

## CYBER-ENABLED ISR AND THE DIGITAL SECURITY DILEMMA AT INDIAN OCEAN MARITIME CHOKE POINTS

Shiza Nasir<sup>1</sup>, Mehnaz Bibi<sup>\*2</sup>, Dr. Anwar Ali<sup>3</sup><sup>1</sup>MPhil Scholar, International Relations, University of Sargodha<sup>2</sup>MPhil, Political Science, Government College University, Faisalabad<sup>3</sup>Government College University, Faisalabad,<sup>1</sup>shiza.uos@gmail.com, <sup>2</sup>mehnazzz09@gmail.com, <sup>3</sup>anwarali@gcuf.edu.pkDOI: <http://doi.org/10.5281/zenodo.21352348>**Keywords**

cyber-ISR, security dilemma, Indian Ocean, maritime choke points, AIS spoofing, undersea cables, Strait of Hormuz, Bab-el-Mandeb, Strait of Malacca

**Article History**

Received: 01 February 2026

Accepted: 17 March 2026

Published: 31 March 2026

Copyright @Author

Corresponding Author: \*

Shiza Nasir

**Abstract**

In the maritime dimension, the Indian Ocean Region (IOR) is a region of strategic importance and it has been contested through naval presence, basing rights and control of sea lines of communication (SLCs) in the past. This article proposes that a parallel and increasingly significant competition has arisen in the digital and orbital spheres: cyber-enabled intelligence, surveillance and reconnaissance (ISR), that is the collection of satellite imagery, Automatic Identification System (AIS) monitoring, undersea sensor networks and submarine cable infrastructure, is now not only a means of maritime domain awareness but also a source of strategic unease for littoral and extra-regional powers. Based on Jervis's security dilemma concept and its application to the cyber domain, the article extends the security dilemma concept to a "digital security dilemma" associated with maritime choke points, where the multi-purpose, hidden, and harder-to-attract nature of cyber-ISR technologies means that the distinction between situational awareness and intelligence preparation for offense is not always clear. In the spirit of case studies, the author discusses AIS spoofing, satellite surveillance, and the weaknesses of undersea cables at the Strait of Hormuz, Bab-el-Mandeb, and the Strait of Malacca, respectively, to illustrate how these add to mutual mistrust between rival parties, such as India, China, Iran, the Houthis, and extra-regional navies. The article ends with policy proposals for confidence-building and regional cyber-maritime governance approaches to help dampen escalatory dynamics while not undermining legitimate security interests.

**1.Introduction**

The world's bulk cargo and a large share of its oil traffic pass through a handful of maritime choke points, which are located in and around Indian Ocean, including Strait of Hormuz, Bab-el-Mandeb and Strait of Malacca (Amar Kumar & Chandrashekhar, 2025; Roshan, 2025). Classical geopolitics has long held that these narrow waterways give someone an advantage in the energy security and trade reliance of faraway powers, if they are able to intercept, block or dominate them. Indeed, the academic and

policy discourses on the Indian Ocean Region (IOR) have turned towards naval force posture, basing agreements, and infrastructure diplomacy, as can be seen in the contrasting metaphors of China's "String of Pearls" and India's "Necklace of Diamonds" (Roshan, 2025). This literature has been more thorough in its discussion of the spread of choke-point security into the digital and orbital sphere, however. Maritime domain awareness (MDA) technologies are not just a stack of technologies; they are actually a dense web of technologies,

many of which were not developed – or even developed very little – a generation ago: commercial and military earth-observation satellites, the Automatic Identification System (AIS), Long-Range Identification and Tracking (LRIT), passive sonar and seabed sensor arrays, autonomous underwater vehicles and the submarine fiber-optic cables that carry the data they generate (National Maritime Foundation, 2021; Bueger & Edmunds, 2026). Intelligence, surveillance and reconnaissance (ISR) is the first line of defense in maritime security, and is being driven by these methods or cyber-enabled ISR (ISR for Global Maritime Security, 2026).

The very same technologies that enable a coastal state to track pirates, traffickers or an incoming threat enable it-or one of its rivals-to maintain a comprehensive, up-to-the-minute map of naval operations, traffic at choke-points, and undersea infrastructure, which can then be utilized for offensive targeting. The dual use is not a novel phenomenon in the study of international relations and is often referred to as the "security dilemma" described by Jervis (1978), who argued that states' responses to others' efforts to create security are interpreted as threatening to the other state and thus that the other state, in turn, takes measures that make everyone less secure. Maritime, however, has two additional factors that add to the dilemma as it's traditionally described: First, that in maritime, the problem of attribution is complicated by the fact that it is hard to determine whether an intelligence gathering satellite pass, an AIS-spoofing incident, or a cable-adjacent survey vessel, is the prelude to sabotage (Edwards et al., 2015); and second, the narrow geographic pinch-points where maritime activity occurs, whereby even a short loss of situational awareness or connectivity can have disproportionate strategic implications.

The crossroads of this article are the intersection of the two. Questions it raises include how the spread of cyber-enabled ISR into the Strait of Hormuz, Bab-el-Mandeb and Strait of Malacca is altering the states versus non-state actors' security dilemma that utilizes, patrols or attempts to control over these choke points. It adds an empirically informed contribution to the theory on cyber security dilemmas (Beckerman, 2022; Slayton, 2017), which thus

far has been mostly confined to the maritime/naval realm, and extends the analysis of threat perception to the maritime/geographic realm, where much of the discussion up to now has been centered on hard naval power.

### 1.1 Significance of the Study

There are three reasons why it is advisable to consider the Indian Ocean choke points as a unique and immediate field of research for this approach instead of a subset of a more global problem in cyber-maritime security. First, there is the sheer density of trade dependence: the volume of global oil shipments is close to 80 percent, and more than a third of the world's bulk cargo traverses this one sea basin, most of it in single, narrow trade lanes, and with the great majority of these going through just three or four – this is so that an ISR related disruption at any one choke point has systemically far reaching repercussions for energy markets and supply chains beyond the littoral states themselves (Navigating the String of Pearls, 2025; Badawi, 2025). Second, the area is already home to all the categories of actors that would be relevant to a digital security dilemma analysis: nuclear powers, a revisionist rising power, a state under sustained kinetic pressure, and a non-state-armed actor with proven ISR-exploitation capabilities, and it is an unusually rich comparative setting within a single geographic compass. Third, the Indian Ocean is currently home to some of the world's latest developments in maritime domain awareness (MDA) infrastructure, such as India's IFC-IOR and China's growing space-based C4ISR architecture, which means that the technological evolution that this article examines is not a hypothetical but a rapidly approaching reality (Comprehensive Maritime Domain Awareness, 2022; Orbital Militarization and India's Maritime Security, n.d.). South Asian countries in particular are highly dependent on energy imports from the Gulf countries, which pass through the same corridors that were studied here, and are directly and immediately affected by the way this digital security dilemma is dealt with.

