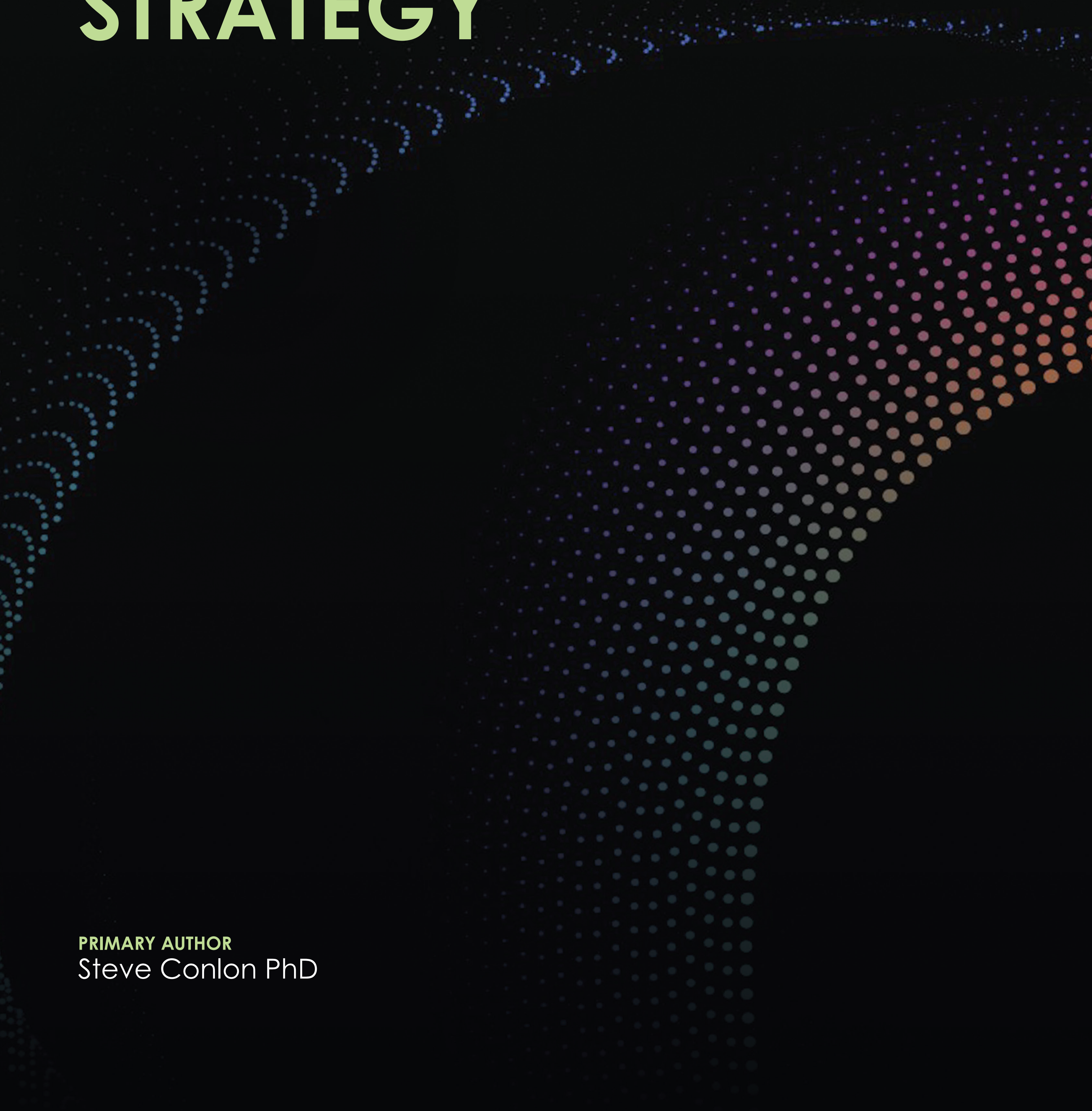
RIVADA

# SUBMISSION ON THE PROPOSED IRISH

# MARITIME SECURITY STRATEGY



PRIMARY AUTHOR
Steve Conlon PhD

THIS PAGE IS INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

***SHOULD THE NATIONAL MARITIME SECURITY STRATEGY INVOLVE THE PRIVATE SECTOR WHO MAY BE OWNERS OR OPERATORS OF CRITICAL MARITIME INFRASTRUCTURE? WHAT ROLE COULD THEY PLAY?***

***WHAT ROLE DO YOU THINK INTERNATIONAL COOPERATION SHOULD PLAY IN THE NEW NATIONAL MARITIME SECURITY STRATEGY? SHOULD THIS INCREASED COOPERATION INCLUDE A FOCUS ON OUR PARTNERS IN THE EU, WITH NEIGHBOURING COUNTRIES AND THROUGH OUR INDIVIDUALLY TAILORED PARTNERSHIP PROGRAMME WITH NATO OR OTHER INTERNATIONAL MARITIME ORGANISATIONS?***

***DO YOU THINK THE NATIONAL MARITIME SECURITY STRATEGY SHOULD BE ACCOMPANIED BY AN ACTION PLAN THAT WILL DETAIL HOW THE STRATEGY WILL BE IMPLEMENTED? WHAT DO YOU THINK THE KEY ELEMENTS OF THIS ACTION PLAN SHOULD BE?***

***ADDITIONAL COMMENTS ON IRISH MARITIME SECURITY OUTSIDE OF CONSULTATION QUESTIONS***

***SUBMISSION CONCLUSION***

## EXECUTIVE SUMMARY

Rivada welcomes the opportunity to submit to the Irish Department of Defence our recommendations for a National Maritime Security Strategy. This marks our fourth contribution to consultations on the State's national security architecture. We hope to support the State's security by freely sharing our expertise in national security—expertise we believe is without equal among Irish private companies.

Ireland's maritime domain, encompassing one of the largest Exclusive Economic Zones (EEZs) in Europe, is increasingly exposed to a complex array of threats. These include the strategic vulnerability of undersea infrastructure, limitations in naval and surveillance capabilities, the rise of hybrid and non-conventional threats, climate-induced disruptions, and the geopolitical ambiguity arising from Ireland's policy of military non-alignment. The absence of a coherent maritime security culture—across both public and institutional domains—further compounds these risks.

This submission identifies five principal threat vectors: (1) the exposure of critical undersea infrastructure to sabotage and espionage; (2) persistent deficits in naval fleet capacity and surveillance technologies; (3) the proliferation of grey zone activities and legal ambiguities in response; (4) the accelerating impacts of climate change on maritime operations and resource competition; and (5) the strategic pressures of a multipolar world on Ireland's sovereignty and autonomy.

Looking forward, our submission outlines a series of emerging challenges, including the weaponisation of the maritime domain through cyber and autonomous systems, the erosion of maritime governance, and the increasing contestation of international legal norms. In response, Rivada advocates for a comprehensive, forward-looking strategy that integrates climate resilience, technological innovation, legal preparedness, and international cooperation.

Key recommendations include:

- Establishing a National Maritime Security Coordination Centre to unify inter-agency operations and intelligence
- Developing a National Maritime Security Doctrine to articulate Ireland's strategic posture and operational thresholds
- Investing in Maritime Domain Awareness (MDA) through autonomous systems, satellite surveillance, and secure communications
- Enhancing cyber resilience across ports, offshore infrastructure, and subsea assets
- Integrating the private sector as a co-producer of maritime security, particularly in intelligence sharing and innovation
- Leveraging international partnerships, including EU frameworks and Ireland's Individually Tailored Partnership Programme with NATO, while maintaining its policy of non-alignment
- Embedding the Rivada Outernet—a sovereign, secure, and resilient LEO satellite network—as a critical enabler of communications, surveillance, and operational continuity across the maritime domain

This submission underscores the need for a whole-of-government and whole-of-society approach to maritime security. Ireland must move beyond reactive measures and adopt a proactive, integrated strategy that reflects its unique geostrategic position, its responsibilities as an EU member state, and its commitment to the international rules-based order.

**Declan Ganley**
Chairman & CEO
RIVADA

S Conlon
**Steve Conlon PhD**
VP Corporate Intelligence
RIVADA

## LIST OF ABBREVIATIONS

**AIS** -Automatic Identification Systems

**CIR** – Committed Information Rate

**CISE** - Common information sharing environment

**CMI** – Critical Maritime Infrastructure

**CSDP** – Common Security and Defence Policy

**DTIF** – Disruptive Technologies Innovation Fund

**EDF** – European Defence Fund

**EEZ** – Exclusive Economic Zone

**EMODnet** – European Marine Observation and Data Network

**EMSA** – European Maritime Safety Agency

**ENISA** – European Union Agency for Cybersecurity

**EUMSS** – European Union's Maritime Security Strategy

**GPS** – Global Positioning System

**IMO** – International Maritime Organisation

**ISF** – Internal Security Fund

**ISR** – Intelligence, Surveillance and Reconnaissance

**IUU** – Illegal, Unreported and Unregulated

**MARSUR** – Maritimes Surveillance

**MDA** – Maritime Domain Awareness

**MPA** – Maritime Patrol Aircraft

**MRV** – Multi-role Vehicle

**NCSC** – National Cyber Security Centre

**NIS2** – Network and Information Systems Directive 2

**OPV** – Offshore Patrol Vehicles

**PACE** - Primary, Alternate, Contingency, Emergency

**RMP** – Recognised Maritime Picture

**SAFE** – Security Action for Europe

**SAR** – Search & Rescue or Synthetic Aperture Radar

**SFPA** – Sea Fisheries Protection Authority

**UMS** – Unmanned Maritime Systems

**UNCLOS** – United National Convention on the Law of the Sea

**UUV** – Unmanned Underwater Vehicle

# GLOSSARY OF TERMINOLOGY

## TERM DEFINITION

**Asymmetric Threats**

Refers to challenges posed by actors—often non-state or irregular forces—who employ unconventional strategies and tactics to exploit vulnerabilities in more powerful or traditional military or security establishments. These threats typically circumvent direct confrontation, relying instead on methods such as terrorism, cyber-attacks, guerrilla warfare, or the use of improvised weapons. The asymmetry lies not only in the disparity of capabilities but also in the unpredictable and often legally ambiguous nature of such actions, which complicates conventional defence and deterrence frameworks.

**CISE (Common Information Sharing Environment)**

A secure, structured network developed by the European Union to facilitate cross-border and cross-sector information exchange among maritime authorities, both civilian and military. CISE enhances maritime domain awareness by enabling timely and coordinated responses to threats such as cyber and physical attacks on critical infrastructure, irregular migration, drug trafficking, and other illicit activities at sea. It supports integrated maritime surveillance and contributes to the EU's broader maritime security and crisis management objectives.

**Common Security and Defence Policy (CSDP)**

A central pillar of the European Union's external action framework, enabling the Union to undertake civilian and military operations beyond its borders in support of international peace and security. Rooted in the Treaty of Lisbon, the CSDP provides the legal and institutional basis for coordinated defence and crisis management efforts among EU Member States. It facilitates joint missions, capability development, and strategic partnerships, while respecting the sovereignty of national defence policies. Through the CSDP, the EU seeks to project stability, uphold the rule of law, and respond to emerging security challenges in a manner that complements NATO and other multilateral frameworks.

**European Union's Maritime Security Strategy (EUMSS)**

A comprehensive framework for safeguarding the EU's maritime interests, ensuring the security of its citizens, economy, and infrastructure at sea. Revised in 2023, the strategy aims to promote international cooperation, uphold international law, and address evolving threats such as cyberattacks, hybrid warfare, and environmental risks. It emphasises enhanced maritime domain awareness, joint naval operations, and capacity-building across civilian and military actors within and beyond the EU.

**Exclusive Economic Zone**

The exclusive economic zone (EEZ) of a State extends up to 200 nautical miles from its baseline, beyond and adjacent to its territorial sea, and is governed by the legal framework set out in Part V of the 1982 United Nations Convention on the Law of the Sea. Within this zone, the State holds sovereign rights for exploring, exploiting, conserving, and managing natural resources—both living and non-living—of the waters, seabed, and subsoil, as well as for activities like energy production from water, currents, and wind. It also has jurisdiction over artificial structures, marine scientific research, and marine environmental protection, along with other rights and duties under international law.

## GLOSSARY OF TERMINOLOGY

### TERM DEFINITION

**FRONTEX**

An agency of the European Union responsible for coordinating border control efforts across EU Member States and Schengen-associated countries. In the maritime domain, Frontex supports surveillance, search and rescue, and law enforcement operations at sea. It deploys personnel, vessels, and aerial assets to assist in managing irregular migration, combatting cross-border crime, and enhancing situational awareness at the EU's external maritime borders.

**Grey zone maritime activities**

Refers to actions undertaken by state or non-state entities within the maritime sphere that deliberately remain below the threshold of conventional armed conflict. These activities are strategically designed to advance political or security objectives while exploiting the legal and normative ambiguities that exist between peace and war. By operating in this indeterminate space, such actions often challenge established international norms and legal frameworks without provoking a direct military response.

**Hybrid Threats**

A form of threat to a State that encompass a broad spectrum of hostile actions orchestrated by state or non-state actors that blend conventional military force with non-military tactics, including cyber operations, disinformation campaigns, economic coercion, and the use of proxy groups. These threats are deliberately designed to exploit the vulnerabilities of open societies and democratic institutions, often operating below the threshold of formal armed conflict. By integrating diverse instruments of power in a coordinated manner, hybrid threats seek to destabilise, influence, or undermine a target state's political cohesion, societal resilience, and strategic autonomy.

**Intelligence, Surveillance, and Reconnaissance (ISR)**

Refers to the integrated activities and systems employed to collect, process, and disseminate information critical to decision-making in both military and security contexts. Intelligence involves the analysis and interpretation of data to produce actionable insights; surveillance denotes the continuous monitoring of areas, persons, or activities; and reconnaissance pertains to the targeted acquisition of information, often in support of specific operational objectives. Together, ISR capabilities enable situational awareness, threat detection, and strategic foresight, forming a cornerstone of modern defence and security operations across multiple domains, including land, air, sea, space, and cyberspace.

**Layer 2 Transport Network**

Refers to a network architecture, such as Rivada's Outernet, that uses satellite constellations to provide data transport at the link layer (Layer 2) of the Open Systems Interconnection (OSI) model. This allows for direct communication between satellites and ground stations, enabling various applications like secure data transmission, disaster recovery, and cellular backhaul.

