Securing the Atlantic Commons: Critical Maritime Infrastructure, Asymmetric Threats, and the Imperative for Cooperative Resilience

Julian Orlando Quintero Ibañez

Abstract

This paper analyzes the escalating threat to Critical Maritime Infrastructure (CMI) across the Atlantic, defining a dual challenge: the coercive grey-zone strategies of state actors targeting seabed infrastructure, and the persistent, innovative asymmetric tactics of transnational criminal networks (TCOs). It posits that the interconnectedness of global energy, communications, and trade flows now depend heavily on shared maritime infrastructure such as cables, pipelines, and shipping routes; these systems collectively represent a growing area of strategic exposure. Focusing on Colombia as a case study, the paper highlights its dual role as both a pivotal CMI node and a focal point for complex maritime challenges , analyzing its position as both an incubator of asymmetric threats (like the evolving narco-submarine) and a key source of operational countermeasures. The paper highlights the profound asymmetry in Maritime Domain Awareness (MDA) capabilities between nations, a gap that is systematically exploited by both state and criminal actors. Building on recognized resilience models and international cooperation mechanisms, the paper proposes a collaborative, data-driven framework to enhance maritime security integration. The paper concludes by recommending that the Atlantic Centre facilitate a sustained, pan-Atlantic dialogue on CMI resilience, leveraging the advanced capabilities of regional anchors like Colombia to build a more secure and cooperative maritime commons.

1. Introduction: The New Geopolitics of Atlantic Seabed and Surface Security

The Atlantic Ocean underpins much of today's globalized economy, serving as both a conduit and foundation for international connectivity. Extending across its depths, the Atlantic hosts a dense web of maritime assets essential to trade, energy, and communications—systems that collectively sustain the flow of global activity.[1] CMI includes the essential assets on, in, or connected to the sea, upon which modern societies depend: transport (ports, shipping), energy (pipelines, offshore platforms), and communications (submarine fiber-optic cables).[2, 3]

This infrastructure is strategically vital. Submarine cables carry over 95% of all intercontinental data traffic, forming the backbone of international finance, while energy pipelines and shipping lanes are

[1] Teixeira, N. S., & Marcos, D. (Eds.). (2019). Evolving human security challenges in the Atlantic space. Jean Monnet Network on Atlantic Studies. https://transatlanticrelations.org/wp-content/uploads/2019/10/29262-D-01_COD_EvolvingSecurity_TXT.pdf
[2] Alexopoulos, M. J., Niemi, A., Skobiej, B., & Torres, F. S. (2024). Enhancing resilience of critical maritime infrastructure through modeling and simulation of sensors configuration. German Aerospace Center (DLR). https://elib.dlr.de/209370/1/MARESEC_2024_paper_7%20%281%29.pdf
[3] Sari, A. (2025, March). Protecting maritime infrastructure from hybrid threats: legal options (Hybrid CoE Research Report 14). The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf

essential for national security of supply.[4, 5] However, this reliance has created profound vulnerability. Because much of this infrastructure is privately owned, there is often a disconnect between its national strategic importance and the security measures available to protect it—an imbalance that adversaries can exploit.[2]

The primary threats to Atlantic CMI do not emanate from conventional naval confrontations but from the ambiguous space of the "grey zone"—aggression calibrated to remain below the threshold of armed conflict.[4, 6] In the maritime domain, this conflict is waged by asymmetric actors, including transnational criminal organizations (TCOs) and state-sponsored proxies, who use sabotage, cyberattacks, and infiltration to achieve strategic objectives with plausible deniability.[7, 8] CMI represents an ideal "soft target" for these actors.[9] Strikes against undersea or port infrastructure can produce severe disruptions, and the ambiguity surrounding attribution often delays coordinated international action.[10] This paper argues that mitigating these asymmetric threats requires a paradigm shift from fragmented national security efforts to a cooperative, pan-Atlantic resilience framework built on robust data integration. A comprehensive framework should reduce disparities in Maritime Domain Awareness (MDA) capacity and capitalize on the operational experience of capable regional partners such as Colombia.[11]

2. The Evolving Asymmetric Threat

The Atlantic maritime security and CMI is challenged by a confluence of sophisticated actors and innovative tactics targeting three principal domains:

- **Energy Infrastructure:** The Atlantic seabed hosts a growing number of offshore oil and gas platforms and a sprawling network of subsea pipelines. On Colombia's Caribbean coast, vital export pipelines such as Caño Limón–Coveñas and Ocensa form strategic targets due to their economic significance and exposure to potential attacks.[12]
- **Communications Infrastructure:** The most critical component is the dense web of submarine

---

[4] NATO International Staff, Defence Policy and Planning Division, & Allied Command Transformation. (2025). 2024 NATO Resilience Symposium report. North Atlantic Treaty Organization. 25-26. https://www.act.nato.int/wp-content/uploads/2025/09/NATO-Resilience-Symposium-2024-Report.pdf

[5] Ministry of Information and Communications Technologies of Colombia. (2015). Colombia already has nine submarine fiber-optic cables. https://www.mintic.gov.co/portal/715/w3-article-13402.html

[6] Cantwell, D. (2017, November 29). Hybrid warfare: Aggression and coercion in the gray zone. American Society of International Law. https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone

[7] Helmus, T. C., Romita Grocholski, K., Liggett, T., Rhoades, A. L., Savitz, S., & Palmer, K. (2024). Understanding and countering China's maritime gray zone operations. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2900/RRA2954-1/RAND_RRA2954-1.pdf

[8] United Nations Institute for Disarmament Research. (2010). Maritime security (Disarmament Forum, Issue 2; UNIDIR/2010/7). https://unidir.org/wp-content/uploads/2023/09/maritime-security-en-319.pdf

[9] NATO & European Union. (2023). Final assessment report of the NATO-EU Task Force on the resilience of critical infrastructure. https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf

[10] Patlove, K. (2025, September 21). Depths of deception: State-backed undersea cable disruptions and the role of international maritime law. American University International Law Review. https://auilr.org/2025/09/21/depths-of-deception-state-backed-undersea-cable-disruptions-and-the-role-of-international-maritime-law/

[11] Espinel Bermúdez, J. R. (2022). Conciencia del dominio marítimo (Maritime domain awareness).Estrategia marítima, evolución y prospectiva. https://doi.org/10.25062/9786280000725.05

[12] Osorio Ceballos, N. A. (2020). Análisis de los costos de atención de las emergencias derivados de los atentados a la infraestructura petrolera: Oleoducto Caño Limón Coveñas https://repositorio.uniandes.edu.co/server/api/core/bitstreams/e404dc0a-7093-4030-9a07-ef1e9adacbfc/content

fiber-optic cables, the central nervous system of the global internet.[13] Damage to these cables, whether in the deep sea or at their landing stations, can disrupt connectivity for entire regions.[14]

- **Commerce and Transport Infrastructure:** High-volume shipping lanes and strategic ports like Cartagena in Colombia are fundamental to the global supply chain but are also hotspots for maritime crime, including armed robbery and smuggling.[15]

2.1. Threat Vector 1: Criminal Innovation (TCOs)

The primary threat comes from TCOs, particularly those from Colombia, which have evolved into sophisticated, multinational-like enterprises with complex logistics and R&D capabilities.[16, 17] Their convergence with terrorist groups creates a symbiotic "blue crime" ecosystem where illicit activities are mutually reinforcing. [18] State actors may also leverage these groups as proxies for deniable, grey-zone attacks on a rival's CMI. [17]

The operational methods of these actors are characterized by continuous innovation. The development of narco-submarines by Colombian TCOs is a prime example. These vessels have evolved from rudimentary semi-submersibles to platforms with transoceanic capabilities. [10, 19] The most alarming development is the emergence of unmanned "drone narco subs," the first of which was seized by the Colombian Navy in July 2025, equipped with a Starlink antenna for remote guidance.[19] This technological leap transforms the operational calculus from one of human risk to one of capital risk. By removing the crew, TCOs can treat interdictions as a manageable cost of doing business, neutralizing deterrence strategies based on arrest and imprisonment.

2.2. Threat Vector 2: Grey-Zone Coercion (State Actors)

Beyond the criminal-proxy nexus, state actors represent a distinct and parallel threat vector. Operating in the grey-zone, their objective is not financial profit but geopolitical coercion.[17] This threat manifests in actions calibrated below the threshold of armed conflict, such as the hostile mapping of seabed cables and pipelines by "research" vessels, or the disruption of data traffic.[14] While TCOs seek to evade detection, these actors seek to demonstrate a credible capability to paralyze an adversary's infrastructure at a time of their choosing, turning CMI into a strategic hostage.

