Network Integration Evaluation (NIE)

In FY14, the Army executed two Network Integration Evaluations (NIEs) at Fort Bliss, Texas, and White Sands Missile Range, New Mexico. NIE 14.1 was conducted in October and November 2013 and NIE 14.2 was conducted in April and May 2014. The purpose of the NIEs is to provide a venue for operational testing of Army acquisition programs, with a particular focus on the integrated testing of tactical mission command networks. The Army also intends the NIEs to serve as a venue for evaluating emerging capabilities that are not formal acquisition programs. These systems, termed by the Army as "systems under evaluation" (SUEs), are not acquisition programs of record, but rather systems that may offer value for future development.

The Army's intended objective of the NIE to test and evaluate network components in a combined event is sound. The NIE events should allow for a more comprehensive evaluation of an integrated mission command network, instead of piecemeal evaluations of individual network components.

NIE 14.1

During NIE 14.1, the Army executed an FOT&E for the Joint Warning and Reporting Network (JWARN) and an operational test for the AN/PRC-117G radio. The Army intended to conduct an FOT&E for the Command Post of the Future (CPOF); however, due to system software stability problems discovered during the pilot test, this operational testing was not executed. The Army also conducted assessments of 14 SUEs. Individual articles providing assessments of JWARN and the AN/PRC-117G radio can be found separately in this Annual Report.

NIE 14.2

During NIE 14.2, the Army conducted a Multi-Service Operational Test and Evaluation for the Joint Battle Command – Platform, an FOT&E for Manpack radio, an FOT&E for Shadow Tactical Unmanned Aerial System, and the first phase of IOT&E for Nett Warrior. Individual articles on these programs are provided later in this Annual Report. The Army also conducted assessments of 13 SUEs during NIE 14.2.

NIE ASSESSMENT

NIE 14.1 and 14.2 were the sixth and seventh such events conducted to date. The Army has developed a systematic approach to preparing for and conducting NIEs, applying lessons learned from previous events. Overall, NIEs have been a satisfactory venue for conducting operational tests of individual network acquisition programs.

Operational Scenarios and Test Design. The Army Test and Evaluation Command's Operational Test Command, in conjunction with the Brigade Modernization Command, continues to develop realistic, well-designed operational scenarios for use during NIEs. Additionally, the 2d Brigade, 1st Armored Division, as a dedicated NIE test unit, is a valuable resource for the conduct of NIEs.

The challenge for future NIEs will be to continue to develop new and more taxing operational scenarios to reflect future combat operations. Future NIEs should include more challenging and stressful combined arms maneuvers against regular conventional forces. Such scenarios would place greater stress on the tactical network and elicit a more complete assessment of that network. Within resource constraints, the Army should continue to strive to create a demanding operational environment at NIEs similar to that found at the Army's combat training centers.

Balance between Testing and Experimentation. There are inherent tensions between testing and experimentation as they each have somewhat different objectives and requirements for exercise control, scenarios, and data collection. For example, experimentation tends to be more freewheeling than operational testing, as it seeks to examine possible new capabilities and tactics in a relatively unconstrained environment. Operational testing, on the other hand, requires more control over the tactical environment, as testing seeks to confirm the performance of acquisition systems with well-defined requirements and concepts of operation. Furthermore, experimental items that interact with systems undergoing operational test may negatively affect test system performance and confound the test results. The Army must continue to give priority to operational test objectives at NIEs and ensure that experimentation and

training demands do not interfere with the requirements for adequate operational testing.

The Army is considering devoting one NIE a year to operational testing and the other annual NIE to experimentation and force development. Such an approach would pay dividends by focusing individual event design on the specific requirements of testing or experimentation.

Instrumentation and Data Collection. The Army should continue to improve its instrumentation and data collection procedures to support operational testing. For example, the Army's Operational Test and Evaluation Command should devote effort towards developing instrumentation to collect network data for dismounted radios, such as the Manpack radio. Additionally, the Army needs to emphasize the use of Real-Time Casualty Assessment (RTCA) instrumentation. An essential component of good force-on-force operational testing, such as that conducted at NIEs, is RTCA instrumentation, which adequately simulates direct and indirect fire effects for both friendly and threat forces. Finally, the Army should continue to refine its methodology for the conduct of interviews, focus groups, and surveys with the units employing the systems under test.

