MARITIME SECURITY UNDER NEUTRALITY: A STRATEGIC FRAMEWORK FOR IRELAND’S SOVEREIGN RESILIENCE

About the Author

Dr Niamh O Riordan. This submission reflects independent research and analysis prepared for the purpose of contributing to Ireland’s maritime security policy discourse. Contact: oriordan.nm@gmail.com

Copyright and Usage

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Ireland’s maritime security architecture is not fit for purpose. With one of Europe’s largest Exclusive Economic Zones, critical subsea infrastructure, and expanding offshore energy assets, Ireland faces credible grey-zone threats—from covert surveillance to cable interference. Yet public debate has largely failed to engage with the mechanics of these threats, and no strategic consensus exists on how to build national capacity.

This submission evaluates three strategic models:

- Full-Spectrum Deterrence, a military-led posture centred on autonomous enforcement through naval assets, surveillance aircraft, and deterrence signalling;
- Civil Resilience, a civilian-led framework built around legal tools, regulatory enforcement, and non-military domain awareness;
- And a Hybrid Strategy, which combines phased civilian surveillance and legal authority with narrowly scoped defensive tools under civilian control.

Each model is tested against three criteria: implementability, operational effect, and political survivability. Full-Spectrum Deterrence delivers theoretical capacity, but exceeds Ireland’s fiscal, institutional, and political bounds. Civil Resilience aligns with legal norms and public sentiment, but lacks coercive or denial capability. Only the Hybrid Strategy performs across all three axes—delivering credible security without breaching neutrality.

It can be built through phased, civilian-led reforms, supported by a structured escalation framework and a non-military denial toolkit. It enables Ireland to detect threats, assert legal rights, and impose friction—without triggering alignment or militarisation.

This is not a compromise model. It is a strategic architecture deliberately calibrated to Ireland’s unique constraints and exposures. It redefines neutrality not as passivity, but as resilient independence: sovereignty exercised through surveillance, law, and readiness—not force projection.

INTRODUCTION

Ireland faces a complex maritime security challenge shaped by structural vulnerabilities and constrained by political tradition. Its EEZ is among the largest in Europe, encompassing critical subsea cables and offshore wind infrastructure vital to European energy and digital connectivity (Government of Ireland, 2022; European Commission, 2023). Yet its current maritime security posture remains fragmented and institutionally underpowered (Commission on Defence Forces, 2022; Doyle & Ní Aoláin, 2023).

This submission argues for an urgent strategic reset—one tailored to Ireland's distinctive political, institutional, and cultural conditions. The threat landscape is defined by grey-zone activity: GPS spoofing, covert seabed mapping, and unflagged vessel incursions. These must be addressed within the constraints of neutrality and limited defence capacity (Sloan, 2022; Laffan, 2023).

Neutrality remains central to Ireland's identity, codified through non-alignment and reinforced by public resistance to militarisation (Devine & Tonra, 2022). But in today's environment, neutrality cannot mean passivity. Effective neutrality requires the capacity to enforce sovereignty, uphold legal entitlements, and respond credibly to sub-threshold coercion (O'Driscoll, 2021; Sloan, 2022).

This submission intervenes in a policy discourse that has struggled to reconcile Ireland's neutrality commitments with its rising maritime exposure. It offers a strategic framework that reframes neutrality not as passivity, but as a mode of active sovereignty under legal constraint. It challenges the assumption that military abstention must imply strategic helplessness, and demonstrates that proportionate, civilian-led enforcement is both lawful and politically viable.

This submission compares three strategic models for maritime security:

- Model 1: Full-Spectrum Deterrence, which advocates significant military expansion to create a credible deterrent (Sloan, 2022; Commission on Defence Forces, 2022).
- Model 2: Civil Resilience, which focuses on civilian surveillance, legal enforcement, and diplomatic tools (Department of Foreign Affairs, 2021; MARA, 2023).
- Model 3: Hybrid Strategy, which combines civilian-led domain awareness with selective defensive capacity under civilian control (Laffan, 2023; Doyle & Ní Aoláin, 2023).

Each model is evaluated in terms of strategic logic, implementation feasibility, and political viability. The hybrid model emerges not as a compromise, but as the only configuration that balances sovereignty, neutrality, and operational credibility. The following sections present this comparative analysis and demonstrate why the hybrid strategy represents Ireland's most realistic and sustainable maritime security path.

STRATEGIC POSTURE AND NEUTRALITY: IRELAND'S MARITIME DILEMMA

Ireland faces a structurally asymmetric maritime security challenge: expansive jurisdiction, rising exposure, and constrained capacity. Its Exclusive Economic Zone (EEZ), at over 880,000 km², is among the largest in Europe and contains assets of strategic importance, including:

- The densest cluster of transatlantic subsea cables in Europe (European Commission, 2023; NATO StratCom, 2023)
- An expanding offshore renewables sector central to the EU's green transition (Marine Institute, 2022)
- Documented grey-zone incursions by non-EU actors (European Commission JRC, 2023; Doyle & Ní Aoláin, 2023)
- Environmentally sensitive fisheries zones vulnerable to IUU exploitation (MARA, 2023)

Despite this exposure, Ireland lacks the basic infrastructure of maritime security. Domain awareness is fragmented across under-resourced civilian bodies with overlapping mandates (MARA, 2023; Bueger, 2021). The Naval Service and Air Corps suffer from personnel shortfalls, ageing assets, and limited reach (Commission on Defence Forces, 2022; Irish Naval Service, 2022). Ireland has no dedicated maritime patrol aircraft, no seabed monitoring, no persistent radar coverage, and no unified operational command (Chapsos & Kitchen, 2021).

This fragility is not simply underinvestment—it reflects a political culture shaped by a particular reading of neutrality. Three overlapping interpretations dominate:

- A legal posture: non-alignment and refusal to host foreign bases (O'Driscoll, 2021)
- An institutional tradition: civilian-led security and diplomatic engagement (Doyle & Ní Aoláin, 2023)
- A normative identity: associating low capability with moral distinction (Devine & Tonra, 2022; Whitman, 2022)

These strands are often conflated, functioning less as doctrine than as strategic ambiguity. As Whitman (2022) notes, Irish neutrality has rarely been concretised in law or force design. McCabe (2023) shows it is sustained rhetorically—not institutionally—relying on public expectation rather than operational doctrine. This produces a paradox: the state affirms its sovereignty by avoiding the capacity needed to secure it.

