

## SITUATIONAL REPORTS

# China's Floating SIGINT Network: What the COSCO Espionage Allegations Mean for India

Author: CNAWS Research Team • Published: September 02, 2026 • Source: Centre for New Age Warfare Studies



## EXECUTIVE BRIEF & KEY FINDINGS

A Reuters investigation published on 1 September 2026 has brought renewed attention to one of the least visible dimensions of China's maritime power. Citing two senior U.S. administration officials, Reuters reported that Chinese state-owned shipping giant COSCO has allegedly operated concealed signals intelligence equipment aboard commercial vessels to collect military communications and other electromagnetic data while sailing near foreign coastlines. According to the officials, the arrangement has existed for decades and allows Beijing to gather information on military communications technologies, encryption developments, vessels, aircraft and strategically important maritime routes across parts of Asia, Europe and North America. China has rejected the allegations as baseless, while COSCO has not publicly responded to the specific claims. The significance of the disclosure extends well beyond COSCO. If the U.S. assessment is substantially correct, it indicates that China's enormous commercial maritime footprint may constitute not simply a logistics reserve for the People's Liberation Army, but a geographically dispersed intelligence collection architecture. Merchant vessels offer Beijing something that dedicated intelligence ships cannot easily replicate. They move routinely through foreign ports and strategic waterways, remain at sea continuously, attract comparatively little security attention and can repeatedly approach areas of military significance under the normal cover of international commerce. For India, the immediate concern is not that every COSCO vessel should now be regarded as an intelligence ship. There is no public evidence supporting such a conclusion. Nor has the U.S. assessment publicly identified India as a specific target of the alleged programme. The larger concern is structural. COSCO maintains extensive commercial access to India and the wider Indian Ocean, while Chinese research vessels, fishing fleets, commercial shipping

*networks and overseas port interests already provide Beijing with multiple potential sources of maritime information. When viewed collectively, these assets could allow China to construct a persistent electronic and maritime picture of the Indian Ocean without maintaining a conspicuous fleet of dedicated surveillance vessels. CNAWS assesses with high confidence that China possesses the organisational, legal and technical foundations to exploit civilian maritime platforms in support of national security objectives. CNAWS assesses with moderate confidence that merchant shipping is increasingly being incorporated into overseas intelligence and surveillance activity. The scale of the alleged COSCO SIGINT programme, the number of equipped vessels and whether Indian military targets have been directly collected remain unknown from publicly available evidence.*

## The Disclosure

Reuters reported that U.S. officials believe COSCO vessels carry what they described as sophisticated SIGINT collection equipment rather than ordinary navigation or communications hardware. The systems allegedly intercept signals associated with military vessels and aircraft and collect information relevant to communications technology and encryption development. The collected material is reportedly used to improve maritime reconnaissance, provide early warning concerning foreign military targets and strengthen Beijing's situational awareness along important maritime routes.

The distinction between ordinary shipboard electronics and purpose-built intelligence equipment is critical. Modern merchant ships already possess radar, satellite communications, AIS receivers, navigation systems and other electronic equipment. The U.S. allegation is therefore not simply that China is exploiting data naturally generated during commercial operations. It is that specialised systems have allegedly been deliberately installed for intelligence collection.

Reuters did not identify individual vessels, disclose the technical characteristics of the equipment or provide evidence allowing independent verification of the U.S. assessment. This limitation should remain central to any analysis. The revelation therefore constitutes a significant intelligence allegation rather than independently proven evidence of a fleet-wide COSCO espionage programme.

Nevertheless, the allegation does not appear in isolation. In April 2025, the China Maritime Studies Institute at the U.S. Naval War College published a detailed assessment of intelligence specialists within China's maritime militia. The study concluded that intelligence collection is a core mission for parts of the militia and identified dedicated maritime reconnaissance units and so-called information boats used to report maritime activity to PLA-linked authorities. More importantly for the COSCO case, the report noted that PLA analysts have argued for exploiting the latent ISR capacity of China's distant-water fishing fleet and Chinese-owned or operated merchant vessels overseas. Its author assessed that such activity was likely already occurring. The Reuters disclosure therefore potentially represents the transition from a previously identified Chinese doctrinal proposition into a more systematic operational capability.

