

SPOTLIGHT:

The Pacific Cloud: Deterrence, Collaboration, & Security



Sponsored by

DELL
Technologies

The Pacific Cloud: Deterrence, Collaboration, & Security

The Great Power competition demands that the U.S. and its allies regain an advantage through secure networks built on cloud computing.

BY BARRY ROSENBERG, Contributing Editor, Technology & Special Projects



Guided missile destroyer USS Decatur arrives at Joint Base Pearl Harbor-Hickam (U.S. Navy photo).

U.S. military preparedness for the Great Power competition isn't going to just be about hardware like a new air missile defense system for Guam or joint training with allies at the Kwajalein Atoll in the Marshall Islands. It's also going to be about having secure networks, data-driven command and control, and artificial intelligence assets to defend U.S. interests and freedom of maneuver in the Indo-Pacific area of responsibility (AOR).

"The Indo-Pacific is the Department of Defense's priority theater," wrote former Acting Secretary of Defense Patrick Shanahan in the DoD's 2019 Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked Region.

Promotion of a networked region is one of three "enduring" U.S. commitments to stability and prosperity in the area, along with preparedness and partnerships. Wrote Shanahan: "The Department is strengthening and evolving U.S. alliances and partnerships into a networked security architecture to uphold the international rules-based order."

To make that a reality, many senior naval officers are calling for the U.S. to set in motion a "Pacific Deterrence Initiative" to compliment the multi-billion-dollar European Deterrence Initiative launched in 2014. Its goal would be to enhance the U.S. deterrence posture in the Indo-Pacific region, increase readiness

and responsiveness of U.S. forces, and to bolster the collective defense, capacity, and security of regional allies.

As a template for what that could look like, the Navy's Indo-Pacific Command (INDOPACOM) wrote its own assessment of how that would work in a 2020 report entitled *Regain the Advantage: U.S. Indo-Pacific Command's Investment Plan for Implementing the National Defense Strategy Fiscal Years 2022-2026*.

To strengthen allies and partners in the Indo-Pacific, "this includes a networked security architecture capable of deterring aggression, maintaining stability, responding to man-made and natural disasters, and ensuring free access to the sea, air, cyber, and space domains."

Investments on Secure Asia-Pacific Networks

INDOPACOM's AOR covers more of the globe than any of the other 10 geographic combatant commands. The region includes roughly half of the world's population and 24 of 36 global mega-cities (population >10 million). Vital to global commerce with 31 percent of the world's economy, this AOR includes the world's busiest international sea lanes, and 9 of the 10 largest ports.

Asia-Pacific is also a heavily militarized region, with 7 of the world's 10 largest standing militaries and 5 of the world's declared nuclear nations. The strategic complexity facing the region is both unique and evolving into an arguably more dangerous state than the U.S. is presently prepared for—especially in the area of cybersecurity where peer adversaries are heavily investing in ways to disrupt and infiltrate U.S. military networks.

"The state of the military networking in the Pacific today is that we're able to meet our challenges and respond to the contingencies that we have," said Randall Cieslak, executive director of Command, Control, Communications, and Cybersecurity for INDOPACOM, speaking during a recent Breaking Defense webcast. "The United States, though, doesn't have a monopoly on intellectual talent and a national workforce that can create innovative capabilities."

"It's a challenge to defend our networks from adversaries who understand technology and can use various ways to attack computing components and networks. We have to continuously create, protect, and enforce encryption and configuration management while engaging in standard hygiene and supply chain risk management so that our components can be trusted to use against adversaries such as China, Russia, and North Korea."

INDOPACOM's *Regain the Advantage* report says that a networked security architecture capable of deterring aggression, maintaining stability, responding to man-made and natural disasters, and ensuring free access to the sea, air, cyber, and space domains is vital to U.S. interests.

For example, one of the critical investments necessary to provide the command and control systems required to strengthen U.S. alliances and enhance partnerships in the region includes what it calls the Mission Partner Environment (MPE).



Randall Cieslak, Executive Director of Command, Control, Communications, and Cybersecurity for INDOPACOM.

