FLOTTE FANTÔME, ALERTES BIEN RÉELLES. QUEL RÔLE POUR LA DÉFENSE BELGE FACE À LA *SHADOW FLEET* RUSSE ?

Frédéric FREZIN

Le pétrolier Eagle S, *navire associé à la* shadow fleet *russe*
File:Crude oil tanker Eagle S at Porvoo 2024-12-31 b.jpg - Wikimedia Commons
Photo : Wikimedia Commons

Bijna onzichtbaar bevaart de Russische schaduwvloot (shadow fleet) *de zeeën, omzeilt zij sancties en test zij het internationale recht. Zij bestaat uit verouderde, slecht verzekerde olietankers met onduidelijke eigenaars. Wat gebeurt er als een van deze schepen – schijnbaar doelloos – in de Noordzee voor onze kust vaart, in de buurt van onze onderzeese kabels, gasleidingen en windmolenparken, of bij de ingang van onze havens? Kan België – een kust- en havenstaat in het hart van de Europese civiele én militaire logistieke stromen – het zich veroorloven om deze schaduwvloot te negeren? En vooral: welke rol kan of moet de Belgische Defensie spelen tegenover deze mogelijke, maar zeker hybride, dreiging?*

Le lieutenant-colonel d'aviation Frédéric FREZIN est officier de renseignement de la force aérienne. Au sein du département d'état-major Stratégie, il a été chargé de l'analyse des menaces hybrides visant les infrastructures critiques dans le cadre des plans de défense. Il a présidé le Hybrid Steering Group *interne à la Défense et représente celle-ci à la plateforme « menaces hybrides » du Centre de crise national, notamment dans le cadre des travaux liés au* Belgian National Risk Assessment. *Il est en outre titulaire d'un post-graduat en relations internationales (ULB), d'un master en politique internationale (KUL) et a suivi une formation avancée au Collège européen de sécurité et de défense (*European Security and Defence College*) en matière de menaces hybrides.*

Une économie de guerre à financer malgré les sanctions

Depuis l'invasion de l'Ukraine en février 2022, les États-Unis et l'Union européenne ont imposé à la Russie un vaste régime de sanctions visant notamment ses exportations d'hydrocarbures. Ce choix n'est pas anodin : avant la guerre, ces ressources représentaient environ 40 % des revenus du budget fédéral russe et plus de 60 % de ses recettes d'exportation[1]. L'objectif de Moscou est de préserver des revenus énergétiques suffisants pour soutenir l'économie nationale et financer son effort de guerre. La « flotte fantôme » – communément appelée *shadow fleet*[2] –

[1] Kurt Engelen, Casting Light on Russia's *Shadow Fleet*: Exposing a Sanctions Evasion Network at Sea, Focus Paper 54 (Bruxelles : Institut royal supérieur de défense (IRSD) / Centre d'études de sécurité et défense, septembre 2025).

[2] Il convient de souligner que la Russie ne représente qu'environ 40 % de la « flotte fantôme » mondiale. Utilisées pour contourner les sanctions internationales, ces flottes ont vu leur usage croître depuis les premières mesures prises contre la Corée du Nord en 2006. La guerre en Ukraine a toutefois intensifié leur déploiement.

s'inscrit dans cette logique comme un instrument de résilience économique : en exportant pétrole et produits énergétiques hors des circuits sous surveillance occidentale, elle réduit l'effet coercitif des sanctions, préserve la continuité des flux financiers – les recettes étant estimées à 10 milliards d'euros[3] – et contribue à maintenir la capacité russe à poursuivre le conflit.