---

[13] The Energy Year. (2025, May 15). Ecopetrol maps: offshore potential, midstream infrastructure and Hocol's national footprint. The Energy Year. https://theenergyyear.com/articles/ecopetrol-maps-offshore-potential-midstream-infrastructure-and-hocols-national-footprint/

[14] Zabala, D. (2024, June). Regulating the submarine cable system in the Caribbean Region. Blue NAP Americas. https://www.bluenapamericas.com/wp-content/uploads/2024/08/DZ-Regulating-the-submarine-cable.pdf

[15] Ávila-Zúñiga-Nordfjeld, A. (2025, March). Coping with sabotage and seabed security threats in the Baltic Sea: A regional maritime security policy. The Hague Centre for Strategic Studies. https://hcss.nl/wp-content/uploads/2025/03/Coping-with-Sabotage-and-Seabed-Security-Threats-in-the-Baltic-Sea-HCSS-2025.pdf

[16] Patel, J. (2023, September 7). Exploring port security threats in South and Latin America. Intelligence Fusion. https://www.intelligencefusion.co.uk/insights/resources/article/exploring-port-security-threats-in-south-and-latin-america/

[17] Yakubu, I. A. (2024). Understanding and addressing the drivers behind the nexus of blue crime, drugs, piracy, and terror prevalent across the Atlantic.

[18] United Nations Office on Drugs and Crime. (2012). Transnational Organized Crime in Central America and the Caribbean: A Threat Assessment. https://www.unodc.org/toc/en/reports/TOCTACentralAmerica-Caribbean.html

[19] CBS News. (2025, July 3). *Drone "narco sub" — equipped with Starlink antenna — seized for the first time in the Caribbean*. CBS News. https://www.cbsnews.com/news/drone-narco-sub-seized-first-time-caribbean-colombia/

2.3. The Cyber-Physical Battleground

In parallel, the cyber vulnerability of CMI is a rapidly growing concern. The increasing digitalization of maritime infrastructure, such as port operational technology (OT) systems, has expanded the attack surface.[20] A 2020 study analyzing four Colombian ports found significant vulnerabilities and a lack of readiness to counter cyber threats.[21] This is compounded by the fact that Colombian government and financial institutions are persistently targeted by cyber threat groups like Blind Eagle (APT-C-36), creating a high-risk environment for CMI. [21]

3. Colombia: A Microcosm of CMI Vulnerability and Resilience

Colombia presents a dual challenge: it hosts important maritime infrastructure while also being a source of evolving asymmetric maritime threats. Analyzing Colombia reveals both the acute vulnerabilities CMI faces and the advanced capabilities that can be developed to counter them.

Colombia's Caribbean coast is a strategic gateway hosting a concentration of vital CMI. The ports of Cartagena and Barranquilla are major commercial hubs.[22] The coast is also a key data conduit, with at least nine international submarine fiber-optic cables making landfall there, connecting South America to the global internet.[23] Furthermore, major oil pipelines like the Caño Limón–Coveñas and Ocensa terminate at the Caribbean port of Coveñas, a primary energy export terminal.[24]

This concentration of CMI is directly exposed to a full spectrum of threats. Colombian ports have faced persistent maritime crime. Historical records indicate that the Caño Limón pipeline experienced a high frequency of sabotage—170 incidents reported in 2001.[13] The continued presence of TCOs and the discovery of narco-submarine construction sites add a persistent physical threat.[12]

In response, Colombia has invested heavily in naval modernization and regional cooperation, developing capabilities that position it as a leading security actor in the Caribbean basin.[19] This "Colombian security paradox"—incubating advanced threats while developing world-class countermeasures—makes it an indispensable partner. Its deep, institutional knowledge is a strategic asset for the entire Atlantic basin.