The result is strategic confusion. Capability is treated not as autonomy, but as liability. Restraint is misread as neutrality; passivity as principle. But in an era of grey-zone coercion, informational asymmetry, and sub-threshold operations, this logic no longer holds. A lack of capacity does not reinforce neutrality—it undermines it. Inaction becomes permissive, not protective.

Neutrality in law is not disarmament. As Henriksen (2021) and Sloan (2022) argue, neutral states may and should maintain credible, non-aligned defensive tools. Sovereign capability is not a breach—it is a precondition of viable neutrality. This view is slowly entering Irish debate, as seen in the June 2025 Dáil session, where non-alignment was affirmed, but few articulated how to defend sovereignty within that frame.

Ireland’s inherited model of neutrality is ill-suited to today’s threat environment. It evolved in a world of clear thresholds and visible wars. It now faces adversaries who act incrementally, deniably, and below the radar of traditional defence postures. If neutrality is to endure, it must be redefined—not as strategic absence, but as credible sovereign restraint.

This submission adopts that position. Neutrality is not the absence of strategy—it shapes it. It must be interpreted operationally: enabling the state to detect, attribute, and lawfully respond without triggering alignment. Capability must be structured for ambiguity: to monitor, deter, and escalate within constitutional bounds.

This submission evaluates three strategic models—Full-Spectrum Deterrence, Civil Resilience, and a Hybrid Strategy—against three core tests: implementability, operational effect, and political survivability. These tests reflect the real constraints of Irish institutional capacity, legal tradition, and geopolitical posture. In assessing operational effectiveness, the analysis draws—where relevant—on functional stress-testing through documented grey-zone threat scenarios. These threats do not take the form of conventional military aggression. They occur below the threshold of armed conflict, but above the threshold of tolerable neglect. A viable strategy must be capable not just of principle, but of practice: attribution, friction, and lawful escalation within the limits of neutrality.

What follows is a structured evaluation of three strategic models—Full-Spectrum Deterrence, Civil Resilience, and a Hybrid Approach—each assessed for its real-world implementability, operational effect, and political survivability. Because in Ireland’s case, the limits are real—but they do not excuse drift. Constraint is not the end of strategy. It is the beginning of it. In short, neutrality does not remove the obligation to act. It defines how that action must be structured.

THREE STRATEGIC CHOICES FOR A CONSTRAINED STATE

Ireland's maritime strategy must begin not with ideal outcomes but with real constraints: limited defence capacity, political commitment to neutrality, and growing exposure in a contested maritime domain (Commission on Defence Forces, 2022; Doyle & Ní Aoláin, 2023). These are not obstacles to circumvent but structural realities that define the boundaries of credible action (Laffan, 2023; Irish Naval Service, 2022).

Within these constraints, three strategic models present themselves—each offering a distinct answer to the same core question: how can Ireland assert sovereignty and defend maritime infrastructure against hybrid threats without violating legal commitments or breaching political norms?

Model 1: Full-Spectrum Deterrence. Proposes a substantial expansion of conventional military capacity and independent force projection. It draws on the logic of sovereign deterrent postures found in Nordic and Baltic states, and echoes recommendations in recent Irish defence reviews (Commission on Defence Forces, 2022; Irish Defence Forces Strategic Framework, 2021).

Model 2: Civil Resilience. Rejects militarisation and builds instead on Ireland's civilian governance model—empowering regulatory agencies, enhancing surveillance, and strengthening legal-diplomatic enforcement. It reflects current institutional practice and Ireland's legalist security tradition (MARA, 2023; Department of Foreign Affairs, 2021).

Model 3: Hybrid Strategy. Combines civilian-led authority with narrowly scoped, non-provocative defence capabilities under strict political control. It aligns with scholarship arguing that neutrality include credible enforcement without alliance entanglement (Laffan, 2023; Doyle & Ní Aoláin, 2023).

These are not theoretical constructs. They respond directly to documented gaps in Ireland's maritime security architecture: overstretched naval assets, institutional fragmentation, and slow or inadequate responses to grey-zone incidents (European Defence Agency, 2023; Marine Institute, 2022). Each model is developed as a complete pathway, including its operational logic, institutional design, and normative implications. The aim of this analysis is not to identify a flawless model, but to determine which one can deliver maritime security that is credible, implementable, and politically survivable—under the real constraints of Irish law, identity, and public expectation (Devine & Tonra, 2022; Doyle & Ní Aoláin, 2023).

What follows is a structured evaluation of each model. The test is not technical elegance but practical sufficiency: which model can operate effectively within the limits Ireland must observe—and still meet the strategic demands it cannot ignore. The conclusion advanced here is that only the hybrid strategy passes all three tests.

MODEL 1: FULL-SPECTRUM DETERRENCE

Full-spectrum deterrence represents the most assertive model of maritime sovereignty Ireland could pursue. It is premised on the principle that effective sovereignty requires not just legal entitlement but the credible capacity to detect, interdict, and deny hostile acts across the entire spectrum of threat—ranging from grey-zone interference to high-end coercion (Sloan, 2022; Doyle & Ní Aoláin, 2023). In this framing, neutrality is not abandoned but redefined: not as abstention, but as autonomous enforcement.

Ireland's exposure is acute: its sovereign waters are among the largest in the EU, its critical subsea infrastructure disproportionately strategic, and its defensive capabilities structurally underdeveloped (Commission on Defence Forces, 2022; Marine Institute, 2022). The full-spectrum model responds not through symbolic adaptation but through a deliberate investment in deterrent posture and domain control.

STRATEGIC ARCHITECTURE

The model would require a multi-domain operational architecture centred on five core components:

1. Persistent Maritime Surveillance via high-end patrol aircraft and UAVs, providing continuous domain awareness across EEZ and critical infrastructure zones (European Defence Agency, 2023).
2. Subsea Situational Control using coastal radar, sonar, and seabed monitoring systems to guard subsea cables, ports, and approaches (Irish Defence Forces Doctrine, 2021).
3. Fleet Modernisation, including the acquisition of multi-role naval platforms capable of sustained presence, interdiction, and escalation management (Irish Naval Service, 2022).
4. Unified Maritime Command with operational authority over joint ISR and maritime assets, enabling coherent decision-making and rapid response (Commission on Defence Forces, 2022).
5. Integrated ISR Ecosystem combining civil and military sensors into a real-time threat detection and attribution capability (European Commission JRC, 2023).

