By: Josephine Pau

Regionalising Maritime Domain Awareness in Southeast Asia

Introduction

China's grey zone tactics in the South China Sea recast the nature of confrontation in the South China Sea, the world's most contested region. Southeast Asian states risk losing invisible battles should they fail to develop more robust and integrated Maritime Domain Awareness (MDA) capabilities at the coastal, surface and sub-sea level. Their pursuit of this capacity is a delicate balancing act between developing indigenous capabilities and choosing between the plenitude of external actors that can provide technology at varying political costs. This article progresses in three parts 1) providing a cursory summary of the PLAN's (People's Liberation Army Navy) grey zone tactics in the South China Sea and Maritime Domain Awareness as an aspect of maritime security, 2) outlining present barriers in partnership and regional initiatives and finally; 3) identifying avenues for progression towards an independent and robust MDA landscape in Southeast Asia. Keeping in mind non-traditional and military threats that drive the maritime landscape, Southeast Asian states should approach the build-up of MDA capacity with mind towards an organised regional front, building up some national capacity within a shared script of good governance and increasing trust-building measures, rather than purporting an overtly militarised narrative in the maritime domain.

Grey-zone tactics and Maritime Domain Awareness

Grey zone tactics are defined as "coercive" geopolitical, economic military, cyber and information operatons activities that surpass regular diplomatic means but fall short of the threshold of kinetic military force (Rand Project Air Force, n.d.). China deploys it as a means of projecting its power in the South China Sea as a means of corroding the rules based order rather than towards specific military objectives (Green et al., 2026) explicitly employing it as 'military operations other than war'. In Southeast Asia, this means exploiting technological and political vulnerabilities. Chinese grey zone activity can coincide with military activity with other actors outside of ASEAN to intimidate and signal disapproval. In projecting its naval power, furthermore, it reasserts its proclaimed economic power as well as military might. For example, in an effort to enforce Chinese claims to exclusive fishing rights in the area, the PLAN sank a Philippine fishing vessel at Reed Bank in 2019 (Mclaughlin, 2022). Southeast Asian states are particularly vulnerable to these tactics, moreso than extra-regional actors like Japan (Rand Project Air Force, n.d.), and it can be assumed that their weakness in this front will invite further Chinese activity and covert antagonism.

Just as ASEAN's inability to define gray zone tactics in its own terms constrains its ability to develop a comprehensive plan to counter it, there has been no forthcoming regional conception of MDA. ASEAN hence faces both problem and solution definition challenges. MDA was a framework initiated by the United States in response to the bombing of the USS Cole in 2000 and September 11, 2001 attacks (RSIS, 2019). Though some analysts attribute fears of its adoption as a term in ASEAN doctrine to an avoidance of US dominated frameworks (D0, 2024), the term has since been adopted by other states and international organisations such as the International Maritime Organisation which defines it as "the effective understanding of anything associated with the maritime domain that could impact security, safety, the economy or marine environment" (International Maritime Organisation, n.d.) . In a security context, it generally entails fusing data from maritime vessel tracking, including Automatic Identification Systems (AIS), radar, satellite patrol and intelligence sources (Frenkel, 2026). It also relies on manned patrol aircrafts and surface vessels. Attribution difficulties in the maritime domain can be compared to that of the field of cybersecurity – attribution must be ascertained with limited information as a result of the inherent uncertainty (Bentham, 2025), and so publicly naming is no longer an establishment of objective fact but a political decision. The ability to detect a threat is constrained by technology, but the act of attribution is an inherently political one, where states can decide to name-and-shame or simply counter the threat and stay silent on an incursion or breach. Malaysia, for instance, has largely kept to the latter strategy, whereas states such as the Philippines take on a more vocal stance (McLaughlin, 2022) towards Chinese incursions on its EEZ.

ASEAN's weakness to grey zone tactics (and by extension, weaknesses in MDA) are two-fold. One is an infrastructural weakness, and the other is a strategic lack of regional coordination, in part enabled by the downfalls of the former but also political disparities.

Ang and Chong (2026) visualise MDA capabilities as a "linked-chain" wherein the first level is a level of data awareness enabled by sensors, satellite imagery and traditional AIS. The second stage enables fusion and interoperability, defining whether data can be correlated with sufficient confidence to enable action. The third stage is accelerated decision-cycle speed, enabling the translation of cues into timely operation response. The final stage is sustainability and retention of skills; it focuses on the ability of states to retain expertise and credible analytics.

