CENTER for STRATEGIC LEADERSHIP CSL

Issue Paper

Center for Strategic Leadership,
U.S. Army War College

August 2005
Volume 12-05

The Fourth Annual U.S. Army War College Reserve Component Workshop

Reinforcing the First Line of Defense: The Role of the National Guard in Critical Infrastructure Protection

By
Professor Bert B. Tussing
Director, Homeland Defense and Security Issues Branch, Operations and Gaming Division (OGD), Center for Strategic Leadership (CSL)
Professor James O. Kievit
National Security Leadership Studies, OGD, CSL
Colonel Richard W. Dillon
Director, Reserve Component Operations and Plans, OGD, CSL

The Department of Defense (DoD) *Strategy for Homeland Defense and Civil Support* asserts that one of the most essential and promising areas of employment for the National Guard in defense of the homeland is Critical Infrastructure Protection (CIP). The strategy's authors believe that the comprehensive assessment of critical infrastructure sites (both DoD and non-DoD), and the protection of those sites as required, are both areas in which the Guard could serve vital functions. Concurrently, the strategy reminds us that the modern threat against our country will call for an "unprecedented degree of shared situational awareness" between the interagency, state, local, tribal and private entities – a requirement that could be greatly facilitated by the traditional relationship between the Guard and the communities it serves.

Seeking to validate this strategic approach and assist in the development of implementing activities, the Center for Strategic Leadership, in cooperation with the Office of the Assistant Secretary of Defense for Homeland Defense (ASD-HD) and the National Guard Bureau (NGB), convened the U.S. Army War College's fourth annual Reserve Component workshop, *Reinforcing the First Line of Defense: The Role of the National Guard in Critical Infrastructure Protection*. The forum was held from 15-17 August 2005, at the War College's Collins Center, in Carlisle, PA. The symposium's participants included the State Adjutants General of Indiana and New York, and representatives from ASD-HD; the Department of Homeland Security (DHS); the Joint Staff; the NGB; U.S. Northern Command (USNORTHCOM); state homeland defense officials from Pennsylvania, Delaware and New Jersey; the National Infrastructure Advisory Council; the Department of the Army staff; and others.

METHODOLOGY

The workshop began with a series of panel presentations on the current and potential role of the National Guard in CIP, from the perspective of agencies and entities within and outside of DoD. A panel of civilian presenters representing perspectives from DHS, DoD, the National Infrastructure Advisory Council, and the State of Pennsylvania was followed by a "military panel" composed of representatives from the Joint Staff, USNORTHCOM, and the NGB. Using these perspectives as a springboard, six separate workshop groups examined a series of ques-

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **AUG 2005**	2. REPORT TYPE	3. DATES COVERED **-**
4. TITLE AND SUBTITLE **Reinforcing the First Line of Defense: The Role of the National Guard in Critical Infrastructure Protection. Issue Paper Volume 12-05, August 2005**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Center for Strategic Leadership,650 Wright Avenue,Carlisle,PA,17013-5049**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES **The original document contains color images.**		
14. ABSTRACT **see report**		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**4**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

tions (based on the DHS' recently released *Interim National Infrastructure Protection Plan* and DoD's *Strategy for Homeland Defense and Civil Support*) to discern potential paths the Guard might take, or reject, in support of CIP. A final plenary session provided the assembled participants an opportunity to review and critique the individual work groups' findings and insights.

OBSERVATIONS AND RECOMMENDATIONS

The diverse organizational viewpoints as well as the depth and breadth of the experience of the individual participants at the workshop provided fruitful exchange in a number of areas, but the greatest focus seemed to center on four topics: Intelligence/Information Exchange, Vulnerability Assessments, Protective Plans, and Standards.

Intelligence and Information Exchange

One clear concurrence in the forum was that the role of the Guard in the intelligence cycle is, and should remain, deliberately limited. Even acknowledging that "countering terrorist reconnaissance activity is central to the successful defense of critical infrastructure,"[1] participants shared near universal reticence to activities that could be remotely associated with the Guard's "gathering intelligence" in a domestic environment. The traditional trust relationship enjoyed by the Guard and its communities was considered too important to risk over what most participants considered an activity better suited to existing law enforcement agencies.

While reticent against Guard personnel participation in the "gathering" component of the intelligence cycle, and also arguing that the Guard is neither configured nor particularly suited to aid in the "analysis" component, participants did feel that the National Guard could serve a significant function assisting in the "dissemination" of intelligence surrounding critical infrastructure and other matters of homeland defense/security. The Guard may occupy a unique nexus for information from both the military and civil authorities, particularly that obtained from sources in DoD and DHS, that can be provided for dissemination to various fusion centers in support of state and local governments (e.g., the Joint Terrorism Task Forces and the Field Intelligence Groups). Participants suggested that the Guard attempt to place "permanent" members in these centers, thereby gaining maximum advantage of security clearances that are frequently hard to obtain in the civil sector, and thus be positioned to serve as an information conduit to and from both public and private sectors in their communities. Concurrently, Guard personnel could be positioned to identify and levy a better set of its own information/intelligence requirements upon the Intelligence Community, particularly in support of public and private CIP concerns. Finally, the National Guard could, in the regular course of its operations, act as a source of a "slightly more informed pool of citizenry" to pass on information of potential significance to what they know to be the proper authorities for action.

Vulnerability Assessments

Participants devoted significant attention, perhaps the lion's share of dialogue within the work groups, to the potential role the National Guard could play in the conduct of vulnerability assessments in support of DoD and state and local governments. Recognizing the fact that there are currently numerous assessment mechanisms utilized by DHS, DoD, and the private sector, the participants held that the Guard should work towards establishing "baseline standards" for its efforts, identifying a set of benchmarks for both training and execution. Mention was made of the fact that Full Spectrum Integrated Vulnerability Assessment (FSIVA) teams would likely be employed to fulfill shortfall requirements for assessments within DoD, to include in support of the Defense Industrial Base.

