrides : de quoi parle-t-on ?

Dans les dictionnaires de référence, le terme « hybride » renvoie à ce qui est composé de deux éléments de nature différente anormalement réunis. Cet adjectif est d'ailleurs associé à des registres aussi divers que la biologie, l'agriculture ou la linguistique. Ce n'est qu'au début des années 2000 que l'adjectif « hybride » est pour la première fois utilisé en association avec un conflit armé. La « guerre hybride » désigne alors une opération militaire qui combine des tactiques régulières et irrégulières. Selon d'autres théoriciens militaires, « la guerre hybride » combine à la fois du « *hard power* » (par des mesures de coercition) et du « *soft power* » (par des mesures de subversion). Enfin, selon une terminologie très otanienne, la guerre hybride consiste à agir sur l'ensemble du « front DIMEFIL », c'est-à-dire sur les fronts diplomatique, informationnel, militaire, économique et financier, mais également sur le front du renseignement et celui du droit. [10]

Si la notion de « guerre hybride » est donc utilisée pour la première fois au début des années 2000 par des officiers américains à propos de l'« insurrection tchétchène » puis de la guerre en Irak, l'UE dévoile sa première définition de la « guerre hybride » en mai 2015. Sans nommer la Russie, cette définition décrit alors les tactiques militaires et non militaires utilisées par Moscou pour dominer politiquement la Crimée, tout en générant de l'ambiguïté concernant l'origine des attaques. En Crimée, le Kremlin a en effet eu recours à une panoplie d'outils hybrides, tels que des cyberattaques, des campagnes de désinformation, les désormais fameux « petits hommes verts » (soldats sans insignes qui ne pouvaient pas être clairement identifiés) ou des « proxys » (forces agissant par procuration pour Moscou). En somme, le Kremlin a eu

recours à toutes sortes de modes opératoires qui lui permettaient de générer des effets stratégiques sans avoir à subir les conséquences d'une opération militaire en bonne et due forme. [11]

En novembre 2015, peu de temps après les attaques terroristes particulièrement sanglantes dont la France a fait l'objet, l'OTAN propose à son tour une définition de la guerre hybride qui précise, pour la première fois, que celle-ci peut être menée non seulement par des acteurs étatiques mais également par des acteurs non étatiques. À l'époque, beaucoup considèrent en effet que l'État islamique (également appelé « Daesh ») constitue la « forme la plus aboutie de l'ennemi hybride ». [12] On estime alors que Daesh est passé maître dans ce qu'on appelle alors la « techno-guérilla » : il combine l'usage du terrorisme et de la guérilla avec des technologies avancées, également utilisées par les armées dites « régulières », tels que les drones, les missiles anti-char et les réseaux sociaux, qui permettent à l'État islamique de mener une guerre psychologique particulièrement efficace. [13]

> Les objectifs poursuivis par les auteurs des « activités hybrides » consistent notamment à renforcer leur influence et à saper la confiance de l'opinion publique dans les valeurs fondamentales et les institutions démocratiques de l'UE et de ses États membres.

Depuis 2016, l'UE préfère utiliser le terme de « menace(s) hybride(s) » plutôt que celui de « guerre hybride », terme adopté par l'OTAN dès 2014, année de l'invasion de la Crimée par la Russie. [14] Depuis 2018, l'UE précise que les objectifs poursuivis par les auteurs des « activités hybrides » consistent notamment à renforcer leur influence et à saper la confiance de l'opinion publique dans les valeurs fondamentales et les institutions démocratiques de l'UE et de ses États membres. [15]

D'après les documents stratégiques les plus récents de l'UE, les acteurs étatiques (ou non étatiques) qui recourent à ce genre de pratiques vont tenter de garder leurs activités en dessous de ce qui leur paraîtra être un seuil au-delà duquel ils déclencheraient une réponse coordonnée (y compris militaire et/ou juridique) de la communauté internationale. Pour ce faire, ils ont recours, souvent de manière « très coordonnée », à une panoplie de modes opératoires (ou d'« outils » [16]) conventionnels et non conventionnels qui leur permettent d'exploiter les vulnérabilités de la cible visée et de créer de l'ambiguïté sur l'origine (ou l'« attribution ») de l'attaque. [17] Certains préfèrent d'ailleurs parler de « guerre du seuil », de « guerre ambiguë » ou de « guerre liminale » (*liminal warfare*, guerre à la limite de la perception) plutôt que de parler de « guerre hybride ». [18]

