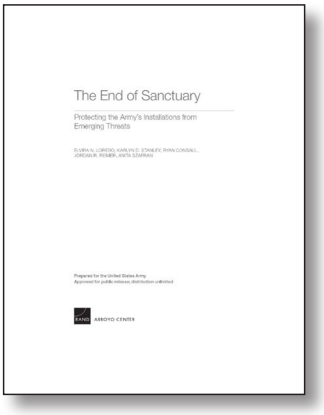

The End of Sanctuary

Protecting the Army's Installations from Emerging Threats

Elvira N. Loredo, Karlyn D. Stanley, Ryan Consaul, Jordan R. Reimer, and Anita Szafran

www.rand.org/t/RRA107-1

RAND researchers catalog innovative and emerging threats to Army installations, identify deficiencies in the Army's current threat assessment methodologies, and develop a framework to respond to these threats. The analysis revealed that the Army is not prepared to defend continental United States installations from complex coordinated attacks against the homeland using unconventional means.

RESEARCH QUESTIONS

- What emerging threats do Army installations face?
- What gaps exist in the threat-assessment methodologies the Army currently uses?
- How can the Army address these gaps, and what resources will be required to do so?

KEY FINDINGS

The innovative use of emerging and existing technologies by adversaries will continuously create threats to the wartime mission of Army installations

- Such emerging technologies as unmanned aerial systems, fifth-generation (5G) communications technology, and the use of social media disinformation by adversaries all pose potential threats to installations that might not have been anticipated.

An installation's ability to perform its wartime mission in a contested environment is not adequately considered under current threat assessment methodologies

- Multiple Army and U.S. Department of Defense organizations provide oversight and guidance about how to conduct installation threat assessments. The assessments have many commonalities but lack consistency and frequency of application. For example, some assessments are conducted every three years and cover only a subset of all installations, while others are conducted only at the request of the garrison commander.

continued on back

Threat assessment methodologies do not include many emerging threats

- The Army assessment processes for identifying current threats do not include manipulation of artificial intelligence, smart city technologies, biometrics, nanotechnology, information warfare, commercial satellites, social media, or industrial control system attacks.

Threat assessment approaches do not consider the combined effects of multiple threats

- When these threats are part of a coordinated effort involving the installation and the surrounding community, they might overwhelm an installation's capabilities.

Army installations are protected using traditional physical security, antiterrorism, and emergency preparedness approaches

- Current Army policies, doctrine, and assessments are focused "inside the wire" and fail to imagine the innovative use of existing or future threats on surrounding communities that will impede the flow of forces on road, rail, and at the ports of debarkation.

RECOMMENDATIONS

- The Army should adopt a comprehensive threat assessment and risk mitigation process. The proposed framework for this process comprises six steps: (1) identify innovative and emerging threats, (2) determine critical functions and processes related to achieving the mission at installations, (3) identify key enablers of those functions, (4) understand vulnerabilities and estimate the risk of given threats, (5) develop mitigation strategies, and (6) conduct wargaming or red-teaming exercises.
- The framework that RAND researchers have proposed should be incorporated in Army policy if it is to be effectively implemented. The framework also should be tested using a pilot project to define the roles of the multiple organizations involved. The pilot could be led by Army Materiel Command (AMC) and U.S. Army Installation Management Command (IMCOM) with the involvement of relevant Army organizations.
- The Army should review current assessments and modify or replace them (as needed) to ensure that they measure how a capable adversary will use combined effects to disrupt an installation's wartime mission.
- The proposed framework's results should be applied during exercises and deployments to training centers to achieve the Army's "train as you fight" goal.
- AMC and IMCOM should update all existing installation contracts with adjacent utilities and critical infrastructure to include current cybersecurity standards.

RAND ARROYO CENTER

RAND Arroyo Center is the Army's federally funded research and development center for studies and analyses. Its mission is to help Army leaders make decisions that are informed by objective, high-quality analysis. For more information visit Arroyo's website at **www.rand.org/ard**.