Network Integration Evaluation (NIE)

The Army conducted one NIE during FY16. NIE 16.2 was conducted in April and May 2016 at Fort Bliss, Texas. In a change from previous years, instead of conducting two NIEs a year to support test and evaluation, the Army conducted a single NIE. Beginning in FY16, the Army is devoting one NIE a year to operational testing and using another annual event, the Army Warfighting Assessment, for experimentation and force development. The first Army Warfighting Assessment was conducted at Fort Bliss in October 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. 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 allow for a more comprehensive evaluation of an integrated mission command network than is possible through piecemeal evaluations of individual network components.

NIE 16.2

During NIE 16.2, the Army conducted a Limited User Test (LUT) for Warfighter Information Network – Tactical (WIN-T) Increment 3 Network Operations/Net Centric Waveform and an LUT for Spider Increment 1A. In addition, the Brigade Modernization Command conducted an operational assessment of the Mid-Tier Networking Vehicular Radio (MNVR). Individual articles providing assessments of WIN-T, Spider, and MNVR can be found separately in this annual report.

NIE ASSESSMENT

NIE 16.2 was the tenth such event conducted to date. NIEs have been an excellent venue for conducting operational tests of network acquisition programs.

Dedicated Test Unit. Since the first NIE in July 2011, the 2nd Brigade Combat Team, 1st Armored Division has served as the dedicated NIE test unit. Having a dedicated test unit stationed at Fort Bliss, Texas, has been a critical element in successful operational testing conducted during NIEs. It has made the planning and execution of complex brigade-sized operational tests of Army networks much more effective than would be the case if new test units were selected for each event. Past experience demonstrates that having a dedicated test unit enables good operational testing. Due to its experience and the organizational learning that has occurred over time, the dedicated NIE test brigade has shown that it is more attuned to incorporating new systems into its formation for testing than has been the case with one-off test units. As a result, the system under test receives a robust evaluation.

A dedicated test unit is desirable in that it relieves the stress on the Army to designate a test unit of appropriate size each time an operational test is on the schedule for a given program. Some tests require large-scale units up to brigade in size and, when testing command and control systems, sometimes even require a division headquarters element. It is not uncommon to require a brigade combat team-sized or battalion-sized unit. Having a dedicated test unit of a mixed composition enables all of those requirements to be met at one place.

Another aspect of good operational testing is a capable opposing force (OPFOR). The dedicated test brigade has been very proficient in creating this OPFOR. Good operational testing requires an aggressive, adaptive threat unit intent on winning the battle in order to adequately stress the system under test and to fully understand its capabilities. A realistic demanding OPFOR requires capabilities which are not easily assembled and integrated. These capabilities include electronic warfare and cybersecurity threats as well as a mix of heavy and light forces. In particular, the integration of electronic warfare and cyber capabilities into an OPFOR requires practice and is not easily replicated by new units tasked to conduct an OPFOR operational testing mission. The units permanently assigned to conduct the NIEs have, over time, demonstrated the ability to employ an effective OPFOR with a variety of combat multipliers to include

electronic warfare and cyber-attack. This OPFOR capability has grown increasingly sophisticated and can be readily adapted to reflect new real-world threat capabilities. This capability may not easily be replicated by a rotational brigade.

For operational reasons unrelated to test and evaluation, the Army has removed 2nd Brigade Combat Team, 1st Armored Division from its mission as the dedicated NIE test unit and has decided to no longer provide a dedicated test unit. This is unfortunate from an operational test and evaluation perspective and, for reasons noted above, the quality of future NIE execution may suffer.

Threat Operations. One of the most significant benefits of NIEs has been the extensive incorporation of threat information operations, such as electronic warfare and computer network operations. Nowhere else has the Army routinely integrated this level of threat capability in either a testing or a training venue. As a result, NIEs have provided numerous insights with respect to operations in this type of threat environment. This capability should be retained and upgraded, as necessary, in future NIEs.

One challenge associated with providing these threat capabilities is cost. They are expensive to provide. The programs of record – or "systems under test" – have borne the cost despite not being funded for these capabilities in their test and evaluation budgets. This has created a funding mismatch before every NIE. The Army should consider centrally funding NIE threat operations to relieve the cost burden on the programs undergoing formal operational testing. This makes particular sense given that the benefits accrue to many of the other systems undergoing some sort of assessment during NIEs, such as "systems under evaluation" and risk reduction events.

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 (ATEC) should devote increased effort towards developing instrumentation to collect network data to support WIN-T operational test and evaluation. WIN-T instrumentation has not been adequate to support a thorough evaluation. Improvements are needed with respect to Simple Network Management Protocol polling and Internet Protocol-packet capture and matching. ATEC should also 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 – 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.

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.

Network Implementation Challenges. Significant questions remain as to how the network will be implemented in each of the three types of maneuver brigade combat teams (Armored, Infantry, and Stryker). For example:

- Armored Brigade Combat Team Integration. It is not clear how the desired tactical network will be incorporated into heavy brigades, as the challenge of integrating network components into tracked combat vehicles remains unresolved. Due to vehicle space and power constraints, the Army has yet to integrate desired network capabilities into Abrams tanks and Bradley infantry fighting vehicles. For example, at the company level it will be some years before the Manpack network radio will be installed on Abrams tanks and Bradley infantry fighting vehicles. Additionally, it is not clear how the mid-tier tactical network will be established at company level, given that the MNVR radio will not be integrated on either of these vehicles. Implementation of the WIN-T network into the Armored Brigade Combat Team is also some years away, as it is dependent upon successful development and fielding of the Armored Multipurpose Vehicle Mission Command variant.
- Infantry Brigade Combat Team Integration. Integration of the tactical network into an Infantry Brigade Combat Team has not been adequately evaluated in 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. Without a vehicular network node, dismounted units cannot connect to the network above company level.

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 networking waveforms brings negative attributes which need to be fully evaluated and understood. For example, networking 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. Networking waveforms and the corresponding software-defined radios were conceived to support data intensive capabilities such as real time video. Such capabilities require high bandwidth, and hence high frequencies, at the cost of shorter ranges. The Army should re-examine whether the current radio and waveform programs best meet the operational needs of maneuver commanders. One clear lesson from previous NIEs is that the two most critical network needs for maneuver commanders at battalion and below are reliable voice communications and GPS-supplied position location information. These needs may be met by a network with much lower bandwidth but increased operating ranges.

Complexity of Use. Network components, including mission command systems and elements of the transport layer, remain very 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. Units remain dependent upon civilian field service representatives to establish and maintain the integrated network. This dependency corresponds directly to network complexity of use.

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. Since networked communications are constantly emitting, they are much more vulnerable to threat electronic direction finding.

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

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