IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

PROGRAMME
EUROPE, STRATÉGIE & SÉCURITÉ

L'UNION EUROPÉENNE FACE AUX MENACES HYBRIDES ET AU DÉFI DE LA PUISSANCE

Général (2S) Jean-Marc Vigilant / Chercheur associé à l'IRIS

Janvier 2025

PRÉSENTATION DE L'AUTEUR

Général (2S) Jean-Marc Vigilant / Chercheur associé à l'IRIS

Jean-Marc Vigilant est chercheur associé à l'IRIS, spécialiste des questions militaires et de défense. Fondateur et président de la société BeVigilant, il est également président de l'association EuroDéfense-France, et membre de l'Institut de recherche et de communication sur l'Europe (IRCE). Général de division aérienne, Jean-Marc Vigilant a exercé de nombreuses responsabilités essentiellement en interarmées, dans un cadre international, le plus souvent au niveau stratégique dans le domaine politico-militaire, en conseillant de hautes autorités civiles et militaires, françaises et alliées. Il a également dirigé l'École de guerre de 2020 à 2022.

PROGRAMME
EUROPE, STRATÉGIE & SÉCURITÉ

Le programme Europe, Stratégie, Sécurité s'attache à décrypter les mutations de l'Europe et de son environnement régional sur le plan politique et stratégique.
Reconnu pour son expertise tant au niveau national qu'international, l'IRIS est partenaire et coordinateur de projets internationaux avec les principaux centres de recherche en Europe, qui permettent à l'Institut de tisser des liens forts avec les décideurs

Les champs d'intervention de ce programme sont multiples : animation du débat stratégique ; réalisation d'études, rapports et notes de consultance ; organisation de conférences, colloques, séminaires ; formation sur mesure.

iris-france.org

@InstitutIRIS
@InstitutIRIS
institut_iris
IRIS
IRIS - Institut de relations internationales et stratégiques

Le monde vit actuellement une transition brutale d'une ère géopolitique à une autre, avec en particulier le retour du rapport de force entre puissances et le recours désinhibé à la violence pour régler des différends politiques. Beaucoup de crises internationales et intérieures sont interconnectées entre elles, par des acteurs communs ou par l'impact croisé de leurs conséquences.

Depuis l'agression délibérée russe en Ukraine en février 2022, les menaces se font plus pressantes dans le voisinage européen, avec notamment la recomposition géopolitique en cours au Moyen-Orient, et le rejet de la présence militaire française et européenne au Sahel au profit de puissances autoritaires, pour n'en citer que quelques-unes. Cependant, la menace terroriste sur laquelle les Occidentaux s'étaient trop focalisés avant l'agression russe n'a pas disparu. Les démocraties occidentales sont aussi directement menacées depuis l'intérieur, par le biais d'ingérences étrangères dans les élections et de manipulation de l'opinion publique conduisant à la perte de confiance dans les institutions et entre la population et ses gouvernants.

Dans ce monde en plein bouleversement, l'Europe semble aujourd'hui affaiblie et atone, incapable de protéger ses intérêts par elle-même, ni de peser sur le cours des événements, attendant ou subissant les décisions d'autres puissances. Mais cet accès de faiblesse est provocateur et invite tous les « carnivores » de la planète à contester ce que nous sommes en tant qu'Européens et à attaquer ce qui nous est cher, le plus souvent de façon ambigüe. C'est d'ailleurs le principe des stratégies hybrides, qui en restant sous le seuil de détection, rendent ces attaques difficilement identifiables et attribuables.

Comment répondre au véritable défi posé par les menaces hybrides, pour les démocraties européennes ?

En premier lieu, en analysant l'évolution de la conflictualité et les aspects historiques et technologiques qui permettent d'expliquer le développement de ces menaces hybrides ;

Ensuite, en identifiant les menaces hybrides auxquelles l'Union européenne (UE) est confrontée, avec un intérêt particulier pour la guerre cognitive que nous subissons en permanence, afin de mieux en comprendre les enjeux ;

Enfin, en faisant des propositions pour que l'UE soit davantage en mesure de faire face aux défis posés par ces menaces hybrides, et renoue avec la puissance.

ÉVOLUTION DE LA CONFLICTUALITÉ

Cette notion d'hybridité n'est pas nouvelle. Il y a 2 500 ans, Sun Tzu décrivait déjà dans son célèbre traité de stratégie, *L'Art de la guerre*, plusieurs principes qui sous-tendent les stratégies hybrides d'aujourd'hui. L'importance de la ruse et de la guerre psychologique, la capacité à saisir les opportunités, l'utilisation des ressources de l'adversaire contre lui-même, sont autant de caractéristiques de ces stratégies hybrides. Pour Sun Tzu, « triompher sans combat est le summum de l'art militaire ». C'est pourquoi il valorise l'impact stratégique de la patience et de l'usure, afin d'éviter l'affrontement direct en mettant l'accent sur l'ambigüité et la combinaison de modes d'action non conventionnels et indirects, pour affaiblir progressivement l'ennemi.