---

## Why COSCO Matters

COSCO is not simply another shipping company. Its importance derives from the extraordinary geographic scale of its operations. COSCO SHIPPING Lines reported that by May 2026 it and its affiliated Orient Overseas Container Line operated approximately 596 container vessels with combined capacity of around 3.6 million TEU. Its network covered 419 shipping routes and called at 663 ports across 146 countries and regions. COSCO SHIPPING Ports separately reported that it operated or managed 387 berths across 40 ports at the end of 2025.

No intelligence service could economically reproduce such geographic access using dedicated intelligence vessels. A commercial vessel can spend weeks moving through strategically significant waters without creating the political signalling associated with the deployment of a PLAN reconnaissance ship. It can transit narrow waterways, approach major ports, remain alongside commercial terminals and revisit the same locations according to predictable shipping schedules. Hundreds of vessels collectively provide something more valuable than an occasional surveillance mission. They provide persistence.

The intelligence value would not necessarily depend upon penetrating encrypted military communications. Passive collection of the electromagnetic environment itself can reveal important information. Repeated observations can identify when particular emitters become active, characterise radar and communications signatures, reveal changes in operating procedures, establish normal patterns of activity and identify deviations from those patterns.

Over a sufficiently long period, such collection contributes to what intelligence professionals describe as an electronic order of battle and a pattern-of-life picture. During a crisis, deviations from the established baseline can become indicators of mobilisation or operational preparation. The real value of merchant-based SIGINT is therefore accumulation. One commercial ship passing an Indian Ocean coastline may collect little of strategic significance. Hundreds of voyages over several years could potentially produce an entirely different intelligence product.

---

## **Civilian Cover as a Feature of Chinese Maritime Strategy**

The alleged COSCO programme should also be examined against China's broader concept of civil-military integration. China's National Intelligence Law states that organisations and citizens shall support, assist and cooperate with national intelligence work in accordance with law. The legislation also authorises Chinese intelligence organisations to conduct intelligence activities outside China through necessary methods and channels. This legal framework does not prove that a particular Chinese company conducts espionage abroad, but it significantly differs from systems in which commercial entities operate at greater institutional distance from state intelligence organisations.

China's National Defense Law similarly requires enterprises and organisations to support national defence requirements and provides mechanisms through which transportation infrastructure and other civilian resources can support military requirements. China's National Defense Transportation Law explicitly promotes military-civil integration in transportation and provides for mobilisation and requisition of civilian transportation resources when necessary.

The U.S. Department of Defense added COSCO-related entities to its Section 1260H list of Chinese military companies in January 2025. The Pentagon describes the list as part of its effort to identify companies contributing to China's Military-Civil Fusion strategy.

More revealing is the evolution of Chinese naval thinking itself. An analysis published by the U.S. Naval Institute in May 2026 examined a January 2025 article by officers from China's Naval Command College discussing the application of Mao's concept of People's War to future far-seas conflict. The Chinese authors reportedly envisaged commercial shipping, distant-water fishing vessels, research ships and other civilian maritime platforms as potential instruments supporting military operations outside China's immediate maritime periphery. Civilian platforms were portrayed as mechanisms through which China could establish presence before a conflict and increase the operational reach of the PLAN.

Taken together, these developments suggest that the military utility of China's civilian maritime sector is neither accidental nor limited to wartime logistics. It is increasingly embedded within Chinese thinking about maritime power.

---

## From Merchant Fleet to Distributed Maritime ISR

The most important analytical question arising from the COSCO disclosure is whether China is constructing a distributed maritime intelligence architecture rather than relying primarily upon traditional reconnaissance platforms.