Necessarily acting on conflict avoidance, Southeast Asian states cannot provide punishment deterrence, and must hence rely on denial deterrence (Irsyad, 2025), hinged on the detection and interception of ships. This fundamental level is still unfulfilled in some states; Malaysia still faces inability to consistently detect, identify and track illegal fishing vessels as a result of limited resources and vast EEZs (Leong, 2025). Traditional detection has hinged heavily on Automatic Identification Systems (AIS), but China's militia vessels disable AIS systems or turn to short range transmitters to complicate geolocation (Do, 2023). This increases the mandate for space-assisted detection, which allows for frequent snapshots of vessels. Currently, the Philippines, Indonesia and Vietnam participate in either QUAD initiated Initiative for Indo-Pacific Maritime Domain Awareness (IPMDA)'s or EU based IORIS (which potentially integrates satellite systems), while other states lag behind. Two challenges emerge from this, the first being that there is unequal takeup amongst ASEAN nations, and the second being that IORIS and IPMDA lack interoperability at the moment. Beyond data collection technology, ASEAN states face an 'AI-Gap', fall behind on technologies required to integrate and make operable the big data received from collection systems. As Chong and Ang (2026) rightly argue, MDA effectiveness today is measured moreso by ability to make timely decisions, and AI platforms enable decision-cycle

speed, producing cues that operators can act more decisively on. Indonesia deploys an AI-driven maritime surveillance network to monitor IUU activity, in cooperation with SRT Marine systems (Digital Watch Observatory, 2025) , but states like Vietnam and Philippines do not yet have the capacity to use advanced analysis tools (The Maureen and Mike Mansfield Foundation, 2023).

Critical Undersea Infrastructure (CUI) must also be consciously accounted for in an ASEAN-MDA strategy. The centrality of undersea cables to livelihoods and connectivity have drawn ASEAN attention, but regional cooperation has centred around expansion and repair (Davenport, 2024) rather than threat or sabotage detection. Repair ships are an economic practicality since undersea cables can be damaged by dropped anchors or natural wear and tear, but the threat of political sabotage is not a foreign concept, especially taking note of incidents in the Baltic Sea since 2023. Cable cutting operations would result in crippling economic losses and direct pains to the average citizen, making their protection a strategic imperative.

As Ang and Sanglee (2026) argue, technological catch-up must be accompanied by the development of stronger institutional foundations. ASEAN lacks a common understanding of MDA, Its conceptual clarity within Chinese doctrine contrasts starkly with Southeast Asia's murky conception of the tactics, with some states lacking a definition of it in domestic law, to say less of the regional level.

Extra-regional partnerships

The European Union, US and QUAD have been key partners in providing the technology to plug detection level gaps in ASEAN state MDA strategies (Do, 2024). EU provided Critical Maritime Routes Indian Ocean Program ii (CRIMARIO) offers IORIS, a web-based platform that accumulates data from AIS and Skylight AI, potentially integrating Copernicus Satellite data and radio frequency data. The EU has thus far invited Indonesia, the Philippines and Vietnam to adopt it, yet take up in Vietnam is slow (Tran, 2023).

Similarly, the QUAD's Indo-Pacific Partnership for Maritime Domain Awareness (IPMDA), announced in 2022, integrates radio frequency and satellite data from the US's Hawkeye360 satellites into web-based sea vision systems. These systems have however remained 'dormant due to diplomatic challenges surrounding the integration…of diverse maritime domain awareness systems'. One such issue is Southeast Asia's use of Russian hardware (Do, 2024). As it stands, the IPMDA reflects some sensitivity to ASEAN state sovereignty conundrums, offering near real time monitoring tool and using "common operating picture" frameworks that do not require deep data sharing (Basu, 2025).

State actors also offer MDA development options. Japan provided the Philippines with coast guard vessels via its Official Security Assistance (OSA) program, and Canada indicated support using its Dark Vessel Detection Program to support anti- Illegal Unregulated Unregistered (IUU) fishing tasks (Do, 2024). One analyst (Laird, 2025) points out the US attempts to export Task Force 59 as a template to ASEAN, as an operational model that would create a "digital ocean" with AI-enabled unmanned surface vessels carrying cameras that transmit images and data via cloud, enabling frequent snapshots. It would utilise unmanned surface vehicles, unmanned underwater vehicles (UUVs) and unmanned aerial vehicles (UAVs), making it a cost-effective option, but its effectiveness ultimately relies on ASEAN states ability to ensure that the mesh network is resilient towards Chinese intervention.

Given the bevy of options, ASEAN states risk operational complexity (as some states adopt both IPMDA and IORIS systems despite their incompatibility). At a regional level, the adoption of different systems by different states may also impede joint efforts. Political disalignments also form a barrier to technological adoption, where the Philippines already relies on US satellite technology, Thailand signed a Memorandum of Understanding with Huawei to develop smart ports (Rahman, 2025).

Regional Level Cooperatives and Avenues for Progression

Experts are united in highlighting the need for a shared approach: MDA must be dealt in a collective, multilateral way, and doing so would reduce the negative externalities created from differing technological levels (RSIS, 2019; The Maureen and Mike Mansfield Foundation, 2023). Regional level initiatives provide promising beginnings but are hampered by a lack of trust –though cooperation and data-sharing is a powerful imperative in building robust and comprehensive MDA systems (RSIS, 2019) ASEAN states remain wary of information sharing initiatives.