La *shadow fleet*, qui compterait entre 400 et 1.000 navires, dont une cinquantaine de méthaniers[4], renvoie ainsi à un réseau structuré de navires, d'armateurs, d'assureurs et d'intermédiaires dont l'objectif est de contourner les restrictions et les contrôles. Parmi les procédés-clés figure le transfert de cargaison en mer (*ship-to-ship*), qui permet de transborder – et parfois de mélanger – des lots entre navires afin d'en brouiller l'origine et de compliquer la traçabilité. Ce dispositif facilite le réacheminement d'une part importante des exportations maritimes de pétrole[5] vers des pays n'appliquant pas les sanctions – principalement l'Inde, la Chine et la Turquie –, avec à la clé une réapparition indirecte de ces exportations sur le marché mondial via des produits raffinés[6].

L'économie d'abord, la déstabilisation ensuite

Au-delà de l'enjeu économique, la *shadow fleet* révèle surtout une dynamique plus préoccupante : l'exploitation de zones grises du droit maritime, ce qui érode la gouvernance internationale et complique l'attribution, avec comme objectif de réduire l'efficacité des sanctions. Cette dynamique ouvre également la voie à une conflictualité plus large, créant une nouvelle menace pour les infrastructures critiques sous-marines. Quelques incidents récents illustrent cette évolution :

[3] Tzimis Stylianos, analyste principal des menaces hybrides maritimes, Centre d'excellence européen pour la lutte contre les menaces hybrides, intervention lors de la conférence intitulée « Expert Conference on Strengthening International Co-operation on Critical Undersea Infrastructure Protection in the Baltic Sea and Globally », 23–24 avril 2025, Helsinki.

[4] Ibidem.

[5] Ces bâtiments assurent jusqu'à 80-90 % des exportations maritimes russes de pétrole.

[6] Tom Keating et Gonzalo Saiz Erausquin, Royal United Services Institute (RUSI), Royaume-Uni, intervention lors de la conférence intitulée « Expert Conference on Strengthening International Co-operation on Critical Undersea Infrastructure Protection in the Baltic Sea and Globally », 23–24 avril 2025, Helsinki.

- Septembre 2022 – Explosions visant les gazoducs Nord Stream 1 et 2 dans les eaux danoises et suédoises, marquant une escalade majeure de la conflictualité sous-marine stratégique[7] ;
- Octobre 2023 – Endommagement grave du gazoduc Balticconnector entre la Finlande et l'Estonie, très probablement causé par le cargo chinois *Newnew Polar Bear* ;
- Novembre 2024 – Coupure inexpliquée du câble de données C-Lion, reliant la Finlande à l'Estonie ;
- Décembre 2024 – Le vraquier chinois *Yi Peng Three* est suspecté d'avoir endommagé deux câbles sous-marins entre la Suède, la Lituanie, la Finlande et l'Allemagne ;
- Décembre 2024 – Le pétrolier *Eagle S,* suspecté d'avoir endommagé volontairement le câble EstLink 2, est intercepté par le navire *Turva* des garde-côtes finlandais.

Parallèlement, la *shadow fleet* concentre plusieurs risques pour la sûreté maritime et l'environnement[8/9] : navires vieillissants, pavillons de complaisance, défauts d'assurance et pratiques de dissimulation. La multiplication de comportements anormaux dans des zones sensibles – brouillage de systèmes de navigation par satellite, falsification du système d'identification automatique *(Automatic Identification System – AIS)* ou *spoofing*, navigation erratique ou encore stationnements à proximité de câbles et de pipelines – suggère des activités pouvant aller de la surveillance/cartographie d'infrastructures jusqu'à des actions de coercition ou de sabotage. Enfin, plusieurs failles structurelles entretiennent cette situation : absence de définition partagée, faiblesse de certains états du pavillon,

[7] Capitaine Mikko Simola, commandant de la Garde côtière dans le golfe de Finlande, intervention lors de la conférence intitulée « Expert Conference on Strengthening International Co-operation on Critical Undersea Infrastructure Protection in the Baltic Sea and Globally », 23–24 avril 2025, Helsinki.

[8] Tzimis Stylianos, analyste principal des menaces hybrides maritimes, Centre d'excellence européen pour la lutte contre les menaces hybrides , intervention lors de la conférence intitulée « Expert Conference on Strengthening International Co-operation on Critical Undersea Infrastructure Protection in the Baltic Sea and Globally », 23–24 avril 2024, Helsinki.

