Tech-centric Partnership in the Indo-Pacific to Deter Digital Curtain

By

Abrar Rahman Namir

From Pakistan in the Indian Ocean to Kiribati in Oceania, a digital curtain is falling across the Indo-Pacific. Various actors are leveraging cyberspace and technological advancements to implement an alternative vision to a free and open Indo-Pacific—a direct affront to democracies and American strategic interests. It is reported that 77 percent of all known state-backed cyber operations emanate from China and its associates, while those attacks attempt to undermine societal institutions in countries such as Taiwan, Japan, Australia, and New Zealand, among others. These incidents reveal China's broader strategic vision, one that entails shaping the regional structure in its favor.

The digital Silk Road (DSR), China's initiative to invest in critical telecommunications and emerging technology in foreign countries, is a vehicle to lower the barriers to cyber coercion and propagate the digital curtain. By embedding its "model of technology-enabled authoritarianism" in recipient nations, Beijing seeks to shape the digital ecosystems of other countries in ways that serve its strategic interests. Such attempts call for a proactive and coordinated response from the United States and its regional partners—one that builds a resilient, tech-driven organization capable of countering China's digital expansion across the the Indo-Pacific.

The United States and China are engaged in a great power competition, one which has seeped into multiple theaters and domains. The Indo-Pacific region is generally understood to be the frontline of this contest.

However, China's burgeoning technological capacity has led to cyberspace being a critical juncture in this competition; one where traditional borders fade, thereby allowing the proliferation of gray zone tactics. Such tactics are deployed in various ways—infiltrating critical infrastructure, cyber espionage, and disinformation campaigns—on key democracies in the region.

Considering the geopolitical significance of the Indo-Pacific, China's attempts to use cyber coercion to cleave the region from the United States' sphere of influence highlights a calculated strategy by the Chinese Communist Party (CCP). The region is home to over 50 percent of the world's population, and 80 percent of global trade volume transits through its channels. It houses "seven of the world's largest militaries, and five American treaty allies."

Moreover, digital connectivity and internet adoption rates are the fastest growing compared to any region in the word, making it rife with opportunities and threats. These vulnerabilities not only indicate further volatility for regional governments but could also undermine American national security.

The list of cyber incidents already attributed to Chinese state-sponsored entities is extensive, and its targets are equally expansive. Advanced persistent threat (APT)—long-term, sophisticated, and entrenched cyber intrusions designed to hack, steal, and/or neutralize systems—have been a weapon of choice for those entities. For instance, APT-30 and APT-40, which targeted Association of South East Asian Nations (ASEAN) members and New Zealand's government, respectively, are reportedly linked to the Chinese government.

Furthermore, American intelligence and cybersecurity agencies recently confirmed that Volt Typhoon, a Chinese state-sponsored entity, compromised American critical infrastructure ranging from telecommunications to water systems; its reach even included US territories such as Guam.

While the specter of ATPs and digital intrusions have entered the purview of several governments in the Indo-Pacific region, individual efforts to deter those threats are futile. This is often due to strategic inertia, a shortage of specialized workers, and asymmetric capabilities.

A consolidated effort by the United States and its regional partners is needed to build consensus, direct resources, and establish a digital enforcement body. This could address those issues while mitigating any potential upheaval from China's tactics. Fortunately, the groundwork for such a partnership is already in place.

On July 1, 2025, the 10th Quad foreign ministers' meeting was hosted by US Secretary of State Marco Rubio, where he was joined by his counterparts from Japan, India, and Australia. It was the second such meeting since January, signifying the importance placed on the vision of the group by the Trump administration.

The measures agreed upon as a result are further evidence to that fact—initiatives to bolster maritime and transnational security, economic security, critical and emerging technology, among others. Therefore, the vast security mandates of those initiatives provide a viable path to constructing a techno-centric partnership while addressing the region's strategic, skills, and capabilities gaps when it comes to deterring China's digital incursions.

The decision to expand the Indo-Pacific Partnership for Maritime Domain Awareness (IPMDA)—a technology-focused initiative to augment the maritime security landscape—provides a practical foundation for a techno-centric partnership. Its stated goal of developing a "common operating picture" for the IPMDA could lead to the basis for a strategic consensus among potential members.

Furthermore, incorporating insights from the first Maritime Initiative for Training in the Indo-Pacific (MAITRI) workshop could assist in closing the skills gap for a regional digital workforce, further adding to the partnership's feasibility.

Additional features which could be utilized for the partnership and address the capabilities gap include the Quad Cyber Challenge and the Quad Partnership on Cable Connectivity and Resilience. The Cyber Challenge seeks to enhance the cyber ecosystem, digital awareness, and resourcing among member nations.

The Partnership on Cable Connectivity and Resilience, on the other hand, bears a more tactical responsibility of strengthening telecommunications infrastructure, specifically, undersea cables—arguably the most critical component of the digital ecosystem. Although these initiatives are focused on Quad member-nations, they could be expanded in a larger forum to engage ASEAN and Pacific subregional organizations such as the Pacific Island Forum, providing more opportunities for resource allocation.

There is institutional and strategic momentum behind the formation of a tech-centric partnership, not to mention the critical security imperative that exists. The broad consensus, coupled with the runway to take near-term action, makes this a prospective enterprise. Such concrete action is necessitated if the US and its regional allies expect to maintain a free and open Indo-Pacific and establish an active deterrent to China, which seeks to write the rules and draw the margins of the evolving digital age.

Abrar Rahman Namir is currently interning at Associated Universities and assisting in the Batteries and Energies to Advance Commercialization and National Security program as a supply chains and trade analyst.