

# MENER LA GUERRE SANS LA DÉCLARER: LA BELGIQUE FACE AUX MENACES HYBRIDES

Frédéric FREZIN



© image generated by AI

**I**n een steeds complexer veiligheidslandschap waar oorlogen nog zelden formeel worden verklaard, wordt België geconfronteerd met toenemende hybride dreigingen. Als gastland van de NAVO en de EU, maar ook als spil in de Europese logistieke en diplomatieke netwerken, speelt ons land een sleutelrol en vormt het een aantrekkelijk doelwit. Dit artikel werpt een strategische blik op hoe België, in een gefragmenteerd institutioneel landschap, zijn weerbaarheid opbouwt tegen cyberaanvallen, sabotage, desinformatie en buitenlandse inmenging. Aan de hand van modellen die gebruikt worden in buurlanden (Noorwegen, Zweden, Finland, Nederland) worden knelpunten blootgelegd en pistes aangereikt voor een systemisch en toekomstgericht veiligheidsbeleid.

*Le major d'aviation Frédéric FREZIN est officier de renseignement de la force aérienne. Il occupe depuis 2024 un poste au sein du desk transversal du département d'état-major Stratégie et pilote les dossiers liés aux menaces hybrides. Tout au long de sa carrière, il a acquis une solide expérience dans l'analyse stratégique des menaces tant conventionnelles qu'asymétriques, aussi bien au niveau national que multinational et opérationnel.*

## **COMPRENDRE LA MENACE HYBRIDE : UNE GUERRE SOUS LE SEUIL**

Les menaces hybrides désignent un ensemble d'activités hostiles, menées par des acteurs étatiques ou non étatiques, qui combinent de manière coordonnée des moyens très variés – notamment numériques, informationnels, économiques, diplomatiques et militaires non conventionnels – dans le but d'affaiblir les fondements d'une société tout en évitant un affrontement militaire direct. Ces menaces se déploient dans une zone grise, en dessous du seuil classique de la guerre formelle, ce qui les rend difficiles à détecter, à attribuer et à contrer. Le caractère asymétrique, diffus et souvent non revendiqué de ces actions renforce leur dangerosité, d'autant qu'elles ciblent volontairement les vulnérabilités spécifiques des sociétés démocratiques telles que la liberté d'expression, la polarisation politique, la transparence des institutions ou encore la dépendance technologique.

Ces activités s'inscrivent dans un continuum entre paix, crise et conflit, brouillant délibérément les repères traditionnels de la conflictualité. Elles visent à saper la cohésion sociale, à éroder la confiance dans les institutions publiques et à influencer les prises de décisions politiques et stratégiques, voire à désorganiser la chaîne de commandement dans les moments critiques. L'ambiguïté occupe une place centrale car elle permet à l'agresseur d'atteindre des objectifs politiques ou stratégiques tout en réduisant les risques de représailles directes. Le rapport coût-bénéfice est systématiquement avantageux, en générant des retombées disproportionnées avec des moyens indirects.

Dans ce contexte, il est essentiel de distinguer deux concepts souvent utilisés de manière interchangeable, mais qui renvoient à des logiques différentes, à savoir les **menaces hybrides** (*hybrid threats*) et la **guerre hybride** (*hybrid warfare*)<sup>1</sup> :

- Les **menaces hybrides** combinent un large éventail de moyens non violents pour cibler les vulnérabilités de l'ensemble d'une société afin de compromettre le fonctionnement, l'unité ou la volonté des cibles, tout en dégradant et en remettant en cause le statu quo. Cette stratégie est principalement utilisée par des acteurs révisionnistes<sup>2</sup> pour atteindre progressivement leurs objectifs sans déclencher de réponses décisives, y compris armées.
- La **guerre hybride** est le défi posé par la complexité croissante des conflits armés, où les adversaires peuvent combiner différents types de guerre et de moyens non militaires pour neutraliser la puissance militaire conventionnelle.

---

<sup>1</sup> Sean Monaghan, « Countering Hybrid Warfare – So What for the Future Joint Force?, » PRISM 8 (Irregular Warfare Center), n° 2 (2019): 87, <https://irregularwarfarecenter.org/wp-content/uploads/8-2-PRISM.pdf>.

<sup>2</sup> Ce terme est utilisé pour désigner des États ou des entités qui cherchent à remettre en cause l'ordre international existant, souvent en contestant les normes, institutions et équilibres de pouvoir établis après la Seconde Guerre mondiale. Le terme est souvent appliqué à des puissances comme la Russie ou la Chine qui utilisent des stratégies hybrides ou non conventionnelles pour affaiblir ou modifier l'ordre géopolitique à leur avantage, sans recourir directement à une guerre ouverte.