## GLOSSARY OF TERMINOLOGY

| TERM | DEFINITION |
|---|---|
| **Maritime Domain Awareness (MDA)** | Refers to the effective understanding of all activities, actors, and conditions within the maritime environment that could impact security, safety, the economy, or the marine ecosystem. It encompasses the collection, integration, analysis, and dissemination of information related to the movement of vessels, cargo, and people across maritime spaces, including territorial waters, exclusive economic zones, and the high seas. MDA serves as a foundational element of maritime security strategy, enabling informed decision-making, early threat detection, and coordinated responses to risks such as piracy, smuggling, illegal fishing, and environmental hazards. It relies on a combination of technological systems, inter-agency cooperation, and international partnerships to ensure situational awareness and uphold the rule of law at sea. |
| **MARSUR (Maritime Surveillance)** | An EU-led initiative developed by the European Defence Agency to enhance maritime situational awareness through the secure exchange of surveillance information among participating Member States and partners. Operating as a federated system-of-systems, MARSUR enables real-time sharing of vessel data, imagery, and maritime intelligence while preserving national data sovereignty. It supports both civilian and military authorities, contributing to a common operational maritime picture and reinforcing the EU's maritime security objectives under the Common Security and Defence Policy (CSDP). |
| **Primary, Alternate, Contingency, and Emergency (PACE) Model** | A hierarchical framework employed to establish robust communication strategies by identifying four distinct and progressively resilient channels of communication: Primary, Alternate, Contingency, and Emergency. This model ensures that, should the preferred method fail, subsequent options are readily available to maintain operational continuity. Each communication method within the model is ideally independent of the others, thereby reducing systemic vulnerabilities. The model is mission-specific rather than unit-specific, and it is developed collaboratively to balance operational requirements with technological, logistical, and security considerations. |
| **Security Action for Europe (SAFE)** | An EU-level financial instrument launched in 2025 to strengthen the Union's collective defence capabilities through joint procurement of critical military equipment. SAFE provides long-term, low-interest loans to Member States and eligible partners for collaborative acquisitions, including maritime assets such as naval platforms, surveillance systems, and missile defence. The programme aims to reduce fragmentation in the European defence market, enhance interoperability, and support the strategic autonomy of the EU, particularly in response to evolving maritime security threats. |

## GLOSSARY OF TERMINOLOGY

### TERM

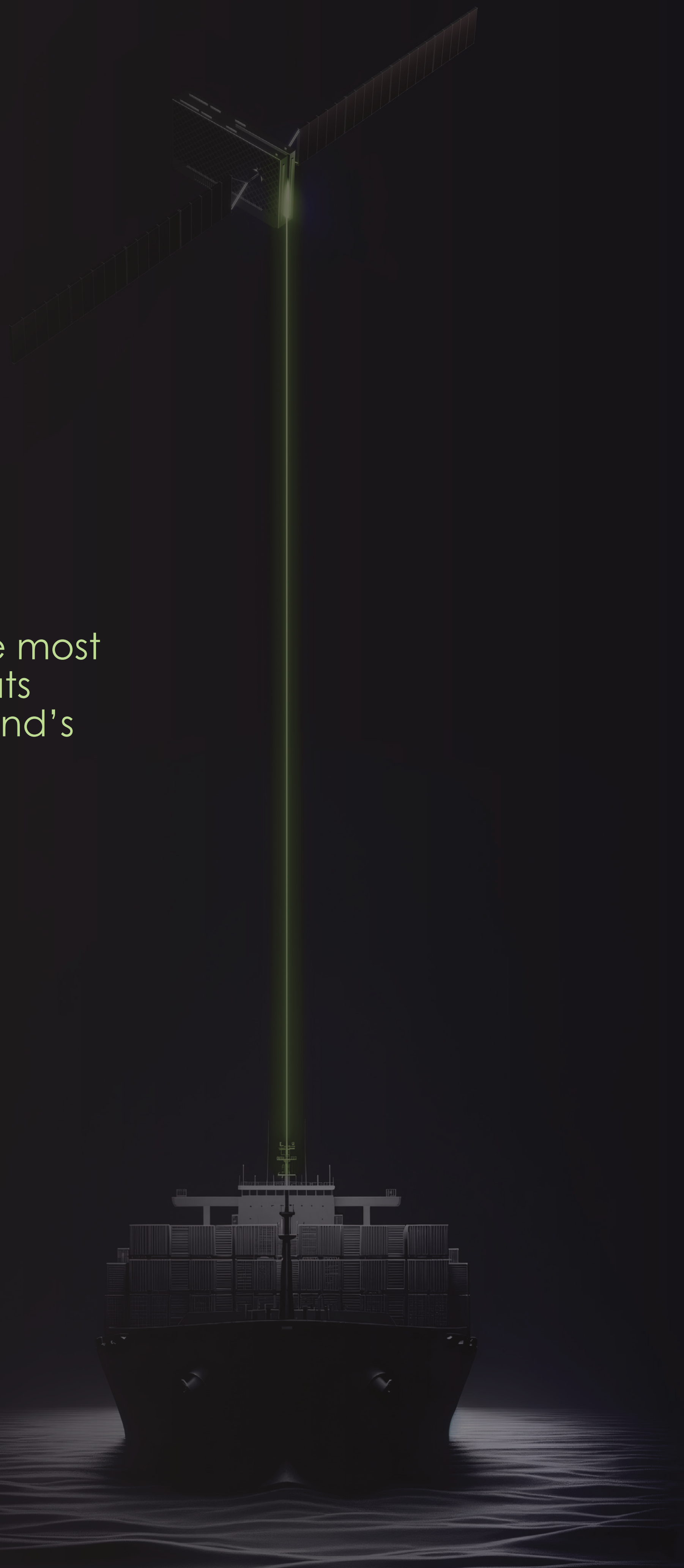
### DEFINITION

**United Nations Convention on the Law of the Sea (UNCLOS)**

Adopted in 1982 and entering into force in 1994, the UNCLOS serves as the foundational legal framework governing maritime affairs at the global level. The UNCLOS delineates the rights and responsibilities of states in relation to the use of the world's seas and oceans, encompassing issues such as territorial waters, exclusive economic zones (EEZs), continental shelf jurisdiction, and the freedom of navigation. It also establishes mechanisms for the peaceful resolution of maritime disputes and promotes the sustainable management of marine resources. By codifying customary international law and introducing new legal norms, UNCLOS plays a pivotal role in maintaining order, security, and environmental stewardship in the maritime domain.

THIS PAGE IS INTENTIONALLY LEFT BLANK

What do you see as the most significant current threats or vulnerabilities to Ireland's maritime security?



## Introduction

Ireland's maritime domain, which includes one of the largest Exclusive Economic Zones (EEZs) in Europe, is increasingly susceptible to a spectrum of contemporary security challenges. These challenges are intricate, multidimensional, and influenced by ongoing technological, geopolitical, and environmental developments. Ireland remains heavily reliant on maritime routes for its energy and trade, with approximately 78 per cent of its energy requirements met through imports via shipping and pipelines, while an estimated 90 per cent of the nation's trade by volume is conveyed by sea. Yet, underpinning these vulnerabilities is a more fundamental concern: the persistent absence of a coherent national security and maritime security culture. This deficiency is not limited to the wider public but is also discernible across government departments and key ministries, where strategic awareness and coordinated policy responses remain underdeveloped. The cultivation of such a culture—grounded in education, institutional alignment, and long-term strategic vision—is not merely desirable but essential to safeguarding Ireland's maritime interests in an increasingly contested and complex security environment.

Five key threats and vulnerabilities include:

### Critical Undersea Infrastructure

Ireland serves as a critical transatlantic nexus for high-capacity submarine communication systems linking Europe and North America, with prominent landings including AEConnect-1, Hibernia Express, and GTT Atlantic. These cables transmit a substantial share of global internet traffic and financial data, rendering them vital not only to Ireland's national interests but also to the broader European and international systems.

Recent movements by foreign naval vessels—most notably those linked to the Russian Federation—have intensified awareness of the risks posed by potential sabotage or interference. In light of the critical nature of this infrastructure, Ireland's limited capacity to effectively monitor and safeguard these assets constitutes a significant security vulnerability.

Procuring a solution for the ongoing vulnerability of subsea cabling can be challenging due to factors such as connection stability, high bandwidth applications or the need for low latency traffic. Rivada Space Networks is building the 'Outernet,' a LEO satellite network providing a truly global layer 2 transport network in space. This Outernet will be able to match and, in some cases, beat terrestrial fibre, making this a great alternative or backup solution for existing subsea fibre network applications. Unlike subsea fibre, which is vulnerable to physical disruptions, be that earthquake, ship anchors or geopolitical conflicts, the Outernet solution offers inherently resilient and redundant pathways in space that can dynamically reroute packets according to fastest routes and network disruptions at any given time. A self-contained architecture that eliminates the need for third party networks and ground stations alongside committed information rates in its service plan makes this an invaluable complement to critical undersea infrastructure.

### Limitations in Naval and Surveillance Capabilities

Ireland's Naval Service continues to grapple with persistent staffing shortages, an ageing fleet, and a deficit in advanced surveillance capabilities. These limitations directly undermine the State's capacity to conduct effective maritime patrols, monitor activity within its waters, and respond swiftly to security incidents across its Exclusive Economic Zone (EEZ).

This capability gap significantly constrains Ireland's ability to address a broad spectrum of maritime challenges, including illegal fishing, narcotics trafficking, and irregular maritime migration. The disparity between the vast scale of Ireland's maritime domain and the limited resources allocated to its protection remains a critical strategic vulnerability.

The recent proposal to acquire a towed array sonar system marks a welcome and timely development in Ireland's evolving maritime security posture. As a nation with a vast maritime domain and increasing exposure to hybrid threats, including the covert presence of foreign submarines and the vulnerability of undersea infrastructure, this investment represents a significant step toward addressing long-standing capability gaps. The sonar system's advanced detection capabilities will enable the Defence Forces to monitor underwater activity with greater precision, enhancing Ireland's ability to safeguard its sovereign waters and critical subsea assets.

This acquisition aligns with the broader objectives outlined in Ireland's Level of Ambition 2 (LOA 2) defence framework and reflects a growing recognition of the strategic importance of maritime domain awareness. By integrating this sonar capability with planned radar systems and investing in personnel training, Ireland is laying the groundwork for a more resilient and responsive maritime security strategy. The move not only strengthens national defence but also contributes to regional stability, reinforcing Ireland's role as a responsible and proactive maritime actor in the North Atlantic.

### Hybrid and Non-Conventional Threats

Contemporary maritime security is increasingly defined by threats that extend beyond conventional notions of military aggression. In recent years, Ireland has witnessed a rise in grey zone maritime activities that, while falling short of open aggression, pose significant strategic concerns. Notably, Russian surveillance vessels such as the Yantar have been observed operating near critical undersea communication cables off the Irish coast, raising fears of covert reconnaissance or sabotage. Additionally, unnotified seabed surveys—often conducted under the guise of scientific research—have taken place within Ireland's Exclusive Economic Zone, potentially mapping infrastructure for future exploitation. Compounding these concerns is the suspected use of civilian vessels, including fishing trawlers and research ships, for intelligence gathering, a tactic that exploits legal ambiguities and complicates attribution. These developments underscore the urgent need for enhanced maritime domain awareness and a robust national security strategy.

Ireland's existing legal instruments and defence architecture are not sufficiently configured to detect, deter, or respond to such ambiguous and evolving threats. Confronting this challenge will necessitate a carefully calibrated approach—one that reconciles Ireland's longstanding policy of military non-alignment with the shifting dynamics of modern security imperatives.

### Environmental and Climate-Related Challenges

Climate change is emerging as an increasingly salient maritime security concern, encompassing both immediate operational hazards and longer-term strategic implications. The growing frequency and intensity of extreme weather events pose tangible risks to maritime safety, coastal infrastructure, and offshore energy assets.

Moreover, environmental pressures on marine ecosystems—particularly fisheries—may exacerbate tensions surrounding access, sustainability, and resource governance. These challenges are further complicated by post-Brexit regulatory divergence (and ever increasing polarisation in UK politics toward its relationship with the EU) and evolving international norms. In response, Ireland must embed climate resilience as a core component of its broader maritime security strategy.

A collapse of the North Atlantic Drift would likely prompt a strategic recalibration by NATO and the EU, with increased focus on the North Atlantic as a zone of instability. Ireland's geostrategic location would become even more central to transatlantic resilience and maritime situational awareness.

Ireland would need to deepen its engagement with EU and NATO maritime security frameworks—while maintaining its policy of non-alignment—to ensure that its interests are represented in evolving regional security architectures. Other security implications of a rapid change in the drift or total collapse include a disruption of maritime and strategic sea lanes, a potential migration or decimation of fish stocks, and a significant increase in more frequent storms and fog, increasing demand for maritime domain awareness (MDA) technologies, and robust SAR coordination mechanisms.

### Geopolitical Pressures and Strategic Ambiguity

While Ireland upholds a policy of military non-alignment, it remains inherently exposed to the shifting geopolitical dynamics of the North Atlantic. The increased presence of both NATO and Russian naval forces in the region, coupled with rising expectations from European Union partners regarding maritime collaboration, places Ireland in a strategically delicate position.

Ireland's geographic location situates it as a critical node within the broader Western security architecture, particularly in relation to transatlantic communication and trade routes. However, the absence of a clearly defined national maritime strategy—one that reconciles Ireland's non-aligned stance with its international responsibilities—risks compounding existing vulnerabilities within its maritime security posture. This ambiguity has been highlighted by the presence of Russian vessels, such as the Yantar, operating near undersea cables off the Irish coast, raising concerns about potential hybrid threats. Similarly, Ireland's limited engagement in EU maritime security initiatives has drawn criticism, particularly during incidents such as the 2022 Russian naval exercises planned within Ireland’s EEZ, which exposed the lack of a coordinated national response mechanism and a unwillingness by the State to invest in its own maritime security. These examples underscore the strategic risks of maintaining a non-committal posture in an increasingly contested maritime domain.

### Conclusion

Ireland’s maritime security landscape is marked by a complex interplay of traditional and non-traditional threats, underscoring the strategic significance of its vast maritime domain. The country’s role as a transatlantic hub for undersea communications cables, coupled with its geographic position on the western periphery of Europe, places it at the forefront of emerging geopolitical tensions and hybrid security challenges. Persistent limitations in naval capacity, surveillance infrastructure, and legal frameworks further exacerbate Ireland’s vulnerability to a range of risks—from foreign interference and grey zone activities to environmental pressures and climate-induced disruptions.

While Ireland’s policy of military non-alignment remains a cornerstone of its foreign and defence posture, it must be reconciled with the realities of an increasingly contested maritime environment. The absence of a comprehensive national maritime strategy—one that integrates climate resilience, technological modernisation, and international cooperation—represents a critical gap in the State’s security architecture. Addressing these vulnerabilities will require sustained investment, strategic foresight, and a nuanced approach that reflects both Ireland’s sovereign priorities and its interconnected role within the broader European and transatlantic security frameworks.

Increased demand for connectivity and operational efficiency whilst incorporating high security has been a complex requirement for vessels in recent years. Solutions would typically display 2 out of 3 of the items mentioned with caveats onboard, be that connectivity at best effort or unknown whereabouts of data travel in the network. The Outernet will be a first for incorporating all these demands into the network, giving customers full control of their Data, bolstered with Committed Information Rate (CIR) based service plans for assured connectivity amongst the continuously evolving threat landscape we see in the maritime industry.

What do you foresee will be the biggest emerging threats/future challenges to Ireland’s maritime security and how would you best prepare for them?

## Introduction

The maritime security environment is undergoing significant transformation, shaped by rapid technological innovation, evolving global power dynamics, and mounting climate-related pressures. While many of today's threats are likely to endure, a range of emerging risks and future challenges are expected to intensify over the coming decade. These developments will place increasing demands on the adaptability and resilience of Ireland's security apparatus, governance structures, and policy frameworks. The most salient of these prospective threats are outlined below, accompanied by strategic considerations aimed at enhancing national preparedness and maritime resilience.

