FONDATION ROBERT SCHUMAN

POLICY PAPER

Schuman Paper
n°819
26 janvier 2026

Jean MAFART

Les menaces hybrides : de la géopolitique à la sécurité intérieure

Si la notion de menace hybride est désormais admise en dépit de son caractère assez flou, un angle mort subsiste dans les discussions européennes et les réflexions stratégiques : le phénomène est encore peu traité du point de vue de la politique de sécurité intérieure.

Certes, on sait depuis longtemps que les menaces hybrides – qu'il s'agisse de cyberattaques, d'incendies volontaires, de désinformation, d'ingérence dans les processus électoraux ou encore d'instrumentalisation des flux migratoires – peuvent nous frapper à l'intérieur de nos frontières. L'Union européenne en a pris acte : les enceintes « justice et affaires intérieures » abordent la question régulièrement et la Commission y accorde une place considérable dans sa stratégie de sécurité intérieure d'avril 2025. C'est même par les menaces hybrides qu'elle justifie, dans ce document, la proposition de doubler les effectifs d'Europol. Mais l'irruption de ces menaces dans les politiques de sécurité intérieure de l'Union et de ses États membres soulève des questions importantes, au plan des principes comme au plan opérationnel, qui demeurent pour la plupart sans réponse.

Il est instructif de parcourir, parmi les articles d'analyse et de doctrine, l'abondante production disponible sur les menaces hybrides : la dimension géopolitique du phénomène prédomine toujours et, si les auteurs abordent parfois la résilience des États européens et des sociétés, on ne trouve presque rien sur la réponse à apporter à ces menaces dans le cadre de la politique de sécurité intérieure ni sur l'indispensable adaptation des instruments de cette politique. En d'autres termes, tout se passe comme si la notion de menace hybride, qui intéresse surtout les enceintes de défense et de politique étrangère, était entrée dans la politique européenne de sécurité intérieure par effraction et n'avait pas encore été pleinement acclimatée à la sphère interne. Si l'on y ajoute que la politique européenne de sécurité intérieure demeure encore peu connue en dépit des proportions considérables qu'elle a prises ces dernières décennies, l'état actuel de la réflexion stratégique est peu propice à la consolidation d'une doctrine sur le traitement des menaces hybrides dans leur dimension interne.

Or une telle doctrine serait bien utile, à l'instar de ce qui existe depuis longtemps dans les sphères de l'OTAN et de la politique de sécurité et de défense commune (PSDC) : le thème des menaces hybrides, désormais invoqué à tout propos mais sans approche cohérente, ne risque-t-il pas d'entraîner la politique européenne de sécurité intérieure dans des errements qui la détournent de sa vocation première ? Et comment associer harmonieusement les compétences de l'Union, de ses États membres et d'autres acteurs quand les menaces hybrides viennent brouiller la frontière entre sécurités intérieure et extérieure, voire entre la sécurité nationale – compétence de principe des États – et les compétences de l'Union ?

QU'EST-CE QU'UNE MENACE HYBRIDE ?

Pour comprendre comment les menaces hybrides sont apparues dans les sphères de la sécurité intérieure, il faut rappeler la généalogie de la notion. Le *Hybrid Centre of*

excellence, organisme de recherche soutenu par l'Union européenne et l'OTAN, fournit une définition : « *Les menaces hybrides sont des activités nuisibles planifiées et menées dans une intention malveillante. Elles visent à affaiblir une cible, telle qu'un État ou une institution, par divers moyens, souvent combinés. Ces moyens comprennent la manipulation de l'information, les cyberattaques, l'influence ou la coercition économique, les manœuvres politiques secrètes, la diplomatie coercitive ou les menaces de recours à la force militaire. Les menaces hybrides recouvrent un large spectre d'activités nuisibles ayant des objectifs différents, allant des opérations d'influence et d'ingérence jusqu'à la guerre hybride.* »

C'est par la notion de « guerre hybride », présentée ici comme le stade suprême de la « menace hybride », que l'« hybridité » est entrée en 2005 dans les débats militaires et stratégiques aux Etats-Unis ; cette notion « *reflète la porosité entre la guerre régulière et la guerre irrégulière* ». Dans ce sens, la « guerre hybride » recouvre une combinaison de moyens militaires et non militaires dont certains auteurs soulignent qu'elle n'a rien de nouveau d'un point de vue historique : la guerre du Péloponnèse en serait un exemple typique. Avant même qu'elle ne s'introduise sous une autre forme dans les discussions de sécurité intérieure, Elie Tenenbaum a montré la progressive dilution de la notion de « guerre hybride », notamment à la lumière de l'invasion de la Crimée par la Russie en 2014 : « *Généralement peu au fait des débats autour de la notion de guerre hybride avant 2014, les spécialistes de la sécurité européenne se sont emparés du terme mais le plus souvent pour désigner la dimension informationnelle, diplomatique, économique ou encore énergétique de la stratégie russe.* » D'une « guerre hybride » ainsi conçue à la « menace hybride », il n'y a qu'un pas : « *Guerre économique, propagande numérique et activisme diplomatique sont ainsi devenus, eux aussi, des menaces hybrides* ». L'auteur n'est pas tendre sur les ressorts d'un tel engouement : « *La guerre hybride serait devenue un enjeu de survie bureaucratique pour de nombreux partenaires (centres d'excellence de l'OTAN, think tanks, etc.), qui choisissent parfois d'altérer le sens du concept pour mieux le faire correspondre à leurs compétences* ».