[1] Department of Defense, *Strategy for Homeland Defense and Civil Support*, June 2005, page 30.

Beyond DoD, however, participants felt it was important to portray the FSIVA's as a capability to be shared with the public and private sector by invitation, not regulation. Assessment requirements that are levied should originate through the Sector Specific Agencies overseeing the critical infrastructure/key resource (CI/KR) sectors, coordinated through both Government Coordinating Councils (GCC) and Sector Coordinating Councils (SCC). In the same spirit, National Guard assessments should be integrated/deconflicted with similar efforts from within DHS, state homeland security offices, local governments, and the private sector, in order to promote synergies and maximize limited resources.

The number and makeup of FSIVA teams was widely discussed. Some held that the current projection of one FSIVA team per Federal Emergency Management Agency (FEMA) region (four additional teams beyond those already extant in California, Colorado, Minnesota, Georgia, New York and West Virginia) would suffice. Others felt that a full-time team should be activated for each of the 54 state and territory jurisdictions, serving as a companion element to the National Guard's Weapons of Mass Destruction-Civil Support Teams (WMD-CST). Most of the forum concurred that a baseline capability for physical assessments could reside in the teams currently envisioned, but that more detailed assessments into specific areas of CI/KR would require augmentation. That augmentation could originate from within the expanded ranks of the National Guard itself, or from subject matter experts within the public and private sectors.

Protective Plans

Discussion surrounding the role of the National Guard in protecting CI/KR generally followed along two paths: one addressing a requirement for developing detailed plans to protect identified critical infrastructure in cooperation with public and private stakeholders; and one addressing a requirement to establish rapid response forces to respond to requirements when other stakeholders' capabilities have been exceeded.

The first concept is built around a notion of "defense in depth." Reiterating the position that the private sector is primarily responsible for the protection of that critical infrastructure it owns, participants suggested that those responsibilities were contained "within the fence line." Following this view, in an extremis situation, the Guard's responsibilities should begin at the fence line, providing a buffer zone of protection for the infrastructure under consideration, the approaches to the same, etc. Deliberate plans for this "outer protection" must be coordinated with public and private plans devoted to these ends, incorporated in overarching "contingency plans" (conplans), and exercised with all appropriate stakeholders. Corollaries could be drawn to the same type of planning for the protection of state and local government assets. Depending upon the size, nature and scope of the plan, coordination could be required with broader DHS conplans (e.g., the new Buffer Zone Protection Plans), or the applicable combatant command (either USNORTHCOM or U.S. Pacific Command).

The requirement for rapid response forces was raised in recognition of the fact that a National Guard force will always, in all likelihood, be the initial military intervention element. By extension, participants recommended establishing standing Rapid Reaction Forces within the National Guard, separate and distinct from the active component Quick Reaction Force (or its Rapid Response Force component) envisioned in current USNORTHCOM conplans. Designed to augment or provide physical protection when other stakeholders' capabilities have been exceeded, participants opined that a National Guard rapid response force could respond to a threat/attack against CI/KR within 12 hours.

Both protection plan concepts were built upon a basic assumption of availability of assets. Ultimately these plans could call for balancing force structure requirements between defense of the homeland in the homeland and requirements for the "strategic reserve." Workshop participants envision a deliberate planning process to create the protective conplans and vet them through DoD. However, most perceive this vetting process not for DoD's approval, but for its awareness.

Standards

Interwoven throughout the dialogue about the National Guard in CIP, irrespective of the particular topic/potential role, was a requirement for creation or recognition of some accepted common "standards." More than once participants were heard to state that it matters less *who* does something within a given state or region as long as it is being done to the *same standard* in all states and regions. Many participants felt that the Guard, as an organization integrated into multiple communities at every level (local, state, and federal), might provide the means to develop, disseminate, and in some cases enforce those required common standards.

CONCLUSION

Given the current mission set of the National Guard, there was clear recognition in the forum of a requirement to balance potential domestic and overseas missions. A litany of questions follows this recognition: Can the Guard afford to have standing multi-functional assessment teams, or can a team be assembled around small, "core elements" when needed? If "protective missions" are planned and allocated, what readiness levels are applicable – and what readiness levels should the Guard be expected to maintain for elements of the "expeditionary strategic reserve." Are there unique training requirements for dealing with citizenry in a protective mission, or can we continue to simply include it as a "lesser subset" of warfighting preparations? How should the National Guard define and measure overall readiness for CIP missions?

This workshop offered an important opportunity for stakeholders in Critical Infrastructure Protection to examine their agencies' requirements and to attempt to better discern how the National Guard can supplement and complement their efforts. The results of the symposium will need to be examined and shared in additional forums in the near future as a part of ensuring efficient, effective utilization of this vital component of the Nation's defense in a mission vital to the security of its people. An unprecedented threat faces our nation that will demand complex solutions through every level of government and into the private sector. The August forum suggests that one conduit for taming that complexity resides in the National Guard.

****

This and other issue papers may be found on the USAWC/CSL web site at http://www.carlisle.army.mil/usacsl/IPapers.asp.

****

The views expressed in this report are those of the participants and do not necessarily reflect official policy or position of the United States Army War College, the Department of the Army, the Department of Defense, or any other Department or Agency within the U.S. Government. This report is cleared for public release; distribution is unlimited.

U.S. ARMY WAR COLLEGE
Center for Strategic Leadership
650 Wright Avenue
Carlisle, PA 17103-5049

OFFICIAL BUSINESS

FOURTH ANNUAL
RESERVE COMPONENT WORKSHOP