Mais, revenons à l'histoire moderne plus près de nous pour comprendre comment on en est arrivé à la situation que nous connaissons aujourd'hui.

À la fin de la guerre froide, les États-Unis ont démontré la suprématie absolue de leur outil militaire lors de la première guerre du Golfe en 1991. Après la débâcle américaine au Vietnam, le monde a découvert avec stupéfaction le résultat de la « révolution dans les affaires militaires » menée par le Département de la Défense américain : généralisation de l'utilisation de l'internet et de l'espace pour l'observation, les télécommunications, et la navigation de précision grâce au GPS, et mise-en-œuvre du concept de bataille aéroterrestre qui préfigurait le combat interarmées. La coalition internationale sous commandement américain, constituée de 35 pays et forte de 500 000 hommes, a libéré en 42 jours de combat le Koweït qui avait été envahi par l'armée irakienne de Saddam Hussein, présentée alors comme la quatrième armée du monde[1]. L'opération appelée *Desert Storm* a débuté par une intense campagne aérienne systématique de cinq semaines, et s'est conclue par une offensive terrestre de cent heures.

Devant cette éclatante démonstration de l'hyperpuissance américaine, les Européens ont alors cru à la « fin de l'histoire » selon la formule de Francis Fukuyama, c'est-à-dire à la supériorité définitive du modèle occidental, à l'ombre de la *Pax Americana*.

Pendant que les Occidentaux s'endormaient sur leur supériorité technologique dans des conflits asymétriques de gestion de crise, au cours desquels leurs forces militaires expéditionnaires opéraient dans des environnements relativement permissifs, leurs adversaires les ont observés.

[1] 1 million de soldats, 5 500 chars, 700 avions de combat.

C'est notamment le cas des Chinois qui ont théorisé dès 1999, le moyen de contourner la puissance militaire occidentale dans un ouvrage célèbre appelé « la guerre hors limites », (*Unrestricted Warfare*). Selon ses auteurs, deux colonels de l'Armée populaire de libération, Qiao Liang et Wang Xiangsui, « le champ de bataille est partout ». Ils expliquent comment l'effacement des limites entre espaces physiques et espaces virtuels d'origine technique permet l'emploi de moyens non militaires dans tous les domaines — y compris financiers, économiques, juridiques, et technologiques — pour prendre le dessus sur les États-Unis en particulier et sur les Occidentaux en général.

Cette mutation de l'espace de bataille est rendue possible par l'accès généralisé aux innovations technologiques, en particulier dans le domaine numérique des technologies de l'information, qui sont par nature duales, c'est-à-dire utiles tant pour des usages civils que militaires.

Au début du XXI^{e} siècle, l'accès facilité à l'innovation technologique a eu deux conséquences déterminantes :

- d'une part, la fin de l'avantage technologique des puissances occidentales ;
- d'autre part, l'apparition de nouveaux domaines d'affrontement liés à ces nouvelles technologies, comme l'espace exoatmosphérique, le cyberespace, les fonds marins, le spectre électromagnétique ou encore le champ informationnel.

L'augmentation de notre dépendance à l'égard de ces nouveaux services et donc la nécessité de défendre nos ressources et nos intérêts dans ces nouveaux domaines ont conduit mécaniquement à l'extension du champ de conflictualité, au-delà de terre – air - mer.

Le concept moderne de guerre hybride est plus précisément théorisé dès 2005 aux États-Unis par le général américain James Mattis et Franck G. Hoffmann dans leur livre *Future Wars*, puis en 2007 dans *Conflict in the 21st Century: The Rise of Hybrid Wars*.

Les conflits en Irak et en Afghanistan ont mis en lumière l'utilisation par les insurgés ou les talibans de tactiques mêlant attaques conventionnelles (comme des embuscades armées) et non conventionnelles (comme les bombes artisanales, la guerre psychologique, ou les campagnes informationnelles).

Mattis et Hoffman voyaient clairement que les futurs conflits impliqueraient davantage de cyberattaques, de désinformation, et de pressions économiques, comme des outils hybrides pour affaiblir les adversaires sans déclencher de guerre totale.

En Europe, les menaces hybrides sont d'abord mentionnées en France dans le Livre blanc sur la défense et la sécurité nationale de 2013, puis portées à la connaissance du grand public lors de l'annexion de la Crimée et du Donbass par la Russie en 2014.