### 1.2 Research Questions

- What is the security-dilemma dynamics created or enhanced by the dual-use and low-attribution nature of cyber-enabled ISR technologies (satellite surveillance, AIS monitoring, spoofing, undersea sensor and cable infrastructure) between state and non-state actors in the Strait of Hormuz, Bab-el-Mandeb, and Strait of Malacca?
- What confidence-building, governance, or technical measures might help mitigate the potential for escalation in competition between the littoral and user states for the maritime-domain-awareness needs at choke points in the Indian Ocean without compromising their legitimate requirements?

### 1.3 Research Objectives

- To propose and introduce a conceptual framework – the “digital security dilemma” for the particular context of maritime choke-point ISR competition that extends and applies the classical security-dilemma theory and cyber security-dilemma theory.
- To examine, based on case evidence provided through comparative analysis, the way that cyber-ISR practices are influencing perception of threats among key actors in the Strait of Hormuz, the Bab-el-Mandeb and the Strait of Malacca, and to make policy-relevant recommendations for the mitigation of escalation.

## 2. Methodology

This article follows a qualitative, theory-building case-comparative design instead of a large-N statistical approach, which suits the nature of the research questions and the practical limitations of the research when working in a domain where familiarity with a significant amount of the relevant incident data is limited because they are classified, contested, and only recently starting to be systematically captured in open-source monitoring efforts like Recorded Future's Insist Group. Three stages of the analysis are followed. First, it brings together the security-dilemma and cyber security-dilemma literatures discussed in Section 3 to identify a series of propositions which can be tested in the context of maritime cyber ISR. Secondly, it tests these propositions on three purposively selected case studies, the

Strait of Hormuz, the Bab-el-Mandeb, and the Strait of Malacca, to ensure maximum variation along the key variable of the actors involved (state vis-à-vis state; non-state vis-à-vis commercial; and latent great-power competition, respectively), with the underlying geographic logic of the choke-point vulnerability remaining constant. Third, it is grounded in a systematic review of primary and secondary open-source research, such as maritime security advisory from the national authorities (MARAD, UKMTO-linked reporting), industry risk assessment (Skuld, ISS Shipping and SAFETY4SEA), and peer-reviewed and working-paper scholarship on maritime domain awareness and Indian Ocean geopolitics, thereby minimizing dependency on any one source of reporting practice.

There are clear limitations to this design, which will be discussed further below: while open-source evidence can be used to confirm state intent in the case of clear, unambiguous ISR-adjacent activity, this is exactly the analytical challenge that the article's theoretical framework is designed to address and not to solve. The comparative case approach was chosen over a single deep case study as actor type and conflict phase must be manipulated systematically to assess how the digital security dilemma plays out, and this is only possible in a ‘relatively constant’ geographic and technological environment in the three-case design.

## 3. Literature Review

### 3.1 The Security Dilemma and offense Defense Theory

The security dilemma (Jervis 1978) helps to explain why states seeking security can nonetheless fall into conflict: what a state does to ensure its security is interpreted by other states as an expression of aggressive intentions which lead to countering or escalation. Jervis related the strength of this interaction to two factors: the offense-defense balance and the distinguishability of the offensive and defensive postures. The security dilemma is doubly dangerous when there is a belief that neither offensive nor defensive power can be distinguished with certainty and when the states of status quo are rational, but fearful of being caught unprepared and therefore act aggressively

(Security Dilemma, 2026; When Does Competition Become Conflict? 2021). Others following the idea of offense/defense theory have added more detail to the situations in which distinguishability can occur, usually by means of costly signals that allow one to distinguish between benign and threatening postures (See Glaser, When Does Competition Become Conflict? 2021).

In many of these publications, the combination of geography, technology, and doctrine has been identified as the key factors that influence a domain's balance of offense/defense, and that these factors evolve over time (When Does Competition Become Conflict? 2021). The strategic significance of maritime choke points is a paradigm case of the power of geography: A relatively modest capability – be it a minefield, a coastal battery, an anti-ship missile or, increasingly, a persistent ISR picture – placed at a choke point can inflict disproportionate costs on transiting forces. This geographic logic is exactly what inspired China to come up with the concept of the 'Malacca Dilemma,' which held that an aggressive country that controlled the Strait of Malacca would be able to block the vast majority of China's energy supplies (Badawi, 2025; String of Pearls, 2026).

It is also worth noting that Sebastian Rosato has written a critique of the theory of offense-defense, which might provide a counterpoint in this literature: Rosato argues that what appears to be good for the defense does not necessarily alleviate the security dilemma because the leaders' subjective perception of the balance often does not correspond with any objective technological assessment (Security Dilemma, 2026). This caution is directly applicable to the maritime cyber-ISR context, and as further sections demonstrate, mere technical evaluation of whether or not a particular satellite pass, AIS pattern, or survey vessel activity is offensive or defensive in purpose is often not enough.

### 3.2 Extending the security Dilemma to cyberspace

Much of the literature, but separate, has questioned the relevance of the security dilemma, which was designed for a world of tanks, missiles, and fortifications, to the cyber world. More recent scholarship has complicated

this, suggesting that instability is not about offense dominating the battle at the hands of the attackers, as they have only one vulnerability to exploit, but about the difficulty in making an attribution (Cyber Posturing and the Offense-Defense Balance, 2013; Cult of the Cyber Offensive, 2020). From a neoclassical realist perspective, Beckerman (2022) discusses the possibility of cyber competition escalating to kinetic conflict and posits that the classical arms-race logic of the security dilemma is a poor match for most cyber interactions, since states tend to respond to cyber incursions quietly and indirectly, but become more vulnerable to kinetic threats when operations pose a threat to a leader's political survival.