The underlying logic is deterrence-by-denial: adversaries are deterred not by declared norms but by visible capability to detect and counter violations. This approach mirrors the layered sovereignty posture of non-aligned Nordic states—such as Finland pre-NATO—who invested in defensive autonomy to avoid strategic dependency (Laffan, 2023).

FEASIBILITY AND POLITICAL LIMITS

Legally, the model remains within the bounds of neutrality. International law permits non-aligned states to defend sovereignty, enforce maritime jurisdiction, and secure infrastructure—provided they avoid offensive alliance commitments (O'Driscoll, 2021; Devine & Tonra, 2022).

However, the political feasibility of this model is critically weak. The June 2025 Dáil debate on maritime security showed no appetite for a hardening of Ireland's military posture. Across parties, TDs foregrounded civil primacy, diplomatic authority, and neutrality preservation. There was no call for conventional military build-up or strategic signalling. On the contrary, multiple contributors expressed concern that even modest increases in defence capacity could erode Ireland's non-aligned credibility (Dáil Éireann Debates, 2025). The core assumptions of this model—coercive capability, doctrinal escalation, and conventional deterrence—are at odds with current parliamentary sentiment.

ANALYTICAL ROLE

As a practical proposal, full-spectrum deterrence is likely to exceed Ireland's fiscal, institutional, and political bandwidth in the short to medium term. But analytically, its value lies as a benchmark: it defines the upper bound of sovereign enforcement capacity. Any alternative model—however more feasible—must still account for what it lacks by comparison. In this sense, full-spectrum deterrence marks the limit of what a truly autonomous Irish maritime strategy could entail, even if that limit currently sits beyond reach (Doyle & Ní Aoláin, 2023).

ROADMAP FOR FULL-SPECTRUM DETERRENCE

The following roadmap outlines the sequencing required to construct a credible full-spectrum maritime deterrent posture. However, this is not a neutral planning exercise. The June 2025 Dáil debate made clear that any movement toward military expansion—even in the name of sovereignty—must navigate acute political sensitivity around neutrality, civil primacy, and defence identity (Dáil Éireann Debates, 2025). As such, this roadmap does not assume inevitability, but rather sets out the steps that would be required were political will, public consent, and fiscal conditions aligned. It proceeds in three phases:

Immediate Term (0–2 Years): Foundation Laying

- Commission a Defence Capability Review focused on maritime threats and institutional readiness to establish a formal baseline.
- Initiate long-lead procurement planning for MPAs, UAVs, and seabed sensors to begin closing the ISR gap.
- Stand up a Maritime Command to centralise authority and overcome fragmented operational control.
- Expand recruitment and technical training in the Naval Service and Air Corps to support system integration and sustained operations.
- Revise the White Paper to formalise expanded roles and establish legal authority for escalated postures.

Medium Term (2–5 Years): Force Assembly

- Deploy stopgap ISR assets, such as leased aircraft or off-the-shelf drone solutions, while awaiting custom platforms.
- Roll out coastal radar and sonar systems, creating a persistent surveillance architecture.
- Begin phased fleet replacement, prioritising vessels optimised for EEZ enforcement and rapid interdiction.
- Conduct neutral-aligned joint exercises with EU and NATO partners to test readiness and demonstrate sovereign capability.
- Develop a military–civilian crisis response protocol, preserving Ireland's tradition of civilian primacy in security.

Long Term (5+ Years): Strategic Maturity

- Operationalise a deterrent posture with real-time situational awareness and independent interdiction capacity.
- Consolidate ISR and command functions in a national maritime operations centre for integrated decision-making.
- Conditioned on political mandate, achieve full-spectrum autonomy in defending Ireland's maritime interests—without reliance on alliance guarantees, and within an updated constitutional interpretation of neutrality.

MODEL 2: CIVIL RESILIENCE

The civil resilience model secures Ireland's maritime domain through law, surveillance, and institutional governance rather than force. It assumes sovereignty can be protected by making hostile acts visible, attributable, and accountable—leveraging Ireland's legalist tradition and preference for civilian-led security (MARA, 2023; Doyle & Ní Aoláin, 2023).

This model assumes that Ireland's most probable maritime threats—subsea cable interference, IUU fishing, grey-zone surveillance—are sub-threshold and non-kinetic. In such contexts, timely detection and legal response are more effective than military deterrence (European Commission JRC, 2023; NATO StratCom, 2023).

Three interlocking components define the architecture:

1. Civilian Institutional Strengthening: Expand mandates and resourcing for MARA, SFPA, the Coast Guard, and environmental agencies. Establish a central civilian maritime coordination centre to fuse surveillance data and direct non-military responses (Commission on Defence Forces, 2022; Doyle & Ní Aoláin, 2023).
2. Layered Surveillance and Attribution: Deploy persistent, technology-driven surveillance using AIS data, satellites, acoustic sensors, UAVs, and seabed monitors. These dual-use tools support both environmental and security goals without militarising oversight (European Defence Agency, 2023; Marine Institute, 2022).
3. Legal and Diplomatic Enforcement: Develop civil-service capacity to assert Ireland's rights via UNCLOS, ITLOS, and bilateral protest. Expand informal EU and NATO-adjacent cooperation to share maritime intelligence without breaching neutrality (Sloan, 2022; European Commission, 2023).

This is not diluted defence. It is deterrence-by-governance: transparency, legal certainty, and reputational cost. It aligns with Irish strategic culture and minimises escalation risk.

Advantages:

- Aligns with constitutional neutrality and public norms
- Builds on existing civilian institutions and frameworks
- Lower fiscal burden than military alternatives
- Strengthens environmental and regulatory outcomes

The 12 June 2025 Dáil debate reflected strong political appetite for this model. TDs prioritised civil agency coordination and legal tools—but failed to address coercive threats like cable sabotage or hostile mapping. The model's legitimacy is high, but its sufficiency remains untested when legal protest confronts strategic indifference (Dáil Éireann Debates, 2025).

Civil resilience assumes adversaries respond to law and reputational cost. It may detect grey-zone interference—but cannot interdict. In scenarios requiring forceful action, it offers enforcement without imposition. It is suitable for day-to-day governance, not crisis response.