[9] Comme l'illustre le naufrage de deux pétroliers russes en mer Noire en décembre 2025.

contrôles d'assurance[10] et certificats CLC[11/12] difficiles à vérifier, coordination et partage de données perfectibles, ainsi que divergences entre partenaires occidentaux[13]. La *shadow fleet* ne contourne donc pas seulement les sanctions, elle fragilise aussi l'ordre maritime, accroît le risque environnemental et expose directement les états côtiers – dont la Belgique – à des menaces hybrides.

Implications spécifiques pour la Belgique

Menaces et risques pour les infrastructures portuaires critiques

Les ports belges – en particulier ceux d'Anvers, de Zeebrugge et de Gand – sont des nœuds logistiques essentiels pour l'économie européenne et représentent, en situation de crise, un maillon clé de l'*enablement*/soutien du pays hôte *(host nation support)* tel que décrit dans la doctrine de l'OTAN. Dans ce contexte, l'arrivée de navires ou de cargaisons d'origine opaque (documentation incomplète, itinéraires atypiques, couverture assurantielle incertaine, mélange possible de lots) peut générer une friction opérationnelle : contrôles renforcés, vérifications documentaires et techniques, voire immobilisation préventive d'un bâtiment. Or la mise à l'arrêt d'un navire suspect en zone portuaire ou à l'approche d'un terminal provoque rapidement des effets en cascade : occupation de postes à quai, saturation des zones de stockage, ralentissement des opérations de manutention et reprogrammation des escales. Cette congestion affecte non seulement les flux commerciaux légitimes, mais peut aussi perturber, en période de tension, la priorité donnée à certains flux critiques, y compris ceux liés au soutien logistique et au

[10] David Bolomini et Jas Mahrra, représentants de l'International Group of P&I Clubs, intervention lors de la conférence intitulée « Expert Conference on Strengthening International Co-operation on Critical Undersea Infrastructure Protection in the Baltic Sea and Globally », 23–24 avril 2025, Helsinki.

[11] La CLC, ou Convention internationale sur la responsabilité civile pour les dommages dus à la pollution par les hydrocarbures, est un traité maritime adopté en 1969 à Bruxelles, puis renforcé par un protocole en 1992. Elle est administrée par l'Organisation maritime internationale (OMI).

[12] Veronika Argal, experte principale des sanctions maritimes, administration des Transports, Estonie, intervention lors de la conférence intitulée « Expert Conference on Strengthening International Co-operation on Critical Undersea Infrastructure Protection in the Baltic Sea and Globally », 23–24 avril 2025, Helsinki.

[13] Tom Keating et Gonzalo Saiz Erausquin, Royal United Services Institute (RUSI), Royaume-Uni, intervention lors de la conférence intitulée « Expert Conference on Strengthening International Co-operation on Critical Undersea Infrastructure Protection in the Baltic Sea and Globally », 23–24 avril 2025, Helsinki.

transit allié. Plus préoccupant encore, un navire suspect immobilisé peut devenir un « point chaud » en matière de sécurité, mobilisant simultanément plusieurs services comme les autorités portuaires, les douanes et la police fédérale.

Par ailleurs, un incident environnemental majeur impliquant un pétrolier à risque (avarie, fuite d'hydrocarbures, incendie ou explosion) dans l'estuaire de l'Escaut, sur les accès à Anvers, ou à proximité de Zeebrugge aurait un impact immédiat sur la continuité des activités : restriction ou fermeture temporaire de zones de navigation, interruption des opérations portuaires, mobilisation de moyens de dépollution, ainsi que coûts économiques et réputationnels élevés.