One mechanism particularly pertinent to the ISR context is described by Edwards et al. (2015): The technical distinction between reconnaissance for intelligence gathering and the intrusion required for an attack that disrupts the network is minimal, meaning a defensive intelligence gathering operation can be seen by the target as an attack of its own, conducted through reconnaissance and not by an actual intrusion. The theoretical pivot point on which the argument of the present article pivots is the indistinguishability problem: Maritime cyber-ISR, just like an attack on maritime traffic, or an attack on undersea infrastructure, represents a physical-digital hybrid version of the indistinguishability problem.

### 3.3 Maritime Domain awareness and ISR Infrastructure

The modern maritime ISR technical architecture is now fairly well known. AIS transponders, required for merchant vessels above 300 gross tons, send out identification and location data which are received by coastal AIS receiver networks and relayed by satellites; only 74 coastal AIS receivers have been installed in India and are working, and can track tens of thousands of merchant vessels passing through the Indian Ocean (India Reinforces Maritime Domain Awareness, n.d.). This information is combined with LRIT reporting, on-shore EOS and radar inputs at information centers like India's Information Fusion Centre for the Indian Ocean Region (IFC-IOR) set up in 2018, inspired by Singapore's Information Fusion

Centre, operating with liaison officers from dozens of partner navies (Bueger & Edmunds, 2026).

There is one more layer, that of satellite-based earth observation. Both synthetic aperture radar (SAR) and electro-optical satellites, which are now being operated by commercial satellite service providers as well as national space agencies, can be used to detect AIS transponders that are intentionally turned off, or dark shipping, and can be used for wide area surveillance in addition to the coastal sensors (Bueger & Edmunds, 2026; National Maritime Foundation, 2021). The case-studies of India utilizing its RISAT satellites to supply its Information Management and Analysis Centre and China building an ISR system across sub-surface, surface, air and space domains, shows how orbital assets have become a key component of choke-point surveillance for both revisionist and status quo powers (Orbital Militarization and India's Maritime Security, n.d.; Comprehensive Maritime Domain Awareness, 2022).

A third, and lesser-studied, layer is the subsurface, encompassing passive solar arrays, seabed sensors and submarine telecommunication cables that provide military acoustic intelligence and the vast bulk of global data traffic. Since 2023, a series of suspected sabotage risks have been reported around submarine cables in the Baltic Sea, Taiwan Strait, and the Red Sea (Submarine Cable Security at Risk, 2025; Critical Undersea Infrastructures, 2026), driving a rapid transformation of this once-unassuming area of technical concern into a known front line of gray-zone competition. The domain is also highly conducive to the same plausible-deniability dynamics that exist in the broader cyber environment, as the damage can be caused by relatively unsophisticated activities (such as anchor-dragging) and ownership of the involved vessels is often hidden behind flag-of-convenience registrations (Submarine Cable Security at Risk, 2025).

The third of these layers is an increasingly important one for AI to be able to overlie and interpret the resulting data streams. The use of AI to identify patterns in maritime traffic that are so dark they are intentionally hidden from

AIS and can only be detected by combining satellite imagery with historical patterns of shipping traffic is now a specialty of maritime analytics companies; such services are now becoming public-private partnerships and determining who has access to analysis—whether it be public or commercial. Reliably identifying anomalous vessel behaviour for safety or counter-trafficking purposes results in outputs that can equally be used to target vessels, and commercial analytics models are often proprietary and opaque, making it difficult for the observed vessel state or external researchers to audit how or why a given vessel or pattern was flagged.

### 3.4 Great Power competition in the Indian ocean Region

The Sino-Indian rivalry that dominates many aspects of the IOR's security dynamics has been well documented in the IOR literature. Despite Beijing's repeated claims of the lack of military motive, China's String of Pearls strategy – the string of commercial and dual-use port facilities from Gwadar in Pakistan to Hambantota in Sri Lanka and finally to Djibouti at the mouth of the Bab-el-Mandeb – is perceived in New Delhi as a strategy of encirclement (String of Pearls, 2026; Roshan, 2025). India's counter, dubbed the Necklace of Diamonds, is the series of access agreements it has secured in Duqm, in Oman, Sabang, in Indonesia, Assumption Island, in Seychelles, and Agalega, in Mauritius, plus the development of the Andaman and Nicobar Command that spans the western passage of the Strait of Malacca (Roshan, 2025). This literature has focused on basing, force posture and infrastructure finance, while comparatively little has been devoted to how the same competition is played out with satellite reconnaissance, AIS-data contestation, and with undersea infrastructure, an aspect the article deals with.

This competition has resulted in a real regional infrastructure and ISR competition rather than a series of bilateral conflicts. In Pakistan, the Gwadar port is individually championed for commercial or narrowly defensive reasons by its host government, and in Sri Lanka, the Ream base is the Hambantota port, in Bangladesh, the naval facilities are in development, and in Cambodia, the naval base at Ream is being

promoted for the same reason; but when viewed as a package, they all read to Indian strategists as forming part of a single encirclement architecture for China's ISR reach into the whole IOR littoral (Badawi, 2025). India has built its own chain of access agreements and forward-deployed surveillance posts from the Andaman & Nicobar Command to listening posts in Madagascar, with radar stations in the Maldives, that are operated for defensive purposes and are subject to the same changes of interpretation by Beijing that prompted their deployment (String of Pearls, 2026). What is comparatively under-explored in the empirical record, then, is the extent to which the ISR and data layer atop the infrastructure, the tasking of satellites, the fusion of AIS data, and the routing of cables create a similar threat perception and dynamic on their own.

### 3.5 Synthesis and Identifies Gaps

Three lines of scholarship exist simultaneously, but do not yet form an organized unity. However, it was not until the literature on security dilemma and offense-defense theory (Jervis, 1978, When Does Competition Become Conflict, 2021) emerged that the analytical tools emerged, which explain why dual-use, indistinguishable capability creates mutual insecurity, but these were developed mainly with reference to conventional and nuclear weapons systems. This vocabulary has already been introduced to the competition context of cyberspace, but has focused on intrusion into networks and computer network attack, not on the physical-digital hybrid infrastructure, satellites, AIS, etc. that forms the basis of maritime awareness in particular. Last, but not least, the extensive empirical research on Indian Ocean geopolitics (Roshan, 2025; Badawi, 2025; Amar Kumar & Chandrashekhar, 2025) has captured in detail the material expansion of ports, bases and naval infrastructure; it has largely neglected, however, the role of ISR and digital infrastructure as a driver of a security dilemma in its own right. The contribution of this article is to bring these three literatures together in a single framework developed in Section 3, which views maritime cyber-ISR as a new arena where security-dilemmas can be played out, one that is autonomous and

increasingly primary at Indian Ocean choke points, rather than just an enabler of the traditional naval competition.