Il convient de noter que ces deux défis ont la même cause fondamentale : des acteurs révisionnistes et des adversaires cherchant à neutraliser le pouvoir conventionnel d'un État pour atteindre leurs objectifs. Cependant, chaque stratégie est conçue pour cibler les composantes distinctes de la capacité d'un État à protéger la sécurité nationale. Pour reprendre les termes de Clausewitz<sup>3</sup>, les menaces hybrides ciblent principalement la volonté (de résistance) d'un peuple et la capacité de décision d'un gouvernement, tandis que la guerre hybride s'attaque avant tout à l'efficacité d'une armée à mener des opérations réussies. Chacun de ces défis exige donc des contre-mesures spécifiques et a des implications variées pour la politique, la stratégie et les capacités de défense à tous les niveaux de la guerre. Chaque défi s'inscrit dans un continuum illustré par le schéma ci-dessous<sup>4</sup> :

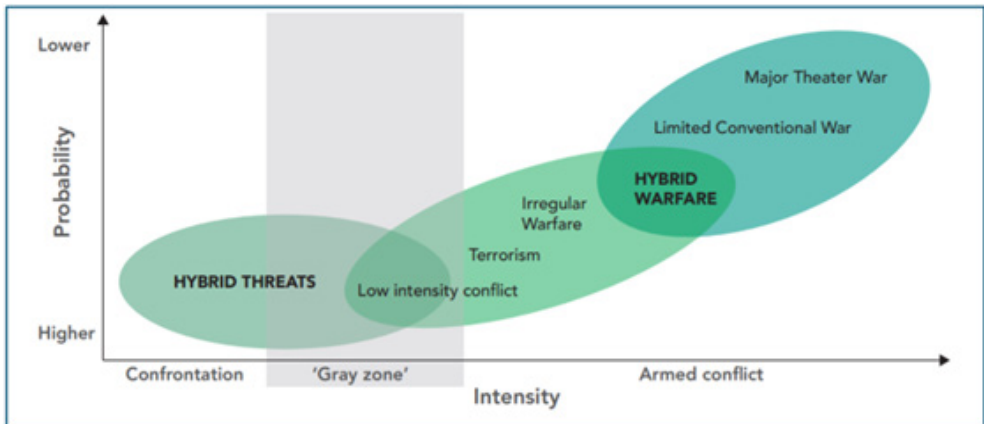


Fig 1: Hybrid Threats et Hybrid Warfare sur un continuum de conflit

Les cas russe et chinois illustrent deux formes caractéristiques de cette menace. La Russie privilégie une approche de confrontation directe en dessous du seuil de la guerre, mêlant désinformation agressive, cyberattaques, sabotage, guerre psychologique et présence militaire dissimulée, comme l'ont démontré les guerres en Ukraine, en Géorgie ou encore les attaques dans le cyberspace européen.

<sup>3</sup> Cette stratégie, qui privilégie l'attaque des volontés politiques et sociales plutôt que des cibles strictement militaires s'inscrit dans une logique clausewitzienne. Selon Clausewitz, « la guerre est un acte de violence destiné à contraindre l'adversaire à exécuter notre volonté » (*Vom Kriege*, Livre I, Chapitre 1). Dans le cadre des menaces hybrides, cela se traduit par des actions visant la population, puisqu'elle est perçue comme un centre de gravité morale et politique.

<sup>4</sup> Monaghan, « Countering Hybrid Warfare, » 87.

Elle s'appuie sur des doctrines de désintégration stratégique et de domination cognitive, héritées des « mesures actives » soviétiques<sup>5</sup>. La Chine, quant à elle, adopte une stratégie d'influence prolongée, fondée sur la captation technologique, l'expansion économique ciblée, la création de dépendances critiques et la modification progressive de l'environnement normatif international à son avantage<sup>6</sup>.

Face à ces approches différenciées, mais complémentaires, il est essentiel de ne pas réduire les menaces hybrides à une simple liste d'outils ou de techniques. Leur efficacité réside précisément dans leur capacité à croiser plusieurs domaines simultanément, à opérer en temps de paix comme en période de crise et à dissoudre les frontières non seulement entre sécurité intérieure et extérieure, mais aussi entre sphères civile et militaire. La Belgique, en tant qu'État ouvert, interconnecté et exposé, doit donc développer une compréhension stratégique de la menace hybride, centrée non seulement sur les moyens employés, mais aussi – et surtout – sur les intentions de l'adversaire et les effets produits sur son tissu démocratique.

