Informations préliminaires

Session I: Protection et sécurité de l'Union européenne. Les menaces hybrides, un facteur externe de déstabilisation pour l'Europe

Introduction

L'Union européenne est une organisation particulière. Il s'agit d'une structure supranationale qui ne ressemble à aucune autre, qu'elle soit contemporaine ou historique, fondéesur des valeurs telles que la démocratie, l'État de droit, la tolérance, le pluralisme et le respect des droits de l'homme. Les valeurs de l'UE comprennent également la coopération loyale, le respect des structures politiques et constitutionnelles fondamentales des différents États membres, le libre marché, la coopération ainsi que le dialogue et le consensus. Une organisation fondée sur des valeurs, des principes et des idéaux est particulièrement exposée à diverses formes de déstabilisation et de menaces. C'est pourquoi les mécanismes visant à la protéger contre la déstabilisation, l'affaiblissement de son attractivité axiologique et sa cohérence interne, ainsi que de sa capacité à agir de manière proactive et à repousser les menaces, sont si importants.

Le renforcement de la résilience est une tâche essentielle pour l'UE. Au-delà du conflit armé à grande échelle en Ukraine, l'UE est confrontée à de nombreuses autres menaces, moins évidentes. Celles-ci mettent en péril l'unité de l'Union européenne et sa capacité d'action et, dans certains cas, remettent également en question ses principes, et toujours - ce qui est en pratique le plus dangereux - érodent la confiance du public en mettant l'équation entre la moralité et la force définie comme la vitalité, l'action efficace, la résilience face aux menaces et aux défis.

Le champ des activités hybrides est presque illimité. Il peut s'agir d'espaces politiques, diplomatiques, de désinformation et de propagande, économiques, culturels, sociaux, militaires et humanitaires. Les menaces hybrides sont diverses et en constante évolution. Ces activités peuvent être menées par des agents des services secrets d'un État étranger et leur collaborateurs, ainsi que - consciemment ou non - par des organisations, des associations, des institutions, des partis politiques, des entreprises, des sociétés et même de certaines figures médiatiques. Ceci dit, il convient de souligner que les actions hybrides sont généralement d'une nature telle qu'il est difficile de les catégoriser clairement et d'en attribuer la responsabilité à des auteurs. Cela rend difficile leur reconnaissance initiale et leur définition.

Actualités

En 2016, l'Union européenne, dans le « Cadre commun en matière de lutte contre les menaces hybrides », a défini les menaces hybrides comme *« une combinaison d'actions répressives et subversives ayant recours à des méthodes conventionnelles et non conventionnelles (c'est-à-dire diplomatiques, militaires, économiques et technologiques) qui peuvent être utilisées de manière coordonnée par des acteurs étatiques et non étatiques pour atteindre des objectifs spécifiques, avec des actions restant en dessous du seuil d'une guerre officiellement déclarée ».*. Elles peuvent être utilisées pour poursuivre divers objectifs stratégiques, opérationnels et tactiques, dont le dénominateur commun est de déstabiliser les États membres et la Communauté dans son ensemble et d'interférer dans leurs processus politiques, sociaux et économiques.

L'approche flexible de l'Union sur cette question découle de la spécificité du phénomène lui-même, qui est complexe, multiforme et ambigu, et reflète les différentes perspectives de sécurité et priorités de politique étrangère des États membres. Cette approche permet de prendre en compte à la fois les menaces venant de l'est (Russie, Bélarus) et du sud (Iran, organisations terroristes, migration irrégulière) et celles à portée mondiale (Chine). Le catalogue des méthodes et tactiques hybrides comprend entre autres les activités de désinformation et de propagande, les cyberattaques, l'ingérence dans les processus politiques (par ex. les élections et les référendums), les pressions économiques, l'instrumentalisation de la migration irrégulière, le soutien de l'État à des groupes armés et l'emploi de mercenaires, les opérations de renseignement de diversion et de sabotage, les activités terroristes ainsi que l'utilisation d'agents chimiques, biologiques, radiologiques et nucléaires (CBRN). Depuis 2015, l'UE a été confrontée à des activités hybrides hostiles provenant principalement de la Russie. Dans une moindre mesure, mais avec une nette tendance à la hausse, ces méthodes sont également utilisées par, le Bélarus, l'Iran et la Corée du Nord, ainsi que par des organisations terroristes et des cercles radicaux.