Menaces directes pour les infrastructures maritimes critiques

Les infrastructures maritimes critiques jouent un rôle essentiel dans le commerce, la sécurité et l'économie de la Belgique. Situées dans les eaux territoriales belges et dans la zone économique exclusive (ZEE) belge, elles comprennent – outre les installations portuaires – des parcs éoliens offshore, des câbles sous-marins (électriques et de données), ainsi que des gazoducs reliant la Belgique et ses partenaires (voir schéma[14]). Ces infrastructures s'inscrivent dans un réseau maritime-industriel plus large et fortement interconnecté en mer du Nord ce qui complique leur protection, renforce les exigences de surveillance et rend indispensable la coopération internationale[15], notamment avec les états voisins. Comme l'a illustré en mer Baltique le cas du pétrolier *Eagle S*, des navires de la s*hadow fleet* pourraient être employés pour des actions hostiles ou de sabotage (notamment en utilisant des drones aériens ou sous-marins) visant des infrastructures critiques en mer du Nord[16].

[14] Serge Scory, Mia Devolder, Nabil Youdjou et Laurence Vigin, Marine Atlas supports Belgium's Marine Spatial Plan, ICAN News, 1er mars 2016. Disponible sur https://ican.iode.org/news/98-marine-atlas-supports-belgium-s-marine-spatial-plan, consulté le 6 août 2025.

[15] Capitaine de corvette Thomas Lambert (2024). Waarom ons veiligheidsbeleid rond kritieke maritieme infrastructuur nood heeft aan een inhaalbeweging, Revue militaire belge, n° 27, 2024.

[16] Il convient de noter que, pour les câbles sous-marins, il existe souvent une redondance suffisante pour compenser la rupture d'un câble isolé (également grâce à l'existence d'alternatives terrestres). Cette résilience limite donc l'impact immédiat d'un incident unique. La situation est toutefois différente pour les îles comme l'Irlande ou le Royaume-Uni, qui dépendent beaucoup plus directement de ces connexions.

Vulnérabilités cyber-maritimes

Les systèmes de gestion portuaire belges sont fortement numérisés et interconnectés avec des réseaux logistiques internationaux, ce qui les rend vulnérables aux intrusions cyber[17]. Ainsi, un navire – notamment de la *shadow fleet* – pourrait servir de vecteur d'attaque en exploitant ses connexions physiques ou sans fil aux infrastructures portuaires pour introduire des logiciels malveillants (*malwares*), altérer les données de navigation ou saboter des systèmes critiques comme la gestion des grues ou la planification des cargaisons[18]. Un tel scénario pourrait provoquer un blocage complet des opérations ou perturber la chaîne d'approvisionnement militaire et civile.