## LA BELGIQUE : CIBLE DE CHOIX ?

La Belgique constitue une cible stratégique pour les menaces hybrides en raison de sa position géographique, ses infrastructures critiques et son rôle central au sein de l'Union européenne (UE) et de l'OTAN. En tant que pays hôte d'institutions euro-atlantiques et soutien affirmé à l'Ukraine, notre pays représente un objectif symbolique pour les campagnes hybrides, notamment celles menées par la Russie.<sup>7</sup>

Les infrastructures critiques belges sont des cibles privilégiées. Les pipelines, lignes de communication, ports et réseaux de transport jouent un rôle-clé dans l'économie et dans la logistique militaire. Le pipeline de l'OTAN géré par la *Belgian Pipeline*

---

<sup>5</sup> Jean Tienhoven, « Hybride oorlogsvoering: Oude Wijn in Nieuwe Zakken? », (certificaat Inlichtingenstudies, 2024), 17-19.

<sup>6</sup> « Lutte contre les menaces hybrides », OTAN, consulté le 15 avril 2025, [https://www.nato.int/cps/en/natohq/topics\\_156338.htm?selectedLocale=fr](https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=fr).

<sup>7</sup> Seth G. Jones, *Russia's Shadow War Against the West* (Washington: Center for Strategic and International Studies, 2025), <https://www.csis.org>.

*Organisation*, ainsi que les hubs logistiques stratégiques (portuaires et terrestres), sont identifiés comme des cibles prioritaires dans le contexte du soutien logistique militaire allié.

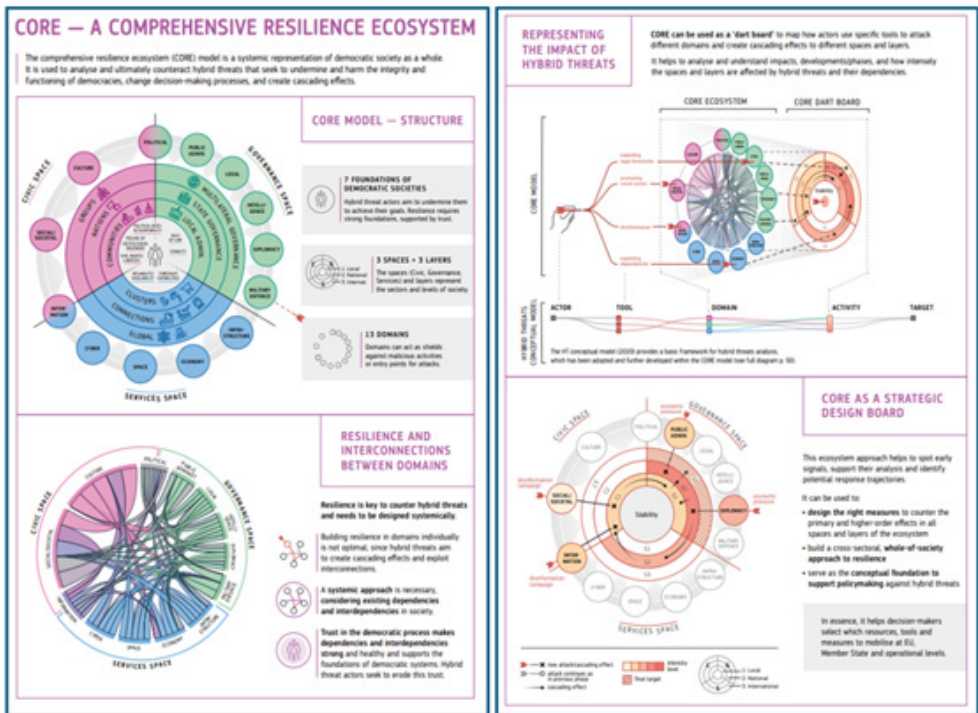
La Belgique abrite également des câbles sous-marins critiques pour les communications intercontinentales, particulièrement exposés aux actions malveillantes. Des tentatives d'interférences physiques russes sur ces câbles ont été observées en Europe. À cela s'ajoutent des activités hybrides plus classiques : désinformation, cyberattaques, espionnage diplomatique, ingérences politiques et violations maritimes.