Les méthodes hybrides peuvent être utilisées à des degrés et à des intensités variables et peuvent être librement combinées par des agresseurs étatiques ou non étatiques dont le modus operandi n'est pas le même. De plus, le catalogue des outils de guerre hybride reste ouvert. Selon les institutions européennes, son expansion est due notamment à la rivalité politique croissante impliquant la Russie (surtout après l'invasion de l'Ukraine) et la Chine, à la situation instable dans le voisinage de l'UE et à la soi-disant weaponisation de nouveaux secteurs (par ex. la santé, le climat et l'environnement).

Depuis 2016, l'UE développe des capacités pour contrer ces menaces hybrides dans quatre domaines : 1) la conscience situationnelle, 2) le renforcement de la résilience, 3) la prévention et la gestion des crises, 4) la coopération internationale (en particulier avec l'OTAN).

La Boussole stratégique de l'UE appelle au renforcement de ces capacités dans le cadre de la réponse coordonnée de l'Union aux crises provoquées par des méthodes hybrides et, surtout, à la création de nouveaux mécanismes et à l'amélioration de leur utilisation. La responsabilité de la lutte contre les menaces hybrides incombe (conformément à l'article 4, paragraphe 2, du TUE) actuellement aux institutions nationales de sécurité (c'est-à-dire services de renseignement , la police et l'armée), qui disposent de l'autorité légale et des pouvoirs d'exécution nécessaires. La Boussole stratégique n'apporte aucun changement dans ce domaine. Les instruments développés dans le cadre de la Boîte à outils hybride de l'UE afin d'obtenir des synergies et une réponse plus efficace sont plutôt destinés à fournir un plus grand soutien aux efforts nationaux de lutte contre les menaces hybrides et à coordonner l'action conjointe des États membres.

Le renforcement de la résilience des pays de l'Union et de leurs sociétés vise à réduire leur vulnérabilité à la désinformation et à la propagande hostiles et à renforcer la protection de leurs infrastructures critiques contre les cyberattaques, le terrorisme, le détournement et le sabotage. La Boussole stratégique accorde une attention particulière au renforcement de la résistance de l'UE à la manipulation étrangère de l'information et à l'ingérence dans les processus politiques.

L'approche de l'UE en matière de lutte contre la manipulation de l'information se compose de quatre éléments adoptés par la Commission européenne en décembre 2018 dans le plan d'action contre la désinformation (*The Action Plan against Disinformation*): 1) renforcer la capacité des institutions de l'UE à détecter, analyser et dénoncer la désinformation; 2) renforcer les réponses coordonnées et collaboratives à la désinformation; 3) mobiliser le secteur privé pour lutter contre la désinformation; et 4) sensibiliser et améliorer la résilience du public en soutenant le journalisme indépendant, les initiatives de vérification des faits (*fact-checking*) et en promouvant l'éducation médiatique.

En réponse aux campagnes de désinformation et psychologique russes, le Service européen pour l'action extérieure a créé en 2015 le groupe de travail *East StratCom*pour pour surveiller, analyser et répondre à la propagande et à la désinformation russes. L'équipe, qui ne comptait à l'origine que trois personnes, emploie aujourd'hui 16 personnes à temps plein, ce qui constitue la meilleure indication de l'importance de cette unité dans l'UE. *East StratCom* surveille les informations publiées dans plus de 20 langues. L'équipe a identifié des dizaines de milliers de cas de désinformation russe, qui ont été répertoriés dans la base de données *EUvsDisinfo*. Elle assure également la formation du personnel des pays partenaires, travaille au renforcement du journalisme indépendant et promeut la connaissance de l'UE et de ses politiques dans les pays du Partenariat oriental. Des tâches similaires sont effectuées par des équipes analogues (six personnes à temps plein chacune) créées en 2017, responsables de la région des Balkans occidentaux (*Western Balkans Task Force*) et du Moyen-Orient et de

l'Afrique du Nord (*South Stratcom Task Force*), qui se concentrent sur la lutte contre la radicalisation, la lutte contre la propagande des organisations terroristes et la désinformation de la Russie et, de l'Iran parmi les autres. Toutes ces équipes font partie de la division «Communication stratégique, task force et analyse de l'information» du Service européen pour l'action extérieure, qui aide les institutions de l'UE à planifier des politiques, des stratégies et des outils de communication stratégique. Il fournit également un soutien (par ex. des analyses et des instructions pour lutter contre la désinformation) aux missions diplomatiques de l'UE, aux missions et aux opérations de la politique de sécurité et de défense commune (PSDC). La division développe également la coopération avec les pays partenaires, le G7, les ONG, la société civile et le secteur privé (par ex. sur l'acquisition de données à l'aide de logiciels et de technologies modernes). L'objectif de ces activités est de sensibiliser le public et de renforcer la résilience des États face à la désinformation dans le voisinage de l'UE.