"In order to compete across all domains, USINDOPACOM, allies, and partners must work from a more resilient, secure, adaptable, and interoperable architecture that supports multi-domain operations," states the report. "MPE is a critical investment that provides for resilient and redundant joint/multinational command and control."

MPE will provide ubiquitous management and automated engagement decision making by accessing a multi-domain sensor network that functions across all domains. This environment uses cloud-based technologies, integrated systems, and secure access controls to provide assured command, control, and communications.

In addition to MPE, another critical investment that INDOPACOM requests are for three "fusion centers:" a Counter Terrorism Information Facility; an Oceania Fusion Center; and an Indo-Pacific Maritime Coordination Center.

The report describes these fusion centers as making up a "resilient C2 infrastructure using MPE with contextual analytics and computing model assessments that generate inferences and illuminate patterns of life associated with transnational threats and other pernicious behavior."

Singapore and the U.S. are already working together multilaterally with five other ASEAN nations including Australia and New Zealand to establish a fusion center focused on information sharing for countering terrorism.

Cloud Computing in the Pacific AOR

Cloud computing is a key element in bringing network security and collaboration to the region, while enabling rapid adoption of new technologies to respond to emerging threats.

“Companies like Amazon and Microsoft are building cloud infrastructures with robust connectivity and processing capabilities,” said Cieslak. “The ability to use that commercial infrastructure, along with our defense infrastructure, can be used to orchestrate an environment for code, decision support tools, programs, software, and mission applications that can be accessed throughout the Pacific and across the world from seabed to space. This is important to our decision making and command of ships, aircraft, and logistics.”



*Vish Nandlall, Vice President
of Technology Strategy and
Ecosystems at Dell Technologies.*

The challenge of creating that infrastructure is what Cieslak called the “tyranny of distance” in the vast Pacific space and the challenge of operating in a denied, degraded, or disrupted communications environment.

Cloud computing can be a game changer in this respect, providing fast, shared access to many applications needed for battlespace

awareness and a common operating picture on the status of troops, vehicles, weapons, supplies, and missions. Within the cloud, all of this data can be tailored to a particular user’s access privileges.

“The only way to truly contend with the distance challenges associated with traditional cloud providers is to adopt a hybrid cloud strategy that views cloud as an operating model vs. a destination,” said Vish Nandlall, Vice President of Technology Strategy and Ecosystems at Dell Technologies. “This means cloud becomes a set of engineering principles and organization design to deliver agile services to edge cloud nodes in a federated deployment model vs. centralized. That advantage allows the mission to bring the compute and storage to the tactical

edge to mitigate the limitations and latency of the network in disadvantaged areas of the AOR.”

In addition, cloud is more suited to working in disrupted environments than traditional perimeter-based networks since it can be built with a far more distributed topology. In the Indo-Pacific region, for instance, that distributed topology might include a number of tactical clouds that are connected to central clouds that can then be interconnected through a Satcom link all the way back to home base. Or they might be connected through multiple, interim hubs through various countries that eventually lead to a large consolidated data center.

The key is to get to the right level of security for cloud applications.

“An area of concern as we migrate different services and applications to the cloud is understanding that we have to apply a different set of security principles to the cloud than we do to typical types of appliance-based architectures,” said Nandlall. “When you’re in a particular area that’s surrounded by four walls, your security perimeter typically mirrors the perimeter of those four walls. When you’re in the cloud, the security perimeters can be everywhere.”

Nandlall suggests that the DoD should move toward something that’s more on the order of the Zero Trust methodology, where there are layers of security down to individual resources and applications.

“We need to spend more time trying to understand what’s under the hood and how workloads are going to be placed in the cloud,” he said. “We need to ensure that we can have integrity of applications and can, in fact, control and restrict which applications are running in which cloud instances. We want to be able to bind specific platforms and virtual machines to applications so that we can create affinities given certain performance requirements.”

Controls are also needed on how much resources an application can consume, especially, for instance, if a cloud environment extends all the way to the edge in a constrained environment.

The challenges facing INDOPACOM in the Indo-Pacific region are immense, but cloud technology offers a way to effectively address and manage the information challenges, ensuring responsiveness and shared, collaborative tools for U.S. and allied warriors.