La Belgique est aussi concernée par la dimension transnationale des menaces hybrides, comme l'illustrent des cas récents en mer Rouge et en mer Baltique. Ces incidents montrent comment des acteurs soutenus par des puissances étatiques peuvent perturber les intérêts européens dans des zones éloignées, affectant directement ou indirectement la Belgique.

La Belgique est perçue à cet égard comme un centre névralgique, dont la déstabilisation – même temporaire – pourrait avoir un impact disproportionné sur les structures euro-atlantiques. Elle doit donc renforcer sa résilience en améliorant ses dispositifs de détection interinstitutionnels et en consolidant la coopération avec ses alliés, pour assurer ainsi la continuité de ses fonctions vitales en cas de pression hybride. Au-delà de cette résilience interne, la Belgique doit aussi adopter une posture stratégique élargie, anticipant les effets de menaces hybrides susceptibles de viser ses ressortissants, ses flux économiques ou ses intérêts sécuritaires, y compris à l'étranger.

## APPROCHE FACE AUX MENACES HYBRIDES : CADRES INTERNATIONAUX

Face à la complexité des menaces hybrides, une réponse globale, systémique et coordonnée est indispensable. Dans ce contexte, le modèle « CORE » du Hybrid CoE (le Centre européen d'excellence pour la lutte contre les menaces hybrides)<sup>8</sup> propose une approche écosystémique, soulignant que les attaques dans un domaine (par exemple, l'information) peuvent avoir des effets en cascade sur d'autres (tels que la confiance, l'économie ou la sécurité). La résilience ne peut donc plus être conçue de façon sectorielle, mais doit mobiliser l'État, la société civile, le secteur privé et les citoyens, comme l'illustrent les schémas suivants<sup>9</sup> :



<sup>8</sup> Hybrid CoE, *CORE – A Comprehensive Resilience Ecosystem* (Luxembourg: Publications Office of the European Union, 2023), [https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE\\_comprehensive\\_resilience\\_ecosystem.pdf](https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf)

<sup>9</sup> Ibid., pp. 10–11.

Bien que la lutte contre les menaces hybrides relève avant tout de la responsabilité nationale, l'UE complète l'action nationale en facilitant la coopération, en développant des outils politiques et en encourageant les bonnes pratiques.<sup>10</sup> La politique de l'UE dans le domaine des menaces hybrides repose sur quatre axes d'action<sup>11</sup> :



**Fig 3: La politique de l'UE contre les menaces hybrides repose sur quatre lignes d'action**

Pour sa part, l'OTAN met en place depuis 2015 une stratégie pour contrer les menaces hybrides, articulée autour de quatre piliers :

1. Préparation : identification des vulnérabilités, coordination des réponses et mutualisation de l'expertise (cyber, communication, infrastructures critiques)<sup>12</sup> ;
2. Dissuasion : renforcement de la posture de défense, amélioration de la réactivité et développement d'un catalogue de réponses adaptées ;
3. Contestation : recours à la communication stratégique et à la planification militaire ;
4. Défense : assistance aux Alliés attaqués et activation potentielle de l'article 5 du traité de Washington.

<sup>10</sup> Le cadre européen repose sur le cadre commun de 2016, la communication conjointe de 2018 et une stratégie en cours d'élaboration axée spécifiquement sur la Russie.

<sup>11</sup> « Hybrid Threats, » Commission européenne, consulté le 17 avril 2025, [https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats\\_en](https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en).

<sup>12</sup> OTAN, *Révision des modalités des Counter Hybrid Support Teams et rôle du Operations Policy Committee Hybrid (OPC Hybrid)*, document AC/332-WP(2025)0003-REV3 [non classifié], transmis par canal sécurisé, janvier 2025.

L'OTAN collabore également avec les centres d'excellence relatifs à la communication stratégique (Riga), à la cybergdéfense (Tallinn) et à l'énergie (Vilnius).

L'UE et l'OTAN reconnaissent donc qu'aucun État ne peut affronter seul une crise hybride. Une coopération renforcée est dès lors essentielle pour éviter les redondances, mieux coordonner les moyens et assurer une complémentarité entre les outils civils (UE) et militaires (OTAN). Des différences d'adhésion ou de priorités entre membres compliquent toutefois cette synergie indispensable.

## **LA RÉPONSE BELGE: UNE ARCHITECTURE EN CONSTRUCTION**

En 2021, la Belgique a adopté une Stratégie de sécurité nationale<sup>13</sup> qui sous-tend sa politique en matière de sécurité. Elle identifie les menaces majeures, dont les menaces hybrides, et repose sur l'idée que les dimensions internes et externes de la sécurité sont indissociables. Elle promeut en outre une approche intégrée, combinant le renforcement de la résilience nationale et l'action extérieure afin d'aboutir à un ordre international fondé sur des règles. Cette vision s'aligne sur les orientations de l'UE et de l'OTAN.

