

Consortium Francophone pour la Sécurité régionale de la mer Baltique à la Mer Noire

David Getsadze

Doctorant (Business and Technology University)
Spécialiste en Chef (Ministère de la Défense de Géorgie)
Tbilissi, Géorgie

Davit.getsadze.1@btu.edu.ge

Résumé— Dans un contexte de menaces hybrides croissantes sur le flanc oriental de l'Europe, cet article propose la création d'un consortium de recherche scientifique francophone dédié au renforcement de la sécurité régionale de la mer Baltique à la mer Noire. S'inspirant de l'Initiative des Trois Mers, notre proposition vise à lui adjoindre un volet de "sécurité numérique" en s'appuyant sur les opportunités de financement du programme Horizon Europe, notamment ses clusters "Sécurité civile pour la société" et "Numérique, Industrie et Espace". Nous présentons le concept d'un projet pilote, "IA-MARIS", centré sur le développement d'une plateforme d'Intelligence Artificielle mutualisée pour la surveillance maritime et la lutte contre la désinformation. Ce projet réunirait des partenaires académiques et industriels de France et des PECO. Cet article constitue un appel à l'action pour utiliser le réseau francophone comme un levier de coopération stratégique afin de bâtir une résilience commune et de renforcer la souveraineté technologique en Europe Centrale et Orientale.

Mots-clés— Menaces hybrides, PECO, mer Baltique, mer Noire, Sécurité régionale, IA, surveillance maritime, désinformation, résilience, souveraineté technologique

Introduction : Un Arc de Sécurité Régional (PECO)

La sécurité du continent européen se joue de plus en plus sur son flanc oriental, un arc stratégique s'étirant de la mer Baltique à la mer Noire. Cette région, largement composée des pays d'**Europe Centrale et Orientale (PECO)**, fait face à un ensemble de défis sécuritaires communs et persistants, allant des menaces hybrides et cyberattaques aux pressions sur la sécurité énergétique et la liberté de navigation. Dans ce contexte, les approches purement nationales se révèlent insuffisantes, appelant à une mutualisation accrue des capacités et à une coopération transnationale renforcée pour garantir une stabilité durable.

Lancée en 2016, l'**Initiative des Trois Mers (I3M)** s'est imposée comme le principal cadre de coopération régionale, visant à accélérer le développement et l'interconnexion des infrastructures entre douze États membres de l'UE situés entre ces trois mers. Bien que son mandat se concentre principalement sur les domaines du transport, de l'énergie et du numérique, la résilience de ces infrastructures critiques est intrinsèquement liée à la sécurité de la région. Les projets de connectivité physique de l'I3M, aussi ambitieux soient-ils, restent vulnérables s'ils ne sont pas doublés d'une architecture de sécurité et de résilience à la hauteur des menaces contemporaines [1].

Cet article avance la thèse selon laquelle il est impératif d'adjoindre à l'I3M un volet de "**sécurité numérique et cognitive**" structuré. Une telle ambition, trop complexe pour être portée par des acteurs isolés, trouve un terreau fertile dans la coopération scientifique et technologique. En s'appuyant sur les outils de financement du programme **Horizon Europe** et sur le dynamisme du réseau de recherche francophone, il est possible de bâtir une infrastructure de sécurité collaborative.

Cette publication proposera un concept de projet pilote visant à illustrer cette approche, en se focalisant sur le développement d'une plateforme d'Intelligence Artificielle (IA) mutualisée. En démontrant la faisabilité d'une telle coopération entre les pays membres de l'I3M et des partenaires stratégiques, nous souhaitons poser les jalons d'une souveraineté technologique partagée, essentielle à la sécurité de tout le flanc oriental européen.

I. LE LEVIER STRATEGIQUE : HORIZON EUROPE ET LA COOPÉRATION INDUSTRIELLE

La vision d'une infrastructure de sécurité numérique partagée pour l'Europe Centrale et Orientale, bien qu'ambitieuse, n'est pas une utopie. Elle trouve un levier de concrétisation puissant dans le programme-cadre de l'Union Européenne pour la recherche et l'innovation, **Horizon Europe (2021-2027)**. Ce programme ne se contente pas de financer la recherche fondamentale ; il est explicitement conçu pour répondre aux grands défis sociétaux et renforcer la capacité industrielle du continent, offrant ainsi un cadre idéal pour la mise en œuvre de notre proposition. Deux de ses Piliers sont particulièrement pertinents pour la structuration d'un tel projet.