---

[20] Uchôa, R. (2025, August 1). The subaquatic frontier of drug trafficking: Technological evolution, asymmetric warfare, and the unmanned paradigm shift. Small Wars Journal. https://smallwarsjournal.com/2025/08/01/the-subaquatic-frontier-of-drug-trafficking-technological-evolution-asymmetric-warfare-and-the-unmanned-paradigm-shift/

[21] Gamboa, G. A., Ramírez-Cabrales, J. F., & Jiménez, J. F. (2020). Cyber Security Vulnerabilities in Colombia's Maritime Critical Infrastructure (MCI). In Smart Innovation, Systems and Technologies. https://www.researchgate.net/publication/341237525_Cyber_Security_Vulnerabilities_in_Colombia's_Maritime_Critical_Infrastructure_MCI

[22] Mascellino, A. (2025, March 11). Blind Eagle targets Colombian government with malicious .url files. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/blind-eagle-targets-colombian-gov/

[23] Carter, L., Burnett, D., Drew, S., Marle, G., Hagadorn, L., Bartlett-McNeil, D., & Irvine, N. (2009). Submarine cables and the oceans: connecting the world (UNEP-WCMC Biodiversity Series No. 31). International Cable Protection Committee; United Nations Environment Programme; UNEP World Conservation Monitoring Centre. http://www.iscpc.org/publications/icpc-unep_report.pdf

[24] U.S. Energy Information Administration. (2019, January 7). Background Reference: Colombia. https://www.eia.gov/international/content/analysis/countries_long/Colombia/pdf/colombia_bkgd.pdf

Two key initiatives exemplify this leadership:

- **Operation Orion:** Launched in 2018, Orion is a Colombian-led multinational naval campaign against maritime drug trafficking, involving dozens of countries and over a hundred agencies.[25] Its success lies in fostering real-time intelligence sharing and coordinated operational responses, demonstrating Colombia's capacity to lead a diverse coalition.[26]
- **Intelligence Fusion Centers of Excellence:** Orion's success is underpinned by a sophisticated intelligence architecture. The International Centre for Research and Analysis against Maritime Narcotrafficking (CIMCON) provides strategic analysis, while the International Operations Coordination Centre (CCOPI) and the Intelligence Fusion Center of the Colombian Navy integrate data and coordinate action.[27, 28] These centers are not just national assets but proven models for the kind of information fusion needed across the wider Atlantic.

4. The Pan-Atlantic Dilemma & The Data Integration Imperative

Although certain Atlantic states such as Colombia have advanced maritime surveillance capacity, substantial disparities in Maritime Domain Awareness persist across the basin.[27] This disparity creates dangerous vulnerabilities that are systematically exploited by TCOs, undermining the security of the entire region.[29]

On one end of the spectrum, the Colombian Navy is actively modernizing its fleet and investing heavily in surveillance to enhance its MDA.[27] In stark contrast, several Atlantic and West African states face resource constraints that limit their ability to monitor territorial waters, including shortages of patrol craft, radar systems, and skilled analysts.[26] TCOs are acutely aware of these gaps and design their operations to exploit them, using the poorly monitored waters of under-resourced states as superhighways for illicit trafficking.[17] This creates a classic "weakest link" problem, where the overall security of the Atlantic is dictated not by its strongest powers, but by its most vulnerable spaces.

Existing regional cooperative mechanisms, such as the Caribbean Regional Maritime Agreement (CRMA) and the Zone of Peace and Cooperation of the South Atlantic (ZOPACAS) for part of the South-American countries, often struggle to translate intent into effective operational outcomes. They are hampered by resource constraints, divergent national priorities, and, most critically, a lack of infrastructure for a persistent, integrated common operational picture. Information sharing is often ad-hoc

---

[25] Dryad Global. (2020, December 29). Anchoring the Caribbean: Colombian Navy's Growing role in the region. Dryad Global. https://channel16.dryadglobal.com/anchoring-the-caribbean-colombian-navys-growing-role-in-the-region
[26] The Watch. (2025, July 11). The cornerstone of counternarcotics: Inside multinational strategy Orion. The Watch. https://thewatch-journal.com/2025/07/11/the-cornerstone-of-counternarcotics-inside-multinational-strategy-orion/
[27] Taylor, L. (2024, November 27). Colombia-led operation seizes world record 225 tonnes of cocaine, and uncovers new Australia trafficking route. The Guardian. https://www.theguardian.com/world/2024/nov/27/colombia-drug-bust-narco-submarine-australia
[28] Barrero Avellaneda, A. M. (2024). Fortalecimiento del Centro de Fusión de Inteligencia Naval del Caribe como herramienta de cooperación hemisférica para Colombia. Revista Fuerzas Armadas, (265), 10–32. https://doi.org/10.25062/0120-0631.4928
[29] United Nations Office on Drugs and Crime. (2025, August 16). Standing on Caribbean Shores, Learning for Arabian Waters: Strategic Maritime Study Tour Concludes in Cartagena, Colombia. https://www.unodc.org/copak/en/Stories/SP1/standing-on-caribbean-shores--learning-for-arabian-waters_-strategic-maritime-study-tour-concludes-in-cartagena--colombia.html

rather than systematic.