Collecte de renseignement

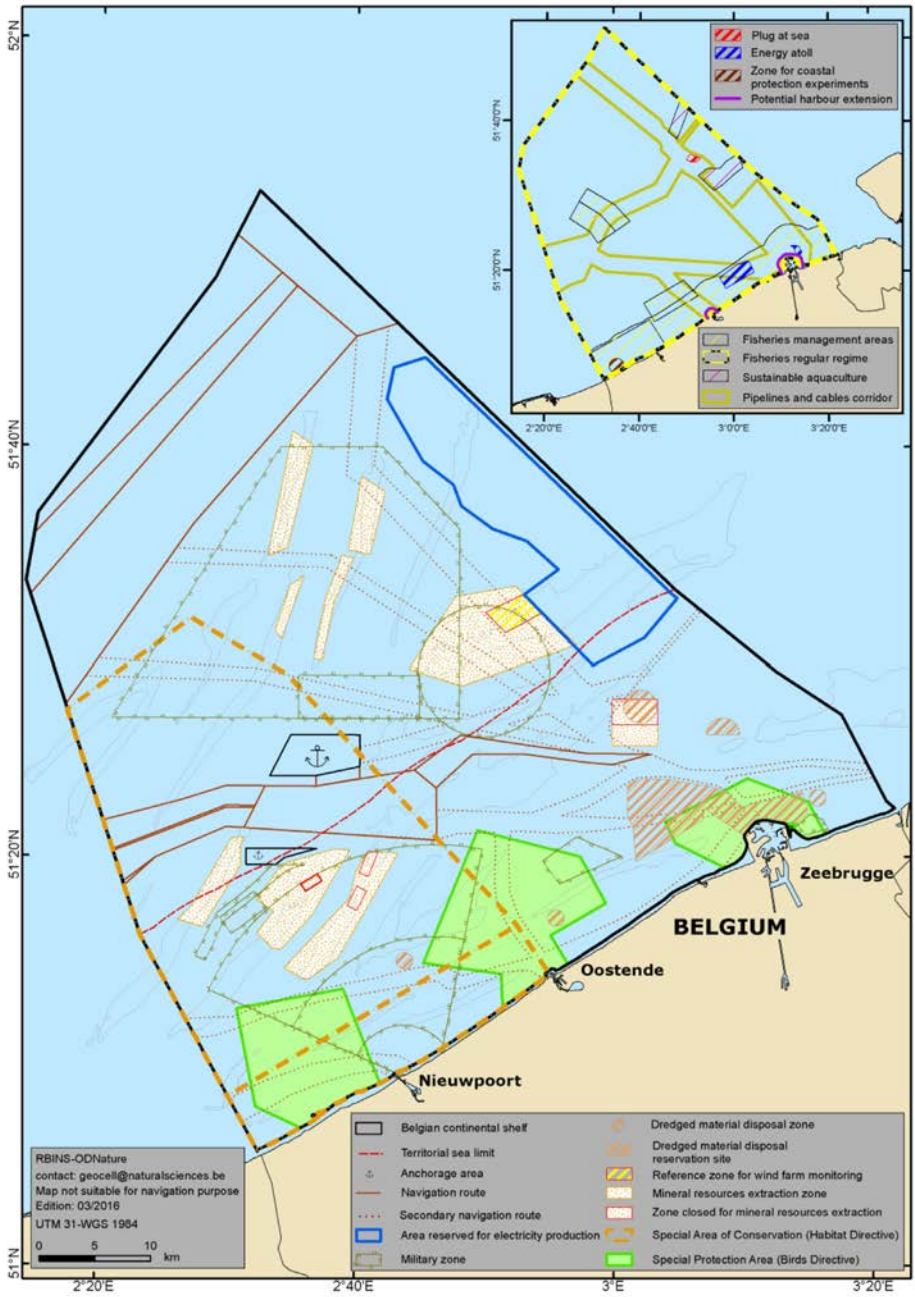
Les navires de la *shadow fleet* obéissant aux ordres de Moscou peuvent recueillir discrètement des données sensibles lors de leurs escales ou transits côtiers, telles que les horaires d'entrée et de sortie des navires militaires, la disposition des infrastructures portuaires ou la configuration des zones de mouillage[19]. Ce risque est particulièrement critique lors du transit et du soutien au déploiement de troupes et d'équipements de l'OTAN via les ports belges en cas de crise, lorsque les flux militaires augmentent et que la pression opérationnelle réduit les marges de manœuvre. En dehors des zones portuaires, ces navires peuvent également servir de plateforme pour des opérations clandestines en mer du Nord, notamment la récupération de capteurs militaires, le dépôt d'équipements d'écoute sur des routes maritimes clés[20] ou encore le déploiement de drones aériens destinés à la reconnaissance, au relais de communications ou au repérage de cibles. Ces

[17] European Union Agency for Cybersecurity (ENISA), Port Cybersecurity – Good Practices for Cybersecurity in the Maritime Sector. ENISA, 2020.

[18] National Academies of Sciences, Maritime Cybersecurity: Protecting Critical Infrastructure at Sea. Washington, DC : National Academies Press, 2022.

[19] Centre d'excellence pour la cyberdéfense en coopération (NATO CCDCOE), Cyber Threats and Maritime Security, NATO CCDCOE, 2021.