ROADMAP FOR CIVIL RESILIENCE

Immediate Phase (0–2 Years)

- Expand MARA’s mandate for integrated maritime oversight
- Create a civilian inter-agency task force (MARA, Coast Guard, SFPA, others)
- Procure commercial AIS/satellite services and autonomous sensors
- Enact EEZ and infrastructure protection legislation
- Launch a diplomatic initiative to reinforce infrastructure norms

Scaling Phase (2+ Years)

- Establish a central Maritime Coordination Centre
- Institutionalise legal escalation protocols for UNCLOS/ITLOS actions
- Formalise bilateral and EU information-sharing frameworks
- Build public–private infrastructure protection standards
- Maintain iterative tech upgrades to adapt to evolving threats

This model delivers legitimate, cost-effective security—but must be paired with escalation capacity to meet full-spectrum threat scenarios. It is necessary, but not sufficient.

MODEL 3: HYBRID MARITIME SECURITY STRATEGY (PROPOSED MODEL)

The hybrid strategy is not a compromise between extremes but a purpose-built design. It integrates Ireland's civilian strengths with narrowly scoped defensive capabilities—acknowledging that neither militarisation nor pure legalism alone is sufficient in a contested maritime domain (Doyle & Ní Aoláin, 2023; European Commission JRC, 2023). Strategic credibility requires capacity; political viability requires restraint. This model delivers both.

It rests on five interlocking components:

1. Civilian-Led Maritime Domain Awareness (MDA): Surveillance of the EEZ is led by MARA and civilian agencies using dual-use technologies—commercial satellites, UAVs, USVs, seabed sensors, and port monitoring. These systems already support environmental and fisheries oversight and can be adapted to security purposes (Marine Institute, 2022; MARA, 2023). Sovereignty is reinforced through capability; neutrality is preserved through institutional design.
2. Maritime Resilience Reserve (MRR): A civilian auxiliary of trained volunteers and maritime professionals would support cable protection, search and rescue, pollution response, and infrastructure contingency. This mirrors Nordic civil defence models, providing scalable surge support without military entanglement (Laffan, 2023).
3. Selective Defensive Military Capability: A limited suite of military tools—such as maritime patrol aircraft, coastal radar, and a rapid-response naval unit—would be acquired or leased under civilian command. These assets are calibrated for attribution, interdiction, and infrastructure protection, not force projection (Commission on Defence Forces, 2022; Irish Defence Forces Doctrine, 2021). They enable consequence delivery while remaining within international law and neutrality doctrine (O'Driscoll, 2021).
4. Legal and Institutional Integration: A unified civil-military governance structure, grounded in updated EEZ legislation and anchored by a Maritime Coordination Centre, would ensure coherent response across agencies during grey-zone activity (Doyle & Ní Aoláin, 2023).
5. Non-Aligned Strategic Partnerships: Ireland would deepen cooperation with EU and regional actors on maritime safety, surveillance, and infrastructure resilience—enhancing deterrence without compromising neutrality (Devine & Tonra, 2022; European Commission JRC, 2023).

This model is modular, scalable, and reversible. It can evolve with public understanding, institutional maturity, and the strategic environment.

ESCALATION AND DENIAL UNDER NEUTRALITY

To counter grey-zone threats credibly without breaching neutrality, the hybrid model introduces a two-part framework: a graduated escalation ladder and a lawful denial toolkit. This provides a structured posture for visibility, attribution, and consequence—without requiring offensive force.

ESCALATION LADDER: PROPORTIONAL, LAWFUL SOVEREIGN RESPONSE

Escalation decisions are triggered by indicators such as AIS spoofing, cable proximity, or exclusion zone breaches. A triage protocol anchored in the Maritime Coordination Centre evaluates the incident and advises the Minister for Defence or Taoiseach. All actions follow pre-agreed legal thresholds and require political authorisation.

STEP	TRIGGER EXAMPLE	ACTION	AUTHORISER	INTENDED EFFECT
1. DETECTION	Suspicious vessel loitering	ISR tasking	Civilian analyst	Awareness without provocation
2. LEGAL FRAMING	AIS spoofing confirmed	Protest / demarche	Minister for Foreign Affairs	Raise reputational cost
3. NON-MILITARY ESCORT	Repeated cable proximity	Deploy RHIB / escort	Minister for Defence	Assert sovereign presence
4. VISIBLE POSTURE	Patterned threat behaviour	Overt patrol / drone surveillance	Cabinet-level approval	Signal readiness
5. LEGAL ESCALATION	Recurrent violations	ITLOS case / EU censure	Taoiseach	Strategic isolation via law

This structure deters through law, visibility, and measured escalation—not force.

DENIAL TOOLKIT: FRICTION WITHOUT FORCE

To frustrate and disrupt hostile actions without escalation, the strategy employs a set of lawful, non-aggressive denial tools:

- Seabed sensors for cable tampering alerts
- UAVs/USVs for vessel tracking and documentation
- RHIBs for rapid civilian shadowing
- Loudhailers, lights, and cameras to expose covert behaviour
- AI-based anomaly detection (e.g., spoofed AIS)
- Crowdsourced reporting from fishing and offshore sectors

These measures degrade adversary freedom of movement, raise operational risk, and enable lawful attribution—without signalling militarisation.

ROADMAP FOR HYBRID STRATEGY

0–2 Years: Build Civil Infrastructure

- Expand MARA’s role as national MDA integrator
- Deploy UAVs, USVs, and seabed sensors
- Stand up MRR with SAR, cable protection, and pollution response roles
- Lease ISR aircraft or long-range UAVs
- Establish Maritime Coordination Centre
- Review EEZ enforcement powers under UNCLOS and Irish law

2–5 Years: Scale Denial Capability

- Acquire patrol aircraft and coastal radar
- Form rapid-response naval unit with neutrality-aligned rules of engagement
- Install seabed acoustic surveillance at cable chokepoints
- Finalise legal and doctrinal escalation frameworks
- Initiate data-sharing partnerships with non-aligned EU actors
- Pass legislation covering cyber-physical maritime interference

5+ Years: Consolidate Credible Capacity

- Maintain persistent surveillance with autonomous sensing and layered redundancy
- Institutionalise ISR upgrade cycles and escalation doctrine reviews
- Create oversight mechanisms and public reporting for democratic legitimacy
- Position Ireland as a model for non-aligned, sovereignty-based maritime resilience

The hybrid model meets all three evaluative tests:

- Implementability: Phased, civilian-led rollout avoids institutional shock
- Operational Effectiveness: Enables legal, credible response across the threat spectrum
- Political Survivability: Anchored in neutrality, legitimacy, and EU-compatible non-alignment

This is not a strategy of passivity or provocation. It is one of sovereign capability—designed for an age of grey-zone interference, infrastructure vulnerability, and strategic ambiguity. It defines thresholds, assigns authority, and deters by readiness. It is a sovereignty strategy, not a warfighting doctrine.