Très concrètement, la Belgique est en train de développer une architecture de planification cohérente articulée autour de trois plans stratégiques interdépendants qui traduisent les objectifs de sa Stratégie de sécurité nationale :

- un plan national de résilience (BNR-P) coordonné par le Centre de crise national (NCCN) ;
- un plan national de défense (BND-P) ;
- et un plan national d'*enablement* (BNE-P).

---

<sup>13</sup> Gouvernement fédéral belge, cellule stratégique Sécurité et Relations internationales, Stratégie de sécurité nationale (Bruxelles : Gouvernement fédéral belge, 2021), [https://premier.be/sites/default/files/2025-02/Strategie\\_de\\_securite\\_nationale.pdf](https://premier.be/sites/default/files/2025-02/Strategie_de_securite_nationale.pdf). [Strategie de securite nationale.pdf](https://premier.be/sites/default/files/2025-02/Strategie_de_securite_nationale.pdf)

Ces trois plans sont coordonnés par la Défense en étroite collaboration avec les services de sécurité, les entités fédérées et le secteur privé.

Cette trilogie assure la cohérence entre posture civile et militaire, avec une approche *whole of government* et *whole of society*. Elle favorise une réponse intégrée aux menaces complexes en impliquant tous les acteurs : l'État, les entités fédérées, le secteur privé et la population.

Dans le prolongement de cette architecture stratégique, et afin d'opérationnaliser la lutte contre les menaces hybrides, la Défense belge traite de manière structurée la problématique des menaces hybrides, tant en interne qu'au travers d'une coordination interdépartementale et de différents forums.

Ces structures permettent une réponse belge cohérente et alignée avec les principes d'interopérabilité et de résilience de l'UE et de l'OTAN. Elles favorisent également la synergie entre les niveaux stratégique, opérationnel et tactique, tout en répondant à l'absence persistante d'une gouvernance centralisée des menaces hybrides, et créent des ponts fonctionnels dans un paysage institutionnel encore fragmenté.

Enfin, l'analyse des stratégies étrangères permet à la Belgique d'enrichir sa propre approche hybride.

## **CE QUE LA BELGIQUE PEUT APPRENDRE : REGARDS NORDIQUES ET NÉERLANDAIS**

Face à la montée des menaces hybrides, certains pays du nord de l'Europe se distinguent par des stratégies de résilience systémique solides. La Norvège, la Suède, la Finlande et les Pays-Bas offrent des exemples pertinents pour la Belgique, en quête de renforcement de sa posture hybride.

Depuis plusieurs décennies, la Norvège applique le concept de *Total Defence*, fondé sur une coopération civilo-militaire institutionnalisée, pilotée quant à elle par les *Norwegian Joint Headquarters* (NJHQ, le Quartier général interarmées norvégien) et structurée par la *Norwegian Directorate for Civil Protection* (DSB, la Direction de la protection civile de Norvège). Ce modèle repose sur trois fonctions vitales : la gouvernance, la sécurité de la population et le fonctionnement de la société (énergie, transports, finances etc.). Chaque domaine est transposé en capacités critiques à maintenir même en période de pression hybride. Des plans de soutien mutuel, une coordination intersectorielle et des exercices réguliers assurent la robustesse du système.



Fig 4: Brochure suédoise  
« In case of crisis or war »

La Suède articule sa résilience autour de la mobilisation sociétale, intégrée dans un système de défense totale. Chaque citoyen a un rôle à jouer, comme le montre la brochure nationale *In case of crisis or war*<sup>14</sup> qui informe sur la préparation individuelle, les conduites à tenir et la détection de la désinformation. La Suède inclut explicitement les menaces hybrides dans sa stratégie de sécurité qui cible la désinformation, le sabotage et les manipulations numériques.

Le modèle finlandais intègre l'ensemble des composantes de la société. Chaque ministère planifie ses fonctions critiques sans recourir à des agences d'urgence distinctes. Le modèle repose sur :

- une coordination gouvernementale et régionale centralisée ;
- le service militaire universel et une large réserve mobilisable ;
- des stocks stratégiques et une infrastructure conçue pour durer ;
- une collaboration civilo-militaire et public-privé efficace.