### 4. Conceptual Framework: The digital Security Dilemma at maritime choke point

This article conceptualizes the digital security dilemma at maritime choke points as a situation in which the acquisition, sharing or denial of cyber-enabled ISR capability by one actor is interpreted as an indicator of an actor's offensive intent because of the structural difficulties involved in attributing offense to defense, the fact that there is a great deal of overlap in the domain of maritime ISR, a lack of attribution, and the high concentration of strategic value in a specific geographic area. The framework is founded on three propositions obtained from the above literature review.

#### 4.1 Indistinguishing of purpose

A satellite pass across the Strait of Hormuz, a survey ship in the vicinity of a landing point for cables in the Bab-el-Mandeb or a prolonged effort to detect AIS anomalies close to the Strait of Malacca can be anything but defensive, for shipping protection, smuggling detection, protection of cable assets or offensive purposes such as target mapping, interdiction rehearsal or locating cables for future sabotage. The purpose of an ISR platform is evident in what data it records and what it records can be used for, but information is seldom available to the state being observed, unlike a warship, whose weapons and flag are readily evident. The same is true in cyberspace, according to Edwards et al. (2015), who argue that intelligence collection and attack preparation are "technically indistinguishable" in cyberspace, and this is now the case in the maritime realm in which both the detection and preparation of attacks are carried out with intelligence satellites, AIS receivers, and undersea survey operations.

#### 4.2 Attribution Friction as an escalation multiplier

The attribution problem of cyber conflicts has been long acknowledged in the studies of cyber conflict (Edwards et al., 2015), and this applies to choke-point cyber-ISR competition as well; as signals can be spoofed, cables can be spoofed or

destroyed by vessels using flags of convenience, and satellite reconnaissance leaves no physical trace at the target. This has a paradoxical double effect. On the other hand, a low-strength attribution reduces the short-term expense of a state pursuing offensive intelligence: If the traffic through the choke point is not likely to be attributed to the attacker, then there is less risk that the attacker will be retaliated against for collecting the data. At the same time, the same weak attribution increases the perceived risk of the target because it does not know and can't really guess who is observing and why, leading it to assume the worst-case scenario and in turn, to take precautionary measures to counter surveillance. In practice, this is already known to be the case; during an investigation of a collision in the Strait of Hormuz in 2025 the fake AIS data of a vessel was used to place its position on shore in Iran, creating more strategic ambiguity than resolution (Security Risks Impacting Global Shipping, 2026).

#### 4.3 Geographic concentration amplifies stakes

Even limited loss of situational awareness, like if a satellite link jams or an AIS traffic is spoofed or a cable is cut, has consequences much greater than the technical level of the incident, as the choke points of an enormous volume of global trade and energy flow into a narrow corridor. A similar cable-cutting attack on a landing station in the vicinity of the Hormuz or Malacca Straits could affect shipping insurance, financial services, and naval control and command over an extensive number of users for over a half month (Testimony before the U.S.-China Economic and Security Review Commission, 2026). The digital security dilemma at choke

points is likely to induce a more acute response, and a lower level of 'precautionary military posture', than similar cyber-ISR competition over open ocean or land.

#### 4.4 Asymmetric actor capacity shapes response options

The fourth argument, implicit but not fully explored in the classical literature nor in the maritime cyber-ISR, has to do with the different response sets those different groups of actor's face when they encounter the same underlying indistinguishability problem. Sovereign satellite and naval ISR powers like India, China, Iran, and extra-regional powers have the option to react to ISR intrusion in the state by conducting reciprocal ISR, diplomatic protest or in extreme cases, kinetic deterrence. Commercial shipping companies and smaller littoral States, however, are generally unable to do anything more than adjust their behavior either by altering their shipping routes, modifying their ships' AIS signature, or buying private armed escort – both of which involve reacting to the risks they face, but don't solve the dilemma and may in some cases, as the Bab-el-Mandeb case demonstrates, create counterproductive incentives. Non-state actors are in a third camp, as they can use the ISR asymmetry offensively at relatively low cost because they lack the equivalent of an equivalent infrastructure that can be similarly targeted by a state adversary, which partially explains why conventional deterrents haven't been successful in the Houthis' use of AIS data.

Table 1 summarises how these three propositions map onto the technology layers of maritime cyber-ISR discussed in the literature review.

*Table 1. The Digital Security Dilemma across Cyber-ISR Technology Layers*

| Technology layer               | Defensive use                            | Perceived offensive use                         | Attribution friction                                            |
|--------------------------------|------------------------------------------|-------------------------------------------------|-----------------------------------------------------------------|
| Satellite ISR (SAR/EO)         | Dark-vessel detection, disaster response | Target-mapping, order-of-battle tracking        | Low but intent unverifiable                                     |
| AIS / LRIT                     | Traffic management, collision avoidance  | Precision targeting via spoofed or scraped data | High signal is falsifiable                                      |
| Undersea cables & sensors      | Data connectivity, ASW listening         | Espionage, chokepoint sabotage rehearsal        | Very high plausible deniability via flag-of-convenience vessels |
| Fusion centres (e.g., IFC-IOR) | Multilateral MDA sharing                 | Intelligence pooling against a specific rival   | Moderate depends on partner composition                         |

## 5. Case Analysis

The three case studies below have been chosen to reflect structurally different scenarios of the digital security dilemma: the Strait of Hormuz is a state to state contestation where the contest is open kinetic conflict; the Bab-el-Mandeb is an example of a non-state contestation where the contest is open ISR asymmetries; the Strait of Malacca is an example of a contest between two great powers, India and China, where the contest has not yet materialized, but where there is a clear longer time horizon.