La coopération entre l'Union européenne et l'OTAN en matière de communication stratégique a pour objectif d'assurer une communication efficace et une action conjointe face aux défis de sécurité. Un exemple de cette coopération est l'interaction entre l'unité East StratCom de l'UE et le NATO Strategic Communications Centre of Excellence (NATO StratCom COE) basé à Riga. Les principaux objectifs de cette coopération incluent le partage d'expériences et de bonnes pratiques, permettant ainsi une complémentarité dans l'analyse et la lutte contre la désinformation. De plus, la coordination des activités dans les domaines de la communication stratégique et de la cybersécurité permet d'atteindre un effet de synergie.. Cette coopération est essentielle dans un environnement géopolitique complexe et en constante évolution.

Le renforcement de la résilience des États de l'UE concerne également des secteurs clés tels que la cybersécurité, les infrastructures critiques, l'énergie, les transports, la défense, le système financier, la sécurité maritime ou l'espace. Cet effort est principalement orienté vers la création d'instruments juridiques et de capacités de réponse aux incidents et aux crises provoqués par des méthodes hybrides (en particulier dans le cyberespace). L'adoption de la directive sur la sécurité des réseaux et des systèmes d'information (dite directive SRI) en 2016 a constitué une avancée significative dans l'approche de l'UE en matière de cybersécurité. Elle oblige les États membres à garantir une norme minimale commune de cybersécurité, notamment par l'adoption de stratégies nationales de cybersécurité ou la création d'équipes d'intervention en cas d'urgence informatique, qui fonctionneront dans le cadre du réseau européen CERT. L'Union a également rendu obligatoire la déclaration des cyberincidents pour les prestataires de services essentiels dans les secteurs de l'énergie, des transports, de la banque et de la finance, des soins de santé, de l'approvisionnement en eau ou des infrastructures numériques. L'UE, par l'intermédiaire de l'Agence européenne pour la cybersécurité (ENISA) et de l'Organisation européenne pour la cybersécurité (ECSO), soutient

également, outre la réglementation, les activités de recherche et la coopération entre les secteurs public et privé. Les capacités de cyberdéfense des États membres sont, quant à elles, développées dans le cadre de quatre projets de coopération structurée de la PESCO, portant sur le partage d'informations sur les cyberincidents, la coordination des opérations, le soutien et la réponse conjointe, ainsi que la recherche et la formation. En décembre 2020, l'Union a adopté une nouvelle stratégie de cybersécurité visant à accroître la résilience des États membres face aux cyberattaques et de mieux protéger les infrastructures critiques contre celles-ci. Un exemple d'action sectorielle dans ce domaine est la boîte à outils de cyberdiplomatie de l'UE destinée à dissuader les cyberagresseurs potentiels (EU Cyber Diplomacy Toolbox). En mai 2019 un régime de sanctions a été élaboré dans ce cadre pour répondre aux cyberattaques perpétrées depuis l'extérieur de l'UE contre des États membres ou utilisant des infrastructures situées en dehors de la Communauté. Les entités figurant sur la « liste noire » en tant que responsables de cyberattaques contre des pays de l'UE ou soutenant celles-ci seront sanctionnées par une interdiction d'entrée dans l'UE ou par le gel de leurs avoirs. Un régime de sanctions similaire a été introduit à l'encontre des États qui utilisent des armes chimiques (la liste classifiée contient 20 substances), en réponse directe à l'utilisation par les services spéciaux russes du gaz neurotoxique Novitchok sur le territoire britannique. Entre 2019 et 2022, l'UE a également apporté un soutien financier d'un montant total de 11,6 millions d'euros à l'Organisation pour l'interdiction des armes chimiques (OIAC) pour ses travaux de lutte contre le développement et l'utilisation d'armes chimiques.

