FONDATION ROBERT SCHUMAN

POLICY PAPER

Schuman Paper
n°787
14 avril 2025

Jean MAFART

Les menaces hybrides, nouveaux horizons de « l'Europe de la sécurité intérieure » ?

Aujourd'hui encore, la plupart de nos concitoyens l'ignorent : l'Union européenne intervient activement en matière de terrorisme, de blanchiment, de trafic de stupéfiants, de protection des frontières ou encore d'harmonisation des législations pénales[1]. C'est pourquoi la stratégie européenne de sécurité intérieure publiée par la Commission le 1er avril est importante : elle définit, dans le cadre des orientations énoncées par le Conseil européen, le programme de travail de l'Union européenne pour les prochaines années. Le bilan de la stratégie de sécurité intérieure précédente (pour la période 2020-2025) montre qu'une telle programmation a une réelle portée : la Commission annonçait de nombreuses initiatives qui ont effectivement abouti même si, à mesure que le temps passe, l'action s'écarte inévitablement des intentions initiales pour répondre aux circonstances.

Les stratégies successives étant des programmes de travail pour une période donnée, aucune ne ressemble réellement à la précédente. Les grands thèmes qui les sous-tendent, à l'inverse, varient assez peu : le terrorisme, la criminalité organisée ou le contrôle des frontières extérieures étaient comme maintenant des préoccupations essentielles des « pères fondateurs » de « l'espace de liberté, de sécurité et de justice » (ELSJ). Le doublement des effectifs de l'agence Europol, chargée d'appuyer les États membres dans la lutte contre la criminalité, et le triplement des effectifs de garde-frontières européens, qui dépendent de l'agence Frontex, sont d'ailleurs les propositions les plus spectaculaires de la nouvelle stratégie même si elles ont déjà été formulées par la présidente de la Commission au début de son second mandat.

Aussi l'irruption d'un thème nouveau ne peut-elle que se remarquer : en l'espèce, on est frappé par la place accordée aux menaces hybrides (un chapitre entier, de huit pages sur les trente du document publié le 1er avril). Triste signe des temps : il n'est plus concevable d'élaborer une politique de sécurité intérieure sans aborder, à côté des thèmes les plus « traditionnels », la menace croissante des opérations de déstabilisation en tout genre venues de Russie ou d'ailleurs. Le lien entre la dimension intérieure de la sécurité et sa dimension extérieure n'est évidemment pas une nouveauté : en France, le *Livre blanc sur la défense et la sécurité nationale de 2008* estimait déjà que « *la distinction entre sécurité intérieure et sécurité extérieure n'est plus pertinente* » Les tensions géopolitiques actuelles et le développement des menaces hybrides le renforcent de manière flagrante. Comment « l'Europe de la sécurité intérieure », conçue initialement pour répondre à des enjeux internes – compenser les effets de la libre circulation entre États membres – peut-elle s'adapter pour mieux prendre en compte les menaces venues de l'extérieur ?

[1] *J. Mafart, « L'"Europe de la sécurité intérieure", méconnue, mérite intérêt et moyens », Libre Belgique, 6 mars 2025.*

LES MENACES HYBRIDES, UN PHÉNOMÈNE QUI BROUILLE LA LIMITE ENTRE SÉCURITÉ INTÉRIEURE ET SÉCURITÉ EXTÉRIEURE

La notion de menace hybride est encore relativement récente dans le langage officiel. En France, la *Revue stratégique* de 2022 définit les « stratégies hybrides » comme des « *combinaisons volontairement ambigües de modes d'actions directs et indirects, militaires ou non, légaux ou non, et souvent difficilement attribuables* », qui « *peuvent avoir des conséquences importantes pour les démocraties car elles visent à les délégitimer, affaiblir leurs forces morales et leur cohésion ou réduire leur potentiel économique et de défense nationale* ».