Les attaques hybrides permettent de rester dans une « zone grise » (entre guerre et paix) et d'éviter une confrontation militaire directe (et les coûts économiques et humains qui vont avec), le risque d'une action militaire ouverte n'étant pas exclu. [19] Une campagne hybride peut en effet se dérouler en plusieurs phases : tout d'abord, la mise en place discrète de la menace (« *the priming phase* »), qui peut se traduire par des campagnes d'ingérences, la mise en place de dépendances économiques et énergétiques, l'élaboration de normes juridiques dans des instances internationales afin de défendre ses propres intérêts. Puis, cette campagne hybride peut entrer dans une phase plus agressive et plus visible de déstabilisation, où

l'attribution des faits devient plus nette. Cette phase se traduit par différentes opérations et campagnes hybrides, telles que des campagnes de propagande – plus virulentes cette fois –, une augmentation des cyberattaques ou des attaques contre des infrastructures critiques (y compris dans l'espace). Cette phase de déstabilisation vise à forcer une décision et/ou renforcer la vulnérabilité de l'adversaire (en favorisant la polarisation sociale ou les dissensions interétatiques par exemple). Cette deuxième phase fait généralement suite à une situation géopolitique particulière : des élections, des sanctions politiques, des accords internationaux ou la mise en place d'alliances. Enfin, cette étape de déstabilisation peut mener à une troisième et dernière phase qui est celle de la coercition, de l'escalade : on passe alors d'une menace hybride à une véritable guerre hybride où l'usage de la force devient central (et non plus superflu), mais où l'« attribution » de l'attaque reste compliquée, ambiguë. [20]

L'invasion de la Crimée par la Russie en 2014 reste le meilleur exemple de ce que peut être une guerre hybride : une kyrielle d'outils hybrides sont utilisés, y compris l'outil militaire, mais l'attribution de la guerre reste ambiguë. *A contrario*, la guerre qui a lieu en Ukraine depuis février 2022, même si elle a été précédée par une phase de déstabilisation, n'est pas une guerre hybride en tant que telle mais bien une guerre de haute intensité, dont l'auteur – à savoir la Russie – est clairement identifié, même lorsqu'il a recours à des outils hybrides telles que des cyberattaques, des campagnes de propagande et de désinformation ainsi que des attaques sur les infrastructures critiques.

La stratégie hybride est désormais perçue, à juste titre, comme un « multiplicateur de forces » (« *force multiplier* »), même face à un adversaire qui aurait le dessus, puisqu'elle s'emploie à réduire le risque d'une réaction militaire. [21] Les attaques hybrides semblent d'ailleurs « soigneusement calibrées » pour ne pas remplir les conditions visées dans la clause d'assistance mutuelle du traité sur l'UE (article 42§7 TUE) et dans l'article 5 du traité de l'Atlantique Nord. [22] L'assimilation d'une ou de plusieurs « menace(s) hybride(s) » à une « attaque armée » n'est en effet pas chose aisée. [23]

En définitive, selon l'UE, quatre éléments importants caractérisent aujourd'hui la stratégie hybride : 1) son côté « hybride », puisqu'elle recourt à la fois à des éléments conventionnels et non conventionnels ; coercitifs ou non coercitifs (subversifs) ; 2) son côté ambigu : les auteurs d'une attaque hybride essaient, dans la mesure du possible, d'atteindre leurs objectifs en passant « en dessous des radars » [24] afin d'empêcher toute réaction ; 3) sa finalité stratégique, puisque la stratégie hybride vise essentiellement à nuire et/ou affaiblir les sociétés démocratiques afin de renforcer l'influence de celui qui s'en sert ; 4) son côté évolutif : on peut passer du stade de menaces hybrides à celui de guerre hybride.

Autrement dit, si une attaque hybride est toujours le fruit d'une combinaison d'outils, toutes les combinaisons ne donnent pas nécessairement une campagne hybride. [25] Ainsi par exemple, une cyberattaque isolée réalisée par un *hacker* isolé afin d'obtenir une rançon n'est pas une attaque hybride. Des campagnes de propagande combinées à des actes terroristes revendiqués ne constituent pas non plus une attaque hybride puisque l'auteur des faits est clairement identifié et que le but ultime de l'opération est de provoquer la terreur.