## Weaponisation of the Maritime Domain through Hybrid and Asymmetric Means

The maritime domain is likely to witness an escalation in hybrid and asymmetric threats, characterised by their ambiguity, deniability, and disruptive potential. These threats increasingly blur the lines between civilian and military activity at sea, and may involve the deployment of autonomous or remotely operated maritime systems, the covert use of commercial vessels for surveillance, and cyberattacks targeting critical maritime infrastructure such as ports, shipping lanes, and undersea cables.

Within the Irish context, these developments are particularly disquieting, given the State's profound dependence on maritime connectivity for trade, communications, and energy security. At present, there exists minimal redundancy in the form of satellite communications to support key State functions and critical infrastructure. This lack of alternative pathways renders undersea data cables, port logistics systems, and offshore installations acutely vulnerable to cyber threats and grey-zone interference, posing a significant strategic risk. It is therefore imperative that Ireland moves to establish resilient communication redundancies through the adoption of a PACE model. This methodology—encompassing Primary, Alternate, Contingency, and Emergency communication channels—offers a structured approach to ensuring continuity of operations in the face of disruption.

Moreover, Ireland's current legal and operational frameworks are not yet fully equipped to detect, attribute, or respond effectively to these forms of non-traditional aggression, which often fall below the threshold of conventional military conflict.

These challenges are compounded by the increasing sophistication of state and non-state actors operating in the maritime space, who may exploit legal grey areas, technological asymmetries, and institutional gaps to pursue strategic objectives without triggering formal conflict.

Rivada welcomes the recent announcement that the State has awarded a contract to Thales DMS France for a towed sonar system. This should be seen as the first step in deploying a subsurface surveillance network that will allow, at a minimum for rapid attribution for damage, which in itself can be a strong deterrent.

***Preparedness Measures:***

- Develop a comprehensive maritime cyber security strategy, aligned with national digital infrastructure policies and international best practice, to safeguard critical maritime assets from cyber intrusion and disruption.
- Enhance inter-agency coordination and intelligence sharing, fostering closer collaboration between civil authorities, the Defence Forces, the private maritime sector, and international partners to improve situational awareness and threat detection.
- Strengthen legislative and operational capacity to address grey-zone activities, including the development of legal instruments that enable timely responses to ambiguous threats within and beyond Ireland's territorial waters.
- Invest in technological capabilities in a considered strategic way, such as maritime domain awareness systems, autonomous surveillance platforms, and cyber defence tools, to improve early warning and response mechanisms. Ensuring the interoperability of such capabilities is paramount to provide an end-to-end, flexible solution that can be leveraged by domestic and international partners. Utilising a solution such as The Outernet to provide a secure platform for the operation and coordination of these systems will provide greater resilience than utilising terrestrial

forms of communication.

- Engage in regional and EU-level maritime security initiatives, ensuring that Ireland's non-alignment is balanced with proactive participation in cooperative frameworks that enhance collective resilience.

### Pressure on Maritime Sovereignty and Autonomy in a Multipolar World

The transition towards a more fragmented and multipolar international order is likely to place increasing strain on Ireland's maritime sovereignty and strategic autonomy. As global power competition intensifies, particularly in the North Atlantic, Ireland may face growing pressure to recalibrate its traditional reliance on neutrality and rules-based multilateralism. The resurgence of great power rivalry—manifested through heightened naval activity by both NATO and non-EU actors—raises complex questions about Ireland's role within evolving regional and global security architectures.

This shifting landscape may compel Ireland to engage more substantively with collective security arrangements, including NATO, the EU's Common Security and Defence Policy (CSDP), and emerging maritime coalitions. Such developments could challenge long-standing policy positions and necessitate difficult decisions regarding the extent and nature of Ireland's defence cooperation. Further, the very contemplation of such policy changes will be seen as opportunity by foreign powers such as Russia to engage in hybrid warfare, sowing seeds of disinformation and social unrest in an effort to discourage a fair and open public debate on the security issues facing Ireland.

The strategic ambiguity surrounding Ireland's current maritime posture risks leaving the State underprepared in the face of mounting geopolitical expectations and operational demands.

Moreover, the absence of a clearly articulated national maritime doctrine limits Ireland's ability to assert its interests, define its responsibilities, and communicate its strategic intent to both domestic and international audiences. This is further compounded by a lack of a unifying national security strategy.

In an era in which maritime domains are increasingly contested, clarity of purpose and capability will be essential to safeguarding national sovereignty while maintaining Ireland's principled stance on non-alignment.

***Preparedness Measures:***

- Undertake a comprehensive strategic review of Ireland's position on maritime non-alignment, assessing its viability and implications in light of emerging collective security expectations and geopolitical realities.
- Develop a national maritime doctrine that articulates Ireland's defence posture, identifies capability gaps, and outlines strategic priorities in a rapidly evolving security environment. This Rivada submission has been authored with the hope that the recommendations in our submission will form the foundations of a strong maritime doctrine for the State.
- Expand participation in joint maritime exercises and EU-led security missions, particularly those focused on surveillance, deterrence, and crisis response, to build operational experience and reinforce Ireland's commitment to cooperative security.
- Enhance diplomatic engagement with EU and North Atlantic partners to ensure Ireland's perspectives are reflected in regional maritime security dialogues and frameworks.
- Invest in strategic maritime diplomacy capacity, enabling Ireland to clearly convey its maritime security objectives and policy positions to both domestic stakeholders and international partners.

### Impacts of Climate Change and Resource Competition

Climate change is poised to become an increasingly consequential driver of maritime insecurity, with wide-ranging implications for Ireland's coastal resilience, economic sustainability, and geopolitical positioning. Rising sea levels, more frequent and severe weather events, and the degradation of marine ecosystems will not only threaten coastal infrastructure and maritime operations but also intensify competition over access to marine resources and space.

In particular, the sustainability of fisheries—already under strain from overexploitation and shifting migratory patterns—may become a flashpoint for regional tensions, especially in the context of post-Brexit regulatory divergence and overlapping Exclusive Economic Zone (EEZ) claims. Simultaneously, Ireland's growing reliance on offshore renewable energy infrastructure, including wind farms, interconnectors, and subsea cables, introduces new strategic vulnerabilities. These assets, often located in remote and difficult-to-monitor areas, are susceptible to both environmental disruption and deliberate interference.

As the maritime domain becomes increasingly congested and contested, Ireland must adopt a forward-looking approach that integrates environmental resilience with security planning. This will require not only technological investment but also robust legal and governance frameworks capable of managing emerging disputes and safeguarding critical infrastructure.

***Preparedness Measures:***

- Mainstream climate resilience and adaptation planning into national maritime, coastal, and spatial strategies, ensuring that infrastructure development and emergency response systems are future-proofed against environmental volatility.
- Invest in maritime domain awareness systems, including real-time environmental monitoring, satellite surveillance, and predictive modelling tools, to enhance situational awareness and early warning capabilities.
- Strengthen legal and regulatory mechanisms to manage resource competition and access rights, particularly in relation to fisheries governance, offshore energy zones, and potential EEZ disputes.
- Promote regional cooperation on climate-related maritime security, engaging with EU partners and North Atlantic stakeholders to develop shared frameworks for environmental monitoring, disaster response, and sustainable resource management.
- Support research and innovation in marine science and climate adaptation technologies, ensuring that Ireland remains at the forefront of evidence-based maritime policy and environmental stewardship.

### Technological Disruption and the Rise of Autonomous Maritime Systems

Rapid advances in artificial intelligence, robotics, and autonomous systems are fundamentally reshaping the maritime security landscape. These technologies offer significant potential to enhance maritime domain awareness, surveillance, and operational efficiency. For Ireland, the deployment of uncrewed surface and sub-surface vessels, aerial drones, and AI-enabled monitoring systems could help mitigate existing capacity constraints within the Naval Service and improve situational awareness across its vast Exclusive Economic Zone (EEZ). This was a recommendation in Rivada's submission to the National Security Strategy, and remains as relevant today.

However, these same technologies also introduce new vectors of risk. Hostile actors may exploit autonomous platforms for covert reconnaissance, sabotage of critical infrastructure, or interception of sensitive data. The dual-use nature of such systems—by which commercial and civilian technologies can be repurposed for strategic or military ends—complicates detection, attribution, and response. Further, the regulatory and ethical frameworks governing the deployment and use of autonomous maritime systems remain underdeveloped, both domestically and internationally. This legal ambiguity creates potential gaps in accountability, oversight, and operational norms at sea.

In the Irish context, the challenge lies in balancing innovation and security—leveraging emerging technologies to bolster national capabilities while ensuring robust governance mechanisms are in place to mitigate misuse and unintended consequences.

***Preparedness Measures:***

- Establish a national governance framework for autonomous maritime systems, developed in consultation with EU partners, the International Maritime Organization (IMO), and relevant domestic stakeholders. This framework should address legal, ethical, and operational dimensions of autonomy at sea.
- Support the development of indigenous technological capacity, particularly in maritime robotics, sensor technologies, and AI-enabled systems, to reduce reliance on external providers and foster

strategic autonomy.

- Expand maritime research and development (R&D) collaboration between academic institutions, the Defence Forces, and the private sector, ensuring Ireland remains informed and responsive to global technological trends.
- Integrate autonomous systems into national maritime strategy, identifying clear use cases for surveillance (such as Earth Observation Satellite services), environmental monitoring, and infrastructure protection, while ensuring interoperability with existing platforms, and those of potential allies.
- Promote international dialogue and norm-setting, contributing to the development of global standards for the safe, transparent, and accountable use of autonomous systems in maritime contexts.
- Ensure that technologies from untrusted vendors are neither acquired or deployed by any agency or partner involved in the security of the State.

### Erosion of Maritime Governance and Rule of Law

The integrity of maritime governance is increasingly under strain, as contested interpretations of international legal frameworks—most notably the United Nations Convention on the Law of the Sea (UNCLOS)—challenge the ability of coastal states to uphold the rule of law within their maritime jurisdictions. For Ireland, such developments pose a direct threat to the effective management of its vast maritime domain, particularly in light of rising incidents of illegal, unreported, and unregulated (IUU) activity, as well as the growing complexity of maritime claims and operations.

As global interest in seabed resources, subsea infrastructure, and strategic maritime corridors intensifies, Ireland must also prepare for potential legal disputes concerning the exploitation of deep-sea minerals or other resources (especially those Ireland has restricted the extraction of), the routing of energy interconnectors, and the protection of undersea data-cable corridors. These issues are further complicated by technological advancements and the emergence of new actors in the maritime space, which may outpace existing legal and regulatory frameworks.

In this evolving context, Ireland's ability to assert its maritime rights, protect its sovereign interests, and contribute to the maintenance of a rules-based international order will depend on sustained investment in legal expertise, diplomatic engagement, and multilateral cooperation.

***Preparedness Measures:***

- Increase investment in legal capacity and international maritime diplomacy, ensuring Ireland is well-represented and influential within key forums such as the United Nations, the European Union, and regional maritime organisations.
- Ensure robust data governance and sovereignty protections over undersea and offshore assets, including digital infrastructure, energy installations, and marine scientific data.
- Promote international norms and confidence-building measures that reinforce freedom of navigation, the sustainable use of marine resources, and peaceful dispute resolution, in alignment with Ireland's commitment to multilateralism and the rule of law.
- Strengthen domestic legal frameworks to ensure alignment with evolving international standards and to provide clear jurisdictional authority over emerging maritime activities.
- Support capacity-building initiatives in maritime law and governance, both domestically and in partnership with like-minded states, to enhance collective resilience against legal ambiguity and norm erosion.

### Conclusion

Ireland's maritime security is entering a period of profound transformation, shaped by a convergence of geopolitical, technological, environmental, and legal developments. As the maritime domain becomes increasingly contested and complex, the State faces a series of emerging threats that will test the resilience of its security architecture, legal frameworks, and strategic posture.

Among the most pressing future challenges is the weaponisation of the maritime space through hybrid and asymmetric means. The use of cyberattacks, uncrewed systems, and grey-zone tactics by state and non-state actors threatens to exploit Ireland's critical infrastructure and limited surveillance capacity. Simultaneously, the rise of autonomous maritime technologies introduces both opportunities and risks, demanding urgent regulatory innovation and investment in indigenous capability.

Ireland's traditional policy of military neutrality will also come under increasing pressure in a multipolar world, as expectations grow for deeper engagement with EU and regional security frameworks. This geopolitical shift necessitates a strategic reassessment of Ireland's defence posture and its role within collective maritime security arrangements.

Climate change and resource competition further compound these challenges. The intensification of extreme weather events, shifting fish stocks, and the expansion of offshore energy infrastructure will create new vulnerabilities and potential flashpoints. Ireland must integrate climate resilience into its maritime planning and strengthen its capacity to manage environmental and resource-related disputes.

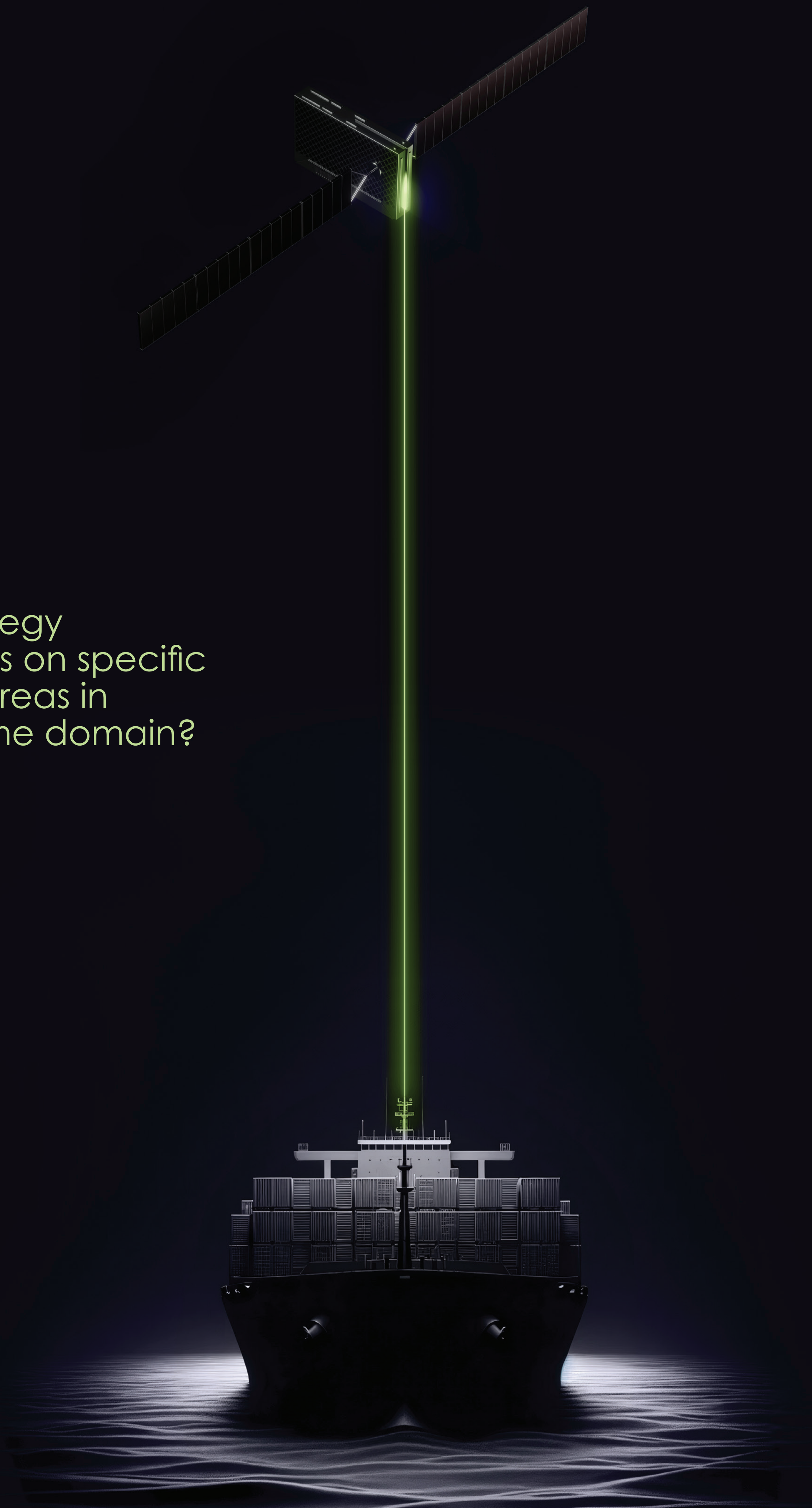
Finally, the erosion of maritime governance and contested interpretations of international law threaten to undermine the rules-based order upon which Ireland has long relied. Legal disputes over seabed resources, data cables, and maritime boundaries are likely to increase, requiring enhanced legal capacity and proactive diplomatic engagement.