### 5.1 The Strait of Hormuz: State-Level contestation under crisis Condition

The Strait of Hormuz is the most recent example of the interplay of contestation and kinetic risk in cyber-ISR. After the escalation of 2026 between Iran and regional and extra-regional forces, the threat level over the Gulf of Oman and Strait of Hormuz has been rated as critical, with vessel numbers in the strait dropping to single numbers per day and a concentration of shipping around the UAE-Oman approaches as operators sought to avoid the area altogether (Maritime Security Update, n.d.). Operating environment degradation was observed and recorded by analysts, including spoofed positions and AIS anomalies, as well as intermittent communications, which all contribute to a risk of routine collision, apart from any deliberate attack (Maritime Security Update, n.d.).

One of the most revealing was the 2025 Front Eagle collision, when a massive LNG ship, Front Eagle, was falsely identified as being ashore in Iran, where it was not and led to difficulties in post-collision investigations and the full picture of who was where in the strait (Security Risks Impacting Global Shipping, 2026). It encapsulates the digital security dilemma in miniature: a technology designed to make operations more transparent, and potentially less likely to be sources of collisions, came to be confused by all parties, with the potential to be used for a range of plausible deniability scenarios, from concealing the location of a naval movement, to hiding the true source of a tanker for sanctions evasion, to simply not knowing from where to begin when a collision occurred. The same tricks are now being used in

Black Sea tankers, and the use of this technique is spreading to other theatres, not just limited to the Gulf (Security Risks Impacting Global Shipping, 2026).

From Iran's perspective, the U.S., the Gulf States, and their allies are constantly monitoring Iran via satellite and AIS, and that intelligence is not shared in the same way. From Iran's point of view, the U.S., the Gulf States, and their allies are constantly monitoring Iran via satellite and AIS, and that intelligence is not shared in the same way. In the eyes of the Gulf shipping states and extra-regional navies, Iranian jamming of GPS, AIS anomalies, and the general mysticism surrounding Iranian naval and proxy operations in the strait are interpreted as preparation to either mine or seize tankers or target them with missiles. Both readings can be justifiably made from the perspective of each of the actors, and, indeed, both are doubly dangerous, as Jervis (1978) described an offense-dominant, indistinguishable security environment.

The practical effect, as demonstrated in the above mentioned JMIC assessments was that ships started to abstain from testing the ISR, and so absorbed the cost of the ambiguity into the cost of commercial shipping (Maritime Security Update, n.d.). This is a unique and overlooked escalation path: the digital security dilemma in Hormuz, at least in its current form, has the form of a chilling effect, but on the economy as each insurance company, charterer, flag state, etc. adjusts its calculations of risk in the absence of any one authoritative narrative of what is going on in the strait at any given moment.

### 5.2 The Bab-el-Mandab: Non-State exploitation of ISR asymmetries

The Bab-el-Mandeb and southern Red Sea corridor have a unique dynamic: a non-state actor, the Houthis, has maintained a multi-year campaign against commercial shipping and relied on a mix of open-source AIS tracking, radar and reported SIGINT to do so, forcing the commercial shipping operators into defensive information practices themselves creating new security-dilemma dynamics. The Houthis have continued to sink or damage several vessels and kill several seafarers since 2023 and attacks have been linked closely to the vessels' perceived ownership, flag or to trade relations with Israel,

or the United States (2026-006 Red Sea Advisory, 2025).

Given that Houthis are seen to rely on AIS data and other identifying information sent out by vessels themselves, shipping operators have responded by modifying their own digital signatures, such as by sending messages out on the AIS to say they are an all-Muslim or all-Chinese crew, or to indicate that they have armed guards, in what maritime security analysts describe as an increasingly desperate defensive countermeasure (Ships Transiting the Red Sea, 2025). In the United States, maritime advisories have been issued going so far as to advise ships not to comply with Houthis' instructions to operate AIS or to broadcast voyage information, arguing that that would "materially assist" the targeting (2026-006 Red Sea Advisory, 2026; 2025-012 Red Sea Advisory, 2025).

This creates unique variant of the digital security dilemma: one non-state actor is exploiting civilian ISR infrastructure – most notably AIS – in an asymmetric way, forcing an international shipping community to enter a defensive equilibrium of increasing security without increasing transparency. The effect has been a split in maritime traffic based on the risk of perceived ownership, with operators of vessels connected to China in some instances still transiting the strait while AIS was on, on the assumption that the Houthis see them as unthreatening, or with others avoiding the corridor entirely or transiting using 'dark' signals (The Ship Operators Shrugging Off Houthi Attacks, 2025). The first option poses a threat to a security-neutral environment, while the second poses a threat to navigational safety, meaning that the security dilemma that arises at the ISR-layer expands out from the naval realm into commercial and diplomatic decision-making.

The Bab-el-Mandeb case also overlaps with the laying of the undersea cables of the framework. The analysts have observed that the Houthis have shown awareness of the strategic leverage they can gain by disrupting maritime systems on a broader front and that the southern Red Sea is one of the most vulnerable areas in the world for cable damage, along with the Baltic and Taiwan Strait (Critical Undersea Infrastructures, 2026; Submarine Cable Security at Risk, 2025). Even a relatively low-tech non-state actor could, through

a "simple" anchor-dragging or opportunist damage, cause harm to the global digital economy, when a significant portion of data traffic flows through Red Sea cable routes.

Another interesting aspect of this case is the fact that the incentive system highlighted in this case is contrary to a straightforward proposition that greater transparency will lead to better maritime security. In basic mode, universal, accurate AIS broadcast is clearly advantageous – aiding in collision avoidance and search and rescue. The rational individual response from a commercial operator of high transparency—for example, by curating or falsifying a commercial operator's own AIS profile—has a negative impact on the reliability of the entire system, which is a collective-action problem overlaid on the security dilemma. It indicates that improvements in data quality alone will not fix the issue, as long as it remains rational to falsify data because of the threat.

### 5.3 The strait of Malacca: The Latent Sino-India Digital Dilemma

The Strait of Malacca case is structurally different yet again, where India and China instead of kinetic conflict, are building out competing ISR infrastructure in a slow-burn manner that is both defensive in nature and strategic in significance, interpreted as encirclement or intrusion by the other. India's Andaman and Nicobar Command, which has been called an "unsinkable aircraft carrier for surveillance and power projection", is positioned to operate at the western approaches of the strait and has a port at Sabang in Indonesia at the mouth of the strait, besides providing satellite-based maritime domain awareness through IMAC and the Information Fusion Centre for the Indian Ocean Region (Roshan, 2025; Orbital Militarization and India's Maritime Security, n.d.).