Des outils hybrides de plus en plus nombreux et diversifiés

Le recours à certains outils hybrides – propagande, sabotage, guerre par procuration –, même de façon combinée, est aussi ancien que la guerre. En réalité, **ce qui a changé c'est surtout le contexte géopolitique qui est devenu plus complexe, plus incertain et plus « flou »** [26], et qui *de facto* favorise, depuis une dizaine d'années, le développement rapide et la diversification de ces outils hybrides. Les nouvelles technologies – telles que l'intelligence artificielle ou les réseaux sociaux – mais également les relations d'interdépendance – financières, énergétiques, alimentaires, technologiques et cognitives – qui existent entre les États favorisent et amplifient l'usage des outils hybrides. En outre, les effets des attaques hybrides sont de plus en plus directs et sévères, alors que paradoxalement ces attaques ne sont pas plus faciles à « attribuer », et ce malgré l'évidence de certains faits.

Ainsi par exemple, la Boussole stratégique considère désormais « l'instrumentalisation de la migration irrégulière, l'utilisation stratégique du droit ainsi que la coercition ciblant notre sécurité économique et énergétique » comme des menaces hybrides. Le document précise en outre que les « activités de manipulation de l'information et d'ingérences menées depuis l'étranger » (ou « FIMI » [27]) sont aussi des menaces hybrides, qui peuvent être particulièrement dangereuses pour nos démocraties. [28] Elles visent en effet à influencer les débats sociétaux, introduire des clivages et interférer avec les processus de prise de décisions démocratiques. [29] **Les sujets polarisants de nature à susciter énervements et radicalité**, – tels que ceux liés aux changements climatiques et aux questions du genre, des minorités ou de l'immigration – sont dès lors des cibles privilégiées par les « acteurs FIMI ». [30]

Quels sont les principaux acteurs des attaques hybrides ?

Si les acteurs étatiques et non étatiques ayant recours aux outils hybrides sont de plus en plus nombreux [31], la Russie de Vladimir Poutine reste actuellement un des acteurs principaux de la stratégie hybride, dont on retrouve des éléments dès 2013 dans la fameuse « doctrine Gerasimov ». Ce document insiste en effet sur la nécessité pour la Russie de recourir, dans les conflits actuels, à des instruments autres que la puissance militaire afin de répondre à la guerre non linéaire menée par les Occidentaux. [32]

> Le président russe semble s'être fixé un double objectif : « ne plus laisser reculer l'influence russe ni avancer l'attrait pour l'Ouest ».

Depuis le fameux discours de Vladimir Poutine prononcé à Munich en 2007 – dans lequel il dénonce « la domination de l'Occident sur l'ordre mondial postbipolaire » [33] –, le président russe semble s'être fixé un double objectif : « ne plus laisser reculer l'influence russe ni avancer l'attrait pour l'Ouest ». [34] Concrètement, cela se traduit par des attaques hybrides massives (cyberattaques et campagnes informationnelles en particulier) à l'encontre de l'Estonie en 2007, de la Géorgie en 2008 et surtout, dès 2014, de l'Ukraine. [35] En outre,

depuis février 2022, on assite au premier conflit de haute intensité qui s'accompagne, en temps réel, d'attaques sur les terrains numérique et informationnel, y compris dans l'espace (en témoigne l'attaque du satellite KA-SAT le jour même de l'invasion). [36] La guerre hybride du Kremlin s'étend également à d'autres États partenaires de l'UE, tels que la Moldavie. Ce pays, dont la candidature à l'UE a été accordée en juin 2022, est en effet victime de campagnes de désinformation massives, d'opérations de sabotage mais également de chantage énergétique concernant son approvisionnement en gaz. [37]

Les pays de l'UE ne sont évidemment pas épargnés : cyberattaques, campagnes de désinformation, ingérence directe dans les élections et dans les processus politiques. [38] Certains États européens – tels que la Pologne et la Finlande – accusent également Moscou et son allié biélorusse d'instrumentaliser les flux d'immigration irrégulière à des fins d'intimidation et de déstabilisation. [39] Ainsi par exemple, les foules de migrants auxquelles a été confrontée la Pologne en 2021 étaient encadrées, dirigées et parfois molestées par des hommes cagoulés et en tenue militaire indéterminée (ce qui fait d'ailleurs fortement penser aux « petits hommes verts » vus en Crimée il y a sept ans). [40]

Les opérations de sabotage des infrastructures critiques – câbles sous-marins et gazoducs en particulier – font également partie des nouveaux modes opératoires hybrides, puisqu'elles permettent à leurs auteurs de « passer sous les radars » tout en mettant à mal la sécurité économique et énergétique des pays visés. Parmi les exemples récents, citons notamment les explosions sur les gazoducs Nord Stream ou, plus récemment encore, l'endommagement du gazoduc et du câble de télécommunications reliant l'Estonie et la Finlande. [41]