<sup>14</sup> Gouvernement suédois, Swedish Civil Contingencies Agency (MSB), *In Case of Crisis or War*, (Karlstad: Swedish Civil Contingencies Agency, 2018), <https://rib.msb.se/filer/pdf/30874.pdf>.

Les Pays-Bas ont opté pour la centralisation par le biais de la *Counter Hybrid Unit* (CHU, l'unité pour la lutte contre les menaces hybrides) au sein du ministère de la Défense. Cette cellule composée de six experts coordonne l'action nationale en lien avec l'OTAN, l'UE et les partenaires bilatéraux. Elle élabore des réponses transversales contre les menaces hybrides en combinant des outils diplomatiques, économiques, stratégiques et militaires. Ce modèle illustre une maturité institutionnelle poussée.<sup>15</sup>

En conclusion, les cas susmentionnés montrent qu'une résilience efficace suppose :

- une clarification des fonctions vitales à protéger ;
- une répartition claire des responsabilités ;
- une mobilisation civilo-militaire intégrée ;
- et une implication active de la population.

En comparaison, la Belgique a posé des bases (cfr. la Stratégie de sécurité nationale et le BNR-P), mais souffre d'un manque de centralisation et d'une implication citoyenne limitée. Les structures existantes manquent aussi de cohérence en comparaison de l'approche unifiée néerlandaise ou nordique.

La Belgique gagnerait dès lors à :

- s'inspirer du modèle néerlandais en envisageant la création d'une unité dédiée à la coordination stratégique contre les menaces hybrides, à l'image de la CHU, afin de centraliser les efforts interinstitutionnels et d'assurer une réponse cohérente, proactive et multi-domaine ;
- adopter une approche *Total Defence* adaptée avec une définition claire des fonctions critiques ;

---

<sup>15</sup> Charlotte Snel, « Hybride dreiging aan de orde van de dag, » *Alle Hens*, n° 8 (2022). [https://magazines.defensie.nl/allehens/2022/08/03\\_hybride-dreiging](https://magazines.defensie.nl/allehens/2022/08/03_hybride-dreiging).

- formaliser un cadre de résilience nationale civilo-militaire coordonné au niveau stratégique ;
- créer des outils de communication de crise à destination du public, calqué sur le modèle suédois ;
- intégrer systématiquement des scénarios hybrides dans les exercices nationaux de gestion de crise ;
- renforcer la coopération structurée avec la Finlande, la Norvège et la Suède, notamment via le Hybrid CoE.

Ces approches offrent en effet à la Belgique un modèle clair : la résilience face aux menaces hybrides n'est efficace que si elle est systémique, planifiée et portée à tous les niveaux de l'État et de la société.

## **CONCLUSION**

Dans un contexte international où les frontières entre paix, crise et conflit deviennent floues, les menaces hybrides constituent une méthode privilégiée pour affaiblir les démocraties sans confrontation directe. En tant que carrefour diplomatique, logistique et institutionnel, la Belgique est une cible stratégique. Elle doit donc évoluer d'une posture réactive vers une résilience intégrée et proactive.

Les menaces hybrides exploitent nos interdépendances, vulnérabilités technologiques, liberté d'information et fragmentation institutionnelle. Il s'agit d'un enjeu systémique touchant l'ensemble du tissu social, économique et politique. La réponse belge doit donc être tout aussi systémique.

À l'échelle internationale, la Belgique s'appuie sur l'OTAN, l'UE et le Hybrid CoE. Ces structures offrent certes des outils et une lecture partagée des menaces, mais leur efficacité dépend de leur intégration dans les politiques nationales.

Depuis 2021, la Belgique a renforcé sa vigilance avec l'adoption d'une Stratégie de sécurité nationale et la mise en place de plans stratégiques, tels que

le BND-P et le BNR-P. Ces efforts ont amélioré l'intégration civilo-militaire. Toutefois, la gouvernance reste à renforcer, de même que la culture partagée de la résilience et de la communication vers les citoyens.

L'analyse des modèles nordiques et néerlandais montre l'intérêt d'une gouvernance centralisée, de l'implication de la société civile et d'une doctrine de défense totale.

En somme, la lutte contre les menaces hybrides doit devenir un pilier transversal de la politique de sécurité nationale. Elle requiert une gouvernance claire, une coordination efficace, une interopérabilité des institutions et une mobilisation conjointe des secteurs public et privé. Ce n'est qu'à ce prix que la Belgique pourra consolider sa résilience et incarner pleinement son rôle dans la sécurité euro-atlantique.

*Mots-clés : résilience, coordination, menaces hybrides.*