Les menaces hybrides sont donc 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 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 du Traité de l'Atlantique nord* ». L'Union européenne a dû prendre acte de la menace hybride dans sa *Boussole stratégique*, qui énonce ses priorités en matière de sécurité et de défense : « *Des acteurs étatiques et non étatiques utilisent des stratégies hybrides, des cyberattaques, des campagnes de désinformation, l'ingérence directe dans nos élections et nos processus politiques, la contrainte économique et l'instrumentalisation des flux migratoires irréguliers. […] Nos concurrents n'hésitent pas à utiliser des technologies émergentes et de rupture pour tirer des avantages stratégiques et accroître l'efficacité de leurs campagnes hybrides.* »

Venues de l'extérieur, ces différentes menaces n'en affectent pas moins la sécurité et la stabilité au sein même des États membres et des sociétés. Les cyberattaques en sont l'exemple le plus évident, qu'il s'agisse de sabotage (pour neutraliser le système information d'une administration publique ou d'une grande entreprise de réseau par exemple), d'espionnage électronique ou de manipulation des processus électoraux. Dans son dernier rapport annuel, 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.* »

Confirmant cette menace grave, l'élection présidentielle roumaine de décembre 2024 a donné lieu à une décision sans précédent : alors que le candidat d'extrême-droite pro-russe était arrivé en tête au premier tour, la Cour constitutionnelle a annulé l'ensemble du scrutin. Entre-temps, les autorités roumaines avaient mis au jour une vaste campagne sur Tik Tok, coordonnée et financée de l'étranger, en soutien à ce candidat qui était inconnu des Roumains quelques semaines auparavant. En mars 2025, la décision de la Cour constitutionnelle roumaine de rejeter la candidature de l'intéressé a suscité des troubles dans le pays : le but initial de « l'opération hybride » n'est sans doute pas atteint, puisque M. Georgescu ne sera pas président de la République, mais de tels troubles constituent eux-mêmes un résultat tout à fait appréciable pour ses concepteurs puisque l'épisode aura contribué à fragiliser la confiance des citoyens dans les institutions démocratiques.

Les opérations d'instrumentalisation des flux migratoires, mode d'action particulièrement cynique, obéissent à la même logique : fragiliser la frontière extérieure de l'Union européenne en est l'objectif immédiat mais il s'agit aussi de saper la confiance dans les institutions et de susciter des divisions. Dans une communication du 11 décembre, la Commission indique qu'en 2024 encore, les flux irréguliers en provenance de Biélorussie ont augmenté de 66 %. Elle précise 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* ».

Le dernier rapport annuel d'Europol sur la criminalité organisée (« SOCTA ») met en évidence un autre phénomène : l'utilisation directe de réseaux criminels

par nos adversaires. « *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'Union européenne et de ses États membres.* » Cette alliance entre guerre hybride et criminalité organisée se manifeste dans de multiples domaines, qu'il s'agisse de sabotage informatique, de captation de données numériques, de campagnes sur les réseaux sociaux à partir de faux comptes ou encore de trafic d'armes. C'est une coopération mutuellement bénéfique : les États impliqués disposent d'un mode d'action supplémentaire, propre à dissimuler leur implication, tandis que les organisations criminelles en tirent des revenus, une protection contre les poursuites ou même un accès à de nouveaux moyens technologiques.

UNE MOBILISATION EUROPÉENNE ACCRUE DANS TOUS LES DOMAINES

La *Boussole stratégique* a été une étape marquante dans la prise en compte des menaces hybrides ; elle prévoit notamment la création d'une « boîte à outils hybride », ensemble d'instruments destinés à faciliter des campagnes coordonnées des États membres face aux agressions. Peu après, des conclusions du Conseil sur les menaces hybrides ont défini des orientations plus détaillées. Pourtant, l'Union européenne n'a pas attendu la *Boussole stratégique* et encore moins la nouvelle stratégie de sécurité intérieure pour prendre en compte les menaces hybrides dans ses politiques. Il en va des menaces hybrides comme du terrorisme ou de la criminalité organisée : bien des initiatives de l'Union concourent à les prévenir même si elles ont une vocation plus large.