Notons enfin que certaines campagnes hybrides qui visent les démocraties en dehors du continent européen peuvent aussi avoir des conséquences sur la stabilité de l'UE et de ses États membres ; en témoignent les campagnes de désinformation et d'ingérence étrangères russes en Afrique subsaharienne, qui ont contribué en partie non seulement aux récents coups d'État au Mali, au Burkina Faso et au Niger mais également à la perte d'influence de la France dans la région. [42]

La Chine fait également partie des pays dont la stratégie hybride préoccupe de plus en plus l'UE et ses États membres. [43] L'Europe est en effet devenue « un des principaux théâtres d'opérations de la grande stratégie chinoise » [44] de Xi Jinping, qui vise à faire de la Chine un « leader global en termes de puissance nationale et d'influence internationale d'ici 2049 », date hautement symbolique pour la République populaire de Chine (puisqu'elle célèbrera les 100 ans de sa naissance). [45]

La « Nouvelle route de la soie » – ce vaste programme de développement des infrastructures de transport visant, depuis 2013, à relier la Chine et le reste du monde par la construction d'immenses segments routiers, ferroviaires et maritimes, spatiaux et cyberspatiaux – constitue la forme la plus visible de cette grande stratégie visant à répondre aux énormes besoins de la Chine et de sa croissance, au point que certains qualifient désormais cette dernière d'« Empire du besoin ». Cette route permet en effet le transfert vers la Chine de toutes les ressources naturelles, semi-finies, financières, intellectuelles et humaines dont « l'Empire du Milieu » a besoin pour mener à bien sa grande stratégie de développement. C'est dans ce cadre que l'Europe est devenue un « espace utile » pour Pékin – autrement dit un espace pour répondre au système de besoins propre à la Chine contemporaine. Contrairement à certaines idées

reçues, la « Nouvelle route de la soie » – ou *Belt and Road Initiative* (BRI) » – ne vise donc pas en priorité à diffuser un « modèle chinois » au reste du monde. [46]

C'est dans ce contexte qu'il faut comprendre les investissements chinois dans le domaine portuaire européen (port du Pirée en Grèce et port d'Hambourg en Allemagne, en particulier), mais également dans le domaine de la recherche (via notamment le programme d'échange scientifique des « Mille talents » ou le déploiement d'instituts Confucius en Europe) ou encore ses investissements dans les domaines des télécommunications et de la 5 G. Tous ces investissements et opérations d'influence, de lobbying, voire d'espionnage en Europe constituent autant de leviers (ou d'« outils hybrides ») que Pékin peut utiliser au détriment des intérêts européens. [47] On se rappelle en décembre 2021, dans le contexte du rapprochement diplomatique de Vilnius avec Taïwan, l'épisode des containers arrivant de Lituanie qui n'étaient plus autorisés à entrer dans les ports chinois en raison de problèmes techniques inopinés. [48]

Certains estiment que, sur le long terme, la menace géopolitique la plus grave proviendra de Pékin et non de Moscou. Pour reprendre les propos du patron du renseignement intérieur allemand, Thomas Haldenwang, « si la Russie est la tempête, la Chine est le changement climatique ». [49]

Pour atteindre ses objectifs, la Chine ne cache en tout cas pas sa volonté de recourir à ce qu'elle appelle la doctrine des « trois guerres » (*Three Warfares*), adoptée en 2003, et qui envisage la guerre sous les angles psychologique, médiatique et juridique. [50] La « guerre dite psychologique » consiste à influencer et perturber les capacités de décision et d'action de l'adversaire par le biais de pressions diplomatiques et économiques et de campagnes de désinformation. La « guerre médiatique (ou de l'opinion publique) » vise quant à elle à influencer et conditionner les perceptions à travers les médias tant chinois qu'étrangers, ainsi qu'à travers l'édition et le cinéma. Enfin, la « guerre du droit » implique l'exploitation et la manipulation des systèmes juridiques dans le but d'obtenir des gains politiques, commerciaux ou militaires. La Chine instrumentalise par exemple le droit de la mer pour faire prévaloir ses ambitions en mer de Chine méridionale. [51]