To prepare for these challenges, Ireland must adopt a comprehensive and forward-looking maritime strategy. This should include:

- Investing in surveillance, cyber defence, and autonomous technologies and utilising a secure non-terrestrial Satellite LEO such as the Outernet to provide for coordination and operationalisation;
- Enhancing inter-agency coordination and international cooperation;
- Developing robust legal and regulatory frameworks;
- Strengthening climate adaptation and environmental monitoring;
- Articulating a clear national maritime doctrine that marries a policy of non-alignment with evolving security realities.

By taking these steps, Ireland can safeguard its maritime sovereignty, protect its critical infrastructure, and contribute meaningfully to regional and global maritime stability in the decades ahead.

Should the Strategy prioritise its focus on specific geographical areas in Ireland’s maritime domain?



## Introduction

While the entirety of Ireland's maritime domain merits protection, the strategic prioritisation of specific geographical areas is both necessary and judicious in light of finite national resources and an increasingly complex maritime risk environment. A future-facing National Maritime Security Strategy must therefore adopt a risk-informed and capability-aligned approach to spatial prioritisation—one that reflects the differentiated strategic, economic, environmental, and infrastructural value of various maritime zones. Such an approach would enable more efficient allocation of surveillance, enforcement, and resilience-building efforts, while also enhancing Ireland's ability to respond to emerging threats in a targeted and proportionate manner. Prioritisation does not imply neglect of less prominent areas, but rather the establishment of a tiered framework that aligns national capabilities with the most pressing vulnerabilities and strategic interests.

## Southwest Approaches and Atlantic Seaboard

Ireland's South and Southwest maritime zones constitute a region of exceptional strategic importance. Serving as the State's principal maritime gateway to the wider Atlantic, these waters host a dense concentration of transatlantic subsea communications cables, major shipping lanes, and expanding offshore renewable energy infrastructure, with more planned. This corridor not only underpins Ireland's economic connectivity and energy transition but also plays a vital role in the broader transatlantic security architecture.

The strategic significance of this region has not gone unnoticed by foreign powers. Recent naval activity—particularly by non-allied actors—has underscored the vulnerability of these waters to surveillance, grey-zone operations, and potential interference with critical undersea infrastructure. The relative remoteness and sparse monitoring of the Atlantic seaboard further compound these risks, creating operational blind spots that could be exploited for covert reconnaissance or sabotage.

Moreover, the increasing density of high-value assets in this region—ranging from data cables and offshore wind farms to energy interconnectors—raises the stakes for both state and non-state actors. As Ireland deepens its integration into European digital and energy networks, the security of these assets becomes not only a national concern but a matter of regional resilience.

***Strategic Recommendation:***

- Prioritise sustained surveillance and protection capacity in the South and Southwest maritime zones. This should include targeted investment in unmanned maritime systems (UMS), aerial intelligence, surveillance and reconnaissance (ISR) platforms, and satellite-based maritime domain awareness tools, enabled by a secure LEO platform such as Rivada's Outernet.
- Enhance legal and regulatory authority to safeguard critical infrastructure, including the development of specific provisions for the protection of subsea cables and offshore energy installations under Irish and international law.
- Establish a regional maritime operations hub along the Southwest coast to coordinate inter-agency response, facilitate real-time intelligence sharing, and support rapid deployment capabilities.
- Strengthen partnerships with EU and transatlantic allies, particularly in the areas of infrastructure monitoring, cyber resilience, and joint maritime exercises focused on hybrid threat scenarios.

## Irish Sea and Eastern Maritime Corridor

The Irish Sea represents one of the most strategically significant maritime zones for Ireland, owing to its dense concentration of commercial shipping, critical infrastructure, and proximity to major ports such as Dublin, Rosslare, and Belfast. This corridor serves as a vital conduit for national and regional economic activity, facilitating the movement of goods, energy, and data between Ireland, the United Kingdom, and continental Europe.

Beneath its surface, the Irish Sea hosts a complex network of subsea cables, gas pipelines, and energy interconnectors that underpin Ireland's digital economy and energy security. Notably, it is suggested that over 70 per cent of Ireland's natural gas is supplied via two interconnector pipelines originating from Moffat, Scotland, which traverse the Irish Sea before making landfall in Meath and Dublin. The strategic dependence on a single source and route for such a critical resource underscores the region's infrastructural vulnerability. The increasing reliance on these assets—particularly in the context of offshore renewable energy development and cross-border energy integration—renders the region a focal point for both strategic opportunity and exposure.

The narrow geography of the Irish Sea, combined with the political sensitivities surrounding North–South and East–West maritime governance, further elevates its importance. Post-Brexit regulatory divergence, overlapping jurisdictions, and the need for coordinated contingency planning all contribute to a complex operational environment. Yet, compounding these challenges is the persistent absence of a coherent national and maritime security culture in Ireland. This deficiency is not confined to the general public but is also evident across government departments and key ministries, where strategic awareness and institutional preparedness remain underdeveloped. The cultivation of such a culture—through education, inter-agency coordination, and long-term strategic planning—is not only essential but must be regarded as a foundational pillar of Ireland's maritime security strategy.

***Strategic Recommendation:***

- Strengthen coordination mechanisms between Irish and UK maritime authorities, with a focus on joint surveillance, intelligence sharing, and operational interoperability.
- Ensure the National Maritime Security Strategy includes formalised protocols for shared threat detection, rapid response, and the protection of critical infrastructure, particularly subsea cables and energy interconnectors.
- Establish a dedicated Irish Sea Security Working Group, involving civil, military, and regulatory stakeholders from both jurisdictions, to address emerging risks and promote regulatory alignment where feasible.
- Invest in region-specific maritime domain awareness capabilities, including real-time monitoring systems and cross-border data integration platforms, to enhance situational awareness and resilience.
- Promote diplomatic engagement and confidence-building measures, aimed at reducing friction and fostering trust in the governance of this strategically sensitive maritime corridor.

### Northwest Continental Shelf and Extended EEZ

Ireland's Northwest Continental Shelf and extended EEZ represent one of the most expansive and under-monitored areas within the State's maritime jurisdiction. Rich in biodiversity, ecologically significant habitats, and valuable fisheries, this region also holds potential for future resource exploration, including deep-sea minerals and hydrocarbons. As global interest in the sustainable exploitation of ocean resources intensifies, these waters are likely to attract increased attention from both commercial and strategic actors.

Climate change is expected to further elevate the strategic relevance of this zone. Shifting migratory patterns of fish stocks, changes in ocean currents, and the gradual opening of Arctic shipping routes may redirect maritime activity through the North Atlantic, increasing traffic and competition in these relatively remote waters. The vastness of the area, combined with limited national surveillance and enforcement capabilities, renders it particularly vulnerable to unregulated and potentially unlawful activity—including illegal fishing, unauthorised surveying, and environmental degradation.

Moreover, the ecological sensitivity of the region demands a careful balance between security, conservation, and sustainable development. As Ireland seeks to assert its rights over its extended continental shelf under international law, it must also ensure that governance mechanisms are in place to prevent exploitation by external actors and to uphold its environmental obligations.

***Strategic Recommendation:***

- Integrate environmental and fisheries protection into Ireland's broader maritime security frameworks, recognising the interdependence of ecological resilience and national security.
- Develop satellite-based monitoring capabilities in partnership with EU agencies such as the European Maritime Safety Agency (EMSA) and FRONTEX, to enhance situational awareness and enable real-time detection of unauthorised activity.

- Establish data-sharing agreements and joint monitoring initiatives with neighbouring states and regional organisations to improve oversight of remote maritime zones and support coordinated enforcement.
- Invest in long-range unmanned surveillance platforms and oceanographic research to build a comprehensive understanding of activity patterns and ecological changes in the region.
- Advance Ireland's legal and diplomatic efforts to secure recognition and protection of its extended continental shelf claims, ensuring that governance frameworks are robust, transparent, and aligned with international law.

### Port and Coastal Infrastructure Zones

Ireland's ports and coastal infrastructure form the backbone of its maritime economy and national resilience. These zones facilitate the movement of goods, support fisheries and offshore renewable energy development, and serve as critical nodes in the country's logistical and supply chain networks. As such, they are increasingly recognised not only for their economic value but also for their strategic vulnerability.

In an era of hybrid threats and digital interdependence, ports are no longer solely at risk from physical disruption. The growing digitisation of port operations—ranging from cargo handling systems to customs processing and energy management—has introduced new cyber vulnerabilities. A successful cyberattack on a major port could have cascading effects on national trade, energy supply, and emergency response capabilities. Moreover, the physical proximity of many ports to urban centres and critical infrastructure amplifies the potential impact of sabotage or disruption.

The strategic importance of these zones is further heightened by Ireland's expanding offshore renewable energy ambitions. As ports are increasingly repurposed to support wind farm construction, maintenance, and grid connectivity, they become essential enablers of the State's climate and energy security objectives. Ensuring their protection is therefore not only a matter of economic continuity but also of national strategic interest.

***Strategic Recommendation:***

- Prioritise cyber resilience programmes tailored to the maritime and port sectors, including regular vulnerability assessments, penetration testing, and the integration of cybersecurity into port infrastructure planning and operations.
- To ensure the resilience and operational continuity of port infrastructure in the face of crises—be they cyberattacks, natural disasters, or hostile interventions—it is imperative to develop a robust and comprehensive emergency preparedness and continuity framework. This framework should be underpinned by a Primary, Alternate, Contingency, Emergency (PACE) communications plan, wherein the Outernet or a comparable self-contained LEO constellation (if available) is integrated as a critical component of the contingency and emergency tiers. By leveraging the Outernet's secure, space-based architecture, ports can maintain uninterrupted, sovereign communications capabilities, thereby safeguarding critical functions and ensuring rapid response and recovery during adverse events.
- Conduct regular inter-agency drills and scenario-based exercises, involving port authorities, An Garda Síochána, the Defence Forces, emergency services, and private sector stakeholders, to test and refine coordinated response protocols.
- Establish a national framework for the designation and protection of Critical Maritime Infrastructure (CMI), ensuring that ports and associated coastal assets are formally recognised and resourced as strategic priorities.
- Foster public-private partnerships to enhance information sharing, threat intelligence, and joint investment in security technologies across the port and logistics sectors.

### Conclusion

In light of the diverse and evolving threats facing Ireland's maritime domain, a geographically prioritised approach to maritime security is not only advisable but essential. While the entirety of Ireland's waters warrants protection, the differentiated risk profiles, strategic assets, and operational challenges across various maritime zones necessitate a more focused and resource-efficient strategy.

The Southwest Approaches and Atlantic Seaboard demand heightened attention due to their role as gateways to transatlantic infrastructure and their exposure to hybrid threats. The Irish Sea and Eastern Maritime Corridor, with its dense shipping traffic and critical energy and data infrastructure, requires robust cross-jurisdictional coordination and contingency planning. The Northwest Continental Shelf and extended EEZ, though remote, are increasingly significant in the context of environmental change, resource competition, and under-regulated activity. Meanwhile, ports and coastal infrastructure zones represent critical nodes of national resilience, vulnerable to both physical and cyber disruption.

By adopting a risk-informed, capability-aligned framework, the National Maritime Security Strategy can ensure that surveillance, enforcement, and resilience-building efforts are directed where they are most needed. This does not imply neglect of less prominent areas, but rather the establishment of a strategic hierarchy that reflects Ireland's evolving maritime interests and vulnerabilities.

Further, the integration of secure, resilient communication systems—such as the Rivada Outernet within a PACE framework—will be essential in ensuring that ports and coastal infrastructure zones can maintain critical functions during crises.

Ultimately, prioritising specific geographical areas will enable Ireland to better safeguard its sovereignty, protect critical infrastructure, and contribute meaningfully to regional and international maritime stability—while ensuring that limited resources are deployed with maximum strategic effect.

To most effectively safeguard Ireland's maritime interests, what strategic investments in technology, infrastructure, or capabilities should be prioritised?

## Introduction

To effectively safeguard Ireland's maritime interests in an increasingly contested, technologically advanced, and climate-impacted environment, strategic investment must be directed towards areas that both enhance national resilience and address critical capability shortfalls. These investments should not only bolster the operational effectiveness of the State's maritime security apparatus but also ensure alignment with broader European Union and international maritime governance frameworks. In this context, the EU Security Action for Europe (SAFE) programme presents a significant opportunity for Ireland to strengthen its maritime security posture through targeted investment, accelerated procurement, and strategic collaboration. The following priority areas are identified as essential to advancing Ireland's maritime resilience and ensuring its preparedness for the complex challenges of the coming decade.

## Maritime Domain Awareness (MDA) and Surveillance Systems

A foundational pillar of effective maritime security is the capacity to maintain persistent, real-time situational awareness across the full breadth of a state's maritime domain. For Ireland—whose Exclusive Economic Zone (EEZ) is among the largest in Europe—this requirement is particularly acute. At present, Ireland's Maritime Domain Awareness (MDA) capabilities remain limited, fragmented, and overly reliant on external sources, including allied intelligence and EU-level surveillance platforms. This dependency creates critical gaps in detection, attribution, and early warning, particularly in remote or under-monitored areas such as the Atlantic seaboard and extended continental shelf.

As maritime threats become more diverse and technologically sophisticated—ranging from unmarked vessels and grey-zone operations to cyber-enabled sabotage and environmental degradation—the need for a robust, sovereign MDA architecture becomes increasingly urgent. Enhancing Ireland's ability to independently monitor, assess, and respond to maritime activity is essential not only for national security but also for fulfilling obligations under EU and international maritime governance frameworks.