[20] Tom Keating et Gonzalo Saiz Erausquin, Shadow Fleet: Russia's Maritime Sanctions Evasion Tactics, RUSI Occasional Paper, 2024. Corroboré par certaines sources ouvertes : Russia-linked cable-cutting tanker seized by Finland 'was loaded with spying equipment' : Lloyd's List ; Eagle S - OpenSanctions.



Le plan d'aménagement des espaces maritimes belges.
Source : https://ican.iode.org/fr/nouvelles/8-english/news/98-marine-atlas-supports-belgium-s-marine-spatial-plan

renseignements, combinés avec des données issues d'autres sources, pourraient être utilisés pour planifier des opérations de sabotage ou des cyberattaques coordonnées contre les installations belges ou les réseaux de l'OTAN[21].

Risques environnementaux

La mer du Nord combine une forte densité de trafic maritime, des activités énergétiques offshore et des zones de biodiversité protégée. Dans ce contexte, la présence de navires associés à la *shadow fleet* constitue un risque majeur pour l'environnement maritime, en raison de bâtiments souvent vieillissants et insuffisamment transparents sur le plan de la maintenance, de la gestion et de l'assurance.

Les incidents recensés (plus de 50 cas graves[22]) illustrent un niveau de sinistralité préoccupant. Un déversement d'hydrocarbures à proximité du littoral belge affecterait les pêcheries, les réserves naturelles, les zones touristiques et les infrastructures offshore (parcs éoliens, câbles, pipelines) avec des conséquences immédiates en matière de dépollution, de continuité d'activité et de coûts environnementaux, économiques et politiques.

Pris dans leur ensemble, ces différents vecteurs de menace – sabotage potentiel d'infrastructures critiques, vulnérabilités cyber-maritimes, capacités de collecte de renseignement et possibilités d'opérations clandestines en haute mer – et risques composent un ensemble particulièrement préoccupant pour la Belgique, dont la convergence impose une réponse appropriée.

[21] UK National Cyber Security Centre (NCSC), Cyber Security for Ports and Harbours, 2022.
[22] Tzimis Stylianos, analyste principal des menaces hybrides maritimes, Centre d'excellence européen pour la lutte contre les menaces hybrides, intervention lors de la conférence intitulée « Expert Conference on Strengthening International Co-operation on Critical Undersea Infrastructure Protection in the Baltic Sea and Globally », 23–24 avril 2025, Helsinki.

Réponse militaire : quel rôle pour la Défense belge ?

Face aux risques et menaces liés à la *shadow fleet* russe, la Défense belge doit assumer un rôle accru au service de la sûreté et de la sécurité maritimes, rôle qui doit s'inscrire dans une réponse interagence et multiniveau articulée entre l'échelon national et les cadres de l'Union européenne (UE)/de l'OTAN.

La priorité consiste à renforcer la contribution belge aux mécanismes européens de connaissance du domaine maritime *(maritime domain awareness – MDA)*. L'intégration active aux systèmes de partage d'information, p. ex. *SafeSeaNet* au niveau de l'UE, avec l'appui de l'Agence européenne pour la sécurité maritime *(European Maritime Safety Agency)* et le croisement de données (AIS, imagerie, renseignements, informations portuaires) améliorent l'identification de comportements à risque : AIS désactivé ou falsifié, changement de pavillon *(reflagging)*, itinéraires anormaux, transferts de cargaison en mer ou incohérences documentaires. L'enjeu n'est pas uniquement d'« observer » : il s'agit de transformer cette connaissance de la situation en alertes actionnables, permettant aux autorités compétentes de décider rapidement d'un contrôle, d'une interception ou d'un arraisonnement. En Belgique, le *Maritieme Informatie Kruispunt* (MIK) joue déjà un rôle central de fusion et d'analyse ; l'enjeu consiste à accroître la capacité de détection précoce et la communication de messages d'alerte à l'intention des autorités compétentes. Le 1er mars 2026, ce rôle a pu donner toute sa mesure au travers de l'opération *Blue Intruder*, lors de laquelle un pétrolier suspecté d'appartenir à la *shadow fleet* russe a été arraisonné en mer du Nord puis escorté vers Zeebrugge. L'opération a débuté au sein du MIK qui, depuis la base navale de Zeebrugge, a assuré la surveillance du navire et l'analyse des données entrantes (comportement de navigation, pavillon, ports fréquentés et éventuels signalements internationaux), avant le feu vert donné par le gouvernement au lancement de l'interception. Cette démarche n'est pas isolée : ainsi, le 20 mars 2026, la Marine Nationale française, avec l'appui du Royaume-Uni, a intercepté et arraisonné en Méditerranée occidentale le pétrolier-cargo *Deyna*, suspecté de naviguer sous faux pavillon mozambicain,