Si la Chine n'est pas le seul pays à recourir à ce genre de stratégie hybride, certains s'inquiètent néanmoins de ce qu'ils appellent la « russianisation des opérations d'influence » chinoises, en particulier vis-à-vis de l'UE et de ses États membres. Jusqu'il y a peu, la Chine était en effet souvent présentée, contrairement à la Russie, comme un pays ne menant pas de « campagnes de désinformation agressives » dans le but d'exploiter les divisions d'une société, et n'ayant pas un champ d'application mondial (mais seulement régional). Si cela était peut-être vrai il y a quelques années, cela ne l'est plus aujourd'hui (certains parlent de diplomatie du « loup guerrier » pour décrire l'agressivité dont peuvent faire preuve certains diplomates chinois). Défendre le Parti communiste chinois (PCC) apparaît désormais plus important que gagner les cœurs et les esprits, y compris à l'égard de l'UE et de ses États membres. [52]

L'offensive de charme lancée par Pékin en Europe entre 2012 et 2016 n'a globalement pas convaincu. [53] L'UE considère en effet la Chine certes comme « un partenaire en matière de coopération », mais désormais également comme « un concurrent économique et un rival systémique ». [54] Autrement dit, et pour reprendre les termes du Haut Représentant Josep Borrell, il convient de « s'engager avec la Chine sur de nombreux fronts », mais également de

réduire les risques dans notre relation avec elle. Tâche en réalité autrement plus difficile qu'avec la Russie. En effet, si le commerce extérieur russe ne représente que 1 % du produit national brut mondial, la part de la Chine pèse vingt fois plus lourd… [55]

Conclusion

Dans un contexte géopolitique caractérisé par une nouvelle forme de rivalité entre « un Sud élargi » (ou « Sud global ») et « un Ouest qui se rétrécit » [56] et perd de son influence, l'UE doit plus que jamais continuer à renforcer sa résilience pour faire face à des attaques hybrides toujours plus nombreuses et aux effets de plus en plus directs et sévères.

Si notre économie ouverte et nos valeurs démocratiques constituent notre force et notre fierté, elles sont également une source de vulnérabilité. La pandémie de Covid-19 et l'invasion de l'Ukraine par la Russie ont mis en évidence les risques de certaines dépendances économiques. [57] **Des régimes autoritaires et des groupes haineux s'acharnent à polariser nos sociétés**, pourtant pacifiques, et rencontrent un certain succès. [58] Les périodes d'élection, de tensions sociales, de crises géopolitiques, d'urgence climatique sont autant de périodes à risque.

Si on ne peut que se réjouir des nombreux outils, documents juridiques, directives, stratégies, groupes de travail et autres commissions spéciales qui ont été mis en place par l'UE pour diminuer nos vulnérabilités face aux menaces hybrides, **les défis restent énormes**. Nos infrastructures critiques, notre économie, nos valeurs et nos outils de communication doivent être protégés et défendus. **Seul un effort durable et conjugué de l'UE et des autres démocraties, impliquant l'ensemble de nos sociétés civiles, peut produire des effets bénéfiques sur le long terme**.

Copyright Janvier 2024-Hoorickx/Diploweb.com

Plus

Cet e-Note en anglais. Estelle Hoorickx, "*Hybrid Threats : What are the Challenges for our Democracies ?*" dans l'IRSD e-Note 54, janvier 2024.

Toutes les publication de l'IRSD et du CESD

Toutes les publications de l'Institut royal supérieur de défense (IRSD) et les e-Notes du Centre d'études de sécurité et de défense (CESD).

P.-S.

Estelle Hoorickx s'exprime ici à titre personnel. Commandante d'aviation, PhD Estelle Hoorickx est chercheuse au Centre d'études de sécurité et défense (CESD), le centre de réflexion de référence spécialisé du ministère de la Défense belge.

Notes

[1] Nathalie Loiseau, *La guerre qu'on ne voit pas venir* (Paris : L'Observatoire, 2022), 453.

[2] Parlement européen, *Résolution du Parlement européen du 9 mars 2022 sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation*, 2020/2268(INI) (Strasbourg : 2022), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_FR.html.

[3] Commission européenne, *Communication conjointe au Parlement européen, au Conseil européen et au Conseil. Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides*, JOIN(2018) 16 final (Bruxelles : 2018), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52018JC0016.

[4] Economist Intelligence Unit (EIU), *Democracy Index 2022* (s.l. : Economist Intelligence Unit, 2022), https://www.eiu.com/n/campaigns/democracy-index-2022/. Depuis 2016, on dénombre davantage de démocraties en déclin que de démocraties en marche dans le monde (International Institute for Democracy and Electoral Assistance – IDEA), *The Global State of Democracy 2023. The New Checks and Balances* (Stockholm : IDEA, 2023), https://www.idea.int/publications/catalogue/global-state-democracy-2023-new-checks-and-balances.