Le **Pilier 2, et plus spécifiquement son Cluster 3, "Sécurité civile pour la société"**, est directement aligné sur les finalités de notre projet. Les appels à projets de ce cluster visent à améliorer la protection des citoyens européens face à des menaces complexes. Ils financent des recherches sur la résilience des infrastructures critiques (qu'elles soient énergétiques, numériques ou de transport), la gestion des frontières, et la lutte contre la criminalité et le terrorisme, y compris dans leurs dimensions hybrides et cybernétiques. Un consortium régional, tel que nous le proposons, serait parfaitement positionné pour répondre à des appels portant sur la surveillance maritime en Mer Noire, la détection des campagnes de désinformation à l'échelle transnationale, ou la protection des corridors de transport de l'Initiative des Trois Mers. Ce cluster fournit la justification "métier" et l'ancrage dans les besoins des utilisateurs finaux (gardes-frontières, analystes de renseignement, opérateurs d'infrastructures) [2]. Parallèlement, le **Cluster 4, "Numérique, Industrie et Espace"**, offre les outils pour développer les briques technologiques fondamentales du projet. Il soutient la recherche de pointe dans des domaines clés tels que l'Intelligence Artificielle, le traitement des données massives (Big Data), la cybersécurité et l'informatique à haute performance. C'est dans ce cadre que pourraient être financés le développement des algorithmes d'IA, la création d'une architecture de cloud sécurisée pour le partage de données entre les partenaires, et l'intégration de sources de données hétérogènes. Ce cluster assure la viabilité technologique du projet et son ancrage dans une démarche d'innovation de rupture, garantissant que les solutions développées soient à l'état de l'art [3].

Cependant, la réussite d'un tel projet ne peut reposer uniquement sur le monde académique. La transition d'un prototype de recherche à une capacité opérationnelle robuste requiert l'implication d'un partenaire industriel majeur. Le programme Horizon Europe encourage fortement ces partenariats public-privé, essentiels pour garantir l'exploitabilité des résultats. Le partenaire industriel idéal pour notre consortium serait un leader européen des technologies de défense et de sécurité, possédant une expertise avérée dans plusieurs domaines critiques : les systèmes de commandement et de contrôle (C5ISR), l'analyse de données multi-sources, la conception de plateformes d'IA de confiance, la cybersécurité et les systèmes d'observation spatiale. Un tel acteur apporterait non seulement son savoir-faire technologique, mais aussi sa connaissance des processus d'intégration et de certification dans des environnements de sécurité exigeants. La présence d'un tel partenaire au sein du consortium serait un gage de crédibilité et un accélérateur pour la mise en œuvre concrète des solutions développées, transformant une collaboration de recherche en une véritable capacité stratégique pour la région.

II. PROPOSITION D'UN PROJET PILOTE : "IA-MARIS"

"Bien que des projets européens antérieurs aient permis des avancées notables dans la surveillance maritime, principalement en Méditerranée, et que des observatoires luttent contre la désinformation au niveau pan-européen, notre proposition IA-MARIS est la première à viser une intégration stratégique de ces deux dimensions de sécurité, avec un focus géopolitique adapté aux défis spécifiques du flanc oriental, de la Baltique à la Mer Noire."

Pour traduire notre vision stratégique en une initiative tangible, nous proposons la mise en place d'un projet pilote collaboratif baptisé "**IA-MARIS**" (**Intelligence Artificielle pour la Sécurité MARitime et la Résilience**). Ce projet vise à développer et à tester une plateforme technologique commune, modulaire et évolutive, conçue pour répondre à deux des défis de sécurité les plus pressants pour la région s'étendant de la Baltique à la Mer Noire : la surveillance maritime et la sécurité cognitive. L'objectif est de démontrer la faisabilité et la valeur ajoutée d'une approche mutualisée, en créant un bien commun numérique au service de la résilience régionale.

A. Module 1 : Sécurité et Surveillance Maritime en Mer Noire

Le premier module d'IA-MARIS se concentrerait sur le bassin de la Mer Noire, un espace géopolitique où la liberté de navigation et la sécurité des infrastructures critiques sont des enjeux permanents. L'objectif est de fournir aux pays riverains partenaires (Roumanie, Bulgarie, Géorgie) une image opérationnelle commune enrichie par l'IA, permettant une meilleure anticipation des menaces.

La plateforme fusionnerait en temps réel des flux de données hétérogènes :

- **Données satellitaires** : Images optiques et radar issues du programme européen Copernicus pour la surveillance de vastes zones maritimes.
- **Signaux radiofréquences** : Données du Système d'Identification Automatique (AIS) pour le suivi du trafic commercial, et détection d'autres signaux.
- **Renseignement en sources ouvertes (OSINT)** : Informations issues des réseaux sociaux, des forums

spécialisés et de la presse pour contextualiser les événements maritimes.

Les algorithmes d'IA développés au sein du projet auraient plusieurs fonctions. Premièrement, la **détection d'anomalies**, comme l'identification de navires "fantômes" ayant coupé leur transpondeur AIS ("dark ships"), la détection de schémas de navigation suspects pouvant indiquer des activités de contrebande ou de pêche illégale, ou encore la surveillance d'activités militaires inhabituelles à proximité des infrastructures critiques (plateformes gazières, câbles sous-marins). Deuxièmement, l'**analyse prédictive**, visant à anticiper les routes probables de navires suspects ou à modéliser les risques de congestion dans les détroits stratégiques. En partageant les alertes et les analyses issues de cette plateforme, les autorités nationales pourraient coordonner plus efficacement leurs actions, passant d'une posture réactive à une posture proactive.