COMPARATIVE ANALYSIS OF STRATEGIC MODELS

A viable maritime security strategy for Ireland must pass three structural tests: it must be implementable within national constraints; it must deliver credible operational effect under real-world threat conditions; and it must survive the political, legal, and constitutional realities of Irish statecraft. These are not ideals—they are preconditions. Any strategy that fails on even one is not viable.

Each test addresses a distinct failure mode:

- Implementation failure produces aspirational plans that collapse under delivery pressures—an outcome familiar from decades of procurement delays and institutional under-resourcing (Commission on Defence Forces, 2022; Irish Naval Service, 2022).
- Operational failure yields symbolic deterrence—postures that signal intent but lack capacity to detect, deter, or respond, especially in grey-zone contexts (Sloan, 2022; European Defence Agency, 2023).
- Political failure results in fragility—models that provoke public resistance, breach neutrality norms, or cannot be sustained through electoral and diplomatic cycles (Devine & Tonra, 2022; O'Driscoll, 2021).

These risks are not theoretical. They reflect the practical boundaries within which Irish security policy must function. The three models examined here—Full-Spectrum Deterrence, Civil Resilience, and the Hybrid Strategy—are assessed against each test. The analysis that follows evaluates their real-world feasibility, strategic performance, and institutional survivability under Irish conditions.Each of the three models under consideration offers distinct strengths. But only one performs consistently well across all dimensions.

IMPLEMENTABILITY: DELIVERING UNDER REAL CONDITIONS

The first test is structural: can a given model be delivered under Ireland’s actual institutional, political, and fiscal conditions? Strategic credibility is not measured in ambition but in execution. A strategy that cannot be operationalised is not a strategy—it is a design for failure.

To evaluate implementability, the Comparative Implementation Matrix below outlines the expected actions under each model across three phases:

- Immediate (0–2 years) – near-term actions that test speed and readiness,
- Medium (2–5 years) – institutional build-out and integration,
- Long-term (5+ years) – sustained posture and capability maturity.

This matrix is not a hypothetical construct. It simulates likely timelines and institutional load under real-world conditions in the Irish state.

Phase	*Full-Spectrum Deterrence*	*Civil Resilience*	*Hybrid Model (Proposed)*
Immediate (0–2 years)	– Launch Defence Capability Review – Initiate procurement planning (MPAs, vessels, missile systems) – Establish Maritime Command – Expand Naval and Air Corps recruitment – Begin White Paper reform	– Expand MARA's remit for domain awareness – Establish inter-agency civilian task force – Deploy commercial ISR and autonomous sensors – Enact EEZ legal reforms – Launch diplomatic norms initiative	– Operationalise MARA-led surveillance – Deploy leased ISR assets (drones, aircraft) – Launch Maritime Resilience Reserve – Establish civil–military coordination centre – Introduce legal scaffolding for grey-zone response – Deploy non-military denial tools (UAVs, seabed sensors, RHIBs)
Medium (2–5 years)	– Acquire high-end platforms – Deploy radar/sonar arrays – Expand Naval Service fleet – Conduct EU/NATO exercises – Reform command doctrine	– Build Maritime Coordination Centre – Institutionalise legal attribution mechanisms – Secure surveillance partnerships – Harden commercial infrastructure	– Scale targeted military tools under civilian control (e.g. patrol aircraft, radar) – Install acoustic arrays at subsea cable nodes – Codify escalation ladder and ROE compliant with neutrality – Expand EU cooperation on non-aligned ISR – Introduce legislation for coercive interference attribution
Long-Term (5+ years)	– Stand-up full deterrence posture – Independent kinetic response capacity – Fused civil–military ops centre	– Fully civilian-led incident response system – Leadership in maritime law and norms – Civilian tech refresh cycles	– Integrated posture combining civil surveillance and selective denial capability – Persistent layered sensing, attribution, and rapid response – Institutionalise biennial reviews, oversight, and public legitimacy

The matrix exposes not just what each model proposes, but how much institutional strain it introduces—and how quickly it can deliver credible capacity.

- Full-Spectrum Deterrence demands systemic military transformation. It requires major capital acquisitions, doctrinal realignment, and long-lead procurement processes. Even under optimal conditions, functional capacity is five years away. This may benchmark sovereign potential, but it cannot deliver timely security in a grey-zone context. Its technical coherence is nullified by its institutional implausibility.
- Civil Resilience is the most immediately feasible. It leverages existing agencies and deploys low-friction tools like commercial ISR, legal protest, and diplomatic signalling. But it is bounded in scope: it cannot deter, interdict, or respond proportionately to coercive action. What it gains in deliverability, it loses in deterrent credibility.

- The Hybrid Strategy is explicitly designed for implementability. It begins with what Ireland already has—civilian domain awareness, legal authority, interagency processes—and sequences upward. It adds a graduated escalation framework and non-military denial toolkit that can be deployed from the start. These features enable presence, visibility, and lawful friction without triggering escalation or breaching neutrality. Medium-term layers include light defensive assets, cable surveillance, and codified rules of engagement.

Critically, the hybrid model scales capability with political legitimacy and institutional maturity. Each layer prepares for the next. Escalation thresholds are built in, not improvised. It avoids institutional shock by design. The Hybrid Strategy is not a compromise. It is a functional architecture engineered to be deliverable, lawful, and proportionate. It is the only model that performs in real time, under real constraints, with real effect.

SCENARIO-BASED FUNCTIONAL TESTING

A strategy is only credible if it can function under pressure. This section evaluates the real-world utility of each model through scenario-based stress testing—a method designed to expose the operational strengths and limits of strategic posture in action, not theory.

WHY SCENARIOS?

Ireland's maritime vulnerabilities do not typically manifest as conventional attacks. They emerge in the grey zone: covert surveillance, cable interference, cyber-physical sabotage, and illegal incursions that test legal thresholds without triggering formal conflict. These threats are ambiguous by design—timelines are short, attribution is difficult, and the wrong response can escalate risk or forfeit control.

Scenario analysis enables structured evaluation of how a strategy performs in such conditions. It is a standard tool in defence planning used to test the coherence of capability, institutional readiness, and legal permissibility across plausible challenge cases.