However, the challenge of these frameworks is not merely technical or resource-based; it is fundamentally geopolitical.[17] The pan-Atlantic "dilemma" is a "competition of frameworks." For key South Atlantic stakeholders, ZOPACAS is a cornerstone of regional policy designed to limit extra-regional military influence. This posture is in direct tension with the NATO-led security architectures that dominate the North Atlantic.[32] Any viable pan-Atlantic proposal, therefore, cannot be a simple extension of Northern models. It must first build trust by federating these disparate regional frameworks, focusing on shared, apolitical threats (such as TCO activity and environmental security) as a necessary foundation for wider cooperation.

These challenges underscore the importance of consolidating data from diverse sources, a persistent obstacle in advancing collaborative maritime security, yet it is essential for transnational coordination and timely responses.[17] A successful model can be found in Singapore's Information Fusion Centre (IFC). The IFC develops a shared maritime security picture by combining two cornerstones: a system of embedded International Liaison Officers (ILOs) who build trust and facilitate face-to-face evaluation of incidents, and a powerful information technology platform that fuses data from multiple sources (AIS, LRIT, etc.) into a common picture.[30] This human-centric yet technologically robust approach to data integration provides a powerful template for overcoming the fragmentation and capability gaps plaguing the Atlantic.

5. Forging a Pan-Atlantic CMI Security Architecture

Addressing the threats to Atlantic CMI requires a new, comprehensive security architecture. This architecture should be a flexible, federated network that respects national sovereignty while promoting interoperability and leveraging the diverse strengths of its members. Its design can draw lessons from mature security models and successful data integration initiatives.

The EU's Directive on the Resilience of Critical Entities (CER) provides a model for a systematic, all-hazards approach, mandating that states and private operators conduct risk assessments and implement resilience measures.[31] NATO's strategy for protecting Critical Undersea Infrastructure (CUI) complements this with a dedicated military-security overlay, focused on deterrence, detection, and defense through multinational patrols and advanced technology.[33]

The cornerstone of a new Atlantic architecture must be an information fusion network that synthesizes the best features of world-leading models. As noted, Singapore's IFC provides a template for building trust through embedded liaison officers and a shared technology platform. The EU's Common Information Sharing Environment (CISE) offers a model for decentralized technical interoperability, connecting disparate national surveillance systems without replacing them.[32] CISE is a voluntary framework that

---

[30] A role model for information sharing? Visiting the Singapore IFC - Christian Bueger, fecha de acceso: september 21, 2025, https://bueger.info/a-role-model-for-information-sharing-visiting-the-singapore-ifc/

[31] KPMG Advisory. (2025). Enhancing infrastructure resilience across Europe: An in-depth analysis of the new Critical Entities Resilience Directive (CER) and its impact on your organization. https://assets.kpmg.com/content/dam/kpmg/be/pdf/RR-Critical-Entities-Resilience-Directive-2025-EN-Brochure.pdf

[32] Monaghan, S., Svendsen, O., Darrah, M., & Arnold, E. (2023, December 19). NATO's Role in Protecting Critical Undersea

makes legacy systems "talk" to each other through a common data model.[33]

A successful pan-Atlantic model must be a flexible "network of networks" that avoids the political and institutional weaknesses of past efforts.[34] This proposed Atlantic CMI Security and Information Fusion Network (ACS-IFN) would be built on the voluntary, coalition-of-the-willing principles of CISE, the IFC, and Operation Orion. However, its primary barrier is not technical, but rather a lack of political trust and commercial incentives for data sharing. Therefore, the ACS-IFN must be designed first as a governance regime (not just a technical platform) that provides a secure, two-way street. It must incentivize private CMI operators to share anomaly data by offering them protected, actionable, and declassified threat intelligence from state partners in return. The Atlantic Centre's role would be that of a strategic convener, facilitating the... agreements that allow different national and regional nodes to cooperate seamlessly.