L'action des fameux « petits hommes verts »[2] dans ces deux provinces ukrainiennes, correspond à la mise en œuvre d'une vision stratégique attribuée au chef d'état-major des forces armées russes, Valeri Guerassimov. Cependant, il n'a jamais reconnu officiellement la paternité de cette doctrine. La confusion est venue d'un article[3] de février 2013, sur la transformation des conflits modernes, dans lequel Guerassimov analysait ce qu'il percevait comme des actions offensives des Occidentaux en Europe de l'Est, notamment en Ukraine, pendant les révolutions de couleurs de 2004. Pour y répondre, il décrit ensuite une approche russe de la guerre hybride et non conventionnelle, dans laquelle la distinction entre guerre et paix devient floue, et les outils non militaires jouent un rôle essentiel dans l'atteinte des objectifs stratégiques.

En Europe, les concepts de menaces et de stratégies hybrides sont devenus un sujet stratégique majeur à partir de 2014, après l'annexion de la Crimée par la Russie. L'OTAN a formellement reconnu les stratégies hybrides au sommet du Pays de Galles en 2014. L'UE, quant à elle, a officiellement adopté le terme de menace hybride dans ses documents en 2015, en réponse à l'utilisation par la Russie de stratégies hybrides en Ukraine.

En avril 2016, l'UE a adopté un « Cadre commun sur la lutte contre les menaces hybrides », dans lequel elle décrit la combinaison de désinformation, de cyberattaques, de pressions économiques, et d'opérations militaires discrètes comme des menaces hybrides.

Les nouveaux domaines de conflictualité, peu ou non régulés, sans cadre juridique ou politique clair, sont devenus des **zones grises**, ni totalement en paix, ni complètement en guerre, dans lesquels nos adversaires ont la possibilité de déployer des stratégies hybrides sous le seuil de confrontation ouverte, tout en rendant très difficile l'attribution des actions hostiles.

[2] Militaires russes sans insignes distinctifs soutenant les séparatistes prorusses et organisant l'insurrection contre le gouvernement légitime.
[3] Valeri Guerassimov, « La valeur de la science est dans la prévoyance », *Voyenno-Promyshlenny Kuryer* (Courrier militaro-industriel), février 2013

MENACES HYBRIDES CONTRE L'UNION EUROPÉENNE

L'**affrontement hybride** correspond à **évolution de la conflictualité** par enrichissement de modes d'action, en abaissant la barrière du droit.

Une **définition plus opérationnelle** de la stratégie hybride est celle donnée par le centre interarmées de concepts, doctrines et expérimentations de l'état-major des armées françaises : il s'agit de la « stratégie d'un acteur, étatique ou non, visant à contourner ou affaiblir la puissance, l'influence, la légitimité et la volonté adverse, en mettant en œuvre une combinaison intégrée de modes d'actions militaires et non-militaires, directs et indirects, licites ou illicites, souvent subversifs, ambigus et difficilement attribuables, visant à paralyser et pouvant être engagés sous un seuil estimé de riposte ou de conflit ouvert, et dans le cadre d'une possible gestion d'escalade ».

En résumé, les stratégies hybrides se déploient sous **trois seuils :** le seuil de détection, le seuil de compréhension et le seuil de réaction.

Pour avoir une idée plus précise des menaces hybrides qui pèsent sur l'UE, il est intéressant d'analyser plus en détail l'approche russe de la **transformation des conflits** modernes décrite par Guerassimov.

Ainsi, il explique que les guerres modernes ne se déroulent plus exclusivement sur les champs de bataille traditionnels avec des moyens militaires. Elles impliquent désormais une **combinaison d'outils militaires et non militaires**, intégrés dans une stratégie globale. Il affirme que les lignes entre la guerre et la paix s'estompent, les conflits prenant des formes nouvelles et plus indirectes.

Selon Guerassimov, les moyens non militaires, tels que la désinformation, les cyberattaques, les pressions économiques, et les actions politiques clandestines, peuvent être aussi efficaces voire plus, que les moyens militaires traditionnels.

Il estime que ces outils doivent représenter environ quatre fois plus d'effort en termes de ressources allouées, que les moyens militaires directs dans les conflits modernes.

Guerassimov souligne l'importance de combiner des moyens conventionnels (forces armées régulières) avec des moyens non-conventionnels :

- Groupes paramilitaires et milices locales (comme en Crimée ou dans l'est de l'Ukraine avec les séparatistes prorusses, ou encore le groupe Wagner en Ukraine et en Afrique, devenu Africa Corps depuis la mort de son chef historique Evgueni Prigogine) ;
- Cyberattaques pour perturber les infrastructures critiques ;

- Désinformation et propagande pour déstabiliser l'ennemi et influencer l'opinion publique ;
- Pressions économiques et sanctions ciblées.

Ces outils peuvent être utilisés pour **affaiblir un État sans jamais déclarer officiellement la guerre**.

Guerassimov accorde une place centrale à la guerre de l'information, en soulignant que la propagande et les opérations psychologiques jouent un rôle crucial pour influencer les populations et semer la confusion chez l'adversaire.

