DKI APCSS SECURITY NEXUS

The DKI APCSS journal for comprehensive security issues throughout the Indo-Pacific region and the world!

Security Nexus Perspective

Cognitive Domain Awareness: A Framework for Partners Already Inside the Cognitive War

By Deon Canyon

Executive Summary

The Indo-Pacific is not approaching a cognitive war. It is already inside one. China's systematic cognitive operations, grounded in People's Liberation Army political warfare doctrine and operationally integrated with economic and diplomatic coercion, are actively targeting the perceptions, decisions, and alliance relationships of regional partners. Taiwan faces coordinated disinformation across every election cycle. Philippines confronts manipulated maritime narratives designed to undermine domestic support for sovereign rights. Pacific Island states are subject to influence operations that condition how entire populations interpret their relationships with great powers. These operations succeed because the region lacks shared awareness of what is happening and coordinated capacity to respond. Cognitive Domain Awareness offers one structured solution, adapting the proven detect-share-assess-act logic of Maritime Domain Awareness to the information environment. It is not a prescription. It is a framework that partners already in the fight can adapt, build on, and own.

Introduction: We Are Already at War

If you are a defense analyst in Manila reviewing footage of Chinese vessels surrounding Ayungin Shoal, a security official in Taipei watching synthetic video of fabricated military incidents circulate on Line during election week, a policymaker in Port Moresby fielding questions about infrastructure projects whose terms were not fully understood when they were signed, or an intelligence officer in

Canberra tracking coordinated inauthentic behavior targeting Pacific partnerships, you are not preparing for a cognitive war. You are already in one.

The People's Republic of China has conducted sustained, systematic cognitive operations across the Indo-Pacific for over a decade. These operations do not announce themselves. They work through manipulated perceptions, eroded trust, delayed decisions, and fractured coalitions. Their objective is not to win a debate. It is to prevent agreement from forming, to raise the cognitive cost of coordinated response until paralysis becomes the default outcome.

This paper is written for the people inside that reality. It does not offer a universal solution. What it offers is a structured framework, Cognitive Domain Awareness (CDA), for understanding what is happening, why it keeps working, and what realistic response options exist for actors operating with real constraints in a contested region. CDA is one approach among several that may help partners develop more strategic, coherent, and self-determined responses to the cognitive war they are already fighting.

I. What Is Being Done to Us: China's Cognitive Operations in the Indo-Pacific

Understanding the exact nature of the threat is a prerequisite for any effective response. China's cognitive operations in the Indo-Pacific are not improvised or opportunistic. They are doctrinally grounded, institutionally resourced, and operationally integrated with economic, diplomatic, and military instruments of statecraft.

Doctrinal Foundation

The People's Liberation Army's political warfare doctrine, formalized through the concept of the Three Warfares (san zhong zhanfa), institutionalizes public opinion warfare, psychological warfare, and legal warfare as coordinated strategic instruments. First articulated in the 2003 amendment to the PLA's Political Work Regulations, the Three Warfares doctrine directs the use of media, law, and psychological pressure to shape adversary perceptions and constrain their decision space before and during conflict. The United Front Work Department, operating under direct Party authority, extends these operations into diaspora communities, academic institutions, media ecosystems, and political networks across the region.

This is not propaganda as the objective is not to persuade audiences toward a particular view. The intent is to condition the informational environment so that opposition becomes harder to organize, alliance commitments appear less reliable, and the costs of resistance, political, economic, and reputational, appear to outweigh the costs of accommodation.

Documented Operations

The operational record is specific and substantial. In Taiwan, China's cognitive operations have been documented across multiple election cycles. During the 2024 presidential election, the PRC deployed coordinated disinformation campaigns across Line, Facebook, and YouTube targeting candidate credibility, fabricating policy positions, and amplifying domestic social divisions. Networks of inauthentic accounts conducted coordinated amplification of Beijing-aligned narratives, with some campaigns showing evidence of coordination with PRC state media. Synthetic video depicting fabricated military incidents was circulated to generate public anxiety about the prospect of conflict. The intent was not to determine the election outcome but to exhaust Taiwan's institutional capacity for distinguishing truth from manipulation.

China's cognitive operations in Philippines support its maritime coercion campaign in the South China Sea. Manipulated video footage was presented as evidence to reframe incidents at Ayungin Shoal, Segunda Thomas Shoal, and Scarborough Shoal, casting Philippine maritime officials as provocateurs rather than defenders of sovereign rights. Social media analysis identified multiple networks of Philippine-language accounts amplifying pro-Beijing maritime narratives, some with direct links to Chinese diplomatic and state media infrastructure. The objective is to complicate Manila's domestic politics, weaken public support for assertive maritime postures, and fracture the alliance signaling value of joint operations with partners.