[5] Angela Stent, *Putin's World : Russia Against the West and with the Rest* (New York : Twelve, 2019).

[6] François Polet, « Comment la guerre Israël – Hamas va accélérer la désoccidentalisation du monde, » *Le Vif*, 24 octobre 2023, https://www.levif.be/international/moyen-orient/comment-la-guerre-israel-hamas-va-accelerer-la-desoccidentalisation-du-monde/.

[7] La dernière enquête de l'ECFR (*European Council on Foreign Relations*) confirme l'attrait des populations non occidentales pour les valeurs occidentales (Timothy Garton Ash, Ivan Krastev et Mark Leonard, « Living in an à la carte world : What European policymakers should learn from global public opinion » European Council on Foreign Relations, 15 novembre 2023, https://ecfr.eu/publication/living-in-an-a-la-carte-world-what-european-policymakers-should-learn-from-global-public-opinion/).

[8] Jérôme Maire, « Stratégie hybride, le côté obscur de l'approche globale ?, » *Revue Défense Nationale*, n° 811 (septembre 2016) : 3, https://www.defnat.com/e-RDN/vue-tribune.php?ctribune=882.

[9] Nicolas Barotte, « Migrants en Biélorussie : le casse-tête stratégique des menaces " hybrides ", » *Le Figaro*, mis à jour le 13 novembre 2021, https://www.lefigaro.fr/international/le-casse-tete-strategique-des-menaces-militaires-hybrides-20211112.

[10] Estelle Hoorickx, « La Défense contre les “ menaces hybrides ” : la Belgique et la stratégie euro-atlantique, » *Sécurité & Stratégie* (Institut royal supérieur de défense), n° 131 (octobre 2017) : 3-4, https://www.defence-institute.be/publications/securite-strategie/ss-131/.

[11] Hoorickx, « La Défense contre les “ menaces hybrides ”, » 5.

[12] Joseph Henrotin, « L’État islamique, forme la plus aboutie de l’ennemi hybride ?, » *Défense & Sécurité Internationale hors-série,* n° 40 (mai 2015), https://www.areion24.news/2015/05/22/letat-islamique-forme-la-plus-aboutie-de-lennemi-hybride/.

[13] Hoorickx, « La Défense contre les “ menaces hybrides ”, » 6-7.

[14] Hoorickx, « La Défense contre les “ menaces hybrides ”, » 3-21.

[15] Commission européenne, *Communication conjointe au Parlement européen, au Conseil européen et au Conseil. Accroître la résilience*, 1 ; Georgios Giannopoulos, Hanna Smith et Marianthi Theocharidou, *The Landscape of Hybrid Threats. A conceptual Model* (Luxembourg : Publications Office of the European Union, 2021), 6, https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

[16] Giannopoulos, Smith et Theocharidou, *The Landscape of Hybrid Threats*, 6.

[17] Hoorickx, « La Défense contre les “ menaces hybrides ”, » 3-21.

[18] Hoorickx, « La Défense contre les “ menaces hybrides ”, » 3-21 ; Jean-Michel Valantin, « La longue stratégie russe en Europe, » *Le Grand Continent*, 10 février 2023, https://legrandcontinent.eu/fr/2023/02/10/la-longue-strategie-russe-en-europe/.

[19] Hoorickx, « La Défense contre les “ menaces hybrides ”, » 8, 10 ; Giannopoulos, Smith et Theocharidou, *The Landscape of Hybrid Threats*, 36.

[20] Giannopoulos, Smith et Theocharidou, *The Landscape of Hybrid Threats*, 36-42.

[21] Giannopoulos, Smith et Theocharidou, *The Landscape of Hybrid Threats,* 15.

[22] Parlement européen, *Résolution du Parlement européen*.

[23] Estelle Hoorickx et Carolyn Moser, « La clause d’assistance mutuelle du Traité sur l’Union européenne (article 42§7 TUE) permet-elle de répondre adéquatement aux nouvelles menaces ?, » *e-Note 40* (Institut royal supérieur de défense), 11 mai 2022, https://www.defence-institute.be/publications/e-note/e-note-40/.

[24] Giannopoulos, Smith et Theocharidou, *The Landscape of Hybrid Threats*, 6.

[25] Giannopoulos, Smith et Theocharidou, *The Landscape of Hybrid Threats*, 33.

[26] Georges-Henri Soutou, « La stratégie du flou, » *Politique Magazine*, n° 131 (juillet-août 2014).