The ACS-IFN would operate on a tiered basis:

- **Tier 1 (Universal Data Integration):** A voluntary information-sharing environment modeled on the EU's CISE, providing a technical backbone for any participating Atlantic nation to share relevant, unclassified maritime surveillance data. This respects national sovereignty while creating a foundational layer of shared awareness.
- **Tier 2 (Targeted Capacity Building):** This tier would focus on closing the MDA gap through intensive, regionally-led training. It would formalize a "South-South" cooperation model, with regional anchors like Colombia serving as centers of excellence. Colombia's CIMCON and naval schools would become the logical training hub for the Southern Caribbean, providing tailored courses on MDA analysis, interdiction, and CMI protection, as the European Commission addresses the Data fusion for maritime security applications.[35]
- **Tier 3 (Coordinated Response):** For the most willing and capable partners, this tier would involve a multinational maritime task group. Inspired by NATO's maritime groups and the success of Operation Orion, this task group would conduct joint surveillance and interdiction operations in high-risk areas, providing a tangible deterrent and response capability.

7. Conclusion: From Asymmetric Threats to Asymmetric Strengths

The security of the Atlantic commons is fundamentally challenged by adaptive, asymmetric actors waging grey-zone conflict, rendering conventional, siloed state-based responses increasingly ineffective. This challenge has entered a disruptive phase, evidenced by the emergence of unmanned, satellite-guided drones, among other dual use technologies. This technological leap, which transforms the TCO risk calculus from one of human risk to one of capital risk, renders conventional deterrence models obsolete

---

Infrastructure. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-12/231219_Monaghan_NATO_CUI.pdf?VersionId=6Usacn9I0OlKjF6t4s4XhehMIVROp74W

[33] The Information Fusion Centre: Challenges and Perspectives. SAFTI MI Library. Retrieved October 21, 2025, from https://saftimi.spydus.com.sg/api/open/1.0/digitalassets/1037918/download

[34] Atlantic Council. (2024, May 22). *Beyond NOFORN: Solutions for increased intelligence sharing among allies*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence-sharing-among-allies/

[35] European Commission. (2024, April 12). Data fusion for maritime security applications. CORDIS. https://cordis.europa.eu/programme/id/H2020_SEC-19-BES-2016

and demonstrates the ineffectiveness of isolated state responses. The analysis presented demonstrates that the path forward lies not in a symmetric arms race, but in transforming this asymmetry from a threat into a strategic strength by building a federated, cooperative security architecture.

Central to this new approach is the proposed Atlantic CMI Security and Information Fusion Network (ACS-IFN). This must be a framework designed to fuse both physical Maritime Domain Awareness (MDA) and cyber threat intelligence, recognizing that digitalized operational technology is a key battlefront. Such a framework must leverage the unique capabilities of all partners and, critically, forge an operational nexus between state agencies and the private operators who own and manage the vast majority of CMI.

To realize this vision, this paper proposes a set of multi-layered, actionable recommendations. The Atlantic Centre is urged to champion this new framework by convening a permanent pan-Atlantic CMI dialogue tasked with co-designing the governance framework for the ACS-IFN. This dialogue must explicitly integrate the private operators of telecommunications, energy, and transport infrastructure not merely as stakeholders, but as creators of the legal, liability, and incentive structures required for this public-private data fusion to function. The Centre should sponsor the feasibility study for the ACS-IFN, ensuring its design addresses incentives for public-private data sharing and cyber-physical intelligence fusion. The Republic of Colombia is positioned to become a cornerstone of this architecture by formalizing its role as a regional MDA training hub and leveraging its CIMCON capabilities.

Finally, this strategy's success depends on Pan-Atlantic partners (including the United States, EU, and Brazil) adopting a nuanced diplomatic approach. This must respect existing regional frameworks, such as ZOPACAS, while fostering apolitical, functional cooperation focused on shared transnational threats. Support must prioritize data integration and fund "South-South" security cooperation, empowering regional leaders like Colombia.

By embracing this integrated, multi-layered strategy, the nations of the Atlantic can move beyond disjointed efforts. Under the guidance of the Atlantic Centre, they can transform their disparate capabilities into a collective, asymmetric advantage, proactively shaping a more resilient and secure maritime commons.