In Pacific Islands, China's systematic cognitive operations work through a different mechanism. Economic dependency created through Belt and Road infrastructure financing is accompanied by narrative conditioning, framing Chinese engagement as development partnership and Western engagement as neocolonial interference. Following the 2022 security agreement with Solomon Islands, coordinated messaging across social media and through Chinese state media affiliates normalized the agreement domestically and delegitimized regional concern. In Papua New Guinea, Fiji, Vanuatu, and elsewhere, influence operations have targeted political elites , using incentives to shape policy positions and regional security frameworks.

Across the region, a consistent pattern emerges. Cognitive operations do not work alone. They are synchronized with economic leverage, diplomatic pressure, and where relevant, military posturing. The cognitive operation sets the conditions and the other instruments exploit them.

Why It Keeps Working

China's cognitive operations succeed not because they are technically sophisticated, though they are increasingly so, but because they exploit structural vulnerabilities that are common across the region. These include information ecosystems with limited institutional capacity for rapid verification; political environments where elite capture and economic dependency reduce incentives to publicly attribute and counter manipulation; alliance relationships where coordination lag creates windows of opportunity for adversary exploitation; and domestic audiences whose trust in government institutions is already contested, making them receptive to narratives that confirm existing skepticism and bias.

The most important condition is the absence of shared awareness. When partners do not have a common picture of what cognitive operations are underway, who is conducting them, and what effects they are achieving, each actor is left to interpret events through its own frame, which is precisely the condition China's cognitive operations are designed to create and sustain.

II. Cognitive Domain Awareness: A Framework Built on Proven Precedent

Building shared awareness of a complex, distributed, fast-moving threat environment is not easy. The maritime domain faced a similar problem in the 1990s. How do sovereign states with different capabilities, legal frameworks, and strategic interests build a common operational picture of activity across a vast, ungoverned space? The answer was Maritime Domain Awareness (MDA), which became foundational to Indo-Pacific security cooperation.

CDA draws directly on MDA's logic. Just as MDA provides shared understanding of maritime activity through a detect-share-assess-act cycle, CDA would enable coalitions to identify cognitive operations as they emerge, attribute them to probable actors, share that understanding across partners, and coordinate responses. The analogy is not perfect. Information is not a ship, and the cognitive domain does not yield to physical interdiction. But the core institutional insight transfers: shared awareness, built through agreed protocols and trusted networks, is the precondition for coordinated action.

Where the analogy requires care is in three areas. First, attribution in the cognitive domain rarely achieves the certainty possible with physical vessels. Partners must develop shared standards for acting on probabilistic assessments rather than waiting for certainty that adversaries will deliberately deny. Second, the cognitive domain is partially constituted by democratic freedoms, free press, open social media, political contestation, that cannot be managed out of existence without destroying what the framework is designed to protect. Responses must work within these constraints, not around them. Third, the speed of cognitive operations exceeds maritime incident timelines significantly; detection-to-response cycles measured in hours matter in ways that maritime equivalents measured in days do not.

With these qualifications acknowledged, the detect-share-assess-act cycle provides a practical structure for how to build cognitive domain awareness under real-world constraints.

Detect: Knowing What Is Happening

Detection begins with the recognition that cognitive operations leave observable traces. Coordinated inauthentic behavior produces statistical anomalies in posting patterns and network amplification. Synthetic media carries forensic signatures, including inconsistent lighting, unnatural audio signals, and temporal artifacts that trained analysis can identify. Narrative campaigns that originate from state-adjacent sources show linguistic and framing patterns that distinguish them from organic public discourse.

For most partners in the region, the immediate detection challenge is not technical sophistication but capacity, the ability to monitor the information environment systematically and distinguish signal from noise at operationally relevant speed. Taiwan's civic-tech ecosystem (Cofacts, g0v, the Taiwan FactCheck Center) demonstrates that detection capacity can be distributed across civil society rather than concentrated in government institutions. They build resilience that is harder to suppress and more contextually sensitive to local language and culture. The Philippine Coast Guard's systematic documentation of maritime incidents created authenticated chains of custody for visual evidence, which demonstrated that detection methodology can be institutionalized even under resource constraints. These are not perfect systems, but they are functional starting points that regional partners can learn from and adapt.

Share: Building Common Pictures

Detection without sharing produces awareness that is isolated rather than collective. The value of CDA to any individual partner scales with the number and quality of other partners contributing to and drawing from a shared picture. This is the force multiplication argument for coalition cognitive awareness, and for smaller partners with limited independent detection capacity, it is the most compelling reason to invest in the framework.