Several existing components support such an interpretation. China's maritime militia already performs surveillance and reconnaissance functions in its near seas. The 2025 Pentagon assessment describes militia personnel and commercial maritime organisations being trained and mobilised to support the PLAN and China Coast Guard. In wartime, the militia may contribute reconnaissance, logistics and other forms of support. Chinese research vessels perform another function. Their oceanographic and hydrographic work can produce data useful for submarine and anti-submarine operations. CSIS research identified 64 active Chinese research and survey vessels during a four-year assessment period and found 13 operating in the Indian Ocean. All 13 displayed organisational connections or behaviours that raised dual-use concerns. Research ships have collected information concerning currents, water conditions and seabed characteristics, all of which have potential military applications in undersea warfare.

Commercial shipping could add the electromagnetic layer. Research vessels can map the physical ocean. Fishing and militia vessels can provide local maritime awareness. Merchant vessels can potentially collect electronic signatures while moving through global trade routes. Chinese-owned or operated ports can provide logistics access and information concerning commercial maritime movements. PLAN vessels and space-based systems can provide higher-end military surveillance.

Individually these systems are very different. Collectively they could produce a multi-layered maritime intelligence network. This is the more consequential interpretation of the COSCO disclosure. The issue is therefore not whether China has created thousands of disguised spy ships. Such a characterisation would exaggerate what is currently known. The more credible possibility is that Beijing has identified selected civilian platforms, routes, companies and personnel that can provide intelligence opportunities when those opportunities align with wider strategic requirements. That model would be cheaper, less visible and much more scalable.

---

## Why the Indian Ocean Matters

The Indian Ocean is particularly suited to this model. China's economy remains heavily dependent upon maritime trade moving through the Indian Ocean and onward through the Strait of Malacca and other passages into the western Pacific. At the same time, the PLAN has expanded its operational presence from anti-piracy deployments in the Gulf of Aden into increasingly regular activity across the wider Indian Ocean.

Yet China remains geographically disadvantaged in the region. India occupies a central position within the northern Indian Ocean, while the Andaman and Nicobar Islands sit near approaches connecting the Indian Ocean with Southeast Asia. Beijing therefore has strong incentives to improve its maritime domain awareness across a region where its naval forces operate far from mainland bases.

Chinese research activity already demonstrates sustained interest in the Indian Ocean operating environment. CSIS found that Chinese research vessels have conducted extensive oceanographic missions across the region. The Xiang Yang Hong 06, for example, undertook a lengthy Indian Ocean expedition involving underwater gliders and profiling floats, while other Chinese research vessels have operated around Sri Lanka and elsewhere in the eastern Indian Ocean. CSIS concluded that information generated by these missions could assist future PLAN submarine operations.

Commercial vessels offer a complementary advantage because they do not need special diplomatic arrangements merely to traverse international shipping routes. A container vessel does not have to request permission to perform an

ordinary commercial voyage through international waters. Unless suspicious equipment or behaviour is detected, its presence may attract little attention.

This creates an intelligence opportunity fundamentally different from that presented by a dedicated Chinese research vessel or surveillance ship whose movement is immediately monitored by regional governments.

---

## **The India Exposure**

COSCO already has a substantial commercial presence in India. COSCO SHIPPING Lines India states that it has operated in the country for around 25 years, with offices in Mumbai, New Delhi, Chennai, Kolkata, Cochin and Tuticorin, and that it provides worldwide container connectivity through 18 services from major Indian ports. Company schedules published during 2026 show services involving Mundra, Hazira and Nhava Sheva on the western coast as well as Chennai and Visakhapatnam in the east.

This should not be interpreted as evidence that COSCO vessels operating from Indian ports are collecting intelligence. It does, however, demonstrate the level of routine maritime access available to the company. If even a relatively small fraction of vessels in a global merchant fleet were equipped for passive intelligence collection, commercially legitimate voyages could place those sensors repeatedly within useful collection range of military activity across multiple countries.