afin de procéder à des vérifications (pavillon, documentation, assurance) ; fin septembre 2025, elle avait déjà abordé au large de Saint-Nazaire le pétrolier *Boracay*, navire sanctionné lié à la *shadow fleet*. Ces exemples montrent que la MDA produit déjà des effets concrets contre les navires à risque, mais ils mettent aussi en évvidence la limite actuelle du dispositif : au-delà du suivi des bâtiments, il faut pouvoir surveiller de manière continue les zones sensibles et les infrastructures sous-marines. Un défi majeur demeure toutefois : la surveillance persistante des infrastructures sous-marines (câbles, pipelines, parcs éoliens), qui requiert des moyens dédiés et une intégration accrue des données.

En complément, la Défense, en renforçant la surveillance maritime, peut faciliter le contrôle portuaire et soutenir les capacités d'inspection et de renseignement maritime. La lutte contre les pavillons de complaisance, le changement de pavillon et les manipulations d'identité nécessitent une approche intégrée. La Défense peut y contribuer par la collecte de signaux, la détection d'itinéraires incohérents et l'identification d'activités anormales, menées dans un cadre interagence, afin d'alimenter les dossiers transmis aux autorités civiles compétentes (douanes, SPF Mobilité – DG Navigation, justice). Le développement de doctrines de renseignement orientées vers le milieu maritime, en coopération avec les services de sécurité intérieure et les partenaires de l'OTAN, permettrait d'anticiper les risques liés à la présence de navires suspects et d'intensifier la surveillance des pavillons à risque. La marine devrait également exploiter pleinement l'extension récente des responsabilités de l'Autorité nationale pour la sécurité maritime *(National Authority for Maritime Security)* aux infrastructures critiques en mer[23]. Cette mission de surveillance pourrait s'appuyer sur des drones autonomes équipés de sonar à balayage latéral, des navires de surface sans équipage *(uncrewed surface vessels[24])* ou des capteurs fixes assurant une veille continue. L'intégration progressive de ces plateformes autonomes représente une opportunité d'augmenter la couverture

[23] Astrea Law, *Update on the New Belgian Maritime Security Act*, 2 mai 2022, disponible en ligne : Update on the New Belgian Maritime Security Act - Astrea, consulté le 8 septembre 2025.

[24] Capitaine de corvette Thomas Lambert et enseigne de vaisseau de 2e classe Michel Buekens, *Protection des infrastructures critiques dans la mer du Nord belge — Recommandations politiques, 24 février 2025.*

et la fréquence des observations tout en réduisant les coûts opérationnels et la dépendance au personnel embarqué. Enfin, cette vigilance doit s'étendre à l'Escaut occidental, en coopération avec les Pays-Bas, compte tenu de la vulnérabilité de l'accès au port d'Anvers.

La Défense belge doit également contribuer au développement d'une capacité nationale de réponse rapide face à l'ensemble des incidents en mer liés aux activités de la *shadow fleet*, qu'il s'agisse d'atteintes environnementales ou de menaces hybrides, comme des actes de sabotage ou des attaques cyber. Dans ce cadre, l'engagement de moyens militaires spécialisés, notamment pour sécuriser la zone, appuyer les opérations techniques et fournir une connaissance de situation renforcée, constitue un apport essentiel. Cette contribution doit s'inscrire dans un dispositif coordonné par le Gouverneur maritime – en tant qu'autorité fédérale compétente – et articulé avec les partenaires néerlandais, français et britanniques afin de renforcer la résilience régionale.