FILLING THE STRATEGIC GAP

The five scenarios used here are based on publicly documented EU and Irish threat assessments (Sloan, 2022; European Defence Agency, 2023). They are not hypothetical—they reflect recurrent operational patterns already observed in Ireland's maritime domain. Yet none were substantively addressed in the June 2025 Dáil debate, which focused heavily on principles but lightly on actual threat mechanics. This gap underscores the need for stress testing: to ground strategic evaluation in the threats Ireland actually faces, not just those it prefers to imagine.

FIVE OPERATIONAL STRESS TESTS

Each scenario targets a distinct stress point in Irish maritime security—detection, attribution, legal escalation, coordinated response, and cross-domain resilience. Together, they provide a multidimensional test of strategic viability:

1. Covert Cable Mapping by Foreign Vessels
   Tests early detection, ambiguous attribution, and options for calibrated response.
2. Unattributed Subsea Cable Sabotage
   Tests infrastructure protection, investigative capability, and legal countermeasures.
3. Grey-Zone Surveillance by State-Linked Vessels
   Tests real-time awareness, capacity to assert jurisdiction, and escalation control under legal constraint.
4. Illegal Fishing and EEZ Incursions
   Tests enforcement coordination, reputational credibility, and ability to assert civilian authority.
5. Cyber-Physical Disruption of Maritime Infrastructure
   Tests resilience of critical systems, interagency response readiness, and capacity to manage hybrid escalation.

Each model—Full-Spectrum Deterrence, Civil Resilience, and the Hybrid Strategy—is evaluated across these scenarios to determine whether it can detect early, respond lawfully, and maintain sovereign control in contested conditions. The models diverge sharply in their ability to meet this test.

COMPARATIVE SCENARIO ANALYSIS: MARITIME SECURITY STRATEGY MODELS

Scenario	***Model 1: Full-Spectrum Deterrence***	***Model 2: Civil Resilience***	***Model 3: Hybrid Strategy (Proposed)***
Cable Mapping by Foreign Vessel	High-end ISR detects activity; military shadowing and interdiction available. Presence deters mapping and imposes reputational cost.	Satellite and AIS-based tools allow detection, but no interception mechanism. State response limited to legal protest; low coercive value.	Layered civilian sensors detect mapping; RHIBs or UAVs enable shadowing. Legal framing and exposure tools raise cost without escalation.
Cable Sabotage Attempt	Seabed patrols may deter attack; post-facto response includes armed patrols or defensive strike. High risk of escalation.	No credible pre-emption or interdiction capacity. Civilian detection unlikely before damage. Response limited to attribution efforts and legal protest.	Seabed sensors may flag precursor activity. Civilian-led triage enables earlier attribution, rapid repair, and escalation via legal and diplomatic channels. Denial tools (e.g. UAVs, RHIBs) raise visibility and disrupt hostile acts—without defaulting to military force.
Grey-Zone Surveillance by Adversary	Armed visibility deters encroachment; proximity patrols assert sovereignty. Military logic effective but escalatory.	Legal protest possible; awareness tools exist, but no presence to reinforce claims. Relies on reputational deterrence.	Escalation ladder enables civilian-led detection, shadowing, and legal framing. Attribution is calibrated and visible, asserting control without provoking confrontation or breaching neutrality.
Illegal Fishing or IUU Activity	Response may exceed proportionality; military enforcement is effective but risks diplomatic friction in low-grade cases.	SFPA and Coast Guard have statutory mandate; effective if resourced. No real-time presence in many offshore zones.	Civilian-led enforcement remains primary. Maritime Reserve augments response. Military assets are withheld unless civil capability is clearly overwhelmed, preserving neutrality and proportionality.
Cyber-Physical Attack on Maritime Infrastructure	Strong coordination and redundancy; military cyber response and ISR available. Deterrent signalling effective but risks overreach.	Civil response possible; limited deterrent or layered defence. Attribution and response likely delayed.	Maritime Coordination Centre fuses attribution, triage, and strategic communication. Civilian and dual-use ISR tools enable early detection; denial assets (UAVs, RHIBs, acoustic devices) are deployed under civilian command. Escalation ladder applies through law, exposure, and diplomatic censure.

These scenarios test not theoretical capacity but operational realism: attribution under ambiguity, deterrence without escalation, and response without political rupture. The models diverge significantly on these axes.

- Full-Spectrum Deterrence performs well where force is unambiguously sanctioned, and capacity is fully resourced. It excels at presence, interdiction, and deterrence through visibility—but only if unconstrained. In the Irish context, its strength on paper is compromised by its political implausibility and procurement burden.

- Civil Resilience is institutionally sustainable and politically safe, excelling in regulatory enforcement, norm signalling, and legal attribution. However, it lacks the coercive leverage or enforcement presence needed in grey-zone or sub-threshold scenarios. Its visibility is passive, and its responses are rarely decisive.

- The Hybrid Strategy balances escalation control with operational effectiveness. It leverages civilian-led surveillance to initiate early detection, then activates a predefined escalation ladder that includes legal protest, non-military shadowing, and denial tactics such as RHIB deployments and anomaly-triggered UAV patrols. This allows Ireland to impose friction and visibility on grey-zone actors without triggering militarisation. Crucially, the model's graduated attribution approach enables calibrated public exposure of adversarial behaviour—a strategic asset when escalation risks are high and legal thresholds ambiguous. It does not rely on deterrence-by-threat, but deterrence-by-readiness, managed through law, transparency, and sovereign control.

Only the hybrid model offers a posture that is proportionate, operationally functional, and politically survivable under real-world conditions.

POLITICAL SURVIVABILITY: ENDURING UNDER IRISH CONDITIONS

The final test is survivability: no strategy, however sound on paper, can endure if it fails Ireland's political, legal, and cultural stress tests. Maritime security policy must be not only operationally credible but governable—aligned with public sentiment, constitutional interpretation, institutional precedent, and Ireland's diplomatic identity as a neutral, non-aligned state (Devine & Tonra, 2022; O'Driscoll, 2021). Survivability is not about whether a model works in theory, but whether it can be implemented—and remain so—under scrutiny, turnover, and international interpretation. A viable strategy must be resilient not only in crisis, but in the democratic process.