For India, five categories of information could be particularly valuable to a sophisticated foreign collector. The first is the electromagnetic signature of coastal and maritime surveillance systems. Radars and communication networks possess identifiable operating characteristics even when the content of communications remains inaccessible. The second is military pattern-of-life information. Changes in the frequency and intensity of maritime or aviation communications may indicate exercises, deployments, readiness changes or unusual operational activity. The third is platform identification. Long-term collection can associate particular electronic signatures with classes of ships, aircraft or other systems. The fourth is communications architecture. A collector does not necessarily need to decrypt a message to learn something useful. Transmission timing, frequency behaviour, network relationships and changes in communications procedures can themselves provide intelligence. The fifth is crisis warning. Once a foreign intelligence service understands what normal activity looks like, unusual electromagnetic activity may help identify military preparations before they become visually obvious.

This means India's vulnerability must be understood cumulatively rather than through individual port calls. A foreign merchant ship does not need to penetrate an Indian naval facility to obtain useful information. Repeated passive observation from normal maritime routes may be sufficient to build a progressively richer picture of the electronic environment.

---

## **A Potential India-Pakistan Dimension**

The western Indian Ocean creates an additional consideration. Chinese commercial shipping networks connect Indian ports with ports across the Gulf, Pakistan, East Africa and Southeast Asia. China also possesses a deeply institutionalised defence relationship with Pakistan, while Gwadar and the China-Pakistan Economic Corridor give Beijing substantial strategic interests along the Arabian Sea.

There is presently no public evidence demonstrating that intelligence allegedly collected by COSCO vessels around India has been transferred to Pakistan. Nevertheless, any Chinese improvement in understanding Indian maritime communications, electronic signatures or operating patterns would possess potential military relevance during an India-China contingency. Depending upon future political circumstances and intelligence-sharing arrangements, portions of

such situational awareness could also indirectly benefit Pakistan.

India should therefore view the issue primarily as a Chinese intelligence challenge rather than automatically describing it as a China-Pakistan joint operation. Conflating the two without evidence would weaken the analytical case.

---

## **What the Disclosure Does Not Prove**

Several limitations are important. The Reuters report does not demonstrate that the entire COSCO fleet carries SIGINT systems. It does not identify the vessels allegedly involved. It does not establish that India is an active collection target. It does not establish that COSCO port investments are themselves intelligence facilities. It also does not demonstrate that Beijing can decrypt modern military communications simply by intercepting them.

These distinctions matter. SIGINT encompasses much more than reading encrypted messages. Signals can reveal platform identities, network structures, operating patterns, technical characteristics and indicators of unusual activity even when their content remains inaccessible.

The intelligence threat is therefore credible without assuming extraordinary Chinese cryptographic capabilities. At the same time, the commercial model has limitations. Merchant ships travel according to commercial requirements rather than intelligence priorities. Their routes are predictable. Equipment can potentially be detected. Crew knowledge and operational security may vary. Host governments can inspect vessels and introduce counterintelligence measures. Using commercial shipping for espionage also carries significant political and economic consequences if exposed. The system should therefore be understood as a supplement to China's dedicated intelligence architecture rather than a replacement for it.

---

## **Indian Response Priorities**

### **1. Treat high-risk commercial maritime platforms as counterintelligence objects**

India does not need to presume that Chinese commercial vessels are hostile. It does need a risk-based system for identifying vessels whose ownership, equipment configuration, operating behaviour or previous movements justify enhanced scrutiny. Commercial status should not automatically exclude a vessel from counterintelligence assessment.

### **2. Expand electromagnetic monitoring around strategic maritime approaches**

India should maintain detailed baselines of the radio-frequency environment around strategically important coastal areas and investigate unexplained collection systems or unusual emissions associated with foreign vessels. Such monitoring should involve the Indian Navy, Coast Guard, intelligence community and specialised technical agencies.

### **3. Integrate commercial shipping into Maritime Domain Awareness**

Traditional maritime surveillance focuses heavily on warships, research vessels and anomalous fishing activity. The COSCO disclosure indicates that merchant shipping requires greater analytical attention. Vessel identity, ownership networks, port-call histories, route changes, unusual loitering and equipment modifications should feed into the wider maritime picture. India's Information Fusion Centre Indian Ocean Region provides a useful institutional foundation for expanding this approach with regional partners.