Il met en avant la nécessité pour **la Russie d'intervenir préventivement en exploitant des conflits latents** ou en s'insérant dans des crises avant qu'elles n'atteignent un point critique.

C'est exactement ce à quoi nous assistons en Europe ou dans des régions du monde où les Européens ont des intérêts. En **Afrique**, sous la pression russe attisant le sentiment anti-français, les forces militaires françaises et européennes ont quitté le Sahel à partir du printemps 2024. Par ailleurs, les difficultés politiques et sociales existantes dans les **territoires ultramarins** ont été exacerbées par des ingérences étrangères, conduisant à des manifestations violentes contre la légitimité territoriale de l'État français en Nouvelle-Calédonie, et en Martinique.

De même, actuellement plusieurs tactiques sont utilisées par la Russie pour **affaiblir le soutien européen à l'Ukraine** : en intensifiant les opérations psychologiques ou d'espionnage sur les réseaux informatiques, en armant le pacifisme, en mobilisant le nationalisme, en exploitant les divisions, en diabolisant les réfugiés et migrants et en ciblant les communautés des diasporas.

Dans un autre registre, les **domaines plus techniques** sont également l'objet de développement de stratégies hybrides.

L'accès à **l'espace** n'est plus l'apanage des grands États et des puissances nucléaires. Avec l'avènement du *New Space*, d'une part le prix du kilo en orbite a drastiquement baissé, passant en 10 ans de plus de 10 000 euros par kg à environ 2000 euros par kg aujourd'hui, ce qui rend l'espace **accessible à tous** les acteurs étatiques ou non. À titre d'exemple, le centre spatial universitaire de Montpellier fabrique des nanosatellites avec des capacités techniques remarquables, à partir d'unités CubeSat de 10 cm de côté, et les déploie en orbite à un coût raisonnable, pour différentes applications de recherche scientifique.

D'autre part, il est désormais plus facile de se soustraire aux lois déterministes de la mécanique spatiale, en manœuvrant dans l'espace. Cela permet à un **satellite patrouilleur** adverse de se rapprocher d'un satellite non coopératif pour l'espionner ou le rendre inopérant par brouillage ou action cinétique. Ce type de manœuvre est difficilement détectable et donc attribuable. Ainsi, un satellite russe *Luch Olymp* s'est approché du satellite militaire de télécommunication franco-italien Antena Fidus en 2018 en orbite géostationnaire, puis un autre objet russe a démontré sa capacité de **manœuvre en orbite** basse en 2024.

De nombreux services s'appuient sur des infrastructures spatiales de plus en plus importantes, avec l'avènement des constellations géantes de satellites. Nous sommes passés de 1 000 satellites en orbite au début des années 2000 à près de 10 000 aujourd'hui, et la croissance de ce nombre est exponentielle, ce qui posera d'ailleurs d'autres problèmes de soutenabilité de l'activité spatiale face à l'augmentation du risque induit par les débris en orbite. À l'heure où notre **dépendance** au secteur spatial n'a jamais été aussi forte, chaque citoyen européen utilisant en moyenne 47 satellites[4] dans sa vie quotidienne, la défense de nos intérêts dans le domaine spatial est devenue un impératif absolu.

De même, dans le **domaine cyber**, les possibilités d'attaque hybride existent sur les trois couches qui composent le cyberespace. La première couche dite physique est constituée de l'infrastructure matérielle formée par les réseaux, serveurs et ordinateurs, qui permettent de faire fonctionner Internet ; la deuxième couche logique et applicative comprend les services comme les logiciels et les applications qui génèrent et transmettent les informations ; la troisième couche cognitive et sémantique désigne la pensée des internautes eux-mêmes. Compte-tenu de notre dépendance accrue aux réseaux et à l'internet, la défense de nos ressources et de nos activités dans l'ensemble du cyberespace contre un acteur malveillant est capitale.

Une partie importante de l'infrastructure Internet se trouve dans **les fonds marins** peu accessibles et donc peu surveillés. Les câbles sous-marins qui y sont déployés parfois jusqu'à plusieurs kilomètres de profondeur sous le plancher de l'océan contiennent les fibres optiques par lesquelles transitent **95 % du trafic internet mondial**. Il est tout à fait possible pour une puissance étrangère d'endommager ces câbles pour perturber le trafic de données ou de s'y connecter de façon discrète pour détourner ou espionner le flux de données. La Russie détient cette capacité et est suspectée de l'avoir utilisée tant en mer noire pour isoler la Crimée, qu'en

[4] Assemblée nationale, « Rapport d'information déposé par la commission des affaires européennes sur la politique spatiale européenne », n°1438, 21 novembre 2018, https://www.assemblee-nationale.fr/dyn/15/rapports/due/l15b1438_rapport-information

mer Baltique pour affaiblir la connectivité sur la façade nord de l'Organisation du Traité de l'Atlantique Nord (OTAN).