Défis

Les défis liés au renforcement de la résilience de l'UE et de ses États membres sont surtout marqués par l'hybridité des actions consciemment et délibérément entreprises par des acteurs cherchant, pour diverses raisons, à fragiliser la cohésion de l'Union. Les caractéristiques des menaces hybrides - notamment leur multidirectionnalité, leur caractère clandestin et l'utilisation de moyens variés qui évoluent dans le temps -constituent un défi majeur pour l'UE.

Un défi observé depuis longtemps est la complexité des menaces hybrides. Bien que l'UE recense tout un catalogue de méthodes de guerre hybride, leur classification complète reste difficile en raison de leur variabilité et de leur nature multiforme. Le deuxième défi majeur réside dans l'élargissement des secteurs susceptibles d'être instrumentalisés " (notamment la sécurité énergétique, la santé, l'information, le changement climatique, la protection de l'environnement ou les nouvelles technologies liées à l'intelligence artificielle). Cela signifie qu'il existe un nombre croissant de secteurs dits stratégiques qui pourraient constituer au moins un domaine potentiel d'action hybride. En outre, la région de la mer Baltique illustre bien le

caractère multidirectionnel et dangereux des actions hybrides. Les activités hybrides de la Russie y comprennent notamment l'utilisation de la flotte fantôme, sabotage du réseau de télécommunications, interférence des signaux GPS ou menaces écologiques.

L'approche de l'UE en matière de lutte contre les menaces hybrides se concentre uniquement sur leur dimension non militaire (c'est-à-dire la désinformation, la propagande, les cyberattaques), sans développer suffisamment de capacité de réponse militaire lors même que l'ensemble du spectre des méthodes hybrides (y compris militaires ou paramilitaires) est utilisé. C'est pourquoi l'Union devrait examiner quel pourrait être le rôle de la force de déploiement rapide (*Rapid Deployment Capacity*) lors d'une crise hybride sur le territoire des États membres, ce qui permettrait d'envoyer un signal clair à l'agresseur pour lui signifier qu'une nouvelle escalade de la situation donnerait lieu à une réponse ferme de la part de l'Union. Ces actions devraient être entreprises en consultation avec l'OTAN, sur la base de la complémentarité entre les deux organisations et en même temps elle devraient renforcer le pilier européen de l'Alliance.

En outre, il semble également qu'un défi important pour l'Union consiste à faire preuve de plus d'audace dans l'utilisation des instruments déjà en place. L'UE devrait définir clairement les conditions d'utilisation de la clause de solidarité ou la clause d'assistance mutuelle. Cela renforcerait la sécurité des États membres, qui pourraient compter sur l'action simultanée et cohérente de l'Union et de l'OTAN (d'autant plus que, dans la lutte contre les menaces hybrides, l'UE déclare explicitement sa coopération étroite avec l'OTAN). L'ambiguïté des actions hybrides crée un risque d'interprétations divergentes de la situation de crise, prolongeant les processus de décision au sein de l'UE et ralentissant ainsi la réponse ou la rendant inadéquate. Il est possible de les minimiser, notamment en élaborant des solutions par le biais de simulations et d'exercices, tant au sein de l'UE qu'en coopération avec l'OTAN, sur la base de scénarios réalistes de crise hybrides . Ces solutions doivent également prendre en compte les formes d'attaques possibles à l'avenir, en utilisant de nouvelles méthodes et tactiques.

Points de discussion

1. L'UE peut-elle contrer efficacement les menaces hybrides plutôt que d'agir uniquement en réaction ?L'UE peut-elle contrer efficacement les menaces hybrides au lieu d'agir en réaction?
2. Comment lutter contre la désinformation et la propagande sans compromettre la liberté d'expression et le pluralisme?
3. Comment informer efficacement le public sur les menaces hybrides?
4. Les outils actuels de l'UE sont-ils suffisants pour lutter contre les menaces hybrides, ou faut-il développer de nouvelles solutions?

5. Comment l'intelligence artificielle peut-elle être utilisée pour déstabiliser l'UE et comment s'en prémunir?
6. Comment protéger les éléments clés du système démocratique contre les ingérences extérieures?
7. Comment maintenir la démocratie et l'État de droit tout en renforçant la résilience de l'UE?