- Full-Spectrum Deterrence fails this test. It would require steep increases in defence spending, redefinition of neutrality, potential constitutional friction, and perceived NATO alignment (Devine & Tonra, 2022; Doyle & Ní Aoláin, 2023). These risks are not hypothetical: in the June 2025 Dáil debate, no speaker endorsed a full military build-out. Across parties, members emphasised civil primacy and warned against perceived alignment. The model's technical coherence is nullified by its political implausibility. As policy, it is brittle.
- Civil Resilience passes, but conditionally. It aligns with public values, legal precedent, and institutional norms. It reinforces Ireland's tradition of civilian-led security and avoids political friction (O'Driscoll, 2021). But acceptability risks masking inadequacy. In the face of sabotage, coercion, or grey-zone escalation, it may fail under accusations of state incapacity. What survives politically today may falter under operational pressure tomorrow (Sloan, 2022).
- The Hybrid Strategy is the only model built to endure. It treats capability not as militarisation but as sovereign self-reliance. It builds incrementally through civilian institutions, without breaching neutrality or requiring constitutional change (Commission on the Defence Forces, 2022). Its design includes a pre-authorised escalation ladder and limited denial toolkit—allowing Ireland to respond visibly and lawfully to coercive acts without triggering militarisation or alignment. It supports neutrality by enabling calibrated, independent action through civilian-led enforcement. It reflects the cautious assertiveness voiced in the June 2025 Dáil debate: upholding neutrality while recognising the need for credible state capacity.

Each model claims internal logic. But only one meets the survivability test. Full-Spectrum Deterrence demands more change than Ireland's system can absorb. Civil Resilience offers too little to meet rising expectations of state responsibility. The Hybrid Strategy alone is structurally viable, politically defensible, and strategically fit for purpose.

INTEGRATED COMPARISON OF STRATEGIC MODELS

The comparative analysis makes clear that no model can be evaluated on a single axis. A viable maritime security strategy for Ireland must satisfy three concurrent tests: it must be implementable within real institutional and fiscal limits; it must enable credible operational response to hybrid and sub-threshold threats; and it must remain politically and constitutionally sustainable over time.

MODEL	IMPLEMENTABILITY	OPERATIONAL EFFECTIVENESS	POLITICAL SURVIVABILITY
FULL-SPECTRUM DETERRENCE	Low – requires major structural and fiscal shifts; delayed impact	High – strong denial and interdiction potential via hard military assets	Low – likely to breach neutrality norms and provoke public resistance
CIVIL RESILIENCE	High – deployable immediately using existing civilian frameworks	Low–Moderate – effective for monitoring and legal assertion but lacks enforcement capacity	High – normatively and institutionally aligned with current state practice
HYBRID STRATEGY	Moderate–High – phased implementation using existing institutions and targeted capacity-building	Moderate–High – escalation ladder and non-military denial toolkit enable proportional, lawful response to grey-zone threats	High – sustains neutrality while building resilience; escalation tools structured to avoid militarisation

The models show distinct profiles:

- Full-Spectrum Deterrence is operationally strong in theory but fails to meet the implementation and survivability thresholds. Its structural demands, political signalling, and normative implications exceed what can be delivered or sustained within Ireland’s current context. Even if effective on paper, its institutional cost and political brittleness render it unworkable in practice.
- Civil Resilience performs well on feasibility and political fit. It aligns with Ireland’s administrative and legal traditions and avoids institutional or diplomatic friction. However, its effectiveness under pressure is limited. It lacks the coercive or responsive tools necessary to meet credible sub-threshold challenges. Its stability is offset by its strategic insufficiency.
- The Hybrid Strategy is the only model that performs well across all three domains. It does not maximise any single axis, but integrates them in balance. Its escalation ladder enables calibrated action without crossing political or legal red lines, while its non-military denial toolkit imposes real-world friction on adversaries. It delivers a surveillance-and-response architecture grounded in civilian institutions, adds controlled defensive capability under neutral command, and retains constitutional and diplomatic coherence. It is not a median position between two extremes. It is a structured convergence of feasibility, function, and legitimacy.

CONCLUSION

Ireland's maritime security risks are now embedded in a changing strategic environment—marked by grey-zone activity, infrastructure vulnerability, and contested jurisdiction. These are not hypothetical concerns. They are material, escalating, and increasingly entangled with wider European and transatlantic dynamics.

In response, three strategic models were evaluated. Full-spectrum deterrence promised capability but failed to meet the political and institutional thresholds required for implementation. Civil resilience was politically aligned and deployable but fell short of delivering credible deterrence or operational response. Only the hybrid model met all three critical tests: implementability, operational effect, and political survivability.

It does so not by compromising between extremes, but by integrating the necessary elements of both. The hybrid model activates Ireland's existing civilian strengths—surveillance, legal authority, institutional coordination—while introducing a narrow suite of defensive capabilities under strict civilian control. Crucially, it incorporates a calibrated escalation ladder and a suite of non-military denial tools, enabling Ireland to deter, disrupt, and attribute grey-zone threats without violating neutrality.

This model reframes neutrality as active sovereignty. It enables readiness without provocation, enforcement without militarisation, and deterrence without alliance dependency. These mechanisms provide not just symbolic reassurance, but practical capacity to operate within a contested maritime environment.

The hybrid model is not the most expansive, nor the most politically frictionless. But it is the only model that aligns what is needed with what is achievable—and what is sustainable. It offers a viable, lawful, and strategically coherent foundation for Ireland's maritime security in an era defined by hybrid threat.

REFERENCES

Barnes, J. E. (2023). US warns of rising threat to undersea cables from adversarial states. The New York Times, 5 March. Available at: https://www.nytimes.com/2023/03/05/us/politics/russia-undersea-cables.html (Accessed: 10 June 2025).

Bueger, C. (2021). Situational awareness in the maritime domain: Towards a research agenda. Marine Policy, 132, 104661. https://doi.org/10.1016/j.marpol.2021.104661

Chapsos, I. & Kitchen, C. (2021). Maritime security in an age of climate change, cyber threats, and hybrid warfare. NATO Review. Available at: https://www.nato.int/docu/review/articles/2021/10/04/maritime-security-in-an-age-of-climate-change-cyber-threats-and-hybrid-warfare/index.html (Accessed: 10 June 2025).

Commission on the Defence Forces (2022). Report of the Commission on the Defence Forces. Government of Ireland. Available at: https://www.gov.ie/en/publication/7aad0-report-of-the-commission-on-the-defence-forces/ (Accessed: 10 June 2025).

