Department of War Strategic Evaluation Public Summary
Baselining Space and Cyber Security Cooperation with Domain-Emergent Allies and Partners (2024-2025)

Strategic evaluations of security cooperation (SC) programs are conducted pursuant to 10 U.S.C. § 383, which says the Secretary of War shall, "maintain a program of assessment, monitoring, and evaluation in support of the [SC] programs and activities of the [Department of War (DoW)]." The Office of the Deputy Assistant Secretary of War for Security Cooperation (ODASW(SC)) commissioned the RAND Corporation to evaluate DoW's security cooperation activities with domain-emergent allies and partners in the U.S. Indo-Pacific Command (USINDOPACOM) and U.S. Southern Command (USSOUTHCOM) areas of responsibility (AOR).

This summary provides unclassified primary findings and recommendations derived from RAND's evaluation. RAND defines domain-emergent nations as relative domain "novices" that are in the early stages of developing space and cyber programs and which have: 1) acknowledged the importance of space and cyber security to national security and collective defense; 2) pursued knowledge and technology in these domains, and potentially national strategies and policies; 3) begun developing organizations, doctrine, and infrastructure to support national space and/or cyber efforts; and 4) invested in advancing their space- or cyber-related capabilities, to include nascent satellite and cyber defense operations.

Enabling proper SC prioritization, planning, and allocation of resources requires careful consideration of how cooperating with maturing space and cyber allies and partners will drive achievement of U.S. strategic objectives as laid out in the administration's Interim National Defense Strategic Guidance, and forthcoming National Defense Strategy.

The evaluation addressed four questions:

1. What U.S. strategic imperatives drive DoW collaboration with domain-emergent allies and partners? What criteria should be considered?

2. What should be the focus of space and cyber SC with emerging allies and partners? What kinds of SC programs, initiatives, and activities could be considered?

3. How might these activities be applied in the context of the USINDOPACOM and USSOUTHCOM AORs?

4. How might application of criteria for space and cyber SC with emerging allies and partners, and increased integration of functional combatant command (CCMD) equities in CCMDs designated with a physical area of responsibility (hereinafter geographic CCMDs) SC processes better enable DoW's SC enterprise to meet strategic imperatives?

26-P-0556

RAND Recommendations.

Guidance, Prioritization, and Planning

- The Office of the Secretary of War should communicate U.S. strategic imperatives and priority partners in the space and cyber domain to U.S. Space Command, U.S. Cyber Command, and the geographic CCMDs.
- Space and cyber expertise should be included in Significant Security Cooperation Initiative planning. It is important to take stock of how CCMDs are organized to enable space and cyber engagement with partners in a way that can bring strategy, SC, and technical expertise together.
- DoW stakeholders utilize the evaluation framework for prioritization and planning.

Authorities and Resources

- Current authorities and funding sources do not fully meet requirements in a timely manner. For cyber and, to a lesser extent, space, the geographic CCMDs utilize Title 22, Operations & Maintenance funds, and commercial solutions to meet DoW and partner objectives.
- Geographic CCMDs should continue to build their non-DoW networks of providers for domain-emergent partners in both space and cyber. Such providers come from government, commercial, and academic sectors and from key U.S. allies.
- Prioritize lower-cost dual-use capabilities, particularly in space, to help ensure domain-emergent partners can sustain those capabilities.

Implementation and Assessment, Monitoring, and Evaluation

- DoW should review the cyber advisory position description, together with the State Department, to ensure that the advisors continue to play a key role in helping partners to reform their institutions to prevent duplication of efforts and avoid gaps.
- The DoW should consider implementing a pilot regional advisory program for both space and cyber to help economize resources.
- To improve DoW's efforts to assess, monitor, and evaluate the effectiveness of DoW security cooperation efforts, develop criteria to determine what shareable data is useful in both space and cyber.
- Baseline assessments are needed for domain-emergent partners in space to improve data sharing efforts from their partner assessments to enable targeted remediation.
- Allowing the General Security of Military Information Agreements to expire after a certain time or imposing time limits for some countries could create opportunities for re-assessment of partner capabilities and their willingness to secure their networks and protect sensitive data. The study did not assess how this measure could potentially disrupt partner activities.
- Align evaluation efforts with monitoring efforts by all geographic CCMDs, wherever possible.