China's driving fear is the Malacca Dilemma: Beijing has almost eighty percent of its energy imports going through the strait and fears that the Indian and Chinese navies—particularly the latter may be able to intercept traffic there, thus rendering the PLA Navy unable to gain situational awareness of the IOR (String of Pearls port network and significant investment in space-based and undersea ISR capabilities to

provide the PLA Navy with independent situational awareness in the IOR) (Roshan, 2025; (Comprehensive Maritime Domain Awareness, 2022). Viewed from New Delhi, however, this same ISR build-out, especially Chinese research and survey vessels in the vicinity of Indian Ocean cable routes and choke points, is interpreted as intelligence preparation and not as defensive hedging, which means that it is being done at a slower tempo than in the Taiwan Strait and the Baltic Sea cable-sabotage incidents (Testimony before the U.S.-China Economic and Security Review Commission, 2026).

While no specific incident has been publicly blamed on Sino-Indian competition in the IOR, the pattern of cable damage indicated by vessels registered under the flag of convenience and AIS transponders with disabled equipment since 2023 in the waters around Taiwan is conducive to the development of a plausible trajectory of such events in the near future (Taiwan Strengthens Patrols, 2025; Testimony before the U.S.-China Economic and Security Review Commission, 2026). A similar concentration of undersea cable runs through and around the Strait of Malacca, while already Chinese research vessels are cruising freely around the IOR under the guise of oceanographic surveys, making Indian maritime security planners think twice about the Taiwan pattern and what this means for the Malacca theatre if tensions between the two countries intensify.

The Malacca case is the classic Jervis-Digital security dilemma two status-quo oriented, yet mutually suspicious actors, both building ISR and infrastructure capacity mostly for its own sea lines of communication – each perceiving the other's buildout as evidence of hostile intent

with the determining signal, declared purpose, largely unconfirmed, given the dual-use nature of satellites, survey vessels and fusion centers.

This is further complicated by the western terminus of China's String of Pearls in the Gwadar port in Pakistan, which is close to the Strait of Hormuz, and far from Malacca but still affects the broader IOR balance affecting Indian threat perception. Historically, Indian naval planners have noted that a Chinese-controlled or Chinese-influenced facility at Gwadar – located near the Hormuz exits and an alternative to the facilities in Karachi and Port Qasim, which are adjacent to India – puts the Chinese in the IOR, and not just at the Malacca approaches (India's Counter Strategic Response, 2026). In Beijing's own defense, the same facility is needed as a counter to the Malacca Dilemma to find an alternative energy corridor that will not pass through the strait. That this two-sided competition is unfolding at the same time, both at Hormuz adjacent Gwadar and at the Malacca approaches themselves, demonstrates how the digital security dilemma at choke points in the Indian Ocean can't be grasped from a case-by-case perspective because decisions made at one choke point feed threat perceptions at another, and vice versa.

## 6. Discussion: Comparative dynamics and Escalation pathways

Taken together, the three cases indicate that the digital security dilemma at choke points in the Indian Ocean is not necessarily the same, but can change systematically as a function of the type of actor involved and the state of the kinetic conflict. This comparison is presented in Table 2 for the three propositions developed in Section 3.

*Table 2. Comparative Manifestation of the Digital Security Dilemma*

| Case              | Primary actors                           | Dominant ISR layer                             | Escalation pathway                                        |
|-------------------|------------------------------------------|------------------------------------------------|-----------------------------------------------------------|
| Strait of Hormuz  | Iran, Gulf states, extra-regional navies | AIS spoofing, satellite ISR                    | Acute active kinetic conflict amplifies ISR ambiguity     |
| Babel-Mandeb      | Houthi movement, global shipping         | AIS exploitation, cable exposure               | Persistent asymmetric targeting sustains defensive spiral |
| Strait of Malacca | India, China                             | Satellite ISR, undersea cables, fusion centres | Latent infrastructure competition precedes crisis         |

The comparison in Table 2 also points to a simple typology of digital security dilemmas which could be transposable to other maritime contexts outside of the Indian Ocean. An acute-symmetric type occurs when two or more states of roughly equal ISR capability contest a choke point with ISR activity occurring at or approaching an active crisis state and typically materializes as chilling effects to the economy and the avoidance of transits by the parties themselves, but not as kinetic exchanges over ISR activity per se, as with Hormuz. An asymmetric-exploitative type occurs when a non-state or other ISR-poor actor takes advantage of the transparency of a civilian system for a large number of commercial actors, such as at the Bab-el-Mandeb, and is likely to emerge as a collective-action problem where individually rational responses to the challenge (e.g., falsification of AIS) reduce system-wide safety. A latent-infrastructure type emerges when two similarly comparable powers develop parallel ISR and basing architectures over a long time without a pressing crisis, as happened at Malacca, and typically presents as incremental capability building that can only be realized when a crisis occurs elsewhere, as the cable-sabotage example in the Taiwan Strait suggests, showing that the underlying tactics can be affected. Understanding these three types of responses may guide regional policymakers in determining the type of response likely to be required in a specific choke point at a specific time, instead of blanket implementing a maritime-cybersecurity policy in an entirely different threat structure.

There are three general analytical comments to make. The first and foremost reason for escalatory risk in each of the three incidents is not simply the physical power, but problems in the data layer: manipulation or ambiguity, as with the falsified AIS data in the Front Eagle incident, or as with the flag-of-convenience vessels and cable sabotage near Taiwan, or as with the Houthis' use of AIS transparency. It reinforces Edwards et al's (2015) argument that it is the indistinguishability rather than offense dominance per se that is the greater driver of instability in cyber-adjacent domains, implying that policies that focus solely on building up physical infrastructure will only solve part of the problem.

Second, the geographic concentration effect shown in Proposition Three seems to interact with actor type in an important way: the concentration effect in Hormuz is an amplification of the deterrence risk, because the signal of any single ISR-related incident could be interpreted as a prelude to war, while the diffuse, non-state threat in the Bab-el-Mandeb is an amplification of the vulnerability effect, because commercial actors lack the deterrence or retaliatory options of states, and must instead adapt behaviorally, by selectively broadcasting AIS signals or performing a "dark transit" at real safety cost.