***Strategic Investments Should Include:***

- Acquisition of long-range Maritime Patrol Aircraft (MPA) and Uncrewed Aerial Systems (UAS) equipped with advanced surveillance payloads, to extend Ireland's reach across its EEZ and support persistent monitoring of high-risk zones.
- Selection of a Secure Satellite Communications (SATCOM) partner. This will enable real-time coordination between naval assets, coast guards, and command centres, especially in remote oceanic areas and provide resilience in Crisis. SATCOM ensures continuity of operations during cyberattacks or infrastructure failures.
- Acquisition of a Synthetic Aperture Radar (SAR). SAR can significantly enhance Ireland's maritime security by enabling persistent, all-weather surveillance of its vast Exclusive Economic Zone (EEZ). It can detect and track vessels operating without AIS transponders, including those engaged in illegal fishing or hybrid activities near undersea infrastructure. SAR imagery also supports early warning and rapid response by providing high-resolution data even in cloud cover or darkness.
- Development of a National Maritime Data Fusion Centre, capable of integrating multi-source data—including satellite imagery, coastal and offshore radar, Automatic Identification System (AIS) feeds, and subsea sensor networks—to generate a comprehensive and real-time Recognised Maritime Picture (RMP), resolving a key capability weakness identified in the Commission on the Defence Forces. This centre should have access to other agency data such as the Sea Fisheries Protection Authority (SFPA), and where appropriate external foreign agency data, through appropriate and secure channels.
- Expansion of partnerships with EU-level initiatives, such as the European Maritime Safety Agency's (EMSA) Integrated Maritime Services and the Copernicus Earth observation programme, to leverage shared surveillance assets and enhance interoperability with European partners.
- Strategic investment in artificial intelligence and machine learning technologies should be prioritised to enhance anomaly detection, predictive analytics, and automated threat classification within the maritime domain—capabilities which may, for instance, assist in identifying trafficking routes exploited by narcotics smugglers.
- Strengthening legal and institutional frameworks to support data sharing, inter-agency coordination, and the operational integration of MDA capabilities across civil, military, and

regulatory bodies.

### Naval Service Fleet Renewal and Personnel Capacity

The Irish Naval Service remains the State's principal maritime security actor, yet it continues to face persistent challenges in both fleet modernisation and personnel capacity. These limitations significantly constrain operational tempo, geographic coverage, and the ability to respond effectively to the increasingly complex and multidimensional threats emerging within Ireland's maritime domain. The current fleet, composed largely of ageing Offshore Patrol Vessels (OPVs), lacks the technological adaptability and mission versatility required to address hybrid threats, cyber vulnerabilities, and subsea infrastructure protection.

Equally pressing is the issue of staffing. Chronic recruitment and retention difficulties have led to reduced crewing levels, operational stand-downs, and a diminished capacity to sustain continuous maritime presence. Without a robust and well-supported personnel base, even the most advanced platforms will be unable to deliver the strategic outcomes required of a modern naval force.

Addressing these challenges demands a dual-track investment strategy—one that simultaneously renews the fleet and revitalises the human capital of the Naval Service.

***Strategic Investments Should Include:***

- Replacement of ageing vessels with Multi-Role Vessels (MRVs) designed to support a broad spectrum of missions, including hybrid threat response, cyber defence, subsea surveillance, and environmental monitoring.
- Introduction of modular systems and adaptable mission payloads, enabling rapid reconfiguration of vessels for diverse operational scenarios—from humanitarian assistance and fisheries protection to intelligence gathering and infrastructure defence.
- Implementation of a sustained, well-resourced programme for Naval Service recruitment, retention, and career development, incorporating competitive remuneration, improved work-life balance, and enhanced technical and leadership training pathways.
- Investment in shore-based support infrastructure, including simulation and training facilities, to ensure personnel are equipped to operate and maintain next-generation platforms and systems.
- Strengthening of civil-military collaboration, particularly in areas such as cyber security, logistics, and maritime research, to broaden the talent pipeline and foster innovation within the Naval Service.

### Cybersecurity for Maritime and Port Infrastructure

As Ireland's maritime infrastructure becomes increasingly digitised and interconnected, the threat landscape is evolving rapidly. Ports, offshore energy platforms, and subsea communication systems now rely heavily on digital technologies for operations, logistics, navigation, and data exchange. This digital integration, while enhancing efficiency and connectivity, also introduces significant vulnerabilities to cyberattack, data compromise, and remote disruption.

Cybersecurity must therefore be recognised as a core pillar of national maritime security. The potential consequences of a successful cyberattack—ranging from port shutdowns and supply chain paralysis to the manipulation of navigational systems or sabotage of offshore installations—could have severe economic, environmental, and strategic repercussions. Moreover, the maritime sector's traditionally low level of cyber maturity, combined with the complexity of public-private ownership models, makes coordinated defence particularly challenging.

To address these risks, Ireland must adopt a proactive and integrated approach to maritime cyber resilience, ensuring that both public and private stakeholders are equipped to prevent, detect, and respond to cyber threats.

***Strategic Investments Should Include:***

- Establishment of a Maritime Cyber Security Centre of Excellence, developed in partnership with the National Cyber Security Centre (NCSC), port authorities, offshore operators, and academic institutions. This centre would serve as a hub for threat intelligence, incident response coordination, and best practice dissemination.

- Mandating and supporting regular cyber-resilience audits for all critical maritime infrastructure, including ports, offshore platforms, and subsea systems. These audits should assess vulnerabilities, test incident response protocols, and ensure compliance with national and EU cybersecurity standards.
- Development of specialised cyber defence units within the Defence Forces, with capabilities tailored to maritime and critical infrastructure protection. These units should be supported by dedicated training programmes for personnel across the maritime sector, including port operators, regulatory agencies, and emergency responders.
- Integration of cybersecurity into port and maritime infrastructure planning, ensuring that new developments are designed with cyber resilience as a foundational principle.
- Promotion of public-private partnerships and international cooperation, particularly with EU cybersecurity initiatives and maritime security frameworks, to enhance collective resilience and information sharing.

## Resiliency of Subsea and Energy Infrastructure

Ireland's maritime domain is home to a dense and expanding network of subsea infrastructure, including transatlantic data cables, energy interconnectors, and offshore renewable energy platforms. These assets are of critical national and international importance, underpinning digital connectivity, energy security, and economic resilience. However, their strategic value also renders them increasingly attractive targets for state and non-state actors seeking to exploit vulnerabilities for geopolitical leverage or disruptive effect.

The covert nature of subsea operations, combined with the technical challenges of monitoring vast underwater areas, makes this infrastructure particularly susceptible to sabotage, unauthorised surveying, and hybrid interference. Recent global incidents have highlighted the ease with which undersea cables and pipelines can be damaged—either deliberately or through ambiguous activity—without immediate attribution or response. For Ireland, whose geopolitical position places it at the nexus of transatlantic digital and energy flows, the protection of these assets must be treated as a national security priority.

***Strategic Investments Should Include:***

- Deployment of Unmanned Underwater Vehicles (UUVs) and autonomous seabed surveillance systems, capable of conducting routine inspections, anomaly detection, and real-time monitoring of critical subsea infrastructure.
- Creation of a dedicated infrastructure protection unit, integrating military, intelligence, and civilian expertise to coordinate surveillance, threat assessment, and rapid response operations related to subsea and offshore energy assets.
- Inclusion of subsea infrastructure within Ireland's national critical infrastructure protection planning, supported by clear legal mandates, escalation protocols, and inter-agency coordination mechanisms.
- Development of an EEZ subsea asset registry and risk map, to support prioritisation of surveillance and protection efforts based on strategic value and threat exposure.
- Strengthening of international cooperation, particularly with EU partners and transatlantic allies, to facilitate intelligence sharing, joint exercises, and coordinated responses to incidents affecting shared infrastructure.

## Maritime Spatial Intelligence and Environmental Monitoring

As climate change accelerates and pressures on marine resources intensify, Ireland will require enhanced strategic foresight to understand and manage the complex interplay between physical, economic, and ecological dynamics within its maritime domain. The ability to integrate environmental intelligence into maritime security and development planning will be essential for safeguarding biodiversity, ensuring sustainable resource use, and mitigating the security implications of environmental degradation.

Ireland's vast and diverse marine territory encompasses sensitive ecosystems, critical fisheries, and expanding offshore infrastructure. These areas are increasingly exposed to climate-driven changes such as ocean warming, shifting species distributions, and more frequent extreme weather events. Without robust spatial intelligence and environmental monitoring systems, the State risks being reactive rather than proactive in addressing these challenges.

Strategic integration of environmental data into maritime governance will also support more informed decision-making in areas such as offshore energy development, fisheries management, and marine spatial planning. This will be particularly important as Ireland seeks to balance economic growth with ecological stewardship and climate resilience.

***Strategic Investments Should Include:***

- Enhanced capacity in marine spatial planning, supported by integrated datasets that combine environmental monitoring, resource mapping, and risk analysis to inform both security and development decisions.
- Investment in dual-use technologies, such as smart buoys, automated sensor arrays, and oceanographic monitoring platforms, capable of collecting real-time data on weather patterns, sea currents, pollution levels, and ecosystem health.
- Integration of maritime environmental data into national security planning, ensuring that climate and ecological intelligence informs threat assessments, infrastructure siting, and emergency preparedness.
- Development of a national maritime environmental intelligence framework, linking scientific research institutions, regulatory agencies, and security actors to facilitate data sharing and coordinated response.
- Participation in regional and EU-level environmental monitoring initiatives, such as the European Marine Observation and Data Network (EMODnet) and Copernicus Marine Service, to enhance Ireland's access to high-quality spatial and environmental intelligence.

## Conclusion

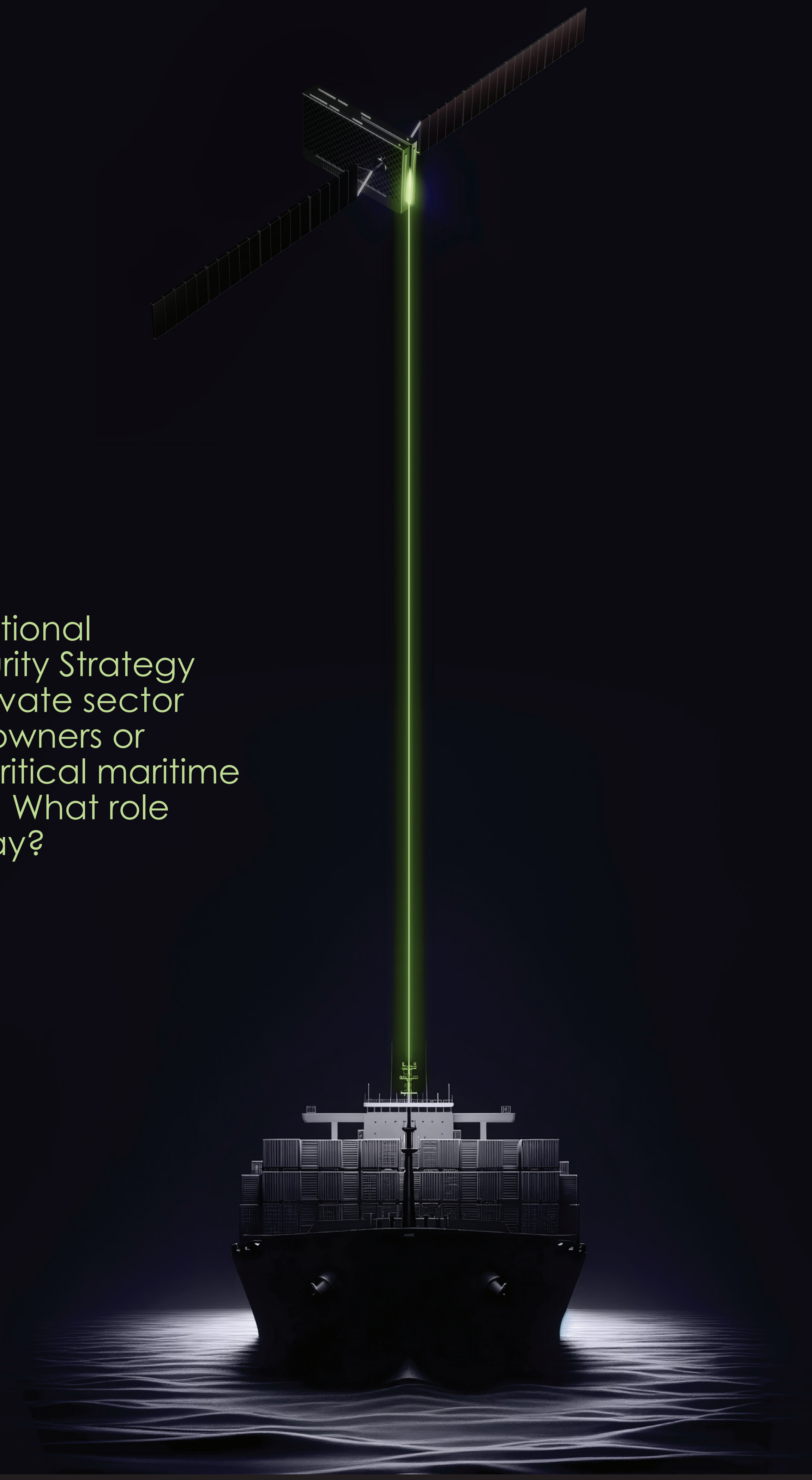
To safeguard Ireland's maritime interests in an era marked by geopolitical uncertainty, technological disruption, and environmental volatility, a coherent and forward-looking investment strategy is essential. The maritime domain is no longer defined solely by traditional naval threats, but by a complex interplay of cyber vulnerabilities, infrastructure dependencies, ecological pressures, and hybrid tactics. In this context, Ireland must adopt a whole-of-government and whole-of-society approach to maritime security—one that is technologically advanced, operationally agile, and strategically integrated.

The priority investment areas outlined—ranging from enhanced Maritime Domain Awareness and fleet renewal to cyber defence, subsea infrastructure protection, and environmental intelligence—represent the foundational pillars of a resilient maritime security architecture. These investments must be underpinned by sustained political commitment, inter-agency coordination, and alignment with EU and international frameworks. Leveraging SAFE to acquire these technologies is paramount.

Crucially, Ireland's approach must be both adaptive and anticipatory. This means not only addressing current capability gaps but also building the institutional foresight and technological capacity to respond to future challenges. By investing in dual-use technologies, fostering innovation, and strengthening civil-military partnerships, Ireland can position itself as a proactive and credible maritime actor—capable of protecting its sovereignty, supporting regional stability, and contributing meaningfully to the global maritime commons.

In short, strategic investment in maritime security is not merely a defence imperative—it is a national resilience priority, central to Ireland's economic vitality, environmental stewardship, and geopolitical agency in the decades ahead.

Should the National Maritime Security Strategy involve the private sector who may be owners or operators of critical maritime infrastructure? What role could they play?



## Introduction

Yes. The private sector must be formally recognised as a core stakeholder within Ireland's maritime security architecture. A significant proportion of the infrastructure underpinning national resilience—such as ports, subsea communication cables, offshore energy platforms, and commercial shipping networks—is owned, operated, or maintained by private entities. The effective protection of these critical systems cannot be achieved through state action alone.

Accordingly, the National Maritime Security Strategy should articulate structured mechanisms for public–private cooperation, encompassing information sharing, joint risk assessments, and coordinated preparedness planning. Establishing clear protocols for engagement will not only enhance situational awareness and incident response but also foster a shared sense of responsibility for safeguarding Ireland's maritime domain.

## Shared Responsibility for the Security of Critical Infrastructure

Private operators of maritime infrastructure—particularly within the energy, transport, and digital communications sectors—are increasingly exposed to a spectrum of threats, including cyberattacks, espionage, sabotage, and hybrid disruptions. Despite the strategic importance of these assets, the delineation of responsibility for their protection often remains unclear, fragmented, or inconsistently applied across sectors.