Sharing requires agreed protocols: common schemas for classifying and communicating cognitive threats, trusted liaison channels, and tiered access arrangements that allow information to flow at appropriate classification levels without exposing sensitive sources and methods. NATO's Rapid Reaction Mechanism and StratCom Centre of Excellence in Riga demonstrate both the value and the friction of alliance-level cognitive information sharing. Intelligence sharing proved effective during the 2022 Russia-Ukraine period, while coordinated public messaging proved slower and more contested. The lesson for Indo-Pacific partners is that sharing architecture needs to be built before the crisis, not assembled during it.

For smaller partners, participation in sharing networks provides leverage that they cannot generate. When Manila shares evidence of Chinese maritime operations with Washington, Canberra, and Tokyo, it converts tactical documentation into strategic coalition signaling. When Pacific Island states share observations of influence operation patterns with regional partners, they contribute to a distributed picture that no single actor could assemble alone. The architecture that makes this sharing systematic rather than *ad hoc* is what CDA provides.

Assess: Understanding What It Means

Raw detection data requires analytical interpretation to become actionable. Assessment involves correlating detection signals across sources, technical forensics, open-source monitoring, intelligence reporting, and partner contributions, to distinguish isolated incidents from coordinated campaigns, establish probable attribution, estimate operational intent, and model likely effects on target audiences and decision-making processes.

Assessment is where the cognitive domain diverges sharply from MDA. Assessing the intent and effect of a cognitive operation requires expertise that spans technical forensics, behavioral psychology, communications theory, strategic intelligence, and deep cultural and linguistic knowledge of the target environment. This is a difficult analytical challenge, and the workforce required to do it well does not currently exist at scale in most regional partner institutions.

Two implications follow. First, assessment is the area where coalition burden-sharing has the most immediate value, with partners contributing complementary expertise to shared analytical products that none could produce independently. Second, assessment standards need to be calibrated to the policy environment. Partners need frameworks for acting on probabilistic attribution rather than waiting for certainty, with agreed thresholds that balance the risk of false attribution against the cost of delayed response.

Act: Responding Coherently

The action layer is where the democratic dilemma becomes most acute. The most effective responses to cognitive operations, rapid public attribution, coordinated messaging, platform enforcement, all require institutional capacities and political will that vary significantly across regional partners, and all carry risks of overreach that partners must manage carefully.

The Philippines has demonstrated that transparency-as-strategy can be powerful even for resource-constrained actors. Systematic public release of authenticated maritime evidence has converted tactical documentation into strategic deterrence, compelling China to escalate the sophistication of its manipulation in response, which is itself a form of operational success. Estonia's institutionalization of cognitive defense as a continuous government function, rather than a crisis response, demonstrates that small states can build durable resilience through sustained investment in digital infrastructure and public education.

For the region, options range from preemptive exposure, publicly attributing and debunking manipulation before it achieves viral spread, to coordinated partner statements backed by shared evidence-based products, to platform engagement based on validated coalition alerts. None of these require authoritarian information control. They require investment, coordination, and political will to name what is happening and respond to it credibly.

III. What This Looks Like in Practice: Institutional Options for Regional Partners

The question most relevant to partners inside the cognitive war is not whether CDA is theoretically sound but what it looks like as an operational reality given their specific circumstances. Three institutional pathways merit consideration, each with distinct trade-offs.

The Fusion Center Pathway

MDA's most successful institutional expression was the dedicated fusion center, Singapore's Information Fusion Centre and India's IFC-IOR being well-developed regional examples, providing 24/7 monitoring, multi-source integration, and coalition interface functions. A cognitive equivalent would provide continuous watch of cognitive threat indicators, correlation of technical and intelligence sources into a common operating picture, attribution coordination across partners, and liaison functions connecting national capabilities.

The trade-offs are real. Dedicated centers require resourcing, raise sovereignty questions about what information is shared and how it is controlled, and involve political negotiation about mandate and location. For partners with less resources and bandwidth, the risk is that CDA becomes underfunded. An alternative is to build cognitive awareness functions into existing structures, cyber fusion centers, intelligence fusion mechanisms, strategic communications, accepting the risk of reduced prioritization in exchange for lower institutional overhead.

The Framework Pathway

Rather than new institutions, partners may invest in frameworks, standards, protocols, and norms, that enable coordination without requiring bureaucratic structures. Common provenance marking protocols for government communications, shared alert classification schemas, pre-established crisis coordination procedures, and regional norm development through multilateral forums like the East Asia Summit or ASEAN Defence Ministers' Meeting Plus all represent investments that create coordination without requiring new institutions.

The limitation is enforcement. Frameworks depend on voluntary compliance and may not hold under crisis pressure when political incentives diverge. They work best as a complement to, not a substitute for, some degree of institutional backing.

The Distributed Network Pathway

A distributed approach leverages existing national capabilities through lightweight coordination mechanisms, working groups, information exchanges, and tabletop exercises, enabling sharing without requiring integrated command structures. Partners choose engagement levels based on specific issues and threat environments, with modular participation allowing different coalition configurations to form around different problems.