Parmi les menaces hybrides, **les plus importantes sont sans certainement les ingérences informationnelles**, par manipulation de l'information, opérations de déstabilisation de l'opinion publique et ingérence électorale, comme ce fut le cas en 2016 aux États-Unis pour la première élection de Donald Trump et au Royaume-Uni pour le Brexit, en 2017 en France pour l'élection du président Macron (« Macron Leaks ») et plus récemment pour les élections générales en Roumanie. Dans cette dernière élection, le candidat d'extrême-droite **Călin Georgescu** favorable à la Russie était inconnu du grand public un mois avant les élections et était crédité de 1 % des voix. Il est devenu dans les 15 jours précédant les élections la neuvième personnalité la plus visible au monde sur Tik-Tok. Une double attaque cyber et informationnelle russe mise-à-jour par les services de renseignement roumains et dont plusieurs éléments ont été confirmés après-coup par Tik Tok, a permis à ce candidat d'arriver en tête des élections générales avec plus de 23 % des voix à la surprise générale. Sur la base de faits établis techniquement et prouvant une ingérence étrangère, ce résultat a été annulé par la cour constitutionnelle roumaine.

L**'information est devenue une arme** très efficace grâce à la forte pénétration des outils numériques dans la société au cours des dix dernières années. Les nouvelles technologies de communication opèrent comme un **effet multiplicateur** des manipulations de l'information.

Dans cet **environnement numérisé et hyperconnecté**, générant massivement de l'information, il serait dangereux de ne considérer que la dimension technique des domaines préalablement cités, sans tenir compte des sciences humaines et sociales. En effet, au-delà de la cyberguerre qui consiste à utiliser des moyens numériques pour maîtriser, modifier ou détruire l'information, une nouvelle forme de guerre se joue aussi dans les cerveaux humains pour altérer la cognition, c'est-à-dire ce que le cerveau fait de cette information.

Appelée « **guerre cognitive** », cette forme de guerre non conventionnelle consiste à exploiter les technologies de l'information en profitant des biais cognitifs d'un groupe de personnes pour les amener à avoir une représentation erronée du monde et, ce faisant, provoquer des altérations de la décision, des inhibitions de l'action ou encore la fragmentation des communautés.

L'impact à une échelle sans précédent des réseaux sociaux, des médias disponibles et de la désinformation voire de la propagande sur les populations, illustre cette convergence entre technologies de l'information et opérations psychologiques. Nos **cerveaux humains sont devenus un nouveau domaine d'affrontement**.

Étant à l'intersection de la cyberguerre et de la guerre de l'information, la guerre cognitive est la forme la plus aboutie de manipulation permettant d'influer sur le comportement d'un groupe d'individus. **La population est devenue l'enjeu de l'affrontement**.

Pour mieux comprendre les mécanismes à l'œuvre, il y a plusieurs aspects à prendre en compte :

D'une part le **biais cognitif** qui est une erreur générale, se fonde sur deux principes biologiques majeurs :

- La valorisation du raisonnement le plus court par minimisation de l'énergie nécessaire (paresse intellectuelle naturelle)
- La très forte contrainte de faire un choix de pensée différent de celui fait initialement

D'autre part, les **algorithmes de super-personnalisation** qui sont responsables de la polarisation croissante des opinions publiques. Les plateformes de réseaux sociaux tendent à favoriser la diffusion de messages « *surprenants et négatifs* », ainsi que l'instabilité émotionnelle et l'extrémisme. Les nouvelles fausses et surprenantes ont 70 % plus de chances d'être retweetées[5].

L'image et le son comportant une importante charge émotionnelle, l'émotion l'emporte très souvent sur la raison. C'est pour cela que les contenus médiatiques qui sont de plus en plus souvent **générées par IA** (*deep fakes*) sont aussi efficaces et dangereux.

RÉPONSES POSSIBLES DE L'UE, RENOUER AVEC LA PUISSANCE

L'Europe est attaquée de toutes parts, par les régimes autoritaires qui contestent l'ordre international établi par les Occidentaux au lendemain de la Deuxième Guerre mondiale et voient comme une menace le pouvoir attractif des démocraties libérales sur leur propre population.

Mais l'Europe est aussi attaquée, car son refus de parler le langage de la puissance l'a convertie en une **proie riche, faible et vieillissante** pour tous les prédateurs géopolitiques. Depuis le V^{e} siècle, les pays européens ont connu la guerre pratiquement à chaque génération, tout en dominant le monde au travers d'empires coloniaux entre le XV^{e} et le XX^{e} siècle. Les deux derniers conflits mondiaux ont culminé dans l'horreur et l'autodestruction de l'Europe avec un total d'environ 65 millions de morts militaires et civils.

[5] D'après Guy-Philippe Goldstein, chercheur sur la guerre cognitive et la polarisation de la guerre froide 2.0.