[27] L'acronyme « FIMI », pour *Foreign Information Manipulation and Interference*, est utilisé par l'UE depuis 2021 (Communications stratégiques, *Tackling Disinformation, Foreign Information Manipulation & Interference*, Service européen pour l'action extérieure (SEAE), 27 octobre 2021, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en).

[28] Conseil de l'Union européenne, *Une boussole stratégique en matière de sécurité et de défense – Pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts, et qui contribue à la paix et à la sécurité internationales*, 7371/22 (Bruxelles : 2022), 22, https://www.eeas.europa.eu/eeas/une-boussole-strat%C3%A9gique-en-mati%C3%A8re-de-s%C3%A9curit%C3%A9-et-de-d%C3%A9fense_fr.

[29] Parlement européen, *Résolution du Parlement européen*.

[30] Parlement européen, *Résolution du Parlement européen*. Selon la lanceuse d'alerte Frances Haugen, les contenus suscitant la réaction « colère » entraîneraient jusqu'à cinq fois plus d'engagements de la part des utilisateurs (Michaël Szadkowski, « Facebook : on sait pourquoi les posts qui énervent étaient plus visibles que les autres, » *Huffpost*, 27 octobre 2021, https://www.huffingtonpost.fr/technologie/article/facebook-on-sait-pourquoi-les-posts-qui-enervent-etaient-plus-visibles-que-les-autres_187899.html).

[31] Russie, Chine, Iran, Corée du Nord, Hezbollah, Al-Qaeda et « État islamique » notamment (Giannopoulos, Smith et Theocharidou, *The Landscape of Hybrid Threats*, 16).

[32] Hoorickx, « La Défense contre les " menaces hybrides ", » 14.

[33] Tatiana Kastouéva-Jean, « Vladimir Poutine : 20 ans au pouvoir, » *Carto*, n° 64, (mars-avril 2021) : 19, https://www.areion24.news/produit/carto-n-64/.

[34] Loiseau, *La guerre*, 19.

[35] Hoorickx, « La Défense contre les " menaces hybrides ", » 5-6.

[36] Estelle Hoorickx, « La cyberguerre en Ukraine : quelques enseignements pour l'OTAN et l'UE, » *e-Note 49* (Institut royal supérieur de défense), 10 juillet 2023, https://www.defence-institute.be/publications/e-note/e-note-49/.

[37] Conseil de l'Union européenne, *Une boussole stratégique* ; Isabelle Lasserre, « Face aux menaces russes, l'Europe se porte au secours de la Moldavie, » *Le Figaro*, 22 novembre 2022, https://www.lefigaro.fr/international/face-aux-menaces-russes-l-europe-se-porte-au-secours-de-la-moldavie-20221122.

[38] Conseil de l'Union européenne, *Une boussole stratégique*. ; Sur les campagnes de désinformation et d'ingérences menées par Moscou vis-à-vis de l'UE, lire également : Estelle Hoorickx, « La lutte euro-atlantique contre la désinformation : état des lieux et défis à relever pour la Belgique, » *Sécurité & Stratégie* (Institut royal supérieur de défense), n° 150 (octobre 2021), https://www.defence-institute.be/publications/securite-strategie/ss-150/.

[39] Nicolas Barotte, « Migrants en Biélorussie : le casse-tête stratégique des menaces " hybrides ", » *Le Figaro*, mis à jour le 13 novembre 2021, https://www.lefigaro.fr/international/le-casse-tete-strategique-des-menaces-militaires-hybrides-20211112 ; Anne-Françoise Hivert, « Au poste de Nuijamaa, en Finlande : " Un policier russe m'a vendu un vélo pour rejoindre la frontière ", » *Le Monde*, mis à jour le 4 décembre 2023, https://www.lemonde.fr/international/article/2023/12/03/tensions-migratoires-a-la-frontiere-entre-la-russie-et-la-finlande_6203632_3210.html.

[40] Aziliz Le Corre, « Frontière polonaise : " La Russie et la Turquie instrumentalisent les migrants pour déstabiliser l'Europe ", » *Le Figaro*, 10 novembre 2021, https://www.lefigaro.fr/vox/monde/frontiere-polonaise-la-russie-et-la-turquie-instrumentalisent-les-migrants-pour-destabiliser-l-europe-20211110.