The Trilateral Cooperative Agreement is one of the 'minilateral' security initiatives that have seen success managing transnational challenges in Eastern Sabah and the Sulu-Celebes Sea between Malaysia, Indonesia and the Philippines. The Information Fusion Centre (IFC), based in SIngapore, also links maritime responders in the Indo-Pacific, providing coordinating capacity. IFC provides a platform to develop trust between states as an information hub that provides human connections between international liaison officers (ILO) to tackle non-traditional security issues such as piracy and humanitarian cases (Ang and Sanglee, 2026) , exchanging information at a level lower than official complaint. The IFC is also well positioned to provide a monitoring role for CUI protection (Chan and Lim, 2026). The Southeast Asia Cooperating and Training (SEACAT) maritime exercises can provide a complementary platform to practice cooperation between ASEAN member states on information sharing protocols (Gatdula, 2025).

Do (2023) argues that where information sharing is ultimately a constraining factor, it should begin on a voluntary basis. Prioritised activity should focus on non-traditional security goals rather than militarised objectives, given the ability of ASEAN to agree on non-traditional security as a common threat in contrast to the hedging strategy towards militarised China. Infrastructure to build up local data management hence becomes the keystone to a broader maritime domain awareness strategy. This presents ASEAN with an opportunity to build ground up connections, especially through the first level of IUU fishing, widely regarded as a non-traditional security threat.

Initiatives at a state level have involved upgrading national capacity via procurement, but procurement patterns and sources have demonstrated a rift between states as well. Malaysia ordered three turkish-built ada class warships for deployment near the strategically contested borneo waters, and the philippines attained new corvettes from south korea, enhancing surface fleet capacity. Singapore also recently purchased Gulfstream G550 surveillance aircrafts (Sato, 2026). In contrast, Cambodia's acquisition of advanced type-056 frigates illustrate how overlapping claims over fisheries and energy sources in the Gulf of Thailand have intersected with political realities.

Cybersecurity capacity, including the preservation of undersea cables must also be strengthened to ensure durability of any MDA strategy. In 2025, ASEAN Defence Ministers' Retreat included the

proposal of a paper exploring military cooperation to secure CUI. This necessarily also includes private actors that are stakeholders in cable management. Traditional cybersecurity should also be strengthened as state-backed actors could complicate AIS identification or infect a vessel's operational technology system with malware (Rahman, 2025).

Conclusion

Where the land divides, the sea unites. Maritime governance and security provides an opportunity for ASEAN as an institution to display common strength, as it did in its backing for UNCLOS and for governance of non-traditional security issues such as the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia ReCAAP which dealt with piracy. Basing MDA initiatives in non-traditional security issues and building trust via institutions and gradual information sharing would enable stronger coordination between states in the future, but the region needs a framework that suits the realities of southeast asian states. It would provide a means of ASEAN states hedging behaviour by using ASEAN centrality as a guiding framework for their MDA decisions, and signal to external actors that in the maritime domain the region faces common challenges and a shared future.

References:

Ang, Eric, and De Xian Chong. "IP26010 | Closing the Gap: AI-Enabled Maritime Domain Awareness in Southeast Asia." *RSIS*, January 15, 2026. https://rsis.edu.sg/rsis-publication/idss/ip26010-closing-the-gap-ai-enabled-maritime-domain-awareness-in-southeast-asia/.

Ang, Eric, and Tita Sanglee. "Human networks anchor maritime security in the Indo-Pacific." *East Asia Forum*, January 27, 2026. https://eastasiaforum.org/2026/01/27/human-networks-anchor-maritime-security-in-the-indo-pacific/.

Basu, Pratnashree. "Why Maritime Surveillance in the Indo-Pacific Starts With Trust Before Data." Lowy Institute, August 21, 2025. Accessed April 29, 2026. https://www.lowyinstitute.org/the-interpreter/why-maritime-surveillance-indo-pacific-starts-trust-data.

Bentham, Jonathan. "Subsea advances and challenges for the Asia-Pacific." International Institute for Strategic Studies, May 16, 2025. Accessed April 29, 2026. https://www.iiss.org/online-analysis/online-analysis/2025/05/subsea-advances-and-challenges-for-the-asia-pacific/.

Chan, Jane, and Nicholas Lim. "IP26039 | Protecting Critical Undersea Infrastructure: Accelerating the Momentum in ASEAN." *RSIS*, March 11, 2026. https://rsis.edu.sg/rsis-publication/idss/ip26039-protecting-critical-undersea-infrastructure-accelerating-the-momentum-in-asean/.