Enfin, sur le plan doctrinal et au sein des cadres de l'OTAN et de l'UE, la Défense belge doit intégrer la menace posée par la *shadow fleet* dans ses scénarios de planification de crise, ses exercices de sécurité maritime et ses partenariats capacitaires.

Conclusion

La capacité de nuisance de la *shadow fleet* russe dépasse le simple contournement logistique des sanctions : elle s'inscrit dans une stratégie hybride combinant résilience économique, opacité juridique, pratiques de dissimulation et risques élevés pour la sécurité et la sûreté maritimes et l'environnement. Elle contribue directement au financement de l'effort de guerre russe en permettant à Moscou de maintenir des flux commerciaux estimés à plusieurs milliards d'euros malgré les sanctions. En exploitant les zones grises du droit international et les failles de la gouvernance maritime, cette « flotte fantôme » met à l'épreuve la capacité des États européens à assurer la transparence, l'attribution et l'application effective des règles en mer. Les incidents récents en mer Baltique illustrent l'émergence d'une

conflictualité sous-marine plus agressive, où des navires civils peuvent servir de vecteurs d'actions hostiles.

Pour la Belgique, les implications sont tangibles. État côtier en mer du Nord, nœud logistique majeur de l'Europe et acteur clé du concept OTAN de l'*enablement*/du soutien du pays hôte, notre pays occupe une position stratégique exposée. Les risques concernent à la fois la continuité d'activité des infrastructures critiques maritimes, la fluidité des flux militaires, la sécurité environnementale et la résilience cyber des systèmes maritimes. S'y ajoutent des menaces de collecte clandestine de renseignement, de cartographie d'infrastructures, de déploiement de capteurs ou de drones, ainsi que la possibilité d'opérations de sabotage menées sous couverture civile. Plus largement, la présence de navires insuffisamment assurés et liés à des structures opaques affaiblit la capacité d'attribution, de responsabilisation et d'indemnisation, et complique l'exercice de l'autorité régulatrice des États riverains.

Dans ce contexte, la réponse belge doit être structurée autour de priorités concrètes : (1) renforcer la MDA et la surveillance des infrastructures sous-marines ; (2) durcir, avec les autorités civiles compétentes, les contrôles documentaires, assurantiels et opérationnels des navires à risque ; (3) consolider l'approche interagences pour améliorer l'attribution et réduire l'impunité ; (4) renforcer la capacité de réponse aux incidents par la planification, l'entraînement et la coopération régionale. Ces efforts ne peuvent produire d'effets durables que s'ils s'inscrivent dans une coordination européenne et transatlantique plus cohérente, incluant une harmonisation des définitions, des actions sur les pavillons et des registres à risque, ainsi que des dispositifs communs de protection des infrastructures critiques.

La *shadow fleet* n'est pas une anomalie passagère : elle s'inscrit dans une conflictualité maritime en mutation, où des vecteurs civils peuvent servir des objectifs stratégiques. Pour y faire face, il faudra mobiliser l'ensemble des instruments de puissance, réglementaires, militaires, diplomatiques et informationnels, afin de préserver la sécurité et l'intégrité de nos espaces maritimes. La Belgique devra,

dans ce cadre, renforcer simultanément sa posture de surveillance, sa résilience portuaire, sa protection des infrastructures offshore et sa capacité d'attribution, afin de réduire les marges d'action laissées à cette *shadow fleet*.

Mots-clés : flotte fantôme,* shadow fleet*, menaces hybrides infrastructures maritimes critiques

Le pétrolier Eagle S*, navire associé à la* shadow fleet *russe*
File:Crude oil tanker Eagle S at Porvoo 2024-12-31 b.jpg - Wikimedia Commons
Photo : Wikimedia