Public Summary

Cyberspace Security Cooperation in the U.S. European Command Area of Responsibility

Strategic evaluations of security cooperation (SC) programs are conducted as required under section 10 U.S.C. 383, which says that the Secretary of War shall "maintain a program of assessment, monitoring, and evaluation in support of the security cooperation (SC) programs and activities" within the Department of War (DoW). The Office of the Deputy Assistant Secretary of War for Global Partnerships (ODASW(GP)) commissioned the National Defense Research Institute of the RAND Corporation, a Federally Funded Research and Development Center, to conduct an evaluation of cyberspace SC activities in the U.S. European Command (USEUCOM) area of responsibility (AOR). This summary provides an unclassified summary of the findings and recommendations of the report.

The evaluation sought to advance DoW's cyberspace SC with allies and partners by evaluating U.S. cyberspace SC activities and providing recommendations for improving the planning, execution, assessment, monitoring, and evaluation (AM&E) of those activities.

The report covered the evaluation of cyberspace SC for fiscal years 2018-2022 within three Balkan countries in the USEUCOM AOR to address the following research questions:

1. What are the strategic objectives and priority mission areas for cyberspace SC with these partner nations (PNs)?

2. How have implemented SC activities impacted PN capabilities and capacity?

3. How can the DoW improve the evaluation of cyberspace SC activities and plans?

Methodology. RAND employed a mixed-methods approach to conduct this research, integrating analysis of publicly available information, documents provided by various stakeholders, and the conduct of semi-structured interviews. The criteria for country selection encompassed identifying countries of varying cyber maturity levels that had a sufficient set of activities conducted under Title 10 U.S. Code.

Key Findings.

Planning. RAND found that cyberspace SC lacked the connective tissue between higher-level guidance and planning activities to tactical implementation. DoW planning for the examined countries did not fully account for PN's existing capabilities, maturity, and resources. Lack of cyberspace expertise at critical planning and programming points exacerbated this problem.

- RAND reviewed planning documents to identify the cyberspace SC objectives of each PN and found they frequently fell short of established best practices for goal setting, lacking the requisite specificity, achievability, relevancy, and time-bound parameters. These objectives were not measurable and, in some cases, too broad. The objectives for all three countries were identical, which also raised questions about whether they were sufficiently tailored to the needs of each PN.

Resources. DoW components often did not budget across multiple programs and budget types far in advance, nor with a sufficient degree of coordination between the PN, the implementing SC organization, the Combatant Commands, and the Defense Security Cooperation Agency.

- RAND found no evidence of resource constraints for cyberspace SC within USEUCOM. Personnel at all levels indicated funding was readily available for nearly any proposed program, citing cyberspace's high priority and relatively lower costs compared to traditional SC programs.

Execution and Assessment. Travel restrictions and delivery issues associated with the COVID-19 pandemic had a significant impact on the execution of cyberspace SC activities. RAND found that AM&E components did not collect data systematically, and assessments were not always conducted at the initiation of a program to determine the PN's needs and requirements. Problems identified with cyberspace SC implementation included identical cyberspace SC solutions for PNs with diverging requirements, long delays in the delivery of commercial-off-the-shelf equipment, and a lack of internal PN integration to meet strategic objectives.

RAND Recommendations.

- **Planning**. Provide access to planning aids and cyber subject matter experts at appropriate intervals to develop an overarching framework to guide the planning process.

- **Budgeting**. Develop a guide to cyber program costs for planners to use in developing budget requests for cyber-related exercises, activities, and technical assistance.

- **Execution.** Ensure cyber activities at all stages of planning and execution are entered appropriately into Socium, the SC data base of record.

- **AM&E.** Develop a framework for funding and conducting holistic, national-level cyberspace SC assessments to include policy and strategic-level stakeholders before DoW cyberspace SC activities are planned and executed.