Deux éléments essentiels doivent donc retenir l'attention : d'une part, guerre et menace hybrides sont des notions géopolitiques issues des cercles de réflexion militaire et stratégique ; d'autre part, l'extraordinaire prospérité de la notion de menace hybride dans ce champ de réflexion – avant même que les cercles de la sécurité intérieure ne s'en emparent – s'est traduite, jusqu'à faire douter de sa pertinence, par un affaiblissement du concept originel. Au demeurant, un autre aspect déroutant de la menace hybride est que, si elle s'apparente d'un côté à la guerre, elle s'apparente aussi à un mode d'action pacifique parfaitement admis : on observe une porosité croissante entre les actions hybrides et ce qui relève de la politique d'influence, que celle-ci soit mise en œuvre par des services diplomatiques, des médias, des organismes de recherche ou des « pseudo-ONG ». Certains auteurs rangent même, parmi les modes d'action hybrides, les investissements chinois dans les infrastructures et la recherche à l'étranger. A côté des actions clandestines – tout aussi traditionnelles, du reste – se développent de nouveaux modes d'action, d'apparence plus ou moins anodine, qui démultiplient les possibilités d'ingérence étrangère et les rendent moins identifiables. L'ambiguïté est un des principes de l'action hybride : ses auteurs « *ont recours […] à une panoplie de modes opératoires* (ou d'"outils") *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* » ; ils s'emploient ainsi, « *même face à un adversaire qui aurait le dessus* », à « *réduire le risque d'une réaction militaire* ».

Les menaces hybrides sont par nature d'origine extérieure et traitées comme telles dans les enceintes compétentes en matière de défense. Dans son *Concept stratégique*, l'OTAN énonce d'ailleurs clairement – manière de répliquer à l'ambiguïté des modes opératoires – que « *les opérations hybrides menées contre des Alliés pourraient atteindre le seuil correspondant à une attaque armée et conduire le Conseil de l'Atlantique nord à invoquer l'article 5* ». Les incursions récentes de drones dans l'espace aérien d'États européens sont un exemple frappant de ces

opérations et de la réaction qu'elles peuvent susciter dans la sphère militaire ; mais on peut désormais déduire de la doctrine de l'OTAN qu'une réponse collective de ses membres n'a rien d'inconcevable – du moins en principe et au-delà d'un certain seuil de gravité – face à une combinaison d'actions hybrides qui pourraient être plus sournoises, comme des actions de sabotage, des cyberattaques ou des ingérences à grande échelle dans une campagne électorale. L'Union européenne a dû prendre acte de la menace hybride dans sa *Boussole stratégique*.

LES INCIDENCES DES MENACES HYBRIDES POUR LA SÉCURITÉ INTÉRIEURE

Venues de l'extérieur, les menaces hybrides n'en affectent pas moins la sécurité et la stabilité au sein des États membres et des sociétés. Dans la sphère numérique, l'Agence européenne de cybersécurité (ENISA) présente un constat peu rassurant : « *A mesure que les tensions géopolitiques et économiques croissent, la cyberguerre s'intensifie, l'espionnage, le sabotage et les campagnes de désinformation devenant des outils essentiels permettant aux nations de manipuler les événements et de s'assurer un avantage stratégique.* » L'élection présidentielle roumaine de 2024 en est une illustration spectaculaire : alors que le candidat prorusse était arrivé en tête au premier tour, la Cour constitutionnelle a annulé l'ensemble du scrutin. Entre-temps, les autorités roumaines ont révélé une vaste campagne sur TikTok, coordonnée et financée de l'étranger, en soutien à ce candidat, inconnu des Roumains quelques semaines auparavant. En mars 2025, la Cour constitutionnelle a rejeté la candidature de l'intéressé, pour le nouveau scrutin présidentiel, suscitant des troubles dans le pays.

Tous modes d'action confondus, une étude montre que le nombre d'attaques hybrides de la Russie en Europe avait presque quadruplé entre 2023 et 2024. Les modes d'action sont devenus variés, qu'il s'agisse d'assassinats, de guerre psychologique ou d'incendies volontaires. L'étude indique ainsi : « *Une quarantaine d'incendies criminels ont été attribués à la Russie en Allemagne et en Pologne* [du 1er janvier 2018 au 30 juin 2025]*, notamment la destruction du centre commercial de Varsovie. En mai 2024, un incendie majeur s'est déclaré à Berlin dans une usine du groupe Diehl, qui produit des missiles sol-air IRIS-T utilisés en Ukraine. La Russie a également été mise en cause dans l'explosion d'un entrepôt en Espagne qui abritait du matériel de communication destiné à l'Ukraine* ».

Les opérations d'instrumentalisation des flux migratoires sont un autre mode d'action particulièrement cynique : l'objectif est de fragiliser la frontière extérieure de l'Union mais aussi de saper la confiance dans les institutions et de susciter des divisions. D'après la Commission, les flux irréguliers en provenance de Biélorussie ont augmenté de 66 % en 2024 ; elle précisait que « *les autorités russes facilitent ces mouvements, puisque plus de 90 % des migrants qui franchissent illégalement la frontière entre la Pologne et la Biélorussie possèdent un visa d'étudiant ou de touriste russe* ».