B. Module 2 : Sécurité Cognitive et Lutte contre la Désinformation

Le second module aurait une portée géographique plus large, incluant les pays baltes, reconnus pour leur expertise en matière de lutte contre les menaces hybrides. Ce volet vise à développer des outils d'IA pour la détection précoce et l'analyse des campagnes de désinformation visant à déstabiliser la région PECO. La complexité de ces campagnes, souvent multilingues et coordonnées sur de multiples plateformes, dépasse les capacités d'analyse humaines traditionnelles.

La plateforme IA-MARIS ingérerait de grands volumes de données publiques issues de sources ouvertes (réseaux sociaux, plateformes de messagerie, sites d'information) dans plusieurs langues de la région. Les algorithmes se concentreraient sur trois tâches principales :

1. **Détection de comportements inauthentiques coordonnés** : Identifier les réseaux de bots ou de trolls propageant un même narratif.
2. **Analyse de narratifs** : Suivre l'émergence et la diffusion de récits hostiles visant à polariser l'opinion publique, à saper la confiance dans les institutions ou à discréditer la coopération euro-atlantique.
3. **Identification de contenus synthétiques** : Détecter l'usage de "deepfakes" (audio et vidéo) dans les campagnes de propagande.

L'outil fournirait aux analystes et aux agences gouvernementales des tableaux de bord et des alertes, non pas pour censurer l'information, mais pour comprendre les tactiques de l'adversaire et préparer des contre-stratégies de communication. Ce module constituerait une première ligne de défense cognitive partagée pour l'ensemble de la région.

C. Structure du Consortium Proposé

La réussite d'IA-MARIS reposerait sur un consortium équilibré, combinant excellence scientifique et pertinence opérationnelle, structuré autour du réseau francophone comme catalyseur.

- **Coordination et leadership scientifique** : Une ou plusieurs universités ou organismes de recherche français, apportant leur expertise en IA et en gestion de grands projets européens.
- **Partenaires académiques régionaux** : Des universités de Roumanie et de Bulgarie (pour l'expertise maritime de la Mer Noire), d'Estonie ou de Lettonie (pour l'expertise en cybersécurité et lutte

informationnelle), et de Géorgie (apportant son expérience unique des menaces hybrides en tant que pays partenaire).

- **Partenaire industriel** : Un leader européen de la défense et de la sécurité, chargé d'assurer l'intégration des technologies, la robustesse de la plateforme et la feuille de route vers une future industrialisation.
- **Comité des utilisateurs finaux** : Un conseil consultatif composé de représentants des marines, garde-côtes, et agences de sécurité des pays partenaires, garantissant que les développements répondent à des besoins opérationnels réels.

CONCLUSION : UN APPEL A L'ACTION DEPUIS LE RÉSEAU FRANCOPHONE

Cet article a présenté la nécessité et l'opportunité de construire une architecture de sécurité numérique et cognitive commune pour le flanc oriental de l'Europe. Face à des menaces hybrides qui exploitent les fragmentations et ignorent les frontières, nous avons soutenu qu'une coopération transnationale, s'étendant de la mer Baltique à la mer Noire, est non plus une option mais un impératif. En liant les objectifs de l'Initiative des Trois Mers aux puissants outils de financement du programme Horizon Europe, nous avons démontré qu'un chemin pragmatique et réaliste existe pour la mise en œuvre de cette vision. Le projet pilote "IA-MARIS", que nous avons esquissé, illustre comment une approche intégrant sécurité maritime et résilience informationnelle peut fournir des capacités mutualisées, au bénéfice des États membres de l'UE comme de leurs partenaires stratégiques essentiels, telle la Géorgie.

Notre proposition se distingue par son ambition d'utiliser le réseau scientifique francophone non seulement comme un

espace de communication, mais comme un véritable levier de coopération stratégique. Dans une région d'une grande diversité linguistique et culturelle, la francophonie peut agir comme un catalyseur, créant un espace de confiance propice à l'émergence de projets complexes dans des domaines aussi sensibles que la sécurité et la défense.

En conclusion, cet article est plus qu'une simple analyse ; il se veut un appel à l'action. Nous invitons nos collègues chercheurs, les innovateurs industriels et les représentants institutionnels présents à ce symposium à considérer cette proposition comme une base de discussion. Ce 4ème Symposium de la Recherche Scientifique Francophone en Europe centrale et orientale constitue le forum idéal pour initier les échanges qui mèneront, nous l'espérons, à la formation d'un consortium. Ensemble, nous avons l'opportunité de transformer une vision partagée en une capacité réelle, démontrant par l'action que la recherche scientifique francophone est un acteur clé dans la construction d'une Europe plus résiliente et plus souveraine.

RÉFÉRENCES

- [1] Three Seas Initiative (2023). Joint Declaration of the 2023 Bucharest Summit. Available : <https://3seas.eu/event/three-seas-initiative-business-forum-bucharest-2023>
- [2] European Commission. Horizon Europe-Cluster 3 :Civil Security for Society. Available : https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en
- [3] European Commission. Horizon Europe-Cluster 4 :Digital, Industry and Space. Available : https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-4-digital-industry-and-space_en