Given the interdependence between public security and privately operated infrastructure, a shared responsibility model is essential. The private sector must be actively engaged not only as a stakeholder but as a co-producer of maritime security. This requires formalised structures for collaboration, clear regulatory expectations, and a culture of joint preparedness.

***Recommended Role for the Private Sector:***

- Participate in a National Critical Maritime Infrastructure Forum, co-chaired by government and industry, to facilitate coordinated risk assessments, contingency planning, and the development of shared recovery protocols. This forum should serve as a platform for strategic dialogue, operational coordination, and trust-building between public and private actors.
- Adopt and maintain minimum security standards, including physical protection measures, access control systems, and robust cybersecurity protocols. These standards should be aligned with national legislation and EU regulatory frameworks, such as the NIS2 Directive, and subject to regular review and compliance audits.
- Undertake regular joint exercises and scenario-based planning, in collaboration with the Defence Forces, An Garda Síochána, and relevant state agencies. These exercises should test response capabilities, identify procedural gaps, and build institutional familiarity with crisis coordination mechanisms.
- Contribute to threat intelligence sharing mechanisms, ensuring that private operators are both recipients and contributors of timely, actionable information related to maritime security risks.
- Invest in resilience-by-design approaches, embedding security considerations into the planning, construction, and operation of maritime infrastructure from the outset.

## Enhanced Cybersecurity Partnership

As maritime operations become increasingly digitised, many private sector operators now manage highly integrated operational technology (OT) and information technology (IT) systems. These systems, while essential for efficiency and competitiveness, also present a growing attack surface for malicious cyber actors. Ports, logistics platforms, and subsea cable operators are particularly attractive targets, given their centrality to national and EU-wide economic and communications infrastructure.

A successful cyberattack on any of these nodes could trigger cascading disruptions—halting trade flows, compromising sensitive data, or severing digital connectivity. In this context, cybersecurity must be treated not merely as a technical concern, but as a strategic imperative requiring close public–private collaboration.

***Recommended Role for the Private Sector:***

- Collaborate with the National Cyber Security Centre (NCSC) to report vulnerabilities, share threat intelligence, and co-develop sector-specific incident response protocols. This collaboration should be formalised through secure communication channels and regular joint briefings.
- Invest in cybersecurity workforce development, ensuring that personnel across all levels of maritime operations—from IT administrators to executive leadership—receive training in cyber hygiene, threat recognition, and incident response.
- Contribute to the design and maintenance of a Maritime Cyber Risk Register, which would support national situational awareness, inform risk prioritisation, and guide investment in protective measures. This register should be dynamic, regularly updated, and integrated into broader national risk assessment frameworks.
- Participate in cyber resilience exercises, coordinated with state agencies, to test preparedness, identify vulnerabilities, and build institutional familiarity with crisis response procedures.
- Adopt international best practices and standards, such as those outlined in the EU's NIS2 Directive and the IMO's cybersecurity guidelines, to ensure consistency and interoperability across the maritime sector.

### Intelligence and Situational Awareness Support

The private sector, particularly those entities that own or operate critical maritime infrastructure—such as ports, shipping companies, offshore energy platforms, and undersea cable operators—possess a wealth of operational data and technical capabilities that can significantly enhance the State's Maritime Domain Awareness. These actors often maintain sophisticated sensor networks, vessel tracking systems, and cyber-physical monitoring tools that generate real-time insights into maritime activity. Leveraging such capabilities through structured collaboration can augment the State's capacity to detect, assess, and respond to emerging maritime threats.

In the context of an increasingly complex maritime security environment—characterised by hybrid threats, cyber vulnerabilities, and geopolitical contestation in the maritime domain—integrating private sector intelligence into national situational awareness frameworks is both pragmatic and necessary. The European Union's Maritime Security Strategy (EUMSS) and the UK's National Strategy for Maritime Security both underscore the importance of public-private partnerships in safeguarding maritime interests. Ireland, as a small island nation with a vast maritime jurisdiction and critical subsea infrastructure, must similarly adopt a whole-of-society approach to maritime security.

***Recommended Role for the Private Sector***

- Voluntary Anomaly Reporting Mechanisms: Establish secure, anonymised channels for the reporting of maritime anomalies, such as GPS spoofing, unregistered or erratic vessel behaviour, and disturbances to subsea infrastructure (e.g., data cables or offshore energy assets). These mechanisms should be underpinned by legal protections and incentives to encourage timely and accurate reporting.
- Integrated MDA Platforms: Facilitate structured collaboration between private operators and state agencies (e.g., Naval Service, Irish Coast Guard, Garda National Cyber Crime Bureau) through interoperable MDA platforms. Shared protocols for data classification, privacy, and cybersecurity must be developed to ensure trust and operational integrity.
- Technological Innovation and Data Fusion: Encourage the co-development and deployment of advanced technologies—such as blockchain for secure logistics tracking, artificial intelligence for anomaly detection, and geospatial analytics for pattern-of-life analysis. These tools can enhance transparency and resilience across the maritime supply chain, aligning commercial efficiency with national security objectives.
- Cybersecurity Collaboration: Given the increasing convergence of physical and digital threats in the maritime domain, private sector actors should be integrated into national cyber threat intelligence networks. This includes participation in joint exercises, information-sharing forums, and

the development of sector-specific cyber resilience standards.

- Capacity Building and Training: Promote joint training initiatives and scenario-based exercises involving both public and private stakeholders. These efforts can build mutual understanding, improve interoperability, and foster a shared security culture across the maritime sector.
- Provision of Secure, Resilient Communications Services: Internet-independent satellite communications will play a vital role in Ireland's Maritime Security Strategy. It is also a paradigmatic example of a capability that Ireland should acquire as a service, rather than seeking to own it or build and operate it itself. The private sector, including inter alia Rivada Networks, can supply the Irish State with resilient communications services far more efficiently and quickly than the State can do itself.

## Capacity Building and Innovation

Ireland's maritime sector is undergoing a period of transformation, driven by the twin imperatives of climate adaptation and technological modernisation. The emergence of a domestic maritime technology and offshore engineering ecosystem presents a strategic opportunity to embed innovation and resilience into the fabric of national maritime security. These capabilities—ranging from uncrewed systems and smart sensors to advanced materials and cyber-physical systems—should be harnessed not only for economic development but also for sovereign capability enhancement.

In line with the objectives of the National Marine Planning Framework, the National Security Strategy, and the Future Defence Force Report, there is a clear rationale for integrating private sector innovation actors into the broader security architecture. Doing so would support the development of dual-use technologies, foster indigenous capability, and reduce reliance on external suppliers in critical domains.

### *Recommended Role for the Private Sector*

- Strategic R&D Partnerships: Collaborate with universities, Defence Forces, and state agencies (e.g., Irish Maritime Development Office, Science Foundation Ireland) to co-develop indigenous solutions in key areas such as uncrewed surface and sub-surface vehicles, persistent environmental monitoring, and subsea surveillance technologies. These partnerships should be mission-oriented and aligned with national security priorities.
- Innovation Funding and Testbeds: Actively participate in joint research and development initiatives supported by the Disruptive Technologies Innovation Fund (DTIF), Horizon Europe, and other EU maritime security instruments. The establishment of maritime innovation testbeds—particularly in offshore renewable energy zones—could serve as real-world environments for trialling and validating new technologies under operational conditions.
- Skills and Workforce Development: Contribute to the creation of robust talent pipelines in maritime cyber security, marine engineering, and resilience planning. This could include support for apprenticeships, postgraduate research, and industry placements, particularly in collaboration with Technological Universities and Centres for Research Training.
- Resilience-by-Design Approaches: Embed security and resilience considerations into the design and deployment of maritime infrastructure and technologies. This includes adopting standards for cyber-physical resilience, supply chain integrity, and environmental sustainability from the outset of innovation processes.

## Introduction of an Executive Innovation Corps

The U.S. Army Executive Innovation Corps (EIC) is a forward-looking initiative designed to embed senior military leaders within private-sector innovation ecosystems. Its purpose is to expose personnel to contemporary practices in data science, emerging technologies, and design-led thinking, thereby equipping them to apply these insights to complex defence challenges. The EIC represents a deliberate shift towards enhancing institutional agility, fostering civil-military collaboration, and accelerating the modernisation of strategic capabilities within the United States Army. We reccommend, given the retention legacy within the Defence Forces that the EIC Model be further enhanced by offering reserve commissioned ranks to highly-skilled and experienced private sector executives who may wish to participate in the program and offer their guidance and leadership.

***Benefits of an EIC-Inspired Programme for Ireland's Maritime Security***

Adopting a similar framework within an Irish context—particularly within the remit of maritime security—could offer tangible and strategic advantages:

- Catalysing Capability Modernisation: By embedding personnel from the Irish Defence Forces, Coast Guard, the Department of Transport and Department of Communication within centres of innovation (including academia, tech sectors, and research institutions), Ireland could accelerate the adoption of advanced technologies and practices, particularly in domains such as surveillance, undersea infrastructure protection, and hybrid threat detection.
- Strengthening Civil-Military Synergies: A bespoke Irish model could enhance cooperation across government departments, academia, and private industry—facilitating a whole-of-nation approach to maritime security and resilience. Such collaboration is increasingly vital given the transboundary nature of contemporary maritime risks.
- Enhancing Strategic Responsiveness: Training Irish Defence and key civil service leaders in innovation methodologies—particularly those drawn from design thinking and systems analysis—would improve the State's capacity to anticipate, prepare for, and respond to emerging maritime security threats. These include not only conventional risks, but also complex, non-linear challenges such as cyberattacks on undersea cables and grey zone activity in the North Atlantic.
- Developing and Retaining Talent: A focus on experiential learning and strategic secondments would serve to attract and retain skilled personnel across the defence and maritime sectors, contributing to long-term institutional capability and knowledge retention. The opportunity to work with private sector commissioned EIC members will also increase the attractiveness of a career in the Defence Forces.
- Safeguarding Sovereignty through Indigenous Innovation: Crucially, such a programme would align with Ireland's non-aligned and peace-oriented defence posture. By building domestic capacity through innovation, Ireland can enhance its strategic autonomy while continuing to contribute to regional and international maritime stability.

The development of an Irish Executive Innovation Corps, modelled on the U.S. Army's initiative but tailored to Irish values and strategic needs, could serve as a catalyst for a more agile, resilient, and future-facing maritime security strategy. It would support Ireland's sovereign interests while reinforcing its commitment to multilateral cooperation and the rule of international maritime law.

## Conclusion

The inclusion of the private sector in Ireland's National Maritime Security Strategy is not merely advisable—it is essential. As owners and operators of critical maritime infrastructure, private entities are central to the resilience and security of the State's maritime domain. Their assets, expertise, and technological capabilities position them as indispensable partners in addressing the complex and evolving threat landscape, from cyberattacks and hybrid disruptions to environmental and geopolitical risks.

A structured, formalised framework for public–private cooperation should be embedded within the Strategy. This includes mechanisms for intelligence sharing, joint risk assessments, coordinated preparedness planning, and collaborative innovation. The private sector must be recognised not only as a stakeholder but as a co-producer of maritime security—actively engaged in shaping, implementing, and sustaining national resilience. An Irish Executive Innovation Corps would accelerate maritime capability, enhance civil-military collaboration, and build strategic resilience through innovation. It would strengthen sovereignty while aligning with Ireland's non-aligned, peace-focused defence posture.

By fostering a culture of shared responsibility, investing in joint capability development, and aligning with EU and international best practices, Ireland can build a maritime security architecture that is both robust and future-ready. The Strategy must therefore serve as a catalyst for deeper integration, mutual trust, and collective action across the public and private sectors.

What role do you think international cooperation should play in the new National Maritime Security Strategy? Should this increased cooperation include a focus on our partners in the EU, with neighbouring countries and through our Individually Tailored Partnership Programme with NATO or other international maritime organisations?

## Introduction

International cooperation should be a foundational pillar of Ireland's National Maritime Security Strategy. Given the transboundary nature of maritime threats—including cyberattacks, terrorism, piracy, smuggling, infrastructure sabotage, and environmental crime—no single nation can address these challenges in isolation. As a medium-sized, non-aligned island state with a disproportionately large maritime domain, Ireland must work strategically with like-minded international partners to enhance its maritime security posture, fill capability gaps, and uphold the international rules-based maritime order.

## Strengthening Cooperation within the European Union Framework

The European Union represents a vital and multidimensional platform for Ireland's maritime security cooperation. As a coastal Member State with extensive maritime borders and responsibilities, Ireland is uniquely positioned to benefit from and contribute to the EU's collective maritime security architecture. The EU's integrated approach—linking maritime safety, border control, environmental protection, and cyber resilience—offers Ireland both strategic depth and operational support in addressing complex maritime threats.

Ireland's active participation in EU maritime initiatives not only enhances national security but also reinforces the Union's broader geopolitical stability and resilience. In an era of increasing hybrid threats and strategic competition in the maritime domain, deeper EU engagement allows Ireland to amplify its influence, access shared capabilities, and contribute to the defence of the European maritime commons.

***Strategic Recommendations***

- Deepen Engagement with the EU Maritime Security Strategy (EUMSS): Ireland should play a more proactive role in shaping and implementing the EUMSS and its associated action plans. This includes participation in joint surveillance operations, maritime situational awareness initiatives (such as MARSUR and CISE), and EU-led crisis response exercises. Such engagement would enhance Ireland's operational readiness and interoperability with European partners.
- Strengthen Operational Ties with EU Agencies: Ireland should expand its collaboration with key EU agencies, including:
- European Maritime Safety Agency (EMSA): for technical assistance, pollution response, and vessel monitoring;
- Frontex (via the Coast Guard Function Forum): to support integrated border management and maritime law enforcement;
- EU Agency for Cybersecurity (ENISA): to align national maritime cybersecurity standards with EU best practices and participate in joint cyber resilience initiatives.
- Advance Interoperability and Data Sharing: Ireland should work with EU Member States to develop interoperable technologies and protocols for real-time data exchange, cross-border incident management, and coordinated maritime surveillance. This includes contributing to the development of common standards for maritime situational awareness platforms and participating in EU-funded research and innovation programmes.
- Leverage EU Funding and Capability Development Instruments: Ireland should maximise its participation in EU funding mechanisms such as the European Defence Fund (EDF), Horizon Europe, and the Internal Security Fund (ISF) to support the development of dual-use maritime technologies and enhance national capabilities in areas such as uncrewed systems, cyber defence, and maritime domain awareness.

## Enhancing Bilateral and Regional Cooperation with Neighbouring States

Ireland's maritime security is inextricably linked to the stability and resilience of its immediate regional environment. The Irish Sea, North-East Atlantic, and surrounding maritime zones are shared spaces of economic activity, ecological interdependence, and strategic vulnerability. In this context, bilateral and regional cooperation with neighbouring states—particularly the United Kingdom, France, Spain, and Iceland—is essential for safeguarding shared maritime interests, protecting critical infrastructure, and responding to transboundary risks.

The post-Brexit landscape has introduced new complexities into Ireland–UK maritime relations, particularly in areas such as fisheries management, customs enforcement, and subsea infrastructure governance. Nevertheless, the enduring geographic proximity and mutual reliance on secure sea lines of communication necessitate a pragmatic and structured approach to bilateral maritime security cooperation.