Davenport, Tara Maria. "The Protection of Submarine Cables in Southeast Asia: The Security Gap and Challenges and Opportunities for Regional Cooperation." *Marine Policy* 171 (October 17, 2024): 106435. https://doi.org/10.1016/j.marpol.2024.106435.

Do, Hoang. "How to Help ASEAN Address South China Sea 'Gray-zone' Challenges." *Nghiên Cứu Biển Đông*, September 25, 2023. https://en.nghiencuubiendong.vn/how-to-help-asean-address-south-china-sea-gray-zone-challenges.56476.anews.

———. "Popular MDA Initiatives and Implications for ASEAN." Daniel K. Inouye Asia-Pacific Center for Security Studies, February 2, 2024. Accessed April 29, 2026. https://dkiapcss.edu/nexus_articles/popular-mda-initiatives-and-implications-for-asean/#_ftn2.

Frenkel, Omer. "Maritime Domain Awareness: Countering Hidden Threats." Cognyte, April 27, 2026. https://www.cognyte.com/blog/maritime-domain-awareness/.

Gatdula, Julia Rocio. "Closing the Undersea Surveillance Gap in Southeast Asia | CSIS." CSIS, September 11, 2025. Accessed April 29, 2026. https://www.csis.org/blogs/new-perspectives-asia/closing-undersea-surveillance-gap-southeast-asia.

Green, Michael J., John Schaus, Jake Douglas, Kathleen H. Hicks, and Zack Cooper. "Countering Coercion in Maritime Asia," March 5, 2026. https://www.csis.org/analysis/countering-coercion-maritime-asia.

Irsyad, M. Raihan. "China's Grey-Zone Tactics Are Reshaping the South China Sea." Modern Diplomacy, December 2, 2025.

https://moderndiplomacy.eu/2025/12/02/chinas-grey-zone-tactics-are-reshaping-the-south-china-sea/.
Laird, Robbin. “Secretary of War Hegseth’S Maritime Domain Awareness Proposal for the South China Sea.” Defense.info, November 14, 2025. https://defense.info/maritime-dynamics/2025/11/secretary-of-war-hegseths-maritime-domain-awareness-proposal-for-the-south-china-sea/.
Leong, Phang Kok. “Securing Malaysia’s Maritime Environment Using Space-Derived Services.” *Contemporary Issues in Air and Space Power* 3, no. 1 (January 1, 2025): bp42323989. https://doi.org/10.58930/bp42323989.
“Maritime Domain Awareness,” n.d. https://www.imo.org/en/ourwork/security/pages/maritime-domain-awareness.aspx.
Maritime Security Programme, Institute of Defence and Strategic Studies (IDSS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. “MARITIME DOMAIN AWARENESS (MDA) Event Report.” Edited by Collin Koh, January 24, 2019. https://rsis.edu.sg/wp-content/uploads/2019/04/ER190425_Maritime-Domain-Awareness.pdf.
McLaughlin, Rob. “The Law of the Sea and PRC Gray-Zone Operations in the South China Sea.” *American Journal of International Law* 116, no. 4 (October 1, 2022): 821–35. https://doi.org/10.1017/ajil.2022.49.
Digital Watch Observatory. “New AI Surveillance System to Monitor Indonesia’s Seas | Digital Watch Observatory,” August 29, 2025. https://dig.watch/updates/new-ai-surveillance-system-to-monitor-indonesias-seas.
Rahman, M. Faizal Bin Abdul. “Geopolitics Meet Digital Security in ASEAN’s Maritime Domain.” Modern Diplomacy, April 16, 2025. https://moderndiplomacy.eu/2025/04/16/geopolitics-meet-digital-security-in-aseans-maritime-domain/.
RAND Project Air Force. “A New Framework for Understanding and Countering China’s Gray Zone Tactics.” Report. *RESEARCH BRIEF*, n.d. https://www.rand.org/content/dam/rand/pubs/research_briefs/RBA500/RBA594-1/RAND_RBA594-1.pdf.
Sato, Daisuke. “Singapore buys Gulfstream G550 surveillance aircraft for maritime security.” *Defence Blog*, February 27, 2026. https://defence-blog.com/singapore-buys-gulfstream-g550-surveillance-aircraft-for-maritime-security/.
The Maureen and Mike Mansfield Foundation. “Policies for Maritime Domain Awareness & Space Technology.” *The Maureen and Mike Mansfield Foundation*, October 25, 2023. Accessed April 29, 2026. https://mansfieldfdn.org/blog/policy-recommendations-for-maritime-domain-awareness-and-space-technology/.
Tran, Bich. “2023/96 ‘Vietnam’s Quest for Enhanced Maritime Domain Awareness’ by Bich Tran,” December 8, 2023. https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2023-96-vietnams-quest-for-enhanced-maritime-domain-awareness-by-bich-tran.