La construction européenne sous la protection des Américains a permis aux pays européens de l'UE et de l'OTAN de jouir de la **plus longue période de paix** depuis l'Empire romain, 80 ans, soit plus de deux générations.

Cependant, avec leur désengagement d'Europe annoncé par les États-Unis et leur « pivot » vers l'Asie-Pacifique, leur nouvelle priorité stratégique, l'UE doit assumer davantage ses **responsabilités stratégiques**, pour défendre ses intérêts et ses valeurs face à des compétiteurs stratégiques de plus en plus assertifs.

Alors **que faire** pour que l'Europe soit mieux préparée pour gérer ces menaces hybrides et défendre ses intérêts ?

La première des choses est d'**augmenter la conscience** des citoyens de l'existence de ces menaces et des situations dangereuses qu'elles génèrent. Bien que nous ne soyons pas en guerre ouverte, nous ne sommes déjà plus en paix, notamment dans les domaines virtuels tels que le cyberespace et le champ informationnel, où les attaques contre nos entreprises, nos organisations et notre population sont quotidiennes et permanentes, de la part de nos compétiteurs stratégiques. Il est donc important de diffuser ces informations le plus largement possible.

L'éducation et la formation des plus jeunes sont essentielles pour développer leur **esprit critique**. Il s'agit de permettre une meilleure compréhension du mécanisme des algorithmes des réseaux sociaux par les utilisateurs, afin de les amener à se poser les bonnes questions : pourquoi reçois-je ce message ? Qui a intérêt à sa diffusion ? Ce réflexe permettrait de renforcer la raison face à l'émotion, et d'éviter de contribuer malgré soi à la diffusion de contenu inapproprié.

Cependant, il est pratiquement impossible de faire changer d'avis une personne qui est convaincue d'une information fausse, en particulier quand elle est enfermée dans sa bulle informationnelle complotiste. C'est pourquoi la meilleure façon d'amener ces personnes à douter de ces fausses informations est de leur **apprendre à utiliser les outils** numériques en ligne à base d'IA pour fabriquer elles-mêmes des *deep fakes* et à programmer un *chat bot* pour qu'il génère du trafic sur un réseau social. La connaissance et la maîtrise des techniques de falsification de la vérité les rendront moins crédules.

De même, il faut promouvoir **l'esprit de défense** parmi nos concitoyens européens. Bien que l'Europe soit devenue très pacifiste pour des raisons historiques, il est toujours surprenant de constater le niveau de défaitisme de certains Européens qui considèrent que sans l'aide des États-Unis au sein de l'OTAN, nous ne pourrons pas nous défendre. Les Ukrainiens nous

démontrent tous les jours que la capacité à se défendre est d'abord un état d'esprit et une farouche volonté de se battre pour défendre ce qui nous est cher.

Pour cela, il est important de sortir de la dépendance mortifère des États-Unis en matière de défense, et de renforcer le **pilier européen de l'OTAN** en même temps que les autres instruments de la PSDC[6] pour une plus grande responsabilité stratégique des alliés européens. D'ailleurs, les Européens considèrent très souvent l'OTAN comme une organisation américaine à laquelle ils participent, alors que celle-ci d'abord une organisation européenne à laquelle les Américains participent et qu'ils dirigent à notre demande. En effet, l'organisation de défense américaine est bien plus grande que l'OTAN et est vraiment mondiale[7].

Vues de l'extérieur du continent européen, les divergences entre alliés européens sont mineures. Cependant, pour développer une **culture stratégique européenne commune**, il est nécessaire de renforcer l'enseignement militaire supérieur européen. Ce projet a été lancé à l'initiative de l'École de guerre française en 2022, en adoptant une approche progressive[8]. L'idée est de créer les conditions d'unité de temps et d'espace, pour permettre aux officiers et fonctionnaires européens non seulement d'apprendre ensemble, mais aussi d'apprendre les uns des autres. Cela les aiderait à mieux connaître l'histoire, la géographie, la politique et la culture militaire de leurs homologues, ce qui leur permettrait de mieux comprendre les positions politiques ou les visions stratégiques de leurs voisins, et donc de mieux percevoir les intérêts communs de leurs pays.

Il est tout aussi important d'accroître la **résilience** de nos sociétés à tous égards, comme le décrit plus loin le cadre commun de lutte contre les menaces hybrides, c'est-à-dire la capacité d'absorber un choc et de repartir. Toutefois, la **cohésion interne** est essentielle pour mieux résister à la guerre cognitive, qui s'appuie sur les tensions ou les divisions existantes au sein de la population ou de la société pour les exacerber et susciter la méfiance au sein des communautés ou entre la population et le gouvernement.

Le principal enjeu pour l'État agressé est de **détecter** l'attaque hybride, **d'identifier** les responsables, puis de **répliquer**. L'État agressé est alors confronté à deux dilemmes :

[6] Politique de sécurité et de défense commune de l'UE.
[7] Jean-Marc Vigilant, « Européaniser l'OTAN : une utopie ou une évidente nécessité pour les Européens ? », *IRIS*, , 16 mai 2024, https://www.iris-france.org/europeaniser-lotan-une-utopie-ou-une-evidente-necessite-pour-les-europeens/
[8] Jean-Marc Vigilant, « A European war college, an opportunity for European Defence? », *The European Security Defence Union,* vol 37 (4/2020), 18 décembre 2020, https://issuu.com/esdu/docs/esdu_2020_vol37/s/11509967 ; Hartmut Bühl, « Strategic leadership in the European Union », *The European Security Defence Union,* vol 43 (2/2022), 29 juillet 2022, https://issuu.com/esdu/docs/esdu_2022_2/s/16474712

interpréter l'agression dont il est victime en dépit de son ambiguïté, et répondre à cette attaque, de façon assumable tout en gérant l'escalade.

Pour autant, compte-tenu de la difficulté d'obtenir des preuves formelles et juridiquement opposables d'une telle attaque, sans compromettre les sources et méthodes des capacités de renseignement et la sécurité des opérations, **l'attribution reste une décision politique**.

Un des défis pour les démocraties victimes d'une attaque hybride est de trouver le moyen d'imposer un coût pour l'attaquant, tout en respectant le droit.

Il existe des instruments spécifiques pour y contribuer, tel que le centre d'excellence sur la lutte contre les menaces hybrides en Finlande. Créé en 2017 après l'agression russe en Ukraine et en Crimée, il analyse les menaces, développe des doctrines et promeut les bonnes pratiques au bénéfice de l'OTAN et de l'UE.

Par ailleurs, lors d'une audition récente devant des parlementaires français, la Dr. Teija Tiilikainen la directrice finlandaise du CoE *for countering Hybrid threats* d'Helsinki a relevé que les deux pays les mieux préparés pour traiter les attaques hybrides étaient la Suède et la France.

Ainsi, il y a quelques spécificités françaises dont d'autres pays européens pourraient s'inspirer pour augmenter leur résilience :

- Une véritable approche interministérielle[9] sous la direction du **Secrétariat général pour la défense et la sécurité nationale** pour analyser les menaces, identifier les attaques et préparer les réponses, dans cinq domaines prioritaires : cyber (ANSSI[10]), champ informationnel (VIGINUM[11]), sécurité économique (SISSE[12]), norme juridique, et le champ opérationnel (EMA[13]).
- Dans la **doctrine militaire française**, la guerre hybride impose une approche de défense et de riposte multidimensionnelle, en associant tous les **instruments de puissance**, militaires (terre, mer, air, cyber, espace), mais aussi civils (diplomatique, médiatique, économique) pour répondre à une menace diffuse et polymorphe. C'est là que pourrait être la vraie plus-value de l'UE dans l'utilisation coordonnée de ces instruments de puissance en complément de l'action militaire.

[9] « Lutte contre les influences étrangères malveillantes. Pour une mobilisation de toute la Nation face à la néo-guerre froide – Rapport », n°739 (2023-2024), *La Galaxie Sénat*, 23 juillet 2024, https://www.senat.fr/rap/r23-739-1/r23-739-1.html
[10] Agence nationale pour la sécurité des systèmes d'information.
[11] Service de vigilance et protection contre les ingérences numériques étrangères.
[12] Service de l'information stratégique et de la sécurité économiques.
[13] État-major des armées.

- Il serait même possible d'envisager une telle action de l'UE dans le cadre d'un accord **Berlin Plus[14] inversé** en soutien de l'OTAN, car cette dernière étant une organisation strictement militaire, elle n'est légitime que pour répondre à des attaques hybrides ayant un impact direct sur sa capacité à mener des opérations militaires. Au travers d'un soutien non militaire, l'UE pourrait agir comme un **multiplicateur de résilience** en renforçant les capacités civiles, économiques et numériques des États membres de l'OTAN, pour répondre plus efficacement à la nature complexe et multidimensionnelle des attaques hybrides.
- D'autre part, si le terme de stratégie hybride a une connotation négative et s'applique à un adversaire, nous devons aussi **être proactifs** et non uniquement réactifs. C'est pourquoi en plus des cinq fonctions stratégiques définies dans le Livre blanc français — connaissances–anticipation, dissuasion, prévention, protection et intervention — la France en a défini une sixième pour répondre en partie à l'hybridité. Il s'agit de la **fonction stratégique Influence** sous la double responsabilité du MEAE[15] et de l'EMA, pour agir sur les perceptions dans un sens favorable à nos intérêts, mais totalement assumable et légal, et toujours hors du territoire national.