Un autre phénomène marquant est le recours à des « sous-traitants », souvent (pour la Russie) des ressortissants d'Europe de l'Est ; les expulsions massives d'agents russes sous couverture diplomatique, par suite de l'invasion de l'Ukraine, ont contribué au développement de cette pratique. Mais le dernier rapport annuel d'Europol sur la criminalité organisée analyse un phénomène plus inquiétant, le recours à des organisations criminelles : « *Les tensions géopolitiques ont offert aux acteurs de la menace hybride des possibilités d'exploiter les réseaux criminels comme outils d'ingérence, tandis que les progrès technologiques rapides – en particulier dans le domaine de l'intelligence artificielle (IA) – remodèlent la façon dont le crime est organisé, exécuté et dissimulé. Ces changements rendent la criminalité organisée plus dangereuse, créant une menace sans précédent pour la sécurité dans l'ensemble de l'UE et de ses États membres.* » C'est ainsi que deux Iraniens ont été interpellés, en 2024, après avoir recruté des malfrats (impliqués dans le trafic de stupéfiants) pour organiser des actions violentes en France et en Allemagne contre des Israéliens ou des intérêts israéliens.

Cependant, l'action hybride et la criminalité organisée ne convergent pas seulement dans leurs modes d'action : leurs finalités se rejoignent largement. Nos adversaires géopolitiques et des organisations criminelles, dont certaines se sentent désormais assez fortes pour s'attaquer aux institutions de l'État, trouvent le même intérêt à déstabiliser les institutions. La collusion entre les uns et les autres, phénomène probablement structurel, va donc bien au-delà d'un simple recours à la « sous-traitance ».

Du point de vue de la sécurité intérieure, la notion de menace hybride s'avère donc pertinente pour désigner les risques d'atteinte à la sécurité des personnes et des biens – y compris la déstabilisation des institutions et des services publics – sur le territoire de l'Union européenne mais à l'initiative de puissances étrangères hostiles. La configuration géopolitique actuelle nous confronte à un double phénomène : d'une part, la prévalence croissante de ces agressions d'origine externe dans le spectre des menaces contre la sécurité intérieure ; d'autre part, la convergence croissante des modes d'action mais aussi des objectifs entre l'action hybride et la criminalité organisée.

INTÉGRER LE TRAITEMENT DES MENACES HYBRIDES AUX POLITIQUES INTERNES DE L'UNION

Un traitement efficace des menaces hybrides, phénomène d'origine externe mais qui peut affecter l'économie, les infrastructures ou les institutions démocratiques à l'intérieur de nos frontières, suppose d'abord de rapprocher politiques externes et internes : il s'agit de pouvoir mobiliser ces dernières – au premier rang desquelles la politique de sécurité intérieure – dans le cadre d'une approche d'ensemble. De ce point de vue, la notion de menace hybride a un intérêt, au plan politique comme au plan pratique : elle peut permettre de surmonter les inévitables cloisonnements entre les différentes politiques publiques. Il s'agit ainsi, par une démarche englobante, de remédier de manière systématique et sans angle mort aux vulnérabilités de l'Union européenne et de ses États membres dans tous les champs d'action qui peuvent être affectés par les actions hybrides.

Cette intégration s'est faite par étapes. Dans ses conclusions de juin 2015 – l'invasion de la Crimée est alors toute récente –, le Conseil européen appelle à une meilleure efficacité de la PSDC et estime nécessaire que « *les instruments de l'UE soient mobilisés afin de faciliter la lutte contre les menaces hybrides* ». Autrement dit, les menaces hybrides sont abordées sous un angle externe (la PSDC) mais l'objectif est de recourir à toutes les politiques européennes pour y faire face. Par la suite, la *Boussole stratégique* a été une étape marquante dans la prise en compte des menaces hybrides ; elle prévoit un ensemble d'instruments destinés à faciliter des campagnes coordonnées des Etats membres face aux agressions. En 2022, des conclusions sur les menaces hybrides ont défini des orientations plus détaillées.

S'agissant de la politique de sécurité intérieure, les conclusions du Conseil du 18 mai 2015 ont souligné « *la nécessité de renforcer encore les liens entre la sécurité extérieure et la sécurité intérieure* » afin de créer des « *synergies entre la PSDC, dans ses dimensions civile et militaire, et les acteurs dans le domaine de la liberté, de la sécurité et de la justice, en particulier les agences de l'UE* (Europol, Frontex et CEPOL) ». Le « cadre commun » publié par la Commission en 2016 résulte de ces orientations politiques. On y trouve, parmi d'autres mesures, la constitution au sein du centre de renseignement (INTCEN) d'une « cellule de fusion » qui « *recevra, analysera et partagera des informations classifiées et de source ouverte* », un effort de surveillance et de protection des infrastructures critiques ainsi que la conception d'un « protocole opérationnel commun » permettant à l'Union et à ses États membres de répondre de manière coordonnée à une attaque hybride.