La politique de cybersécurité en est un très bon exemple. La stratégie de cybersécurité de 2020, publiée conjointement par la Commission et le Service européen d'action extérieure (SEAE), a donné lieu notamment à la directive NIS 2 du 14 décembre 2022 (ou 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 encore le secteur spatial. L'Union européenne s'est aussi dotée d'une « unité conjointe de cybersécurité » qui propose des équipes de réaction rapide et développe une politique de prévention des cyberattaques avec les institutions publiques et les entreprises. En outre, comme le Conseil européen l'y avait invitée dans ses conclusions du 22 mai 2024, la Commission a présenté en février dernier une révision du plan d'action de 2017 qui organise la réponse commune de l'Union et de ses Etats membres aux crises de cybersécurité.

Une deuxième directive du 14 décembre 2022 doit être mentionnée : elle porte sur la résilience des entités critiques. Les Etats membres sont désormais tenus d'adopter une stratégie nationale de résilience et de procéder à une évaluation des risques au moins tous les quatre ans. Ces « entités critiques » – qu'il s'agisse de l'énergie, des transports ou encore du secteur bancaire – sont-elles-mêmes tenues de procéder à une évaluation des risques, de prendre des mesures préventives, d'organiser des contrôles et des exercices. Un troisième texte du 14 décembre 2022 complète cet arsenal : le règlement sur la résilience opérationnelle numérique du secteur financier, ou règlement DORA. Par ailleurs, les agissements de la Russie en Mer baltique ne sont pas étrangers au plan d'action publié en février 2025 pour protéger les câbles sous-marins.

La protection des institutions démocratiques, quant à elle, donne lieu à une véritable profusion d'initiatives qui ont une évidente vocation interne – l'État de droit est malheureusement menacé au sein même de l'Union – mais visent aussi à répondre à des ingérences venues de l'étranger. Le « plan d'action pour la démocratie européenne » de décembre 2020 a donné lieu à plusieurs textes importants comme le règlement du 13 mars 2024, qui renforce notamment les règles de financement des partis politiques européens. Le 26 avril

2024, la Commission a publié des « lignes directrices pour l'atténuation des risques systémiques en ligne pouvant affecter les processus électoraux » : destiné aux principaux moteurs de recherche et plates-formes Internet (ceux qui ont plus de 45 millions d'utilisateurs actifs dans l'Union), ce document publié en application du *Digital Services Act* (DSA) du 19 octobre 2022 impose aux entreprises concernées des mesures d'atténuation des risques, par exemple à l'égard de l'intelligence artificielle générative. La Commission a aussi présenté, en décembre 2023, une proposition de directive destinée à encadrer les activités de représentation d'intérêts pour le compte de pays tiers. On attend enfin la publication prochaine du « bouclier de la démocratie », destiné à mieux lutter contre les menaces hybrides dirigées contre la démocratie, notamment la désinformation en ligne. Il est révélateur que ce futur « bouclier » soit mentionné dans la stratégie de sécurité intérieure de 2025 : une fois encore, confirmation est faite que notre sécurité intérieure ne peut se concevoir sans prendre en compte des menaces d'origine extérieure.

Quant à l'instrumentalisation des flux migratoires, elle trouve un début de réponse dans le règlement « situations de crise » du 14 mai 2024 : celui-ci permet de faire face à des flux massifs à la frontière extérieure, notamment en dérogeant aux règles normales d'examen des demandes d'asile. On ne peut ignorer parallèlement la construction de clôtures par certains États membres : 13 % de la frontière extérieure (qui représente une longueur totale de 12 000 km) seraient désormais clôturés[2]. Si la Commission européenne a toujours refusé de financer de telles infrastructures, d'importantes ressources budgétaires ont été mobilisées à la demande du Conseil européen pour améliorer la sécurité de la frontière extérieure, notamment par des équipements technologiques de détection (radars, caméras, drones, etc.).

