RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No. 014 – 14 February 2023

No. 014/2023 dated 14 February 2023

Technology Providers and Maritime Security Roles in Southeast Asia

Jeffrey Payne

SYNOPSIS

Technology providers are driving an innovation wave to deliver unprecedented volumes of relatively high-quality information to Southeast Asia's maritime security community. This is a game changer for maritime domain awareness, enhancing the community's ability to make positive decisions. However, ***JEFFREY PAYNE*** *notes that technology providers do not answer maritime security challenges, and users have tough decisions ahead in taking advantage of technology solutions to build better order at sea.*

COMMENTARY

Technology Provider Interests in Maritime Security

The maritime community is benefitting from a wave of technological innovation. Most of the technologies being integrated into the community are retools of existing applications, but a growing number of private technology providers are developing maritime-specific technologies. The interests of these providers in the maritime domain are defined by the varied missions and aims of the stakeholders whom they serve. Yet, regardless of whether they build automated platforms or develop algorithms for data correlation, each of these actors is in the business of information and share in the common purpose of expanding the volume of information available for maritime security.

Most technology providers in the maritime domain fall into one of three categories:

1. market-driven firms, whose interest is in serving customers willing to pay for their technologies and data offerings;

2. academic institutions whose scientific endeavours generate technology by-products with application for the maritime community; and
3. advocacy groups or NGOs that develop technology to address their own needs and, in turn, share the data obtained with the larger community of maritime professionals.

Taken as a whole, these institutions are a patchwork distinct from other elements of the maritime community, due to both their creative focus on data and the way they engage with other components of the larger community, such as governments and private sector shipping/logistics firms.

Private sector advancements in low earth orbit satellite imagery, for example, were primarily focused on terrestrial uses, and the maritime community found utility only in a limited data set pertaining to coastal waters. This situation is changing as shipping companies, logistical firms and governments request that the coverage of such satellites be expanded to include greater sea areas. Likewise, sensor technology and unmanned vehicle development have matured to now acquire maritime application because of private sector investment, academic experimentation and advocacy efforts. Furthermore, the application of artificial intelligence algorithms and telecommunication data expansion facilitated the insertion of qualitative data into the growing data sets now available to the maritime community.

Authorities, Rules and Norms Governing Providers

As technology providers are a disparate patchwork, there is no single authority or set of rules that specifically governs their operations, but providers are increasingly governed by commercial regulations, intellectual property regimes and national security laws. Market-driven providers are limited by the terms of the contracts they enter into with customers and local laws where agreements were signed, including any laws that prohibit technology transfers to third countries. For example, US-based firms that, individually or in partnership with US government institutions, enter into agreements with foreign governments must adhere to and are protected by laws like the National Technology Transfer and Advancement Act. NGOs and academic institutions must generally adhere to various regulations governing their work, but such regulations often provide more flexibility than those pertaining to market-driven firms.

Laws governing technology in ASEAN member states are less restrictive than those in Western states. But this state of affairs could change as such technologies take on a greater security dimension.

Providers and Threat Perception

In general, technology providers seek to diminish the scale of maritime threats. Whether by accumulating data that helps to chart safer courses for commercial vessels or to enhance responder efficacy during disaster relief operations, the aim is to make maritime security efforts more reliable and more efficient.

Based on their individual institutional focus or driven by the components of the technology they employ, providers routinely address a variety of maritime threats such as trafficking at sea, illegal, unreported and unregulated (IUU) fishing, illegal dumping,

and piracy. How these providers direct their technology towards maritime threats often depends upon their larger connections within the maritime community and on how the consumers of their technology define and prioritise threats.

Provider Contributions to Maritime Security

Technology providers expand the reliability and scale of information available to the maritime community. The data they deliver does one of three things:

1. provide greater clarity on how best to make maritime security operations more effective;
2. reveal gaps within maritime security efforts that help identify areas where enhancement is needed, whether by adopting new tools or amending current policy; and
3. provide more reliable data on deficiencies within security arrangements.