Une communication de 2018 précise l'action. Mais il est revenu à la présidence finlandaise du Conseil – pour des raisons géopolitiques qu'on devine aisément – de mobiliser les ministres de l'Intérieur afin de renforcer l'action de l'Union et de ses agences pour mieux détecter et combattre ces nouvelles

menaces. Sous cette présidence, en 2019, le Conseil s'est doté d'un groupe de travail permanent sur les menaces hybrides. Les conclusions de décembre 2019 réaffirment deux principes : d'une part, « *la responsabilité de la lutte contre les menaces hybrides incombe au premier chef aux États membres* » (au titre de leurs missions de sécurité nationale), l'action de l'Union européenne étant complémentaire ; d'autre part, une « *approche globale de la sécurité* » doit impliquer l'ensemble des acteurs, nationaux et européens, civils et militaires, publics et privés.

Assez logiquement – mais dans des proportions spectaculaires – la stratégie de sécurité intérieure de 2025 accorde une large place au sujet avec huit pages sur trente. Le document confirme l'approche « transversale » des menaces hybrides : un chapitre présente des instruments élaborés et discutés dans des enceintes diverses, loin des enceintes spécialisées dans les menaces hybrides.

Le thème de la « résilience des entités critiques » est un excellent exemple de cette approche. Une directive du 14 décembre 2022 impose aux États membres d'adopter une stratégie nationale de résilience et une évaluation des risques au moins tous les quatre ans. Ces « entités critiques » sont variées (énergie, transports, secteur bancaire) ; elles sont tenues de procéder à une évaluation des risques, de prendre des mesures préventives, d'organiser des contrôles et des exercices. Un règlement porte sur la « résilience opérationnelle numérique du secteur financier ». Un tel dispositif implique de nombreuses administrations européennes et nationales, bien au-delà des ministères de l'Intérieur, et une multitude d'acteurs privés.

A la suite de la stratégie de cybersécurité de 2020 a été adoptée en 2022 la directive NIS 2, (SRI 2, en français, comme « sécurité des réseaux et des systèmes d'information »). Alors que la directive NIS 1 était applicable à sept secteurs, comme la santé, l'énergie, le secteur bancaire ou les fournisseurs d'eau, la nouvelle directive englobe les administrations publiques, la gestion des déchets ou le secteur spatial. En outre, comme le Conseil l'y a invitée, la Commission a présenté en février 2024 une révision du plan d'action de 2017 qui organise la réponse commune aux crises de cybersécurité. Adoptée le 6 juin 2025, cette révision l'a été par les ministres chargés des télécommunications (et non ceux de l'intérieur).

Citons enfin la réglementation numérique où la prise en compte des menaces hybrides suppose une mobilisation de nombreux acteurs publics et privés, bien au-delà des cercles traditionnels de la politique de sécurité. Le *Digital Services Act* (DSA) du 19 octobre 2022 impose par exemple aux principaux moteurs de recherche et plateformes Internet (ceux qui ont plus de 45 millions d'utilisateurs actifs dans l'Union) des mesures d'atténuation des risques, notamment à l'égard de l'intelligence artificielle générative : c'est une manière parmi d'autres de prévenir les ingérences étrangères dans les processus électoraux. Du reste, la protection des institutions démocratiques est presque devenue une politique européenne à part entière : le « plan d'action pour la démocratie européenne » de décembre 2020 a donné lieu à plusieurs textes, par exemple sur le financement des partis politiques européens. Le 12 novembre 2025, la Commission a publié son « bouclier de la démocratie », destiné à mieux lutter contre les menaces hybrides dirigées contre la démocratie, notamment la désinformation en ligne ; il est très révélateur que ce futur « bouclier » ait été annoncé dans la stratégie de sécurité intérieure.

Concept géopolitique en vogue et initialement lié à la politique étrangère et la politique de défense, la menace hybride s'est donc largement introduite dans les politiques internes de l'Union européenne. Il aura fallu, pour y parvenir, que s'opère un double processus : un rapprochement entre politiques externes et internes ; et un rapprochement entre ces politiques internes, afin que les enjeux de sécurité intérieure y soient pleinement pris en compte. Dans ce second processus, la notion de menace hybride joue au fond un rôle comparable à celui qu'a joué le terrorisme depuis les attentats du 11 Septembre : dans les deux cas, il s'agit de prendre acte que la menace a pris des dimensions variées et qu'il convient de la traiter dans l'ensemble des politiques internes pertinentes.

Alors que le contre-terrorisme était autrefois l'apanage des services de police et de renseignement, il fait désormais intervenir le contrôle des flux bancaires, le numérique ou encore le contrôle des armes à feu. La même dynamique est à l'œuvre dans le domaine des menaces hybrides.

Il reste, pour la politique européenne de sécurité intérieure, à accomplir en matière de menaces hybrides ce qu'elle a accompli en matière de terrorisme : se doter, au-delà des concepts et des stratégies, d'une véritable organisation opérationnelle.