Similarly, regional collaboration in the North-East Atlantic—through both formal and informal mechanisms—can enhance collective situational awareness, facilitate joint responses to environmental and security incidents, and support the resilience of offshore energy systems and undersea cables that underpin both national and European connectivity.

***Strategic Recommendations***

- Formalise Bilateral Coordination with the United Kingdom: Establish structured maritime security coordination mechanisms with the UK, encompassing intelligence sharing, port and harbour security protocols, and joint planning for the protection of critical subsea infrastructure. This could be operationalised through a bilateral maritime security working group or a memorandum of understanding between relevant agencies.
- Expand Regional Cooperation with Coastal Neighbours: Explore joint exercises, data-sharing agreements, and contingency planning initiatives with France, Spain, and Iceland. Particular emphasis should be placed on offshore renewable energy security, marine pollution response, and the management of transboundary environmental risks in shared maritime zones.
- Engage Actively in Regional Forums: Strengthen Ireland’s participation in regional maritime organisations such as the North Atlantic Coast Guard Forum, which facilitates operational coordination among North Atlantic states, and the OSPAR Commission, which supports the protection of the marine environment in the North-East Atlantic. These platforms offer valuable opportunities for joint training, information exchange, and the development of interoperable response protocols.
- Promote Regional Maritime Domain Awareness (MDA): Collaborate with neighbouring states to develop shared MDA capabilities, including the integration of sensor networks, vessel tracking systems, and environmental monitoring platforms. This would support early warning, coordinated response, and resilience-building across the region.

## Constructive Engagement with NATO through Ireland’s Partnership Programme

Ireland’s Individually Tailored Partnership Programme (ITPP) with NATO provides a pragmatic and flexible framework for enhancing national maritime security capabilities while respecting Ireland’s long-standing policy of military neutrality. The ITPP enables Ireland to selectively engage with NATO’s extensive expertise, training infrastructure, and strategic foresight in areas directly relevant to non-combat maritime security, such as cyber resilience, infrastructure protection, and maritime domain awareness.

Given the increasing convergence of physical and digital threats in the maritime domain—particularly in relation to subsea infrastructure, hybrid interference, and environmental disruption—constructive engagement with NATO can serve as a force multiplier for Ireland’s national capabilities. Importantly, this cooperation can be pursued in a manner that is consistent with Ireland’s values, legal frameworks, and international positioning as a non-aligned but globally engaged state.

***Strategic Recommendations***

- Leverage NATO Centres of Excellence: Engage with NATO’s Centres of Excellence, particularly the Centre for Operations in Confined and Shallow Waters (COE CSW) and the Maritime Security Centre of Excellence (MARSEC CoE). These institutions offer valuable opportunities for policy learning, scenario-based training, and the development of best practices in maritime security operations relevant to Ireland’s geostrategic context.
- Participate in Non-Combat NATO Activities: Ireland should continue to participate in non-combat NATO-led initiatives, including joint exercises, workshops, and knowledge exchange forums focused on infrastructure protection, subsea monitoring, and maritime situational awareness.

These engagements can enhance Ireland's preparedness for hybrid threats and improve interoperability with both military and civilian partners.

- Identify Areas of Mutual Benefit: Focus cooperation on areas of shared interest such as disaster response, maritime cyber defence, and civil–military interoperability. This includes exploring synergies between NATO's resilience agenda and Ireland's national security priorities, particularly in relation to critical infrastructure protection and emergency coordination.
- Maintain Transparency and Public Trust: Ensure that all engagements under the ITPP are transparent, well-communicated, and subject to democratic oversight. This will help maintain public confidence in Ireland's neutrality while demonstrating the tangible benefits of selective international cooperation in enhancing national resilience.

## Global Maritime Governance and Rule of Law

Ireland has long positioned itself as a principled advocate for multilateralism, international law, and the rules-based global order. This commitment must be sustained and deepened in the maritime domain, where the erosion of legal norms, environmental degradation, and illicit maritime activity pose growing threats to global stability and sustainable development. As a small, open, and globally connected island nation, Ireland has both a strategic interest and a moral imperative to support the integrity of international maritime governance.

The maritime domain is increasingly contested—whether through unlawful claims to maritime zones, unregulated exploitation of marine resources, or the use of grey-zone tactics to undermine freedom of navigation. In this context, Ireland's voice is particularly valuable in championing legal clarity, environmental stewardship, and equitable access to ocean resources. By aligning its maritime security strategy with its broader foreign policy values, Ireland can contribute meaningfully to the preservation of global maritime commons.

***Strategic Recommendations***

- Maintain Leadership within the International Maritime Organization (IMO): Ireland should continue to play an active role in shaping emerging regulatory frameworks at the IMO, particularly in relation to autonomous shipping, maritime cyber security, and environmental protection. This includes advocating for high standards of safety, transparency, and accountability in the governance of new maritime technologies. To this end the Defence Forces should create a Naval legal branch with expertise in maritime and fisheries law, as recommended by the Commission on the Defence Forces.
- Forge Alliances with Like-Minded Maritime Nations: Build coalitions with other small and medium-sized maritime states—such as New Zealand, Norway, and Portugal—to promote shared values in ocean governance, maritime law, and peaceful dispute resolution. These alliances can amplify Ireland's influence in multilateral forums and support the development of inclusive, science-based maritime policies.
- Support Capacity Building in Developing Coastal States: As part of its international development agenda, Ireland should provide targeted assistance to developing coastal nations in areas such as fisheries governance, maritime law enforcement, and port security. This not only strengthens global maritime governance but also reinforces Ireland's reputation as a constructive and values-driven international actor.
- Promote Ocean Diplomacy and Legal Norms: Ireland should use its diplomatic platforms—such as its seat on the UN Commission on the Limits of the Continental Shelf and its engagement with UNCLOS processes—to advocate for the peaceful resolution of maritime disputes and the protection of marine biodiversity beyond national jurisdiction.

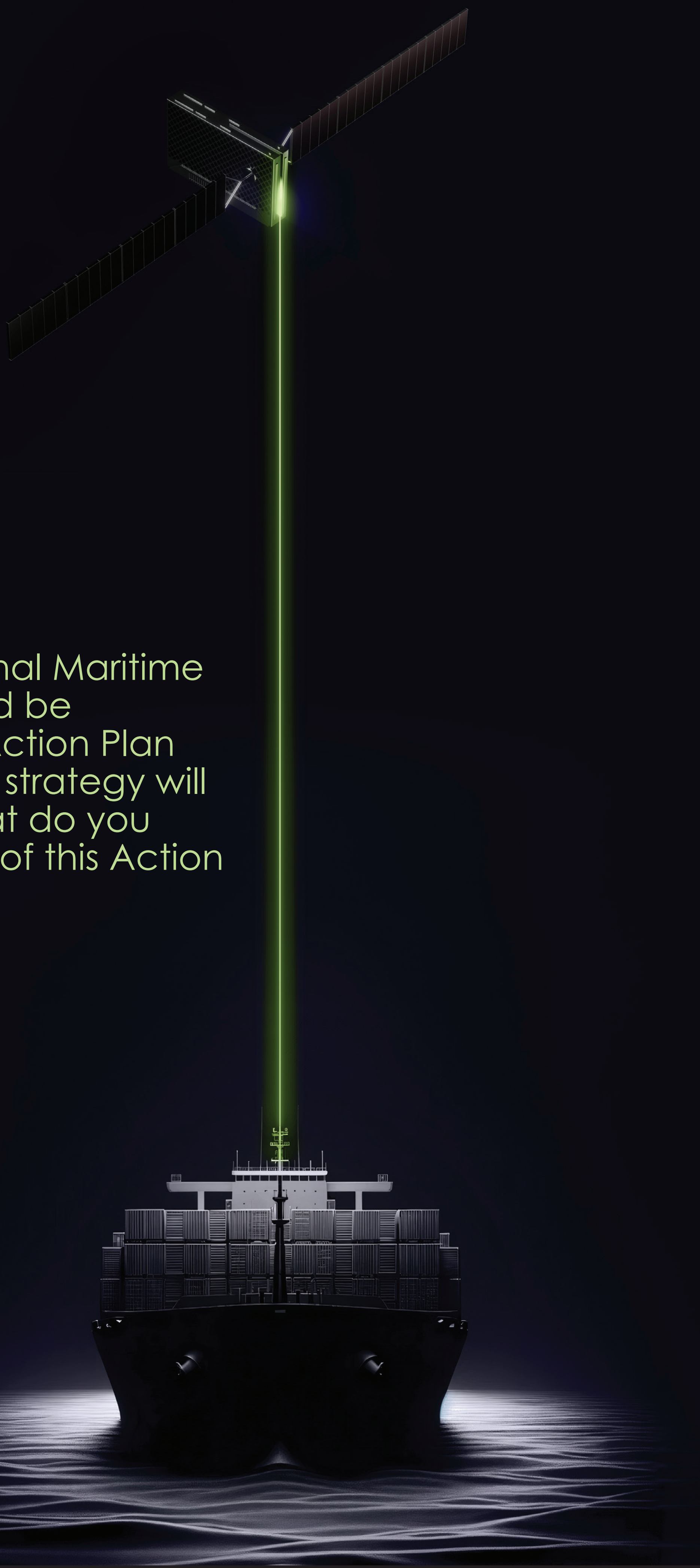
## Conclusion

International cooperation must be embedded as a strategic cornerstone of Ireland's National Maritime Security Strategy. In an era marked by transboundary threats, technological convergence, and geopolitical uncertainty, Ireland cannot safeguard its maritime domain in isolation. Instead, it must pursue a layered and principled approach to international engagement—one that reflects its values, leverages its partnerships, and enhances its sovereign capabilities.

Within the European Union, Ireland should deepen its integration into collective maritime security frameworks, aligning with EU agencies, funding instruments, and operational platforms to strengthen resilience and interoperability. Bilaterally and regionally, structured cooperation with neighbouring states—particularly the United Kingdom, France, Spain, and Iceland—will be essential for managing shared risks in the Irish Sea and North-East Atlantic.

Through its Individually Tailored Partnership Programme with NATO, Ireland can selectively access world-class expertise in maritime domain awareness, cyber defence, and hybrid threat response, while maintaining its policy of military neutrality. At the global level, Ireland must continue to champion the rules-based maritime order, contributing to international legal norms, environmental governance, and capacity building in developing coastal states.

Taken together, these avenues of cooperation will enable Ireland to build a resilient, adaptive, and forward-looking maritime security posture—one that protects national interests, supports regional stability, and upholds the integrity of the global maritime commons.



Do you think the National Maritime Security Strategy should be accompanied by an Action Plan that will detail how the strategy will be implemented? What do you think the key elements of this Action Plan should be?

## Introduction

Yes, the National Maritime Security Strategy should unequivocally be accompanied by a comprehensive and binding Action Plan. Without such a mechanism, the Strategy risks remaining aspirational rather than operational. As articulated throughout this submission, Ireland's maritime domain is subject to a rapidly evolving spectrum of complex threats—ranging from hybrid warfare and cyberattacks to climate-induced disruptions and strategic infrastructure vulnerabilities. Addressing these multidimensional risks demands more than a declarative framework; it requires a clearly structured roadmap for implementation, accountability, and resourcing. The following are our recommendations as key elements to the Action Plan:

### Establishment of a National Maritime Security Coordination Centre (NMSCC)

A central coordinating entity must be established to unify inter-agency operations, integrate intelligence functions, and ensure coherence across civilian, military, and private sector actors. This Centre should have statutory authority and direct reporting lines to the highest levels of Government.

### Development and Adoption of a National Maritime Security Doctrine

Ireland currently lacks a doctrinal foundation that articulates its maritime posture, operational thresholds, and strategic intent. An Action Plan should mandate the creation of such a doctrine, grounded in the principles of sovereignty, non-alignment, and international cooperation, but flexible enough to respond to grey-zone and hybrid threats.

### Prioritisation of Maritime Domain Awareness

The Action Plan must accelerate the development of persistent, sovereign MDA capabilities. This includes investment in surveillance platforms, AI-enabled data fusion, and the integration of autonomous systems and satellite infrastructure. The Rivada Outernet—offering a resilient, secure low Earth orbit satellite communications network—should be embedded as a sovereign enabler for real-time coordination and operational continuity.

### Cybersecurity and Infrastructure Resilience Measures

Ports, subsea cables, and offshore energy installations require enhanced cyber-defence mechanisms. The Action Plan should lay out specific responsibilities for both public and private entities in bolstering the security of Operational Technology and Information Technology systems under the NIS2 Directive and beyond.

### Legal Preparedness and Normative Reform

Existing legal frameworks are insufficient to address the ambiguities of hybrid maritime threats. The Action Plan must propose a legal review and reform agenda that enhances enforcement capabilities, clarifies jurisdictional boundaries in the EEZ, and strengthens attribution protocols.

### Private Sector Integration

As outlined in the submission, the private sector is both a critical stakeholder and a co-producer of security. The Action Plan should define roles, establish structured engagement forums, and incentivise collaborative risk-sharing, innovation, and intelligence-sharing mechanisms.

### Geospatial and Environmental Intelligence Infrastructure

Climate change is a driver of maritime instability. The Action Plan should mandate the integration of environmental monitoring into national security planning, including predictive modelling, maritime spatial planning, and dual-use data infrastructure.

### International Cooperation and Strategic Diplomacy

The Action Plan should formalise Ireland’s engagement with EU initiatives, NATO’s Partnership Programme, and regional bilateral mechanisms. It must articulate pathways for interoperability, burden-sharing, and participation in joint maritime exercises and situational awareness platforms.

### Institutional Capacity Building and Public Security Culture

A recurring theme in our submission is the lack of a coherent maritime security culture within the public and institutional domains. The Action Plan must prioritise educational initiatives, awareness campaigns, and civil–military training programmes that foster long-term cultural and institutional transformation. The Action Plan should include robust milestones for the introduction of an EIC as part of this capacity building.

In summary, an Action Plan is not merely a supplementary document—it is the operational spine of the Strategy. It must be detailed, funded, and accountable, ensuring that Ireland’s NMSS moves from aspiration to enactment in a manner that reflects the complexity and urgency of its maritime security environment.

# Additional comments on Irish Maritime Security outside of Consultation Questions

## Strategic Vulnerability of Undersea Infrastructure in a Grey Zone Conflict Context

Ireland's policy of military non-alignment, coupled with its limited deterrence and surveillance capabilities, may render it an attractive operating environment for grey zone activity—particularly in relation to critical subsea infrastructure. Transatlantic data cables, energy interconnectors, and offshore platforms represent high-value targets for state and non-state actors seeking to exploit legal ambiguity and attribution challenges.

The increasing willingness of actors such as the Russian Federation to engage in sub-threshold operations—often deniable and legally ambiguous—poses a particular risk to Ireland, which hosts a disproportionate share of EU–US digital infrastructure. The absence of a dedicated subsea surveillance fleet or persistent unmanned monitoring capability further compounds this vulnerability, creating exploitable gaps in both deterrence and response.

***Recommendation:***

The Strategy should articulate a clear legal, diplomatic, and operational framework for responding to grey zone threats against undersea infrastructure. This should include the activation of EU solidarity mechanisms, the development of contingency arrangements with trusted partners, and the establishment of protocols for attribution, deterrence, and rapid response.