Third, the Malacca case has shown that the digital security dilemma does not have to be a constant threat in the future. The Taiwan Strait and Baltic Sea cases illustrate a potential trajectory in which gray-zone cable interference can grow to a "known instrument of coercion" that an actor wishing to rewrite history will deem acceptable in terms of the costs to the target state and its national security. As in the Taiwan and Baltic cases, it appears that Sino-Indian ISR competition is not a distant reality, but a near term risk indicator, and the region's policy makers should take note of this.

There is a methodology limitation that should be recognized. Presented information in this article is based on open-source reporting, maritime security advisories, and secondary, academic literature, and motive attributions, especially relating to motives of the Chinese state behind the activities of the cables, should be considered informed inference rather than fact. In a way, this limitation is another argument for the argument made here: just as the digital security dilemma creates a limitation for regional militaries and intelligence services a confidence-based limitation exists for open academic research, which requires transparency-oriented policy measures discussed below.

## 7. Policy Implications and Recommendations

With respect to the answer to RQ2, the above analysis indicates that a number of complementary measures may be implemented in order to lower the risk of escalation from RQS that can be undertaken without the littoral and user states sacrificing their legitimate MDAS.

### 7.1 Data Integrity Confidence-Building measure

Regional and flag state authorities should focus on technical and regulatory measures to enhance the verifiability of AIS data such as cross-checking AIS broadcasts against independent satellite tracking and flagging any discrepancies in AIS data through existing fusion centers like IFC-IOR, as distinct from the mere presence of AIS itself, the incidence of AIS spoofing and falsification is the driver for several documented incidents (Security Risks Impacting Global Shipping, 2026; Bueger & Edmunds, 2026).

### 7.2 Multilateral Undersea Cable Protection Protocols

Littoral states bordering the Strait of Hormuz, Bab-el-Mandeb and Strait of Malacca should implement joint monitoring, and quick response mechanisms similar to the emerging Quad Partnership for Cable Connectivity and Resilience, specifically (Under Sea Cables, n.d.; Truman National Security Project, 2025).

### 7.3 Track 1.5 Dialogue on Satellite and AIS Transparency Norms

There are opportunities for India and China to engage in bilateral cyber maritime negotiations on voluntary norms for transparency among research vessels, such as around cable routes and satellite reconnaissance patterns, through existing regional forums or a new bilateral forum, and to establish norms in line with the principles of offence-defense theory, which prioritizes distinguishability as a stabilizing mechanism and precedents from other international nuclear and conventional confidence and security-building measures (When Does Competition Become Conflict?, 2021).

### 7.4 Protecting Non-State and Commercial Actors Protecting Non-State and Commercial Actors

Guidance should be continued on selective disclosure of AIS data during periods of heightened ISR threat, as demonstrated in the Bab-el-Mandeb case, and this guidance should be developed by flag states and the International Maritime Organization (IMO) to reflect current ad hoc practices – rather than by blanket

disabling of AIS data, as this would reduce AIS's original collision avoidance and search and rescue (SAR) role (2026-006 Red Sea Advisory, 2026; Ships Transiting the Red Sea, 2025).

### 7.5 Regional Academic and Track-2 Capacity Building

Lastly, the relative lack of scholarship on the linkages between security-dilemma theory and maritime cyber-ISR, which was identified in Section 2.5, opens possibilities for implementation by South Asian and IOR-based research centers. Regional think tanks and university centers are ideally suited to develop the databases of incidents which could be derived from satellite, AIS, and undersea-cable data as outlined in the conclusion below, to host Track 2 dialogues without the diplomatic authority that is official government engagement, and to educate the next generation of analysts who will be able to interpret satellite, AIS, and undersea-cable data in an integrated manner. Supporting this indigenous analytical capability would help diminish the reliance of the IOR states on threat assessments generated largely by outsiders outside the region by commercial intelligence providers, and help littoral states establish their own standards for suspicious versus routine ISR activities in their own choke points.

## 8. Conclusions

The authors of this article have proposed that the classical security dilemma theorized by Jervis (1978) and later extended to maritime environments such as the Indian Ocean by others like Beckerman (2022), Slayton (2017), and Edwards et al. (2015) is particularly pronounced at maritime choke points due to the interplay between the low attributability and dual-use nature of satellite ISR, AIS, and undersea cable infrastructure and the geographic concentration of strategic value found in narrow straits. The Strait of Hormuz case demonstrates how this dilemma exacerbates the active kinetic conflict; the Bab-el-Mandeb case illustrates how it can be used to exploit a non-state actor against a diffuse commercial enemy; and the Strait of Malacca case illustrates how it can grow in a stealth manner between two great powers without being noticed until a crisis occurs. Both

times, the core analytical conclusion is the same: It's not the amount of ISR capability that leads to instability, it's the failure to reliably separate its defense from its attack. Structural solutions to this challenge of digital security must go beyond purely hardware-based thinking about maritime security and create governance structures, standards for data integrity and norms of transparency to differentiate defensive from offensive ISR postures not in words but in action.

There is a need for future research to expand this framework empirically by systematically collecting and collating incident level data on AIS anomalies and cable disruption incidents in the Indian Ocean choke points, preferably using an exclusive IOR region-wide database provided by IOR research institutions and not from outsourcing the information to extra-regional commercial providers of risk intelligence. Any such research should also investigate the ability of new technologies, such as quantum-resistant satellite communications, blockchain-verified AIS reporting and multilateral cable-monitoring sensor networks, to meaningfully decrease the friction for attribution identified in this analysis as the main driver of escalatory risk and determine if the largely latent Sino-Indian cable-monitoring security dilemma in the Strait of Malacca is following a more aggressive trajectory like the one seen at the Strait of Hormuz and in the Taiwan Strait. As ISR increasingly becomes a critical factor for states in the Indian Ocean in terms of both understanding and contestation, the choke points that have been crucial to Indian Ocean geopolitics over the centuries will likely continue to provide the most piercing lens on the contestation.