ORGANISER UN « CONCERT EUROPÉEN » DANS LE CADRE DE LA POLITIQUE EUROPÉENNE DE SÉCURITÉ INTÉRIEURE

La particularité de la politique européenne de sécurité intérieure, plus que de la politique commerciale par exemple, est d'entremêler en permanence les compétences de l'Union et celles de ses États membres. C'est encore plus vrai en matière de menaces hybrides puisque celles-ci relèvent pour une grande part des missions de sécurité nationale que les traités européens confient aux seuls États membres[1]. Ce n'est donc pas sans bonnes raisons que le « cadre commun » de 2016 confiait à ces derniers la responsabilité principale de la lutte contre la menace hybride. Or deux aspects essentiels menacent cet équilibre : d'une part, l'aggravation de la situation géopolitique a conduit l'Union européenne – à commencer par la Commission – à prendre des initiatives parfois spectaculaires dans le domaine de la sécurité et de la défense (ce que n'ont pas manqué de dénoncer certains États membres, notamment l'Allemagne) ; d'autre part, le caractère très englobant, voire flou, de la notion de menace hybride est propice à toutes les confusions entre le champ de responsabilité de l'Union et celui des États.

Ici réside un premier défi : parvenir à organiser un véritable « concert européen » en matière de menaces hybrides, entre l'Union européenne, les Etats membres et une multitude d'acteurs privés, le tout en lien étroit avec les sphères de la PSDC. Dans cette perspective, une première question à traiter est celle de la capacité d'anticipation de l'Union européenne ou, pour mieux dire, du renseignement. On a déjà entendu sur ce sujet délicat des propositions dont la variété reflète celle des points de vue mais aussi, peut-être, un certain flottement.

Un cadre de réflexion utile est la stratégie de « préparation » (*preparedness* et *readiness*) qu'a entreprise l'Union européenne à la suite du « rapport Niinistö » d'octobre 2024. Si le rapport et les travaux européens qu'il a inspirés portent sur la préparation à toutes formes de crise, ils réservent évidemment une large place aux menaces hybrides. Or le rapport ne se borne pas à préconiser une meilleure efficacité dans l'échange et l'exploitation du renseignement, dont il fait à juste titre un aspect majeur de la préparation aux crises : il propose d'« *élaborer, en collaboration avec les États membres, une proposition sur les modalités d'un service de coopération en matière de renseignement à part entière au niveau de l'UE […] sans faire concurrence aux services de renseignement nationaux des États membres* ». Cette incursion prudente dans le renseignement, compétence des États membres, traduit un aspect délicat du problème : en affaiblissant la distinction entre sécurités intérieure et extérieure, les menaces hybrides brouillent, encore plus qu'auparavant, la frontière entre les compétences de l'Union et celles des États membres. Du reste, le rapport Niinistö propose la création d'un réseau « anti-sabotage » : l'articulation entre l'Union et ses États y est tout aussi sensible puisqu'on est dans le domaine du renseignement et même du contre-espionnage.

La « stratégie européenne pour une union de la préparation » publiée en mars 2025 propose ainsi de doter l'Union européenne d'une capacité propre d'information et d'anticipation et d'un « centre opérationnel de crise au sein de la Commission ». Le plus simple serait de renforcer la *Single Intelligence Analysis Capacity* (SIAC), qui dépend du Service européen d'action extérieure (SEAE) et dont fait partie l'INTCEN. C'est en tout cas ce que propose la stratégie de « préparation ». De même, la stratégie de sécurité intérieure demande « *instamment* » aux Etats membres d'« *intensifier l'échange de renseignement*

[1] C'est au nom de cette compétence de sécurité nationale que, par exemple, le règlement Europol du 8 juin 2022 n'autorise pas l'agence à introduire elle-même dans le système d'information Schengen (SIS) des signalements concernant des suspects sur la base d'informations provenant de pays tiers : les Etats membres s'étaient fermement opposés à cette proposition de la Commission. Encore s'agissait-il de terrorisme et non de contre-espionnage, mission essentielle dans la lutte contre les menaces hybrides mais qui relève du cœur de la souveraineté étatique.

avec la SIAC » et « *améliorer l'échange d'informations avec les organismes et organes de l'UE* ».

Plus qu'une intégration européenne des fonctions de renseignement, qui n'a aucune chance de se réaliser dans un avenir prévisible, c'est donc encore une fois la notion de réseau ou de concert qu'il convient de promouvoir. La communauté du renseignement s'est organisée depuis longtemps, en dehors du cadre des institutions et des agences européennes mais en coopération étroite avec elles. De ce point de vue, les principes énoncés par le « cadre commun » de 2016 conservent toute leur pertinence : « *Dans la mesure où la lutte contre les menaces hybrides touche à la sûreté de l'État et à la défense nationale ainsi qu'au maintien de l'ordre public, la responsabilité première incombe aux États membres, la plupart des vulnérabilités nationales étant propres au pays concerné. Cependant, de nombreux États membres sont confrontés à des menaces communes, qui peuvent également cibler des réseaux ou des infrastructures transfrontières. On peut réagir plus efficacement à ces menaces par une réponse coordonnée, au niveau de l'UE, faisant appel aux politiques et aux instruments de l'UE […]* ».