For Indo-Pacific partners navigating relationships with both the United States and China, the distributed model's flexibility is an advantage. Participation does not require alignment. Partners can contribute to and draw from CDA networks at levels calibrated to their circumstances. The corresponding limitation is speed: distributed coordination is slower than centralized response, and cognitive operations are designed to exploit exactly that lag.

The Democratic Constraint as Design Parameter

Whichever institutional pathway partners pursue, the democratic governance constraint must be treated as a design parameter rather than an obstacle. Cognitive defense mechanisms that concentrate information control, expand surveillance infrastructure, or enable government override of media and platform content will, rightly, face legitimacy challenges in democratic societies. They will also be exploited by adversaries who will use them as evidence that democratic governments are no different from authoritarian ones.

The most effective cognitive defense tools for democratic societies are not surveillance and control but transparency and resilience. Authenticating official government communications so that fabricated alternatives face credibility barriers. Investing in public digital literacy so that citizens are harder to manipulate. Building civic-tech infrastructure that distributes detection capacity across society. Establishing fast, credible, evidence-based response protocols that can be deployed before false narratives solidify. None of these require sacrificing democratic norms. All of them require sustained institutional investment and political commitment.

IV. What We Need to Do Together: The Coalition Imperative

No regional partner can build effective cognitive domain awareness alone. The threat is transnational, the required expertise is distributed, the information sources are too vast for any single actor to monitor comprehensively, and the deterrent effect of attribution and exposure scales with the number and credibility of partners standing behind it. Rather than being optional, a coalition approach is a structural requirement for CDA to work.

This has specific implications for how partners think about the value of regional security architecture. Mechanisms like the Quad, Five Eyes, AUKUS, and bilateral alliance frameworks increasingly need cognitive domain functions built into their operating architecture, not as add-ons but as core capabilities. The question of how to extend cognitive awareness cooperation to ASEAN partners, Pacific Island states, and other regional actors who face significant cognitive threat exposure but possess limited technical capacity is one of the most important practical challenges facing the coalition.

Capacity asymmetry is real and requires honest engagement. Japan, Australia, South Korea, and the United States possess technical and institutional capabilities that most regional partners do not. Building a genuinely useful coalition cognitive awareness architecture means investing in capacity transfer, forensic tools, analytical training, and institutional design support, that enables smaller partners to contribute meaningfully rather than simply receive. A coalition in which some partners only consume and never contribute is not sustainable and will not generate the distributed resilience the region needs.

The comparative cases examined in this paper, Taiwan's civic-tech model, Estonia's digital infrastructure approach, NATO's alliance coordination experience, and the Philippines' transparency strategy, all demonstrate that effective cognitive defense is achievable across a range of resource levels and institutional contexts. They also demonstrate that no single model is universally applicable. What works in Taiwan's specific threat environment and civil society context requires adaptation before it transfers to Fiji or Bangladesh or Sri Lanka. Coalition cognitive awareness must be designed with that diversity in mind.

Conclusion: A Framework for Strategic Agency

The cognitive war in the Indo-Pacific is not a future threat. It is the present condition in which regional partners are making decisions, managing alliances, and attempting to protect their populations and sovereign interests. China's cognitive operations are sophisticated, doctrinally grounded, and operationally integrated with the full suite of its strategic instruments. They are working, in part, because the region has not yet developed the shared awareness and coordinated response capacity that would make them significantly more costly to conduct.

Cognitive Domain Awareness will not end that war. No single framework will. What it offers is something more achievable and more immediately valuable: a structured basis for understanding what is happening, building shared pictures across partners, interpreting the operational significance of cognitive threats, and coordinating responses that are credible, legitimate, and proportionate.

The partners most exposed to cognitive operations in this region, Taiwan, the Philippines, Pacific Island states, Southeast Asian nations navigating great-power competition, are not passive victims of a contest happening above them. They are strategic agents with real constraints, genuine capabilities, and the most direct stake in developing effective responses. This framework is offered in that spirit: not as a solution delivered from outside but as a tool that partners inside the cognitive war can adapt, challenge, and build on in ways that serve their own strategic circumstances.

The cognitive domain is now a battleground. The question is not whether to engage it but how to do so with enough coherence, coordination, and clarity to make engagement meaningful. CDA is one answer to that question. The conversation about what works, and what does not, needs to happen urgently, across the region, among the partners who are already in the fight.

The views expressed in this article are those of the author and do not reflect the official policy or position of DKI APCSS, the Department of War, or the U.S. Government. The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense (DoD) of the linked websites, or the information, products, or services contained therein. DoD does not exercise any editorial, security, or other control over the information you may find at these sites.

March 2026