Dáil Éireann Debates, Vol. 1012, No. 3, 12 June 2025. Houses of the Oireachtas.

Department of the Taoiseach (2023). Consultation on the National Security Strategy. Government of Ireland. Available at: https://www.gov.ie/en/consultation/xyz (Accessed: 10 June 2025).

European Commission Joint Research Centre (2023). Maritime Security Threats to Critical Undersea Infrastructure in Europe: Assessment and Policy Implications. Brussels: JRC. (Accessed: 10 June 2025).

European Defence Agency (2023). Defence Data 2022: Key Findings and Analysis. Brussels: EDA. Available at: https://eda.europa.eu/publications-and-data (Accessed: 10 June 2025).

European Union Agency for Cybersecurity (2023). Threat Landscape for Subsea Cables. ENISA, September. Available at: https://www.enisa.europa.eu/publications (Accessed: 10 June 2025).

Henriksen, A. (2021). Neutrality and non-alignment in the twenty-first century: The case of Ireland. Irish Studies in International Affairs, 32(2), 145–162. https://doi.org/10.3318/isia.2021.32.2.145

Irish Naval Service (2022). Operational Readiness Review: Strategic Capabilities and Constraints. Haulbowline, Department of Defence Internal Report.

McCabe, S. (2023). Irish neutrality: Myth, memory and manoeuvre. Irish Political Studies, 38(1), 45–67. https://doi.org/10.1080/07907184.2023.2178450

NATO (2023). NATO 2023 Strategic Concept. Brussels: NATO Public Diplomacy Division. Available at: https://www.nato.int/strategic-concept (Accessed: 10 June 2025).

Sloan, E. (2022). Securing subsea cables: The strategic blind spot. RUSI Journal, 167(4), 68–76. https://doi.org/10.1080/03071847.2022.2087797

UNCLOS (1982). United Nations Convention on the Law of the Sea, 10 December 1982, 1833 U.N.T.S. 3.

Whitman, R. G. (2022). European neutrality: Strategic ambiguity or obsolete doctrine? Survival, 64(6), 75–90. https://doi.org/10.1080/00396338.2022.2136723

GLOSSARY

Attribution (in security context)
The process of identifying the actor responsible for a security incident—such as cable tampering or grey-zone interference—using legal, forensic, and intelligence corroboration.

Civil-Military Governance
A structured mechanism by which civilian authorities retain oversight over security operations involving military components, ensuring alignment with democratic and legal norms.

Civil Resilience
A strategic model that prioritises civilian institutions, legal instruments, and regulatory mechanisms to maintain maritime security without resorting to militarisation.

Defensive Military Capability
Limited, non-offensive military assets employed under strict civilian control to protect sovereignty and infrastructure without violating neutrality.

Deterrence
The strategic concept of preventing hostile actions by demonstrating the capability and political will to respond effectively.

Domain Awareness (Maritime Domain Awareness – MDA)
The ability to monitor, understand, and respond to maritime activities, including detection of anomalies and emerging threats.

EEZ (Exclusive Economic Zone)
A maritime zone established under UNCLOS in which a coastal state has special rights to explore and exploit marine resources, typically extending 200 nautical miles from the coast.

Escalation Framework
A predefined sequence of state responses to security incidents, escalating in intensity while remaining within legal and political limits.

Full-Spectrum Deterrence
A comprehensive military posture designed to deter threats across the entire conflict spectrum, including grey-zone activities.

Grey-Zone Activity
Actions by state or non-state actors that fall below the threshold of armed conflict but undermine national interests—e.g., covert surveillance, cyber operations, or subsea mapping.

Hybrid Strategy (in this context)
An integrated model combining civil resilience with limited, defensively postured military capabilities to meet security needs without breaching neutrality.

Interagency Coordination
Operational integration and information-sharing among civilian and military agencies responsible for maritime security.

ISR (Intelligence, Surveillance, and Reconnaissance)
Technologies and practices used to monitor, track, and analyse potential threats across security domains.

Legal Framing
The process of defining security incidents using legal instruments—such as violations of UNCLOS—to facilitate formal state responses and diplomatic leverage.

Neutrality (Irish context)
Ireland's policy of military non-alignment, characterised by its non-membership in military alliances, refusal to host foreign bases, and restriction from offensive military actions.

Non-Military Escort
The deployment of unarmed state vessels—such as Coast Guard cutters or RHIBs—to monitor or guide foreign ships away from sensitive maritime areas without escalation.

Posture (Visible Posture)
The deliberate and observable display of national capabilities—such as patrols or surveillance operations—to deter adversaries and signal resolve.

Resilience Reserve (Maritime Resilience Reserve – MRR)
A civilian auxiliary force trained to support maritime infrastructure protection, environmental response, and emergency coordination in non-combat roles.

Sovereignty Assertion
Peaceful, visible actions by the state to affirm jurisdiction and control over its maritime domain, often through patrolling or legal declarations.

Strategic Isolation
The use of legal, diplomatic, or reputational tools to constrain an adversary's operating space following violations of international norms.

Subsea Infrastructure
Critical underwater systems—such as fibre-optic cables and energy pipelines—vital to national and global connectivity and economic functioning.

Survivability (of a strategy)
The degree to which a strategy can endure over time within political, legal, and cultural constraints, particularly in a neutral state context.

Triage Protocol (Security Triage)
A structured process for rapidly assessing, classifying, and escalating security incidents to ensure proportionate and timely responses.

UNCLOS (United Nations Convention on the Law of the Sea)
The international treaty that defines states’ maritime rights, obligations, and jurisdictions, including EEZs, territorial waters, and navigational freedoms.

ACRONYMS

ACRONYM	FULL FORM
AIS	Automatic Identification System
EEZ	Exclusive Economic Zone
EDA	European Defence Agency
EU	European Union
ISR	Intelligence, Surveillance, and Reconnaissance
ITLOS	International Tribunal for the Law of the Sea
IUU	Illegal, Unreported, and Unregulated (fishing)
MARA	Marine Area Regulatory Authority
MDA	Maritime Domain Awareness
MPA	Maritime Patrol Aircraft
MRR	Maritime Resilience Reserve
NATO	North Atlantic Treaty Organization
RHIB	Rigid-Hulled Inflatable Boat
SAR	Search and Rescue
SFPA	Sea-Fisheries Protection Authority
UAV	Unmanned Aerial Vehicle
UNCLOS	United Nations Convention on the Law of the Sea
USV	Unmanned Surface Vehicle