On pourrait donc s'étonner de l'annonce de la création d'un service de renseignement propre à la Commission. C'est ce qu'a fait le Financial Times et ce qu'ont dénoncé plusieurs députés européens. En réalité, cette initiative de la Commission semble porter davantage sur la sécurité interne ; elle doit être rapprochée de la création d'un « collège de sécurité », qui vise à mieux informer les commissaires sur l'état des menaces, et d'une tendance générale au renforcement des procédures de sécurité. Or, précisément, la lutte contre les menaces hybrides passe par une meilleure sécurité des institutions européennes. Habituées à la transparence et aux procédures démocratiques, ces institutions ont longtemps été négligentes sur le risque d'espionnage et d'ingérence, qui s'aggrave sous l'effet des menaces hybrides. C'est pourquoi, en coopération avec les États membres et la communauté européenne du renseignement, un effort a été entrepris ces dernières années. Il s'est traduit par exemple par le règlement du 13 décembre 2023 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union. Il reste que, du point de vue de la prévention comme de la répression de l'espionnage ou des ingérences, les institutions européennes dépendent largement des services de police et de renseignement des États membres, à commencer par ceux de la Belgique ; c'est donc aussi la responsabilité des États que de doter enfin les institutions de l'Union d'un cadre de protection suffisant.

Un deuxième défi à traiter est celui des agences européennes, et notamment d'Europol : non seulement la Commission a appelé à doubler ses effectifs et à en faire une « agence de police véritablement opérationnelle » mais elle le justifiait par la nécessité de lui confier davantage de moyens face aux menaces hybrides. On lit ainsi dans la stratégie de sécurité intérieure que « *le mandat actuel de l'Agence ne couvre pas les nouvelles menaces pour la sécurité, telles que le sabotage, les menaces hybrides ou la manipulation de l'information*. » La Commission fait ici référence aux ressources (humaines et opérationnelles) et aux moyens juridiques. Fraîchement accueillies par la plupart des États membres, ces propositions faiblement étayées ont peu de chances d'aboutir dans leur intégralité. La perplexité des États ne tient pas seulement à l'absence de toute évaluation argumentée du besoin en effectifs : il faut aussi y voir une question de doctrine.

Le premier point de doctrine tient à la nature d'Europol : son « mandat » (règlement du 11 mai 2016) en fait une agence de « prévention de la criminalité grave », destinée à appuyer les services de police des États membres, et qui n'a pas vocation à traiter le phénomène des menaces hybrides dans son ensemble. S'il est probablement erroné de faire *stricto sensu* du « renseignement » une compétence exclusive des États membres – la police judiciaire induit elle-même une activité de renseignement « pré-judiciaire » –, l'agence Europol et les services de police des Etats membres ont pour vocation première de traiter les menaces hybrides dans un cadre pénal. De ce point de vue, une

action hybride n'a pas d'existence en tant que telle : il peut s'agir d'un sabotage, d'un incendie volontaire, d'une intrusion dans un système informatique ou encore d'un assassinat. Tel est d'ailleurs le sens de propos récents de la directrice exécutive Catherine de Bolle : « *La guerre hybride en tant que telle ne relève pas du mandat d'Europol. Cependant, nous nous occupons des activités criminelles qui recoupent les tactiques hybrides, telles que les cyberattaques, la désinformation utilisée à des fins de fraude ou d'extorsion et l'utilisation abusive de l'IA. Europol travaille en étroite collaboration avec les États membres et d'autres organismes de l'UE afin d'échanger des renseignements et de renforcer la résilience de l'Europe* ».

Un deuxième point de doctrine tient à la question sensible de l'« attribution ». Désigner publiquement l'auteur d'une agression hybride est un choix, opérationnel et politique, qui relève de la sécurité nationale et de la politique étrangère. Cette attribution publique, par l'État visé, peut apparaître comme une forme nécessaire de réplique : désigner publiquement un agresseur est la seule manière de dissiper l'ambiguïté inhérente aux modes d'action hybride et, dans certains cas, de justifier des contre-mesures ou des sanctions. Tel est le choix qu'a fait la France, en avril dernier, lorsque le ministre des Affaires étrangères a désigné le GRU russe comme l'auteur de cyberattaques contre « une dizaine d'entités françaises depuis 2021 ». Une doctrine d'attribution claire est même « essentielle à la dissuasion ». A l'inverse, les circonstances peuvent rendre l'attribution inopportune. Ce choix de souveraineté appartient évidemment aux seuls États, et l'on peut comprendre qu'ils ne souhaitent pas d'une agence européenne conçue comme instrument de lutte contre les menaces hybrides en tant que telles.

S'il est donc illusoire de voir dans Europol le bras armé de l'Union européenne dans la lutte contre les menaces hybrides dans leur ensemble, remarquons en revanche que l'action judiciaire – et l'implication des services de police d'une manière générale – est certainement appelée à se développer : la réponse aux menaces hybrides ne peut se concevoir uniquement du point de vue de la résilience et de la prévention, sur lesquelles ont porté l'essentiel des efforts européens depuis une dizaine d'années. La collaboration croissante entre les « acteurs hybrides » et les organisations criminelles, de même que la convergence croissante de leurs objectifs et modes d'action, ne fait d'ailleurs que justifier encore davantage cet effort judiciaire. Dans cette perspective, le développement des moyens humains et techniques de l'agence répond sans doute à un besoin opérationnel (qui reste à évaluer en détail) et il ne doit pas être exclu de compléter le règlement Europol en vigueur quant aux catégories d'infraction qui déterminent le champ de compétence de l'agence. On peut aussi noter avec intérêt que les ministres de l'Intérieur, réunis le 8 décembre 2025, ont annoncé leur intention de « *doter les services répressifs des capacités nécessaires* » face aux drones.

