Network Integration Evaluation (NIE)

In FY15, the Army conducted two Network Integration Evaluations (NIEs) at Fort Bliss, Texas, and White Sands Missile Range, New Mexico. NIE 15.1 was conducted in October and November 2014, and NIE 15.2 was conducted in April and May 2015. 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," 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 15.1

During NIE 15.1, the Army conducted an FOT&E for Warfighter Information Network – Tactical (WIN-T) Increment 2. An individual article providing an assessment of WIN-T Increment 2 can be found separately in this annual report.

NIE 15.2

During NIE 15.2, the Army conducted an FOT&E for the Distributed Common Ground System – Army and a Limited User Test for the Mid-Tier Networking Radio. Individual articles on these programs are provided elsewhere in this annual report.

NIE ASSESSMENT

NIE 15.1 and 15.2 were the eighth and ninth such events conducted to date. The Army has developed a systematic approach to preparing for and conducting NIEs and 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, continue 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.

Future NIEs should continue to develop new and more demanding operational scenarios to reflect future combat operations. Future NIEs should include 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.

Testing and Experimentation. Beginning in FY16, the Army will devote one NIE a year to operational testing and another annual event to experimentation and force development. The latter event is to be called an Army Warfighting Assessment, the first of which will be conducted in October 2015. This new approach is intended to pay dividends by focusing individual event design on the specific requirements of either 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 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 place greater emphasis on the use of Real-Time Casualty Assessment instrumentation, which is an essential component of good force-on-force operational testing, such as that conducted at NIEs. A Real-Time Casualty Assessment is intended to accurately simulate 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 that includes a sizeable armored force and significant indirect fire capabilities. Threat capabilities should be upgraded each year to reflect real-world threat developments.

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, remain 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.

Networking Waveforms. The Army is committed to using networking waveforms, such as the Soldier Radio Waveform and Wideband Networking Waveform, to implement a networked tactical communications network. While networked communications at lower tactical levels may create enhanced operational capability, the use of these networking waveforms brings negative attributes, which need to be fully evaluated and understood. For example, these waveforms, due to their higher frequencies, have shorter ranges and are more affected by terrain obstructions compared to the legacy Single Channel Ground and Airborne Radio System waveform. Establishing and maintaining networked communications is complex and difficult. For example, loading the initial network plans in all the necessary radios, updating the network to accommodate a new unit task organization, and conducting a communications security changeover are lengthy and cumbersome tasks requiring 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. Networked radios also have a much higher power consumption resulting in significantly higher battery consumption rates for dismounted radios. Finally, since networked communications are constantly emitting, they are much more vulnerable to threat electronic direction finding.

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.

Stryker Brigade Combat Team Integration. The WIN-T FOT&E conducted during NIE 15.1 revealed significant issues with the integration of WIN-T into Stryker vehicles. In both the Stryker Point of Presence vehicle and the Stryker Soldier Network Extension vehicle, WIN-T components were poorly integrated from a human factors perspective. The placement of these components in the vehicles interfered with Stryker crew operations and negatively affected unit mission execution.

Infantry Brigade Combat Team Integration. Integration of the tactical network into an Infantry Brigade Combat Team has not been evaluated at NIEs due to the lack of a light infantry unit assigned to the NIE test unit. Integration of the network into the light forces will be challenging given the limited number of vehicles in the Infantry Brigade Combat Team. 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.

Spectrum Management. The intended tactical network places a greater demand upon the available electromagnetic spectrum than has been the case with non-networked communications. The network topology requires more discrete frequencies, which will place greater stress on a tactical unit's capability to allocate and manage the available spectrum. This challenge will be even more significant for large tactical units, such as divisions, operating in the same geographical area of operations.

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 capability to secure and defend its tactical network. The Army should ensure that brigade-level cybersecurity teams are appropriately manned and trained.

Air-Ground Communications. The Army has yet to integrate radios into its rotary-winged aircraft which are capable of operating in the same network as ground forces at the company level and below. This remains an important operational gap.

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