Les menaces hybrides étant multiformes, il n'est pas surprenant que la réponse de l'Union européenne le soit aussi. Mais les menaces hybrides sont aussi très évolutives, obligeant l'Union européenne à s'adapter en permanence ; l'effort accompli ces dernières années est donc loin d'épuiser la question. La nouvelle stratégie de sécurité intérieure en donne un aperçu : parmi les nombreuses mesures qui s'annoncent, on trouve par exemple la révision prochaine du *Cybersecurity Act*, un règlement du 17 avril 2019 qui fixe les missions de l'ENISA et définit le cadre européen de certification en matière de cybersécurité, une stratégie pour les 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) et des travaux portant spécifiquement sur l'instrumentalisation des flux migratoires (sujet sur lequel la Commission a déjà publié une communication en décembre 2024).

QUELLES ADAPTATIONS POUR LA POLITIQUE DE SÉCURITÉ INTÉRIEURE ?

Les développements consacrés aux menaces hybrides par la stratégie publiée le 1er avril traduisent une pleine prise en compte de l'imbrication croissante entre sécurité intérieure et sécurité extérieure. Pourtant, deux politiques publiques distinctes demeurent, avec des acteurs différents. Certes, l'Union européenne s'emploie depuis longtemps à éviter qu'elles soient complètement coupées l'une de l'autre : dans des conclusions récentes, par exemple, le Conseil se penche sur la bonne articulation, en matière de terrorisme et d'extrémisme violent, entre les politiques intérieures et extérieures de l'Union. Dans ce domaine comme dans d'autres, les enceintes « justice et affaires intérieures » (JAI) et les enceintes relevant de la politique de sécurité et de défense commune (PSDC) ont parfois des réunions communes. De même, le plan d'action sur les câbles sous-marins a fait l'objet d'une présentation aux ministres de l'intérieur en Conseil JAI, en mars dernier.

Le développement des menaces hybrides invite cependant à des remises en cause plus profondes : la nouvelle stratégie, à cet égard, doit être rapprochée d'autres travaux européens. En septembre 2024, Ursula von der Leyen annonçait une stratégie de « préparation dynamique » dans le cadre d'une approche globale des crises. Le mois suivant fut publié le rapport de l'ancien président finlandais Sauli Niinistö sur la préparation (*preparedness*

[2] An assessment of the state of the EU Schengen area and its external borders – A merited trust model to uphold Schengen legitimacy, *Parlement européen, mai 2023.*

et *readiness*) aux crises, sur lequel se fondent les travaux actuels. Il est frappant d'y constater que, parallèlement à la présence croissante des menaces hybrides dans la politique de sécurité intérieure, celle-ci est aussi considérée comme un élément essentiel de la lutte contre les menaces hybrides. On y retrouve ainsi la question des frontières : Sauli Niinistö juge essentiel « *d'assurer un contrôle efficace des frontières extérieures de l'Union par tous les moyens disponibles* ». De même, la question de l'accès aux données numériques pour les services enquêteurs, problème de police judiciaire et de renseignement très prégnant dans les enceintes « JAI » depuis plusieurs années, apparaît dans le rapport 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 du 1er avril reprend ces orientations.

C'est donc assez naturellement qu'on en vient aux questions de renseignement. Aux termes de l'article 4 du traité sur l'Union européenne (TUE), « *la sécurité nationale reste de la seule responsabilité de chaque État membre* ». C'est ce qui garantit la compétence des Etats membres en matière de renseignement. C'est ainsi que le Conseil s'est fermement opposé, dans le règlement Europol du 8 juin 2022, à ce que l'agence fût habilitée à introduire elle-même dans le système d'information Schengen (SIS) des signalements concernant des suspects (notamment en matière de terrorisme) sur la base d'informations provenant de pays tiers. En pratique, pourtant, la distinction entre la sécurité nationale et les compétences de l'Union a beaucoup perdu de sa netteté, soit sous l'effet de la jurisprudence européenne – l'arrêt *Tele 2* de la CJUE, en particulier, a remis en cause la possibilité pour les Etats membres d'obliger les opérateurs de téléphonie et d'Internet à conserver les données de connexion de leurs abonnés pour les besoins éventuels des enquêtes[3] – soit par la volonté des États membres eux-mêmes. Un exemple, parmi bien d'autres : même si elle a aussi une finalité judiciaire, la directive PNR du 27 avril 2016 – adoptée à la demande insistante du Conseil – organise un dispositif de recueil et de traitement de données à des fins purement administratives de prévention, c'est-à-dire à des fins de renseignement[4].