Ces évolutions sur le rôle des services de police dans la lutte contre les menaces hybrides rejoignent un aspect intéressant du rapport Niniistö. Celui-ci n'envisage pas seulement les menaces hybrides comme une atteinte à la sécurité intérieure : il aborde aussi l'apport de la politique de sécurité intérieure face aux menaces hybrides. La question de l'accès aux données numériques pour les services enquêteurs, par exemple, est un problème de police judiciaire et de renseignement très prégnant dans les enceintes spécialisées depuis plusieurs années ; mais elle apparaît désormais comme un enjeu de résilience européenne. Rejoignant les conclusions du « groupe de haut niveau » sur l'accès aux données, constitué en juin 2023 par le Conseil et la Commission, le rapport recommande notamment de « *veiller à la création d'un cadre solide pour l'accès légal aux données chiffrées afin de soutenir la lutte des autorités des Etats membres contre l'espionnage, le sabotage et le terrorisme, ainsi que la criminalité organisée* ». La stratégie de sécurité intérieure reprend ces orientations.

De même, il conviendra de préciser le rôle de l'agence Frontex : la lutte contre l'immigration irrégulière et la lutte contre les menaces hybrides justifient un renforcement de la frontière extérieure de l'Union et une surveillance accrue de ses abords. En septembre 2025, la proposition de bâtir un « mur

anti-drones » a fait quelque bruit mais les réflexions de la Commission sur la menace liée aux drones sont plus anciennes : une communication de 2023 livrait déjà une analyse et des propositions assez détaillées, notamment sur le développement conjoint (entre l'Union et les Etats membres) de « solutions anti-drones ». Plus récemment, la Commission a mobilisé des financements importants en la matière et elle projette de constituer un « centre d'excellence » au sein de son centre de recherche d'Ispra, en Italie (qui a d'ailleurs été survolé par un drone, probablement russe, en mars 2025). Cette question des drones, inscrite à l'ordre du jour du Conseil JAI du 8 décembre 2025, suscite au sein de l'Union des discussions délicates sur les missions de Frontex.

La Commission souhaite proposer des évolutions législatives permettant à l'agence de renforcer son action contre les drones : comme l'agence elle-même, elle revendique la possibilité pour Frontex d'accéder à l'ensemble des données relatives aux menaces (notamment celles de la SIAC) et de coopérer étroitement avec les armées et les services de renseignement des Etats membres. Il est aussi question de renforcer les moyens opérationnels de l'agence contre les drones aériens et maritimes. Pour autant, les États membres seront très attentifs à ce que Frontex ne soit pas érigée en agence de lutte contre les menaces hybrides à la frontière. Les discussions actuelles sont très représentatives des incertitudes liées à la répartition des rôles entre l'Union et ses États membres sur un phénomène – les menaces hybrides en général et les drones en particulier – qui remet en cause la *summa divisio* traditionnelle entre les compétences européennes et les missions de sécurité nationale. Là encore, la solution réside probablement dans la notion de « concert », c'est-à-dire la capacité des acteurs à travailler en réseau pour éviter que des chevauchements de compétences, structurels ou ponctuels, mais de toute façon inévitables, ne dégénèrent en conflits de compétences.

Cependant, dans cette perspective pragmatique, l'Union européenne présente au moins deux fragilités. La première tient à l'absence de vision d'ensemble du phénomène des menaces hybrides et d'impulsion politique en matière de sécurité intérieure : le double processus à l'œuvre –rapprochement entre les dimensions externe et interne d'une part, entre les politiques internes d'autre part – reste inachevé. Certes, la Commission dispose de cette vision, comme le montre sa stratégie de sécurité intérieure : le document traduit, plus encore que la précédente stratégie (2020), un effort méritoire de prise en compte de l'ensemble des menaces hybrides par la politique européenne de sécurité intérieure. la révision du règlement sur la cybersécurité du 17 avril 2019 a été présentée le 20 janvier 2026, un plan sur la sécurité des ports (afin de renforcer la sécurité des infrastructures portuaires mais aussi des chaînes logistiques), un nouveau plan d'action sur le risque NRBC (nucléaire, bactériologique et chimique) ou encore des travaux portant spécifiquement sur l'instrumentalisation des flux migratoires (sujet sur lequel la Commission a publié une communication en décembre 2024). En décidant de soumettre toute initiative législative à une étude d'impact préalable en matière de sécurité et de « préparation », la Commission a franchi une étape dans la prise en compte globale du phénomène, au-delà des acteurs habituels de la politique de sécurité intérieure. Par ailleurs, une impulsion politique existe au niveau des chefs d'État et de gouvernement, comme l'atteste le chemin parcouru dans les différentes politiques internes de l'Union. Dans ses conclusions de décembre 2024, le Conseil européen proclame que « *l'Union européenne et les États membres continueront de renforcer leur résilience et d'utiliser pleinement tous les moyens disponibles pour prévenir et décourager les activités hybrides de la Russie et y réagir* ». Enfin, le Conseil aborde fréquemment la question des menaces hybrides et, en décembre 2024, les ministres de l'Intérieur et de la Justice ont adopté des « orientations stratégiques » qui leur accordent toute leur place (non sans rappeler que « le principe selon lequel la sécurité nationale reste de la seule responsabilité de chaque État membre doit être explicitement pris en compte »). C'est aussi dans cet esprit que le plan d'action sur les câbles sous-marins a fait l'objet d'une présentation aux ministres de l'Intérieur en mars 2025.