### **4. Strengthen port security screening**

Foreign merchant vessels already undergo regulatory and security processes. Intelligence-risk screening should increasingly include unexplained antenna arrays, non-standard electronic systems and equipment inconsistent with legitimate commercial requirements. Such inspections need to remain legally grounded and intelligence-led to avoid disrupting normal maritime commerce.

## **5. Harden communications discipline**

The most effective response to passive collection remains reducing exploitable information. Strong encryption alone is insufficient if operating patterns, unnecessary emissions or predictable communications behaviour reveal valuable metadata. Communications security, emission discipline and periodic red-team assessments should form part of maritime readiness.

## **6. Build a regional counterintelligence picture**

China's maritime presence cannot be assessed from Indian waters alone. Information sharing with Indian Ocean partners concerning suspicious vessel behaviour, research missions and unusual port activity would allow patterns to emerge that may remain invisible when incidents are examined individually.

---

## **Strategic Assessment**

The September 2026 COSCO disclosure should not be viewed merely as another allegation of Chinese espionage. Its importance lies in what it potentially reveals about the architecture of Chinese maritime power.

For decades, assessments of China's naval expansion have focused primarily on the number of PLAN destroyers, frigates, submarines and aircraft carriers entering service. That approach captures only the visible component of China's maritime capability. China possesses another maritime resource that few states can replicate at comparable scale. It has one of the world's largest commercial shipping systems, an enormous distant-water fishing fleet, the world's largest research-vessel ecosystem, extensive port investments, a maritime militia and an expanding blue-water navy.

China's strategic advantage may lie in connecting these systems. The Reuters allegations suggest that commercial shipping could contribute an electromagnetic intelligence layer to this architecture. Research vessels can improve understanding of the physical ocean. Maritime militia and fishing vessels can increase surface awareness. Commercial vessels can potentially sample the electronic environment. Overseas ports can sustain commercial and potentially military activity. Dedicated military and space-based systems can fuse higher-quality intelligence with information generated by these civilian networks.

The result would not necessarily resemble a traditional intelligence fleet. It would resemble a distributed sensor network hidden within normal maritime activity. For India, this represents an uncomfortable counterintelligence problem because the northern Indian Ocean is simultaneously a strategic military space and one of the world's busiest commercial maritime environments. Attempting to exclude Chinese commercial shipping entirely would impose substantial economic costs and would be neither practical nor necessary. Ignoring the intelligence potential of those platforms would be equally unwise.

India therefore requires a distinction between commercial access and strategic trust. Chinese merchant vessels should continue to be treated according to international maritime and commercial law. At the same time, the assumption that a civilian hull necessarily performs only civilian functions is increasingly difficult to sustain in the context of China's Military-Civil Fusion system. The most important lesson from the COSCO allegations is therefore not that every Chinese container vessel should be regarded as a spy ship. It is that in China's emerging model of maritime power, the

distinction between the merchant fleet, the intelligence network and the naval reserve may become increasingly conditional. For India, understanding that convergence will be essential to maintaining maritime information superiority in the Indian Ocean.

*The immediate threat from the reported COSCO programme remains moderate but potentially significant, because the scale and geographic distribution of specialised collection equipment remain unknown. The longer-term structural threat is high. If Beijing succeeds in integrating selected commercial shipping, research vessels, maritime militia, overseas infrastructure and military sensors into a common intelligence architecture, China could acquire persistent maritime awareness across areas where continuous deployment of dedicated PLAN surveillance platforms would otherwise be expensive, conspicuous and politically difficult. The Indian response should therefore focus less on searching for individual "spy ships" and more on identifying the network that connects civilian presence with military intelligence requirements. That network, rather than any single COSCO vessel, is the real strategic issue exposed by the September 2026 disclosure.*