Threat Operations. An aggressive, adaptive threat intent on winning the battle is an essential component of good operational testing. The Army continues to improve threat operations during NIEs, particularly with respect to threat information operations such as electronic warfare and computer network operations. NIEs should incorporate a large, challenging regular force threat. This threat should include a sizeable armored force and significant indirect fire capabilities. The threat force should also include appropriate unmanned aerial vehicles.

Logistics. The Army should place greater emphasis during NIEs on replicating realistic battlefield maintenance and logistical support operations for systems under test. Field Service Representative (FSR) support plans, maintenance and repair parts stockage, and the quantity and management of system spares do not accurately reflect what a unit will observe upon fielding. Easy access to and over-reliance on FSR support results in the test unit not having to realistically execute its field-level maintenance actions. Failure to accurately replicate "real world" maintenance and logistics support causes operational availability rates and ease of maintenance to be overestimated in NIEs.

NETWORK PERFORMANCE OBSERVATIONS

The following are observations of tactical network performance during NIEs. These observations focus on network performance deficiencies that the Army should consider as it moves forward with integrated network development.

Complexity of Use. Network components, both mission command systems and elements of the transport layer, are excessively complex to use. The current capability of an integrated network to enhance mission command is diminished due to pervasive task complexity. It is challenging to achieve and maintain user proficiency.

Common Operating Picture (COP). Joint Publication 3-0, (Joint Operations) defines a COP as "a single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness." With current mission command systems, units have multiple individual COPs (e.g., for maneuver, intelligence, and logistics) based upon the corresponding mission command systems, instead of a single COP that is accessible on one system. The Army is seeking to resolve this problem, and these efforts should continue.

Unit Task Reorganization and Communications Security (COMSEC) Changeover. Operational units frequently change task organizations to tailor for tactical missions. The process to update the networks to accommodate a new unit task organization remains lengthy and cumbersome. Similarly, COMSEC changeover is a lengthy, burdensome process, which requires each individual radio to be manually updated. This process typically requires in excess of 24 hours for a Brigade Combat Team to complete. This is an excessive length of time for a unit conducting combat operations.

Armored Brigade Combat Team Integration. The challenge of integrating network components into tracked combat vehicles remains unresolved. Due to vehicle space and power constraints, the Army has yet to successfully integrate desired network capabilities into Abrams tanks and Bradley infantry fighting vehicles. It is not clear how the desired tactical network will be incorporated into heavy brigades.

Infantry Brigade Combat Team (IBCT) Integration. Integration of the network into the light forces will also be challenging given the limited number of vehicles in the IBCT. Most of the key network components, such as Joint Battle Command – Platform, are hosted on vehicles. The challenge of linking into the tactical network is particularly acute at company level and below, where light infantry units operate dismounted. Future NIEs should examine the IBCT tactical network, which has not been addressed to date.

Soldier Radio Waveform (SRW) Range. Testing at NIEs continues to demonstrate the shorter range of SRW vis-à-vis the legacy Single Channel Ground and Airborne Radio System (SINCGARS) waveform. This is not surprising given that SRW operates at a much higher frequency than does SINCGARS. Higher frequencies have shorter ranges and are more affected by terrain obstructions. NIE test units, particularly when operating dismounted, have consistently found SRW ranges to be unsatisfactory in supporting tactical operations and prefer using SINCGARS due to its longer range.

Dependence on FSRs. Units remain overly dependent upon civilian FSRs to establish and maintain the integrated network. This dependency corresponds directly to the excessive complexity of use of network components.

Survivability. An integrated tactical network introduces new vulnerabilities to threat countermeasures, such as threat computer network attacks and the ability of a threat to covertly track friendly operations. The Army should continue to improve its capabilities to secure and defend its tactical network. In particular, the Army should ensure that brigade-level cybersecurity teams are appropriately manned and trained.