Cependant, la réponse européenne aux menaces hybrides ne peut être pleinement intégrée à la politique de sécurité intérieure que si les ministres de l'Intérieur en ont acquis la responsabilité principale au plan interne : un échelon d'impulsion et de coordination puissant est nécessaire, avec une vision d'ensemble de la menace mais aussi des progrès accomplis dans tous les domaines. C'est ici que la double nature du Conseil peut être précieuse : les ministres de l'Intérieur étant à la fois compétents pour la politique européenne de sécurité intérieure dans tous ses aspects – quand bien même les textes sur la cybersécurité, le numérique ou la résilience du secteur financier sont discutés dans d'autres formations du Conseil – et responsables de la sécurité nationale dans leur Etat membre, il leur revient de débattre d'une stratégie complète et de veiller à la bonne prise en compte de la menace dans l'ensemble des politiques internes de l'Union. De même qu'ils se réunissent en « Conseil Schengen » depuis 2022, on pourrait imaginer que le Conseil JAI arrête un programme de travail spécifique sur la dimension intérieure des menaces hybrides et en examine périodiquement l'état d'avancement. On pourrait aussi imaginer que le Conseil se dote d'un coordonnateur pour les menaces hybrides, de même qu'il a institué en son sein, en 2004, un coordonnateur pour le contre-terrorisme : il ne s'agit pas de bâtir un édifice institutionnel pesant mais de garantir la prise en compte des objectifs de sécurité et d'assurer la fluidité nécessaire entre les différentes politiques européennes concernées.

La seconde fragilité tient à ce que les chevauchements de compétences entre l'Union et ses États membres ne peuvent que s'accroître et, pour l'heure, aucun mécanisme efficace ne permet de traiter d'éventuels conflits de compétences. Les conseils d'administration des agences, qui traitent de questions stratégiques et des grandes priorités, ne sont pas l'enceinte pertinente : il reste sans doute à imaginer des modalités souples de concertation directe entre les nombreux acteurs européens et nationaux qui sont amenés quotidiennement, à un titre ou à un autre, à traiter des menaces hybrides en matière de sécurité intérieure. Ce pourrait être une des missions d'un coordonnateur européen que d'entamer des discussions sur un tel cadre de concertation.

Enfin, une politique efficace de lutte contre les menaces hybrides, par la multitude des acteurs que celles-ci sont susceptibles d'affecter, suppose que les pouvoirs publics parviennent à y associer pleinement les entreprises – à commencer par les « opérateurs d'importance vitale », soumis à une législation européenne devenue très exigeante. Les acteurs économiques en sont conscients, comme le montre la multiplication des initiatives prises dans les grandes entreprises pour se protéger des attaques informatiques, de l'espionnage, des actions d'atteinte à la réputation ou encore des dégradations physiques. C'est une « culture de la sécurité » qui s'affirme, en même temps qu'une culture de la « résilience » et de la « gestion de crise ».

En même temps que se renforcent les directions de la sécurité (du moins pour les entreprises qui en ont les moyens), c'est un ensemble de processus et de méthodes qui doivent peu à peu s'imposer aux cadres dirigeants et à l'ensemble des branches des entreprises[2]. Pourtant, celles-ci ne peuvent accomplir seules un tel effort : au-delà des actions de sensibilisation qu'ils peuvent organiser auprès des acteurs économiques sur la protection des données industrielles par exemple, les pouvoirs publics doivent être en mesure d'énoncer une vision claire des menaces, de diffuser une doctrine de prévention et, lorsque c'est nécessaire, d'organiser une étroite coopération opérationnelle entre les acteurs publics et privés (soit pour faire face à une crise lorsqu'elle survient soit dans le cadre d'exercices de crise organisés conjointement). La protection de notre potentiel économique et de nos infrastructures ne passe pas seulement par la législation européenne ; elle requiert aussi un investissement accru de l'Union et de ses États membres dans leurs relations avec les acteurs économiques.

***

La question des menaces hybrides confronte la politique européenne de sécurité intérieure à des

[2] C. LEWANDOWSKI, la Sécurité des entreprises, Paris, Que sais-je ?, 2025

défis redoutables : conçue historiquement pour accompagner l'instauration de la libre circulation entre États membres, l'« Europe de la sécurité intérieure » doit aujourd'hui adapter ses instruments à un phénomène qui s'impose à elle de l'extérieur. Au-delà des efforts de coordination entre les sphères PSDC et JAI, il s'agit de se mettre en ordre de marche face à une menace dont l'ampleur, mais surtout la nature, sont inédites. De nombreuses questions demeurent sans réponse, et l'empirisme prendra sans doute une part considérable à cet effort d'adaptation. Encore faut-il bien cerner les problèmes et identifier les vulnérabilités à résoudre.

Jean Mafart

Préfet, ancien directeur des affaires européennes et internationales du ministère de l'intérieur, auteur de la Politique européenne de sécurité intérieure (Bruylant, 2025), membre du comité scientifique de la Fondation Robert Schuman

Retrouvez l'ensemble de nos publications sur notre site :
www.robert-schuman.eu

Directeur de la publication : Pascale JOANNIN
ISSN 2402-614X