[41] Aurélie Pugnet, « [Analyse] Assurer la sécurité des câbles sous-marins : deuxième défi européen après les gazoducs ?, » *B2 Pro Le quotidien de l'Europe géopolitique,* 21 octobre 2022, https://club.bruxelles2.eu/2022/10/analyse-assurer-la-securite-des-cables-sous-marins-deuxieme-defi-europeen-apres-les-gazoducs/ ; Olivier Jehin, « [Actualité] Sabotage sur un gazoduc reliant Estonie et Finlande. L'UE et l'OTAN en alerte, » *B2 Pro Le quotidien de l'Europe géopolitique*, 11 octobre 2023, https://club.bruxelles2.eu/2023/10/actualite-gazoduc-et-cable-endommages-entre-lestonie-et-la-finlande-lotan-alertee/.

[42] « Traquer l'ingérence russe pour saper la démocratie en Afrique, » *Éclairage*, (Centre d'études stratégiques de l'Afrique), 10 juillet 2023, https://africacenter.org/fr/spotlight/traquer-ingerence-russe-saper-democratie-afrique/ ; AB Pictoris, Pierre Verluise et Selma Mihoubi, « La Russie en Afrique francophone depuis les indépendances : quels moyens pour une lutte d'influence franco-russe (1960-2023) ?, » *Diploweb.com*, 18 février 2023, https://www.diploweb.com/La-Russie-en-Afrique-francophone-depuis-les-independances-quels-moyens-pour-une-lutte-d-influence.html ; Guillaume Soto-Mayor, Admire Mare et Valdez Onanina, « Comprendre la désinformation en Afrique, » *Le Grand Continent*, 26 octobre 2023, https://legrandcontinent.eu/fr/2023/10/26/comprendre-la-desinformation-en-afrique/.

[43] Communication stratégique, groupes de travail et analyse de l'information (STRAT.2), *1st EEAS Report on Foreign Information Manipulation and interference Threats. Towards a framework for networked defence* (Bruxelles. : Service européen pour l'action extérieure (SEAE), 2023), https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-inter

ference-threats_en.

[44] Jean-Michel Valantin, « Comment la Chine a fait de l'Europe son " espace utile ", » *Le Grand continent*, 25 avril 2023, https://legrandcontinent.eu/fr/2023/04/25/comment-la-chine-a-fait-de-leurope-un-espace-utile-x/.

[45] Colon, *La guerre de l'information* (Paris : Tallandier, 2023), 389.

[46] Valantin, « Comment la Chine. »

[47] Luc de Barochez, « L'inconscience de l'Europe face aux agents chinois, » *Le Point hors-série. Chine, le temps de l'affrontement*, n° 12 (octobre-novembre 2023) : 45. Philippe Le Corre, « Avec l'Europe, un dialogue de sourds, » *Le Point hors-série. Chine, le temps de l'affrontement*, n° 12 (octobre-novembre 2023) : 52-53 ; Parlement européen, *Résolution du Parlement européen,* BY, BZ.

[48] Frédéric Lemaître, « La guerre hybride de la Chine contre la Lituanie et l'Union européenne, » *Le Monde*, 23 décembre 2021, https://www.lemonde.fr/international/article/2021/12/23/la-guerre-hybride-de-la-chine-contre-la-lituanie-et-l-union-europeenne_6107121_3210.html.

[49] de Barochez, « L'inconscience de l'Europe. »

[50] Hoorickx, « La Défense contre les " menaces hybrides ", » 7.

[51] Colon, *La guerre de l'information,* 372-373.

[52] Paul Charon et Jean-Baptiste Jeangène Vilmer, *Les opérations d'influence chinoises* (Paris : IRSEM, 2021), 619, 623-624, 630, https://www.irsem.fr/rapport.html.

[53] Le Corre, « Avec l'Europe, » 52.

[54] Conseil de l'Union européenne, *Une Boussole stratégique*, 8.

[55] Nicolas Gros-Verheyde, « [Verbatim] Recalibrer la relation avec la Chine. La leçon du Gymnich en Suède. Les points clés du non paper du SEAE, » *B2 Pro Le quotidien de l'Europe géopolitique*, 15 mai 2023, https://club.bruxelles2.eu/2023/05/verbatim-comment-recalibrer-la-relation-avec-la-chine-la-lecon-du-gymnich-en-suede/.

[56] Raoul Delcorde, « Qu'est-ce que le Sud global ?, » *La Libre Belgique*, 6 février 2023, https://www.lalibre.be/debats/opinions/2023/02/06/quest-ce-que-le-sud-global-HEQVIJUG5FERJK52QZFYJUPMY4/.

[57] Commission européenne, *Communication conjointe au Parlement européen et au Conseil relative à la « stratégie européenne en matière de sécurité économique »,*

JOIN(2023) 20 final (Bruxelles : 2023), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52023JC0020.

[58] Loiseau, *La guerre*, 517.