Enfin, le **Cadre commun sur la lutte contre les menaces hybrides** (ou *Common Framework for Countering Hybrid Threats*) développé par l'UE en 2016, reste toujours pertinent et vise à renforcer la coopération et les capacités des États membres face aux menaces hybrides. Il se fonde sur une vision partagée des défis posés par les menaces hybrides et définit des lignes directrices pour renforcer les capacités de détection, de prévention, et de réponse aux activités hybrides.

Les principaux objectifs du **Cadre commun** sont :

- Améliorer la coordination entre les institutions et les États au sein de l'UE et de l'OTAN
- Développer une compréhension commune des menaces hybrides
- Renforcer les capacités de prévention et de détection
- Garantir une réponse rapide et efficace dans le cadre d'une approche globale
- Renforcer la résilience des infrastructures critiques
- Encourager la coopération avec des partenaires extérieurs

[14] Les Accords de Berlin Plus du 14 mars 2003, posent les fondements de la coopération OTAN-UE en donnant à l'UE accès aux moyens de planification et capacités de commandement de l'OTAN pour des opérations dirigées par l'Union et dans lesquelles l'OTAN dans son ensemble n'est pas engagée.
[15] Ministère de l'Europe et des Affaires étrangères.

De nombreuses initiatives pour contrer les menaces hybrides existent déjà au sein des États-membres et d'autres propositions mériteraient d'être développées pour renforcer les capacités générales de l'UE dans ce domaine.

CONCLUSION

Le général André Beaufre, un des pères de la dissuasion nucléaire française, avait théorisé les trois marches de l'escalier menant à la guerre : **compétition, contestation, confrontation**.

Désormais, dans le monde globalisé et plus complexe dans lequel nous vivons, ces trois phases peuvent se dérouler simultanément, en fonction des sujets, des domaines et des acteurs, avec notamment la mise en œuvre de stratégies hybrides sous le seuil de l'affrontement direct. Ainsi, deux pays peuvent être partenaires sur un sujet et en opposition sur un autre, avec une constante : **ce qui n'est pas protégé est pillé, et ce qui est pillé est contesté**.

Il est donc grand temps aujourd'hui pour l'Europe de **renouer avec la puissance**, d'accepter le rapport de force imposé par ses compétiteurs stratégiques et de retrouver la volonté de se battre pour protéger ses valeurs et défendre ses intérêts dans tous les domaines et contre toutes les menaces, d'où qu'elles viennent.

Pour cela, il faut échapper au sentiment de défaitisme qui sévit en Europe, d'ailleurs peut-être instillé par des puissances étrangères, et selon lequel sans l'aide des Américains, les Européens sont incapables de se défendre. **L'UE est la deuxième puissance économique du monde** avec une population de 450 millions d'habitants et un PIB de 20 300 milliards d'euros[16]. Son budget cumulé de défense atteint 279 milliards d'euros[17] pour 1,3 million de militaires dans ses forces armées. Bien sûr, l'UE doit faire plus et mieux dans ce domaine, mais elle ne doit donc pas craindre la Russie, qui pointe au 9ème rang mondial en PIB nominal avec 2 100 milliards d'euros [18] et est moins riche que l'Italie, pour une population de 142 millions d'habitants. Son budget annuel de défense a atteint 113 milliards d'euros[19] en 2024 pour 1,1 million de militaires dans ses forces armées.

L'UE doit reprendre confiance en elle et réaffirmer sa détermination à se défendre par tous les moyens, y compris en employant la force militaire, pour que la peur change de camp. L'amélioration de sa crédibilité dépendra de sa préparation mentale et matérielle pour

[16] Estimation 2023 selon le Fonds monétaire international.
[17] Selon l'Agence européenne de Défense en 2024.
[18] Estimation de la Banque Mondiale en 2023.
[19] Selon Military Balance 2024.

véritablement assumer sa responsabilité stratégique. C'est à ce prix qu'elle pourra préserver la paix et défendre la liberté et les valeurs qui lui sont chères.

« *Life is not about waiting for the storm to pass...It's about learning to dance in the rain*. » Vivian Greene

L'expertise stratégique en toute indépendance

PROGRAMME
EUROPE,
STRATÉGIE &
SÉCURITÉ

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

2 bis, rue Mercœur - 75011 PARIS / France
+ 33 (0) 1 53 27 60 60
contact@iris-france.org

iris-france.org

L'IRIS, association reconnue d'utilité publique, est l'un des principaux think tanks français spécialisés sur les questions géopolitiques et stratégiques. Il est le seul à présenter la singularité de regrouper un centre de recherche et un lieu d'enseignement délivrant des diplômes, via son école IRIS Sup', ce modèle contribuant à son attractivité nationale et internationale.

L'IRIS est organisé autour de quatre pôles d'activité : la recherche, la publication, la formation et l'organisation d'évènements.