## Ireland's Role as an EU Periphery and Atlantic Gateway

Ireland's geographic position at the western edge of the European Union confers upon it a unique strategic role as a gateway to the North Atlantic. It is the closest EU Member State to North America and hosts a dense concentration of transatlantic sea lanes, air corridors, and submarine cable landings. This role is becoming increasingly salient in light of NATO's renewed focus on the North Atlantic, the militarisation of the Arctic, and the potential emergence of new maritime routes due to climate change.

Ireland is simultaneously a transit corridor and a potential chokepoint for European logistics and communications, particularly as continental vulnerabilities prompt a westward reorientation of strategic infrastructure. This evolving geostrategic context demands a more proactive Irish posture in long-term maritime foresight and resilience planning.

***Recommendation:***

Ireland should invest in strategic foresight and scenario planning capabilities to anticipate and prepare for future developments in Atlantic security. This includes assessing the implications of shifting geopolitical dynamics, climate-induced route changes, and the evolving role of Ireland in European and transatlantic maritime resilience.

## Legal and Normative Gaps in Hybrid Maritime Threat Response

Ireland's domestic security architecture is structured around a clear separation between civil and military functions, with legal constraints governing the deployment of Defence Forces in domestic contexts. However, hybrid maritime threats—such as unattributable sabotage, cyber intrusions, and coercive actions by ostensibly civilian vessels—do not conform to traditional models of threat classification or response.

For instance, a foreign-flagged research vessel operating lawfully within Ireland's Exclusive Economic Zone (EEZ) may engage in seabed mapping or electronic surveillance with hostile intent, yet fall outside the scope of immediate interdiction. Similarly, cyberattacks on port logistics or navigation systems may be difficult to attribute, legally ambiguous, or fall below the threshold of criminality.

***Recommendation:***

The Strategy should recommend a comprehensive review of Ireland's legal frameworks and inter-agency protocols for responding to hybrid maritime threats. This should include the development of intelligence-led preventive mechanisms, clarification of thresholds for Defence Forces support to civil authorities, and the establishment of flexible legal instruments to address ambiguous or low-attribution activities.

### Ireland's Soft Power and Maritime Diplomacy Potential

Ireland's policy of military non-alignment is complemented by a longstanding international reputation as a principled advocate for multilateralism, peacekeeping, and the rule of law. These soft power assets—rooted in Ireland's diplomatic credibility and normative leadership—offer significant potential to shape emerging maritime governance frameworks. In an increasingly contested maritime environment, Ireland can play a constructive role in promoting responsible state behaviour, ethical innovation, and inclusive ocean governance.

Key areas where Ireland's diplomatic influence could be particularly impactful include:

- The development of international norms for the use of autonomous vessels and artificial intelligence in maritime security;
- Climate adaptation and coastal resilience, particularly in support of small island developing states (SIDS) disproportionately affected by rising sea levels and marine degradation;
- The protection of the global maritime commons, including biodiversity beyond national jurisdiction and the sustainable use of ocean resources.

***Recommendation:***

Ireland should develop a coherent maritime diplomacy agenda that complements its domestic security strategy. This agenda should prioritise engagement through United Nations fora, EU diplomatic mechanisms, and targeted capacity-building partnerships, enabling Ireland to shape global maritime governance in line with its values and strategic interests.

### Securing Ireland's Blue Economy and Marine Innovation Ecosystem

Ireland's expanding blue economy—encompassing offshore renewable energy, aquaculture, marine biotechnology, and ocean data services—represents both a strategic opportunity and a growing security concern. As marine infrastructure becomes more technologically advanced and spatially distributed, it also becomes increasingly exposed to a range of emerging threats, including economic espionage, intellectual property theft, and environmental sabotage.

Floating infrastructure, autonomous platforms, and marine innovation zones (such as testbeds and research facilities) are particularly vulnerable to dual-use exploitation and covert interference by hostile actors seeking commercial or strategic advantage. These risks are compounded by the often limited physical and cyber protection measures in place across experimental or pre-commercial maritime installations.

***Recommendation:***

The Strategy should explicitly incorporate economic security considerations into Ireland's maritime security framework. This includes the protection of research and development assets, the resilience of maritime trade and logistics routes, and the safeguarding of marine science and innovation infrastructure from both physical and cyber threats.

### Establish a National Maritime Security Coordination Centre

Ireland's maritime security responsibilities are currently dispersed across multiple departments and agencies, leading to potential gaps in coordination, information sharing, and operational response. A dedicated, cross-governmental coordination centre—modelled on best practices from other EU states—could serve as a central hub for maritime intelligence fusion, crisis management, and strategic planning.

***Recommendation:***

Reorganise and resource the Maritime Security Unit into the National Maritime Security Coordination Centre to integrate civil, military, regulatory, and private sector inputs, ensuring a unified operational picture and rapid decision-making during maritime incidents.

### Develop a National Maritime Security Doctrine

Ireland lacks a clearly articulated doctrine that defines its maritime security objectives, principles, and operational thresholds. This absence creates ambiguity in both domestic planning and international engagement.

***Recommendation:***

Mandate the publication of a National Maritime Security Doctrine. Such a doctrine should outline Ireland's strategic posture, threat environment, and guiding principles for engagement, deterrence, and resilience—anchored in its policy of non-alignment and commitment to international law.

### Enhance Legal Preparedness for Maritime Emergencies

The current legal framework does not adequately address the complexities of hybrid threats, ambiguous actors, or rapid escalation scenarios in the maritime domain. Ireland's policy of military non-alignment and lack of a formal maritime security strategy can delay coordinated responses to maritime incidents. This creates uncertainty for partners like the UK and EU, who may be forced to intervene unilaterally in Irish waters during crises, raising legal and diplomatic complications.

***Recommendation:***

Conduct a legislative review to identify and amend gaps in Ireland's ability to respond to maritime emergencies, including provisions for pre-emptive action, inter-agency tasking, and Defence Forces support in non-traditional threat contexts. Review all protocols for engaging our allies and European agencies, ensuring they are agile and responsive enough to react to rapidly changing events, to retain Ireland's sovereignty and avoid unilateral responses.

### Integrate Maritime Security into National Risk Assessment Frameworks

Maritime threats are often underrepresented in national risk registers and resilience planning, despite their potential to disrupt critical infrastructure and economic continuity.

***Recommendation:***

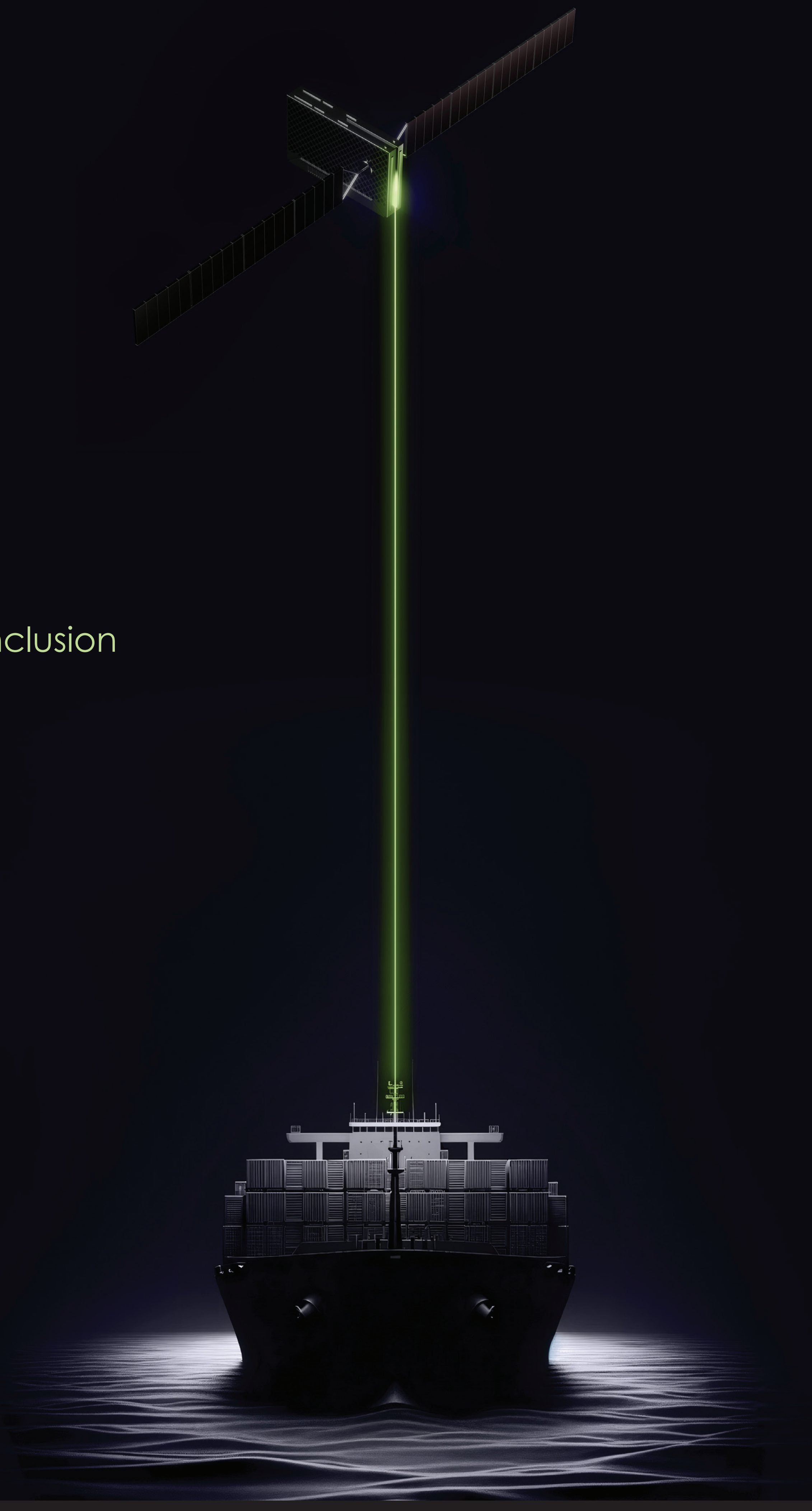
Ensure that maritime security risks—particularly those related to subsea infrastructure, cyber threats, and climate-induced disruptions—are fully integrated into Ireland's National Risk Assessment and National Risk Register processes.

### Leverage Ireland's Role in Global Maritime Norm-Setting

Ireland's diplomatic credibility and legal expertise position it to lead in shaping emerging maritime norms, particularly in areas such as autonomous systems, seabed governance, and climate security.

***Recommendation:***

Champion international initiatives on responsible maritime innovation, including the regulation of autonomous vessels, protection of marine biodiversity beyond national jurisdiction, and ethical frameworks for maritime AI.



# Submission Conclusion

## FINAL WORD & SUMMARY

Ireland's maritime security environment is undergoing profound transformation. Geopolitical volatility, technological disruption, hybrid threats, and climate-induced pressures are converging to redefine the risks and responsibilities associated with our maritime domain. As a non-aligned island state with one of the largest EEZs in Europe, Ireland's maritime space is no longer peripheral—it is central to the strategic integrity of the State. It underpins our economic resilience, energy security, digital connectivity, and environmental stewardship. Yet, it remains insufficiently protected, under-monitored, and strategically vulnerable.

This submission has highlighted a series of persistent and emerging challenges that demand urgent and coordinated action. Chief among these is the critical weakness in our naval capacity. The Irish Naval Service continues to suffer from acute staffing shortages, fleet obsolescence, and operational overstretch. These deficiencies severely curtail the State's ability to conduct effective maritime patrols, monitor subsea infrastructure, or respond in real time to threats within its jurisdiction. Without a credible and modern maritime force, Ireland's ability to assert sovereignty, enforce its laws, and protect national interests at sea will continue to erode.

At the same time, the strategic value and vulnerability of undersea infrastructure—particularly transatlantic communications cables and energy interconnectors—have become glaring. Ireland has become a critical node in global digital and energy networks, but it remains overly dependent on physical assets that are easily mapped, and sabotaged by adversarial actors. The growing sophistication of hybrid tactics and grey-zone operations, as seen in the activities of Russian vessels near Irish waters, underscores the inadequacy of current capabilities to detect, attribute, or deter such actions.

In this context, sovereign, resilient, and secure communications capabilities must be treated as essential national infrastructure. The Rivada Outernet offers a transformative opportunity in this regard. By establishing a Layer 2 low-Earth orbit satellite transport network, the Outernet delivers ultra-secure, non-terrestrial communications with low latency, high redundancy, and real-time rerouting capability. It provides a space-based contingency framework that is immune to many of the vulnerabilities inherent in subsea systems—be they technical, environmental, or geopolitical. The Outernet aligns with the PACE model and can serve as the communications backbone for a resilient maritime security architecture. This is not a theoretical advantage—it is a tangible enabler of operational continuity and sovereignty in an increasingly contested maritime domain.

Beyond technological investment, this submission also emphasises the importance of structural and cultural reform. Ireland lacks a coherent maritime security doctrine, and there remains a broader absence of national security literacy across sectors. These gaps inhibit effective policy development, strategic foresight, and coordinated action. The introduction of a National Maritime Security Coordination Centre, coupled with the development of a National Maritime Security Doctrine, would provide the institutional scaffolding required to unify action, streamline intelligence-sharing, and embed a whole-of-government approach to maritime defence.

We further recommend the establishment of an Irish Executive Innovation Corps, modelled on international best practice, to embed Defence Forces and civil service personnel within centres of innovation. This would enable cross-sectoral learning, accelerate capability development, and deepen civil–military collaboration—particularly in domains such as cyber resilience, autonomous systems, and maritime surveillance.

The private sector, too, must be recognised as a co-producer of maritime security. Much of the State's critical maritime infrastructure—including ports, offshore energy installations, and subsea communications networks—is owned or operated by private actors. Their integration into the national security framework must be formalised through structured risk-sharing, joint contingency planning, and collaborative technology development. Resilience can no longer be viewed as the exclusive preserve of the State; it must be distributed, embedded, and sustained across all sectors of national life.

Ireland's policy of military non-alignment remains a defining feature of its foreign and defence posture. However, non-alignment must not become strategic inertia. In the face of intensifying pressure from state and non-state actors alike, Ireland must articulate a clear, proactive maritime security strategy that reflects the realities of our geopolitical environment. This includes deeper engagement with EU and NATO partners—particularly through surveillance, information-sharing, and joint exercises—while preserving our sovereign decision-making and principled neutrality.

The future security of Ireland's maritime domain will not be determined by passive adherence to past assumptions, but by the choices we make now. These choices must be strategic, informed, and grounded in an honest assessment of the threats we face. We must be willing to invest not only in equipment and technology, but in institutions, talent, and partnerships. We must build the legal, diplomatic, and operational frameworks that will allow us to defend our maritime interests with credibility and confidence.

In conclusion, this submission calls for a decisive shift in Ireland's maritime security paradigm. It is a call to action—to think long-term, act cohesively, and invest meaningfully. It is a call to recognise that our maritime domain is not merely a space of opportunity, but also one of responsibility and risk. By integrating the Rivada Outernet, strengthening naval capacity, embedding innovation, and embracing genuine partnership across public and private sectors, Ireland can chart a new course—one that secures our sovereignty, protects our people, and upholds our role as a responsible actor in an increasingly turbulent world.

RIVADA.COM

RIVADASPACE.COM

RIVADA