## REFERENCES

- Amar Kumar, & Chandrashekhar. (2025). From Hormuz to Malacca: India's strategic arc against China's string of pearls. *International Journal of World Politics*, 2(2), 15–35. [https://doi.org/10.34218/IJWP\\_02\\_02\\_002](https://doi.org/10.34218/IJWP_02_02_002)
- Badawi, H. (2025). China's string of pearls strategy: Asserting maritime dominance in the Indian Ocean. *International Journal of Politics and Security*, 7(1). <https://doi.org/10.53451/ijps.1401481>
- Beckerman, C. E. (2022). Is there a cyber security dilemma? *Journal of Cybersecurity*, 8(1), Article tyac012. <https://doi.org/10.1093/cybsec/tyac012>
- Bueger, C., & Edmunds, T. (2026). Satellites, AI and information-sharing platforms for the maritime domain: Have new technologies revolutionized maritime security? *International Affairs*. <https://doi.org/10.1093/ia/iia037>
- Comprehensive maritime domain awareness (CMDA) in the Indian Ocean region. (2022). Indian Aerospace and Defence News. <https://iadnews.in/comprehensive-maritime-domain-awareness-cmda-in-the-indian-ocean-region/>
- Critical undersea infrastructures: A framework to address threats in a post-physical context. (2026). *Georgetown Journal of International Affairs*. <https://gjia.georgetown.edu/conflict-security/critical-undersea-infrastructures-a-framework-to-address-threats-in-a-post-physical-context/>
- Cult of the cyber offensive: Misperceptions of the cyber offense/defense balance. (2020). *Yale Journal of International Affairs*, 15(1). <https://www.yalejournal.org/publications/cult-of-the-cyber-offensive-misperceptions-of-the-cyber-offensedefense-balance>
- Cyber posturing and the offense-defense balance. (2013). *Journal of Strategic Studies*. <https://doi.org/10.1080/13523260.2013.771031>
- Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2015). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences*, 112(3), 2825–2830.

- India reinforces maritime domain awareness but challenges remain. (n.d.). Center for International Maritime Security (CIMSEC). <https://cimsec.org/india-reinforces-maritime-domain-awareness-challenges-remain/>
- India's counter strategic response to China's 'string of pearls' in the Indian Ocean: An analysis from the Belt and Road Initiative (BRI) perspectives. (2026). ResearchGate. <https://www.researchgate.net/publication/403320357>
- Indian Ocean: Exploring maritime domain awareness. (n.d.). Institute of Peace and Conflict Studies (IPCS). [http://www.ipcs.org/comm\\_select.php?articleNo=4825](http://www.ipcs.org/comm_select.php?articleNo=4825)
- Intelligence, surveillance, and reconnaissance (ISR) for global maritime security. (2026). ResearchGate. <https://www.researchgate.net/publication/400936431>
- Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, 30(2), 167–214. <https://doi.org/10.2307/2009958>
- Lethal attacks show strengthened Houthi control over Red Sea transit. (2025). The Washington Institute for Near East Policy. <https://www.washingtoninstitute.org/policy-analysis/lethal-attacks-show-strengthened-houthi-control-over-red-sea-transit>
- Maritime domain awareness in India: Shifting paradigms. (2021). National Maritime Foundation. <https://maritimeindia.org/maritime-domain-awareness-in-india-shifting-paradigms/>
- Maritime security update: Gulf Region / Strait of Hormuz and Red Sea. (n.d.). Skuld. <https://www.skuld.com/topics/port/port-news/asia/maritime-security-update-gulf-region-strait-of-hormuz-and-red-sea/>
- Navigating the string of pearls. (2025). Leeds Policy Institute. <https://www.leedspolicyinstitute.org.uk/post/navigating-the-string-of-pearls>
- Orbital militarization and India's maritime security: From surveillance to strategic response. (n.d.). CESCUBE. <https://www.cescube.com/vp-orbital-militarization-and-india-s-maritime-security-from-surveillance-to-strategic-response>
- Roshan, H. (2025). The great game at sea: An analysis of the Sino-Indian strategic competition in the Indian Ocean. IMPRI India. <https://www.impriindia.com/insights/sino-indian-strategic-competition/>
- Security dilemma. (2026). In *Wikipedia*. [https://en.wikipedia.org/wiki/Security\\_dilemma](https://en.wikipedia.org/wiki/Security_dilemma)
- Security risks impacting global shipping – November 2025. (2026). ISS Shipping. <https://www.iss-shipping.com/security-risks-impacting-global-shipping-nov-2025/>
- Ship operators shrugging off Houthi attacks. (2025). The Washington Institute for Near East Policy. <https://www.washingtoninstitute.org/policy-analysis/ship-operators-shrugging-houthi-attacks>
- Ships transiting the Red Sea try to avoid attacks via AIS messages. (2025). SAFETY4SEA. <https://safety4sea.com/ships-transiting-the-red-sea-try-to-avoid-attacks-via-ais-messages/>
- Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, 41(3), 72–109. [https://doi.org/10.1162/ISEC\\_a\\_00267](https://doi.org/10.1162/ISEC_a_00267)
- String of pearls (Indian Ocean). (2026). In *Wikipedia*. [https://en.wikipedia.org/wiki/String\\_of\\_Pearls\\_\(Indian\\_Ocean\)](https://en.wikipedia.org/wiki/String_of_Pearls_(Indian_Ocean))
- Submarine cable security at risk amid geopolitical tensions & limited repair capabilities. (2025). Recorded Future, Insikt Group. <https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats>

- Taiwan strengthens patrols against China's undersea cable sabotage. (2025). Indo-Pacific Defense FORUM. <https://ipdefenseforum.com/2025/09/taiwan-strengthens-patrols-against-chinas-undersea-cable-sabotage/>
- Testimony before the U.S.-China Economic and Security Review Commission. (2026). U.S.-China Economic and Security Review Commission. [https://www.uscc.gov/sites/default/files/2026-03/Jason\\_Hsu\\_Testimony.pdf](https://www.uscc.gov/sites/default/files/2026-03/Jason_Hsu_Testimony.pdf)
- Truman National Security Project. (2025). When the lights went dark in Penghu: Why Taiwan should employ SMART cables for strategic defense. <https://www.trumanproject.org/truman-view-blog/when-the-lights-went-dark-in-penghu-why-taiwan-should-employ-smart-cables-for-strategic-defense>
- Under sea cables: Veiled threats in hybrid warfare. (n.d.). Global South Forum. <https://www.globalsouthforum.org/article/under-sea-cables-veiled-threats-in-hybrid-warfare>
- When does competition become conflict? Technology, geography, and the offense-defense balance. (2021). *Journal of Global Security Studies*, 6(4), Article ogab007. <https://doi.org/10.1093/jogss/ogab007>