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* ». Conscient de s'aventurer en terrain miné, Sauli Niinistö s'exprime avec une extrême prudence. Pourtant, cette proposition met en évidence un aspect fondamental : en affaiblissant la distinction entre sécurité intérieure et sécurité extérieure, les menaces hybrides brouillent aussi, encore plus qu'auparavant, la frontière entre les compétences de l'Union et celles de ses Etats membres. Du reste, le rapport Niinistö propose aussi la création d'un réseau « anti-sabotage » : une fois encore, l'articulation entre l'Union et ses États membres est délicate puisqu'on est dans le domaine du renseignement et même du contre-espionnage.

Dans une perspective « souverainiste », ces différentes évolutions pourraient conduire à redouter de nouvelles atteintes aux compétences des États membres. Ce serait assez vain : la faiblesse – et le paradoxe – d'une approche purement « souverainiste » tient à ce que, plus on perçoit les évolutions européennes comme exogènes et attentatoires aux prérogatives des États, plus on a tendance à se rendre impuissant faute de comprendre comment le vecteur extraordinairement puissant de l'Union européenne, en dépit de ses lenteurs, peut être utilisé pour promouvoir des politiques efficaces. L'intérêt des réflexions actuelles sur « l'Europe de la sécurité intérieure » et sur son articulation avec les menaces extérieures tient plutôt à ce qu'elles nous invitent à organiser un véritable concert européen. Les États membres sont seuls responsables devant les peuples

[3] *« Si l'efficacité de la lutte contre la criminalité grave […] peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte » ; CJUE, 21 décembre 2016, Tele 2 Sverige, § 103. – En France, la jurisprudence du Conseil d'Etat a permis de maintenir un dispositif opérationnel d'exploitation des données de connexion ; CE, 21 avril 2021, no 393099, Quadrature du Net.*

[4] *Les données PNR sont celles que fournissent les voyageurs au moment de la réservation, notamment lors de l'achat d'un billet d'avion (identité, adresse, date du voyage, moyen de paiement, itinéraire complet, etc.). Combinées avec les données API (les données fournies au moment de l'enregistrement du voyageur), elles permettent d'opérer une démarche d'analyse de risque à grande échelle pour détecter les passagers qui correspondent à des « profils de risque » prédéfinis (notamment en matière de terrorisme ou de trafic de stupéfiants). Les données PNR peuvent aussi être confrontées aux fichiers de police européens ou nationaux à des fins de recherche de personnes ou d'investigation judiciaire.*

de leur bien premier, la sécurité ; il ne peut en être autrement même si la Commission donne parfois l'impression d'avoir une idée derrière la tête (pourquoi doubler ou tripler les effectifs d'une agence avant même d'avoir évalué les besoins ?).

L'apport de l'Union et de ses agences en matière de sécurité est devenu décisif, y compris dans des domaines, comme le terrorisme, où certains États membres entendaient rester seuls maîtres à bord il y a encore une quinzaine d'années. Tous ont beaucoup appris des crises de la décennie écoulée, qu'il s'agisse des vagues migratoires, des attentats terroristes ou du COVID : il est maintenant prouvé qu'ils sont capables de s'organiser de manière souple et réactive pour traiter des crises à l'échelon européen. C'est sans doute à un tel effort d'organisation et de travail en réseau, dans le respect des compétences de chacun, que nous invitent aujourd'hui les menaces hybrides. Les travaux de l'Union européenne sur la préparation aux crises seront donc décisifs : un des enjeux essentiels est de mettre en relation des acteurs et des politiques publiques encore trop séparés. En ce sens, la nouvelle stratégie européenne de sécurité intérieure est d'une portée très supérieure aux mesures qu'elle contient.

Jean Mafart

Préfet, ancien directeur des affaires européennes et internationales du ministère de l'intérieur, auteur de la Politique européenne de sécurité intérieure (Bruylant, à paraître)

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

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