Technology can provide shocks to the system that warn stakeholders to rethink existing patterns and established tradition. Often, providers are affiliated with maritime domain awareness efforts, but this is just one means by which they contribute to maritime security.

Examples of how providers further maritime security include the US Naval Forces Central Command's Task Force 59, which, through a public-private partnership, employs a variety of technological tools to make the interdiction of illicit actors at sea more efficient. The Indo-Pacific Partnership for Maritime Domain Awareness (or IPMDA) – an undertaking of the Quad minilateral – leverages public-private partnerships to expand information sharing. The same is true of other national and regional maritime security-focused efforts throughout the Indo-Pacific and Southeast Asia. Still another example is how technology providers integrate themselves into various efforts designed to further maritime domain awareness. The data provided by these technology providers, whether through algorithmic analysis of compiled data or the creation of verifiable data from sensors, makes it easier for the maritime community to draw the attention of stakeholders not familiar with the maritime domain.

The US Navy's Task Force 59 integrates manned and unmanned systems for maritime operations. Such technology providers would be able to contribute their various maritime expertise to stakeholders who may not be familiar with the maritime domain. *Image from DVIDS.*

Provider Impact on Maritime Security

The expansion of technology provision for the maritime community is a game changer for maritime domain awareness. Compared to 20 years ago, the impact of technology is undeniable. But what is now a focal point of concern is the lack of connectivity among various technology providers, which continues to weigh down maritime security efforts. Providers, like much of the overall maritime community, often remain isolated from one another. Progress has been made, especially over the past 25 years, but structural connectivity still lags behind intent.

Technology does not solve problems of trust, but progress in the technological sector shows that trust is not the only factor in improving connectivity. As more data is accumulated, particularly from private sector actors, it is clear that maritime security threats affect multiple actors over large geographic areas. This makes conversations about information sharing less complicated.

Despite offering new opportunities for the larger community, technology providers create their own challenges in the collection of too much data and the protection of that data. The days of data shortages are quickly being replaced by a wealth of data from the private and public sectors. This can overwhelm maritime security services. How this challenge is addressed will be an ongoing debate among both providers and the larger maritime community. In addition, as new data systems become available and increasingly interconnected, the ability to isolate data sources becomes difficult, making institutions more vulnerable to cyber criminality.

Tools Used by Technology Providers

Technology providers do not directly answer maritime security challenges; their role is in providing tools for the community to better address the challenges. The tools vary and many have already been mentioned – low earth orbit imagery, sensor/buoy systems, unmanned platforms, and computational innovations. Added to this list are networking advancements, scientific experiments and telecommunication progress.

Provider Evolution

There is no doubt that the maritime domain is experiencing a transformative period due to technological innovation. Twenty years ago, the technological applications directed towards the maritime domain were in their infancy. Advances in computing and satellite design have since lowered the costs of acquiring low earth orbit imagery. What was once unaffordable to all but the wealthiest is now accessible to a much wider percentage of the maritime community. Maturation in sensors, buoys, and unmanned system design has likewise lowered the barriers to access such technologies. Today, hundreds of small and medium firms, research institutions and academies across the globe are actively developing technological, computational and exploratory products. It will be a matter of when, not if, ASEAN states become home to numerous technology providers.

Additional Context

Innovations in the past decade are providing more data than ever before, but innovation alone does not improve the security environment. How to use technology more seamlessly within existing operations, how to more readily share the data accumulated with others, and how to ensure that data remains reliable are the more critical questions. Technology providers already help shape the conversation on maritime security, and their future role will certainly grow.

Jeffrey PAYNE *is an Assistant Professor at the Near East South Asia (NESA) Center for Strategic Studies. The views presented here are the author's alone and do not reflect the policy or position of the NESA Center, the National Defense University, or the United States government. This IDSS Paper was commissioned by the Maritime Security Programme.*

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg