
Director, Operational Test and Evaluation


**Distributed Common Ground System – Army
(DCGS-A) Increment 1 Release 2**

Follow-on Operational Test and Evaluation (FOT&E) Report



January 2016

This report on the Distributed Common Ground System – Army (DCGS-A) fulfills the provisions of Title 10, United States Code, Section 2399. It assesses the adequacy of testing and the operational effectiveness, operational suitability, and cybersecurity posture of the DCGS-A.


J. Michael Gilmore
Director

This page intentionally left blank.

Executive Summary

This report provides the Director, Operational Test and Evaluation's (DOT&E's) operational evaluation of the Distributed Common Ground System – Army (DCGS-A) Increment 1, Release 2. The evaluation is based on the Follow-on Operational Test and Evaluation (FOT&E) conducted by the Army Test and Evaluation Command (ATEC) from May 2 – 14, 2015, during the Army's Network Integration Event (NIE) 15.2, at Fort Bliss, Texas. The FOT&E included cybersecurity test events conducted by ATEC, the Army's Threat System Management Office (TSMO), and the National Security Agency (NSA) during March through June 2015. Additional data came from a data synchronization test at the DCGS-A Ground Station Integration Facility (GSIF) at Aberdeen Proving Ground, Maryland, in September 2015. A team composed of ATEC, DOT&E, and Program Management Office personnel designed and conducted the GSIF event.

The FOT&E was adequate to evaluate the operational effectiveness, suitability, and survivability of DCGS-A, but inadequate to quantify performance details of DCGS-A functionality. ATEC conducted the test events in accordance with the DOT&E-approved test plan, but did not conduct the data collection, reduction, and analysis as described in the test plan. ATEC's test database did not provide sufficient data for a quantitative assessment of intelligence fusion, targeting, and data synchronization functions. The GSIF event added sufficient additional data to supplement the evaluation of data synchronization; DOT&E used these data to identify the cause of data synchronization issues discovered during the FOT&E.

The FOT&E included both Combined Arms Maneuver (CAM) and Wide Area Security (WAS) scenarios. The event mixed live and simulated units and replicated corps-level enemy regular forces and insurgents, which fought friendly division, brigade, and battalion-level units.

To evaluate the system's ability to help users find, process, exploit, and disseminate intelligence information, ATEC inserted 10 vignettes—5 for CAM and 5 for WAS—into the test scenario. These vignettes were operationally realistic story lines such as finding and destroying facilities that manufacture improvised explosive devices (IEDs), and finding and targeting enemy troop movements. To support the vignettes, the test team injected intelligence data elements (such as intercepted communications, situation reports, satellite pictures, and full motion videos), that corresponded to the vignettes into a database containing terabytes of other information, including actual intelligence from combat theaters.¹ This large, realistic database comes from the Training Brain Operations Center (TBOC). The Army uses the TBOC database for intelligence analyst training. A key objective of the FOT&E was to evaluate the unit's ability to use DCGS-A to discover the injected data elements, and use the data elements to reach accurate conclusions regarding the enemy actions.

DCGS-A is operationally effective. The test unit successfully received, processed, exploited, and disseminated intelligence data with DCGS-A. The unit provided actionable

¹ The Training Brain Operating Center (TBOC) derives intelligence data from combat theaters. The test team modified names and other details of the TBOC data to fit with the NIE scenario.

intelligence to commanders, enabling them to make timely decisions. The test brigade commander stated that DCGS-A helped produce useful intelligence products in hours instead of days or weeks. Test data from the vignettes and test logs captured sufficient evidence that the unit was able to rapidly find relevant information and draw accurate conclusions about the enemy's actions. The test unit did not always accurately attribute the troop and equipment to the correct enemy unit, but did accurately capture the movement of enemy troops and equipment.

The Army resolved the system shortfalls which were reported in the DOT&E's November 1, 2012, memorandum and classified Initial Operational Test and Evaluation (IOT&E) report:^{2,3}

- Database discrepancies: The IOT&E version of DCGS-A had a different database structure and protocols for the Top Secret/Sensitive Compartmented Information (TS/SCI) and Secret enclaves. DCGS-A Release 2 implemented the same Tactical Entity Database (TED) for both enclaves, markedly improving system performance.
- TS/SCI enclave: During the IOT&E, DCGS-A intelligence fusion tools were available to users only in the TS/SCI enclave. This meant all Secret information had to be sent through a cross-domain solution to the TS/SCI enclave to exploit, and the product then had to be sent back to the Secret enclave, again through the cross-domain solution, to share with other command and control systems. This workflow made the unit's work process unnecessarily time consuming. DCGS-A Release 2 resolved this shortfall by making intelligence fusion tools available in both enclaves.
- Cybersecurity: The IOT&E revealed many cybersecurity vulnerabilities. The Army mitigated many of the vulnerabilities with DCGS-A Release 1, and mitigated all major vulnerabilities with Release 2. The remaining cyber security shortfalls are attributable to the Army's tactical network environment.

DCGS-A is operationally suitable, provided the Army intensively trains DCGS-A users, and provides refresher training to units in garrison. DCGS-A is a complex system and the skills required to use it are perishable. The operational availability (A_o) of DCGS-A satisfied the requirements at all echelons and reliability of the system improved from IOT&E. There were no hardware failures during the FOT&E; however, software failures were still a challenge for users. The system required reboots about every 20 hours for users who had heavy workloads such as the fire support analysts and data managers in the BCT Tactical Operations Center (TOC). The extensive unit-level training over three training events leading to the FOT&E gave the unit the chance to develop and train the tactics, techniques and procedures to use the system in support of

² DOT&E memorandum to the Undersecretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), Subj: Deployment Decision for Distributed Common Ground System – Army (DCGS-A) Release 1.

³ DOT&E, Distributed Common Ground System – Army (DCGS-A) Software Baseline 1.0 (DSB 1.0) Initial Operational Test and Evaluation (IOT&E) report, October 2012 (SECRET).

the mission. For users to be able to operate DCGS-A effectively, the Army needs to continue to provide such comprehensive training.

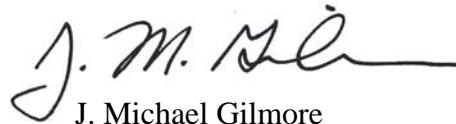
The DCGS-A program manager successfully managed DCGS-A cybersecurity risks, but DCGS-A is not survivable because of the vulnerabilities of the Army tactical networks that interface with DCGS-A. The vulnerabilities inherited from interfacing systems and networks reduce the cybersecurity of DCGS-A as well as other systems on the networks.

DOT&E recommends the Army take the following actions:

- Institutionalize the training provided to the FOT&E test unit so that all DCGS-A equipped units receive intensive, scenario-driven, collective training.
- Improve DCGS-A training to include standard procedures for:
 - Coordinating TED changes among the DCGS-A users at different TOCs, such as between brigade and battalions.
 - Metadata tagging for data posted on the DCGS Integration Backbone (DIB).
- Maintain DCGS-A unit readiness via continuous use of DCGS-A in garrison.
- Train the users about the pros and cons of each method of data synchronization.
- Improve reliability by tracking and correcting software faults.
- Improve the cybersecurity posture in all Army tactical networks.

ATEC should resolve the following systematic shortfalls with data collection, reduction, and analysis during testing.

- Demonstrate the end-to-end process of collecting, reducing, and analyzing the data before an operational test.
- Conduct a developmental test with operationally representative networks and the operational test instrumentation before an operational test of complex networked systems.
- Attribute all performance anomalies to system performance, test process, or data collection and reduction before the test ends.
- Analyze data sufficiently to identify and resolve anomalies and inconsistencies during the test.


J. Michael Gilmore
Director

This page intentionally left blank.

Contents

System Overview1

Test Adequacy7

Operational Effectiveness.....13

Operational Suitability33

Survivability41

Recommendations45

Operational Vignette Details.....A-1

Classified Annex B.....Under Separate Cover

This page intentionally left blank.

Section One

System Overview

This report provides the Director, Operational Test and Evaluation's (DOT&E) operational assessment of the Distributed Common Ground System – Army (DCGS-A) Increment 1, Release 2. The assessment is based on the Follow-on Operational Test and Evaluation (FOT&E) conducted by the Army Test and Evaluation Command (ATEC) from May 2 – 14, 2015, during the U.S. Army's Network Integration Event (NIE) 15.2, at Fort Bliss, Texas. The FOT&E included cybersecurity test events conducted by ATEC, Threat System Management Office (TSMO), and the National Security Agency (NSA) during March through June 2015. Additional data came from the data synchronization test at the Ground Station Integration Facility (GSIF) at Aberdeen Proving Ground, Maryland, in October 2015. A team composed of ATEC, DOT&E, and Program Management Office personnel designed and conducted the GSIF event.

Mission Description and Concept of Employment

DCGS-A Increment 1 is designed to provide timely, relevant, accurate, and targetable data processing, exploitation, and dissemination to Service members. DCGS-A Increment 1 is designed to be fully interoperable with the Army's Unified Mission Command System and to provide access to data, information, and intelligence to support battlefield visualization and Intelligence, Surveillance, and Reconnaissance (ISR) management. It provides flattened network-enabling information discovery, collaboration, production, and dissemination to combat commanders and staffs along tactically useful timelines. The intelligence staff will use DCGS-A Increment 1 to provide a persistent and dynamic view of the operational environment to the commander. DCGS-A Increment 1 fuses data for integration into a common operational picture and supports a prediction of enemy intent based upon an understanding of actions.

DCGS-A Increment 1 operates throughout the distributed operational Department of Defense Intelligence Information Enterprise environment. Using the Global Information Grid and multiple security-level access to national gateways, DCGS-A Increment 1 users should receive near real time assured access to entire regional and national-level architectures. DCGS-A Increment 1 is designed to enable situational understanding that permits commanders to operate effectively in all phases of operations.

DCGS-A Increment 1 provides basic ISR tools to support Mission Command activities, and advanced ISR tools for military intelligence professionals and geospatial analysts. DCGS-A capabilities will include indirect access to National Technical Means, Airborne Reconnaissance Low, Guardrail Common Sensor, weather, Moving Target Indicator, Unmanned Aircraft System (UAS), Rivet Joint, U-2, and ground signals intelligence (PROPHET). At the BCT, Ranger Regiment and Special Operations Aviation Regiment, ground station capabilities will include direct connectivity with PROPHET, Army UAS, and E-8 Joint Surveillance Target Attack Radar System (JSTARS). At the Division Headquarters G-2 ground station, capabilities will include direct connectivity with Sky Warrior UAS and E-8 JSTARS.

DCGS-A Increment 1 provides Space Operations Officers at Division Headquarters a space perspective in mission analysis in order to develop space input to intelligence preparation of the battlefield. Figure 1-1 depicts DCGS-A intelligence domains/analytic tools available to the operator.



Figure 1-1. DCGS-A Intelligence Domain Displays⁴

Program Description

DCGS-A Increment 1 combines 16 stove-piped legacy applications into one comprehensive system. DCGS-A Increment 1 completed an Initial Operational Test and Evaluation (IOT&E) in 2012. The Army called the system DCGS-A Software Baseline 1.0 (DSB 1.0) at the time of IOT&E. DOT&E evaluated DSB 1.0 to be not effective, not suitable, and not survivable.⁵ The Army reconfigured the system as Release 1 with only the Secret enclave, and fixed major cybersecurity shortfalls. DOT&E reported that fielding DCGS-A Release 1 will provide users capabilities at least as good as those provided by the currently fielded versions of DCGS-A, as well as providing a number of incremental upgrades incorporated in the latest versions of the system's hardware and software.⁶ The Office of the

⁴ Acronym used in Figure 1-1: Imagery Intelligence (IMINT); Human Intelligence (HUMINT); Moving Target Indicator (MTI); Signal Intelligence (SIGINT).

⁵ DOT&E, Distributed Common Ground System – Army (DCGS-A) Software Baseline 1.0 (DSB 1.0) Initial Operational Test and Evaluation (IOT&E) report, October 2012 (SECRET).

⁶ DOT&E memorandum, Subject: Deployment Decision for Distributed Common Ground System – Army (DCGS-A) Release 1.

Secretary of Defense approved a Full Deployment Decision for Increment 1 in December 2012.⁷ The Army designed Release 2 to provide enhanced capabilities for:

- Handling Top Secret/Sensitive Compartmented Information (TS/SCI)
- Aligning workflows with the intended operational employment
- Increasing efficiency of entity data transfer within the system and between systems
- Correlating entity data
- Transferring information across security domains

Figure 1-2 below shows how the Army plans to deploy DCGS-A to fixed sites, corps/divisions, brigades, and battalions in support of intelligence missions. DCGS-A delivers the components identified in the lower left-hand side of the picture. The Army will configure each echelon and unit from the common set of components.

Figure 1-3 shows the DCGS-A applications available to the DCGS-A operators to perform their functions. The majority of the components are commercial off-the-shelf and government off-the-shelf. In addition to the applications resident on the DCGS-A server, DCGS-A also provides widgets via the Ozone Widget Framework.⁸ Selected widgets are shown in Figure 1-4.

⁷ Memorandum, USD(AT&L), Subject: Distributed Common Ground System-Army Increment 1 Program Full Deployment Decision Acquisition Decision Memorandum, December 14, 2012.

⁸ A widget is a small application with limited functionality that can be installed and executed within a web page.

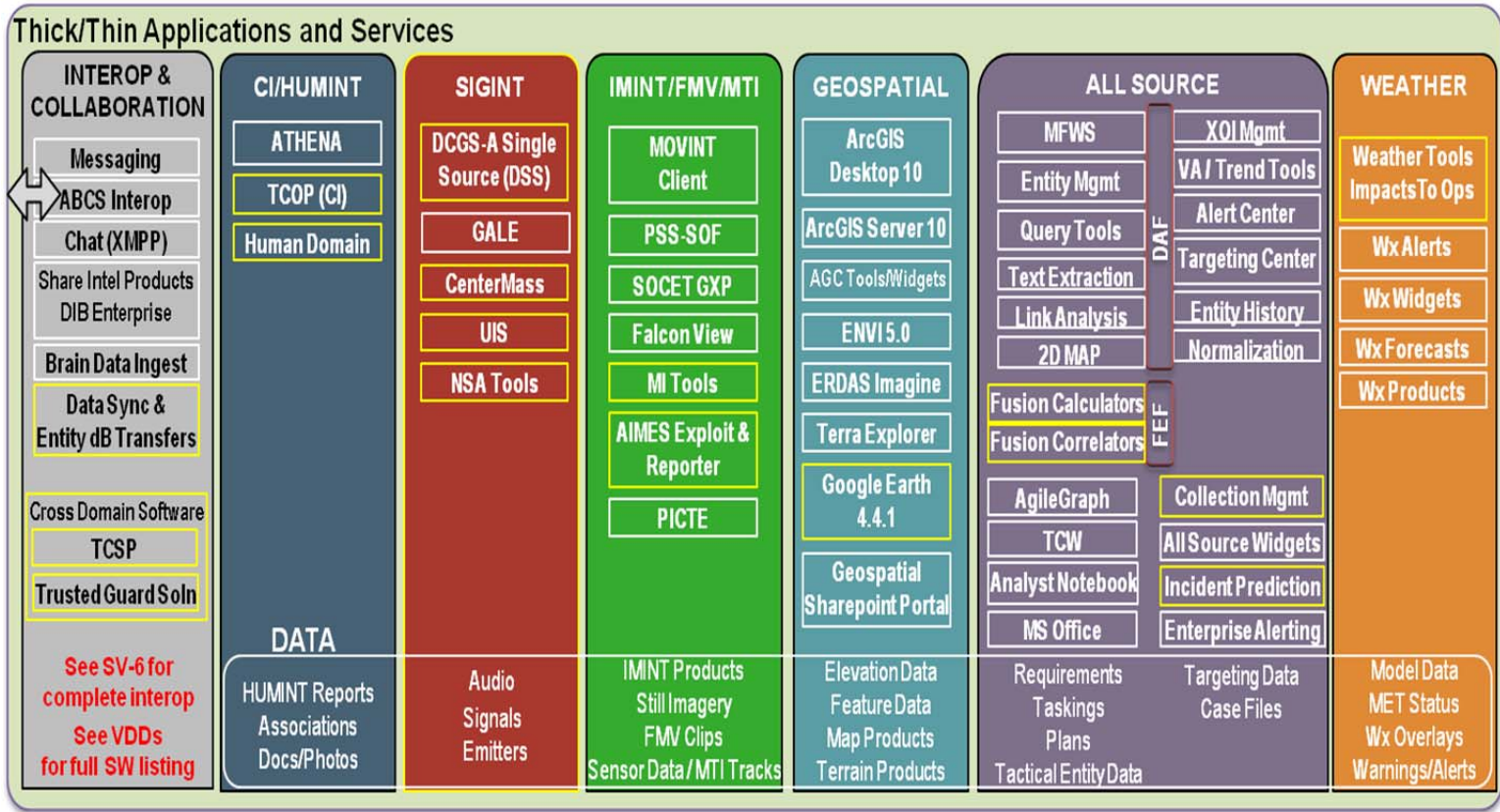


Figure 1-3. Applications Delivered in DCGS-A Increment 1, Release 2¹⁰

10 Acronyms used in Figure 1-3: Extensible Messaging and Presence Protocol (XMPP); Database (dB); Version Description Document (VDD); Software (SW); Counter Intelligence (CI); human intelligence (HUMINT); Advanced Tactical HUMINT Nexus-Army (ATHEN-A); Theater Common Operational Picture (TCOP); DCGS-A Single Source (DSS); Generic Area Limitation Environment (GALE); Unit Identification System (UIS); National Security Agency (NSA); Movement Intelligence (MOVINT); Precision Strike Suite, Special Operations force (PSS-SOF); Soft Copy Exploitation Toolkit, Global Exploitation Products (SOCET GXP); Motion Intelligence (MI); Advanced Intelligence Multimedia Exploitation Suite (AIMES); Primary Image Capture Transformation Element (PCTE); Imagery Intelligence (IMINT); Full Motion Video (FMV); Moving Target Indicator (MTI); Aeronautical Reconnaissance Coverage Geographic Information System (ArcGIS); Army Geospatial Center (AGC); Exelis Visual Information Solutions (ENVI); Earth Resources Data Analysis System (ERDAS); Multi-Function work Station (MFWS); DCGS-A Applications Framework (DAF); Fusion Exploitation Framework (FEF); Threat Characterization Workstation (TCW); Extended area Of Interest (XOI); Vulnerability Assessment (VA); Weather (Wx); Meteorological status (MET status)

V3.2 WIDGETS			
ATHENA	QUERY	WEATHER	SYNAPSE
CollectionRequirements	Common Query	Admin Config	Recordset Browser
Image Viewer	Query Tree	Advanced Viewer	CSV Import
Messages	TED Query	Basic Sensor	Domain Master
Query	TED Properties Editor	Forecast	
Relationship Viewer		IWEDA	AUXILIARY WIDGETS
Reports	TOOLS	IWEDA Rules	Common Record
Unit Status	DIB Upload	KML	XOI Editor
Upload	Data Mover Status	Message Config	GeoPrint
	Help	NBC Met	
GEOSPATIAL	Home	Overlays	ADMIN ONLY WIDGETS
GeoDiscover	IST	Point IWEDA	Logs (Kibana)
GeoExport	Name Variant	Products	Zabbix
GeoWebView	Self Service	Reachback WMS	Common Admin
Common Map	STRIPE	Sensor Config	Access Manager
XOI Manager	Widget Workflow Analyst	Sensor Viewer	Puppet
	Widget Workflow Designer	Solar/Lunar Calculator	JR2
HUMINT	Widget Workflow Monitor	WRE Location	Athena Admin
BAT Query		Warnings	
BAT Dossier			
DIMS-F Query			
DIMS-F Dossier			

Figure 1-4. Applications (Widgets) available to DCGS-A through the Ozone Widget Framework¹¹

¹¹ Acronyms used in Figure 1-4: Extended area Of Interest (XOI); Human Intelligence (HUMINT); Biometric Automated Toolset (BAT); Detainee Information Management System-Fusion (DIMS-F); Tactical Entity Database (TED), DCGS Integration Backbone (DIB); Intelligence, Surveillance, and Reconnaissance (ISR) Synchronization Tool (IST); Staff Tool for Rapid Incident Prediction and Evaluation (STRIPE); Integrated Weather Effects Decision Aid (IWEDA); Web Map Service (WMS); Kelyhole Markup Language (KML); National Broadcasting Company Metrocast (NBC Met) ; Weather Running Estimate (WRE); Comma Separated Values (CSV)

Section Two

Test Adequacy

Test Conduct

The Army Test and Evaluation Command (ATEC), in conjunction with the U.S. Army Brigade Modernization Command, conducted the DCGS-A FOT&E from May 2 – 14, 2015 at Fort Bliss, Texas during Network Integration Evaluation (NIE) 15-2. ATEC conducted the FOT&E in accordance with the DOT&E-approved test plan, but did not accomplish the data collection, reduction, and analysis as described in the approved test plan. ATEC, the Army's Threat System Management Office (TSMO), and the National Security Agency (NSA) conducted additional cybersecurity testing for the DCGS-A Top Secret/Sensitive Compartmented Information (TS/SCI) enclave March through July 2015.

The test scope included a mixture of live and simulated friendly and enemy forces. The test followed the NIE "Attica" Scenario, replicating Wide Area Security (WAS) and Combined Arms Maneuver (CAM) operations:

- Live:
 - Friendly Force: Army 2nd Brigade Combat Team (BCT), 1st Armored Division Tactical Operations Center (TOC), three subordinate battalion TOCs and selected company elements.
 - Opposing Force: Elements of fictional Ellisian Army, local insurgents, and rogue Attican military elements portrayed by 1-35 armored battalion command staff and some company elements; fictional Laconian Army helping the opposing force with cyber and electronic warfare attacks on friendly forces.
- Simulated:
 - Friendly Force: Army division/adjacent brigade
 - Opposing Force: Ellisian corps, division and brigade units, and insurgent units.

Figure 2-1 below shows the test architecture for the FOT&E. The architecture adequately represented an operationally realistic employment of DCGS-A.

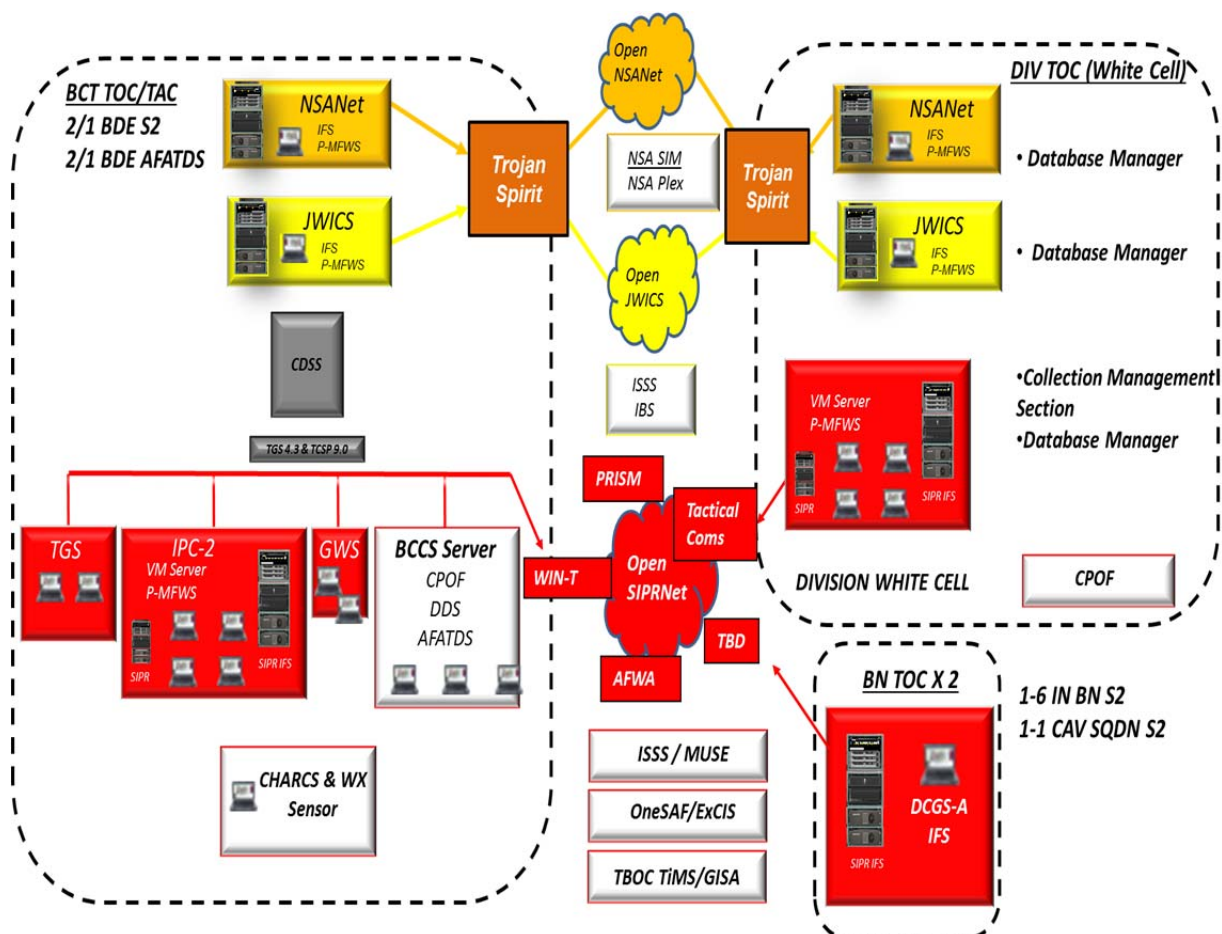


Figure 2-1. FOT&E Test Architecture¹²

The assessment design focused on the operational value of the DCGS-A; that is, its ability to help intelligence professionals find, process, and exploit relevant information, and provide the intelligence to the BCT commanders and staff. Testers injected 10 operational

¹² Acronyms on this figure: Advanced Field Artillery Tactical Data System (AFATDS); Air Force Weather Agency (AFWA); Army Electronic Proving Ground (EPG); Army Operational Test Command (OTC); Army Training and Doctrine Command (TRADOC); Automated Scripter Simulator Exercise Trainer (ASSET); Battle Command Common Services (BCCS); Command Post of the Future (CPOF); Counterintelligence Human Intelligence Automated Reporting and Collection System (CHARCS); Cross Domain Solution Suite (CDSS); Defense Dissemination System (DDS); Geospatial Workstation (GWS); Intelligence Fusion System (IFS); Intelligence Modeling and Simulation Evolution (IMASE); Joint Test Suite (JTS); Joint Worldwide Intelligence Communication System (JWICS); Limited User Test (LUT); Multiple Unmanned Aerial Vehicle Simulation System (MUSE); National Security Agency Network (NSANet); One Semi-Automated Force (OneSAF); Portable Multi Function Workstation (P-MFWS); Secret Internet Protocol Router Network (SIPRNet); Tactical Ground Station (TGS); TRADOC Tactical Internet Management System (TiMS); Warfighter Information Network–Tactical (WIN-T); Weather (WX); IMASE Simulation and Scoring Subsystem (ISSS); Virtual Machine (VM); Integrated Broadcasting System (IBS), Training Brain Operations Center (TBOC); Intelligence Processing Center – 2 (IPC-2); Planning Tool for Resource Integration, Synchronization, and Management (PRISM); Ground Intelligence Support Activity (GISA); Extensible C4I Instrumentation Suite (ExCIS); Command, Control, Communications, Computer and Intelligence (C4I).

vignettes developed by the Brigade Modernization Command (BMC) and ATEC into the overall NIE 15-2 “Attica” scenario. Five vignettes represented WAS story lines and five represented CAM story lines. A key FOT&E objective was to observe how many of the injected vignettes the test unit would find using the intelligence clues provided by DCGS-A.

The vignettes were operationally realistic story lines such as finding and destroying facilities that manufacture improvised explosive devices (IEDs), and finding and targeting the enemy troop movements. To support the vignettes, the test team injected realistic intelligence data elements such as intercepted communications, situation reports, satellite pictures, and full motion videos. These data elements were injected into a database containing terabytes of other information including actual intelligence from combat theaters.¹³ This large, realistic database is called Training Brain Operations Center (TBOC), and is used for Army intelligence analyst training. The objective of the FOT&E was to observe the unit’s ability to successfully discover the injected data elements, and then use them to reach accurate conclusions regarding the enemy actions.

ATEC collected data from network instrumentation, logs from DCGS-A and the supporting simulation, copies of unit intelligence products, and observer and data collector notes. ATEC also collected surveys and questionnaires from the users, including the System Usability Scale (SUS). ATEC, however, did not reduce the collected data sufficiently to address all 10 vignettes in detail, or to assess the details of intelligence fusion, targeting, and data synchronization. The lack of sufficient data precluded DOT&E from performing a robust quantitative analysis on those functions.

The cybersecurity assessment covered all three security domains in DCGS-A; Secret, Joint Worldwide Intelligence Communications System (JWICS), and National Security Agency Network (NSAnet). The Army conducted the cybersecurity test in two phases. The first phase was performed during NIE 15.2. The Army Research Laboratory Survivability and Lethality Analysis Directorate (ARL/SLAD) completed a Cooperative Vulnerability and Penetration Assessment (CVPA) on the Secret enclave from March 16 through April 2, 2015. TSMO with ARL/SLAD conducted an Adversarial Assessment against the Secret-level networks from April 19 through May 21, 2015.

The second cybersecurity test phase was an assessment of the Secret, JWICS, and NSAnet enclaves on a DCGS-A system in the Program Management Office’s Ground Station Integration Facility (GSIF). ARL/SLAD completed CVPAs from April 13 – 19, 2015 on the Secret enclave, and from April 13 – 24, 2015, on the JWICS network enclave. ARL/SLAD conducted another test from September 21 – 25, 2015, on the Secret enclave to validate fixes to problems found during the FOT&E. TSMO and ARL/SLAD completed an Adversarial Assessment against the JWICS network enclave from June 1 – 6, 2015. The NSA completed a

¹³ The actual intelligence from combat theater is derived from the Training Brain Operating Center (TBOC) data. TBOC uses actual intelligence from the theater, but modifies the names and other details to fit with the NIE scenario.

CVPA of the NSANet enclave from May 1 – 6, 2015, and an Adversarial Assessment from June 1 – 6, 2015.

The Program Office and ATEC conducted a data synchronization excursion in the GSIF from September 14 – 24, 2015, under operationally realistic network conditions. The test provided sufficient data to evaluate detailed performance characteristics for data synchronization, and identify the causes of data synchronization issues observed during FOT&E.

Test Adequacy

The FOT&E was adequate to evaluate the operational effectiveness, suitability, and survivability of DCGS-A, but inadequate to quantify some performance details of DCGS-A functionality. ATEC conducted the test events in accordance with the DOT&E-approved test plan, but did not conduct the data collection, reduction, and analysis as approved by DOT&E. ATEC's test database is not sufficient for a quantitative assessment of key functions including intelligence fusion, targeting, and data synchronization. DOT&E sent a memorandum to ATEC on June 29, 2015, to identify data shortfalls, and made specific recommendations to improve the process for future ATEC operational tests.¹⁴ The GSIF event provided sufficient additional data to provide a quantitative evaluation of data synchronization. This quantitative evaluation was critical to identify and fix a data synchronization issue discovered during the FOT&E.

The DOT&E-approved Test and Evaluation Master Plan specified that data necessary to characterize DCGS-A needed to come from the Developmental Test-2 (DT-2) conducted in September 2014 at Fort Huachuca, Arizona. However, ATEC failed to provide sufficient data from the DT-2. The DOT&E memorandum dated March 11, 2015, documented specific shortfalls, and recommended that ATEC demonstrate the data collection, reduction, and analysis process before the FOT&E.¹⁵ The memorandum also recommended that ATEC expand the operational effectiveness measure by using operational vignettes and associated intelligence information in the FOT&E test plan. ATEC's FOT&E plan complied with DOT&E's recommendations, and the operational vignettes injected in the test plan allowed adequate evaluation regarding the DCGS-A's contribution to mission success. However, ATEC did not succeed in executing the data reduction as recommended in DOT&E's memorandum and specified in ATEC's test plan.

Following the FOT&E, the ATEC-provided data were incomplete in many cases, and contained many anomalies that could not be resolved. ATEC's database contained 275 folders with 6,090 files; far too many to conduct a timely evaluation. In accordance with the test plan, ATEC should have produced a coherent and authenticated database organized by the measures of performances.

¹⁴ DOT&E memorandum to ATEC, Subject: Inadequate Data Collection, Reduction, and Analysis (DCRA) for the Distributed Common Ground System – Army (DCGA-A) Increment 1, Release 2 Follow-on Test and Evaluation (FOT&E), June 29, 2015.

¹⁵ DOT&E memorandum to ATEC, Subject: Distributed Common Ground System – Army (DCGS-A) Developmental Test-2 (DT-2) Results and Impacts to the DCGS-A Follow on Test and Evaluation (FOT&E) Plan, March 11, 2015

ATEC did not deliver sufficient data to calculate metrics such as the percentage of successful correlation, a key metric for intelligence fusion. By the time data reduction progressed sufficiently to discover inconsistencies and anomalies, the ATEC team could not reconstruct events sufficiently to resolve the anomalies. At the end of the record test, ATEC reported that only 61 of the 113 measures of performance identified in the test plan had sufficient quantitative data to support a quantitative evaluation. The key measures associated with the intelligence fusion, data synchronization, and targeting were not among the 61.

This page intentionally left blank.

Section Three

Operational Effectiveness

Mission Accomplishment

DOT&E evaluated the ability of DCGS-A to contribute to mission success by observing how well the test brigade equipped with DCGS-A could find intelligence data and exploit them to arrive at an accurate enemy situation assessment. To facilitate that evaluation, the test team developed operational vignettes, which were story lines that describe enemy activities. Table 3-1 below shows the 10 vignettes used for the FOT&E. Once the vignettes were developed, the test team produced operationally representative intelligence data corresponding to those vignettes, such as videos or pictures showing enemy actions or communications indicative of enemy intentions. The test team then injected those intelligence data into the intelligence database used for the NIE, which contained the terabytes of other data unrelated to the vignettes.

The Network Integration Evaluation (NIE) intelligence database was composed of data from the Army Training and Doctrine Command's (TRADOC) Training Brain Operations Center (TBOC), which contains terabytes of intelligence data, including data from combat theaters. TRADOC uses TBOC for operationally realistic Soldier and leader training. During FOT&E, the test unit continued to generate and store operationally representative intelligence data in the database.

Five of the ten vignettes (1, 2, 5, 6, and 9) emulated Wide Area Security (WAS) story lines, while the other five vignettes (3, 4, 7, 8 and 10) emulated Combined Arms Maneuver (CAM) storylines. Vignette 2 was played three times (2a, 2b, and 2c) because the test unit found and destroyed the improvised explosive device (IED) factory much quicker than expected (2a), and the enemy set up a second location, which the test unit found and destroyed again (2b). The enemy set up a third location, and the test unit found it, and was planning to destroy that location when the test ended (2c).

During the test, daily synchronization meetings with members from the Brigade Modernization Command (BMC), ATEC, and DOT&E confirmed that the test unit used DCGS-A to discover and exploit the intelligence data associated with all 10 vignettes, and made appropriate operational recommendations to counter the enemy actions. The test unit analysts completed the expected intelligence actions for all five WAS vignettes. These actions include activities such as posting a signals intelligence report for the vignettes and developing an intelligence summary report. The test data confirm that the test unit completed the expected intelligence actions for two of the five CAM vignettes. Shortfalls in ATEC's data collection prevented DOT&E from fully confirming the detailed intelligence actions associated with all five CAM vignettes. Appendix A describes the 10 vignettes in detail.

Table 3-1. Operational Vignettes

	Vignette	Who	26	27	28 APR–1 May	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th	13th	14th		
			Sun	Mon	Tue–Fri	Sat	Sun	Mon	Tue	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur		
Target Insurgent Leader	1	1-1 CAV	Target Insurgent Leader																	
Target IED Factory	2a	1-6 IN	TGT IED Factory																	
Target IED Factory	2b	1-6 IN											TGT IED Factory							
Target IED Factory	2c	1-6 IN											TGT IED Factory							
Target Reserve Forces	3	2/1 AD & 1-1 CAV							Target Reserve Force											
Target Air Defense Radars	4	1 AD & 2/1 AD	Target ADA Radars																	
Disrupt SVBIED Attack	5	2/1 BCT							Disrupt SVBIED Attack											
Disrupt Assassination Plot	6	1-6 IN	Disrupt Assassination Plot																	
Engage Enemy Recon	7	1 AD & 1-1 CAV	Engage Enemy Recon																	
Target Heavy Insurgents	8	1-1 CAV	Target Heavy Insurgents																	
Target Rogue ANA Leader	9	1-1 CAV	ANA Ldr																	
Target Ellisian Invasion	10	1 AD	Invasion																	

Wide Area Security (WAS) Operations Vignettes

The five vignettes for WAS operations are similar to operations conducted over the past several years by deployed Army forces. The unit maintained situational understanding of insurgent structure and activities with DCGS-A and provided link diagrams (see Figure 3-2) and daily intelligence summaries, and discovered and targeted high value individuals consistent with the vignettes.

Vignette 1 Target Insurgent Leader

DCGS-A enabled the test unit to find and neutralize an insurgent leader in four days. Test unit analysts used historical information provided via DCGS-A to determine that a known insurgent leader was meeting with an arms supplier and leader of a rogue host nation military unit. During the pilot test, the unit found and killed the rogue military leader. Following the death of the rogue military leader, intelligence analysts determined that the rogue military organization chose a new person to take over the arms trafficking role of his deceased predecessor. Analysts then used signals intelligence, human intelligence (HUMINT), and GEOINT provided by DCGS-A to track, locate, target, and kill the new rogue military leader.

Vignette 2a Target Improvised Explosive Device (IED) Factory

DCGS-A enabled the test unit over five days of operations to discover and target an IED factory. Analysts used historical data provided via DCGS-A to identify a village as a known IED cache site, and to identify the lead IED maker. Geospatial Intelligence (GEOINT) analysts used DCGS-A to find imagery showing increased vehicle activity and the presence of crates in the village. The analysts concluded that IED training was taking place and used signal intelligence and HUMINT to confirm the presence of a lead IED maker in the village. Analysts used DCGS-A to conduct terrain analysis of the village to identify avenues of approach and egress, probable threat locations, and hazards. DCGS-A's intelligence support enabled the unit to target the factory.

Vignette 2b Target IED Factory

The test unit used DCGS-A, over five days of operations, to discover and target a second IED factory. DCGS-A provided intelligence that indicated IED activities had moved from the first village to the second village. Analysts using DCGS-A identified the building being used as the new IED factory and confirmed increased activity at the suspected IED site. GEOINT provided by DCGS-A enabled identification of potential enemy positions and avenues of approach during battle planning. The test unit secured the IED factory based on the intelligence input provided by DCGS-A.

Vignette 2c Target IED Factory

The test unit discovered the third of three IED factories over six days of operations. HUMINT provided by DCGS-A revealed that insurgents were setting up checkpoints and stealing fuel from detained vehicles, and further revealed that villagers reported hearing explosions near the third IED factory. Other intelligence provided by DCGS-A revealed that IED experts were experimenting with fuel oil in the village. Analysts used intelligence reports to learn that stolen vehicles were sent to the village. DCGS-A GEOINT identified bomb-making residue in fresh craters near the village and DCGS-A terrain analysis identified travel routes to the village. An unmanned aerial vehicle confirmed enemy positions in village. The test ended as unit took action on the third IED factory.

Vignette 5 Disrupt Suicide Vehicle-Borne IED Attack

DCGS-A enabled the unit to determine indications of an impending vehicle borne improvised explosive device (VBIED) attack. Historical information and HUMINT reports indicated VBIED preparation in vicinity of Zamania. Analysts noticed increased enemy reconnaissance near a friendly force headquarters, and received HUMINT reports of insurgents planning VBIED activities. The DCGS-A analyst created vehicle be-on-the-look-out (BOLO) list on the TED, and disseminated the intelligence with the Automated product tool. The analyst received reports via the DCGS-A about stolen vehicles near IED factory in Zamania. The All-Source analyst used DCGS-A Link Diagram to assess the organization preparing the attack. GEOINT Intelligence identified a vehicle at a known IED factory. The HUMINT analysts identified the VBIED vehicle and driver. GEOINT products showed that a VBIED was at a known IED factory, and a HUMINT analyst later reported that the vehicle had left. The analysts advised guards to exercise extreme caution when the vehicle was reported at the entry control point. The test unit stopped the vehicle and detained insurgents.

Vignette 6 Disrupt Assassination Plot

DCGS-A enabled the test unit to determine existence of an assassination plot against a local mayor. The unit used DCGS-A to produce intelligence summaries and link diagrams, and confirmed that there were historical precedents for insurgents conducting assassinations in the mayor's village. HUMINT sources indicated that the mayor might be the target of an assassination attempt, causing the friendly forces to place the mayor on the list of individuals to protect. Analysts used DCGS-A's GEOINT tools to evaluate sightlines in the mayor's village. Human and SIGINT assembled with DCGS-A revealed insurgents had placed a bounty on the

mayor, and that assailants were on standby. The mayor announced a press conference, but insurgents kidnapped him before the conference. The unit used DCGS-A to find intelligence that the insurgents planned to bring the mayor to his press conference and execute him. Even though the intelligence section informed the test unit commander about the plot, the commander decided that other concurrent operations were a higher priority and chose not to intervene to prevent the assassination.

Vignette 9 Target Rogue Attican National Army (ANA) Leader¹⁶

DCGS-A enabled the test unit over four days of operations to find and neutralize an insurgent leader. Analysts used DCGS-A to review historical information and used link diagram to identify associations that indicated a rogue Attican National Army (ANA) leader was involved in smuggling weapons. Analysts used DCGS-A to discover intelligence revealing meetings between the rogue leader, his associates, and regional members of an insurgency. DCGS-A provided GEOINT confirmed smuggling operations. The test unit used DCGS-A to fuse information from multiple intelligence sources to monitor the rogue leader's movement. The test unit designated the rogue leader their top priority target on the high value individuals target list. Using the intelligence fused by the DCGS-A, the unit learned that the insurgents and rogue ANA leader were causing increased enemy activity in a local village. The commander used the DCGS-A-provided intelligence to task subordinate unit to target and eliminate the rogue leader. The battle damage assessment from the brigade's operations section confirmed the death of the rogue leader.

Combined Arms Maneuver (CAM) Vignettes

Five of the vignettes (3, 4, 7, 8, and 10) involved conventional CAM operations. The results for these vignettes are less conclusive. The test unit was successful in identifying and targeting enemy vehicles and equipment, but was less successful in attributing the equipment and troop to the correct enemy units.

Vignette 3 Target Reserve Forces

The test unit used DCGS-A to locate and target enemy troops and equipment, but the unit did not consistently associate equipment with the correct enemy unit structure. The intelligence analysts used DCGS-A to correctly identify the initial invasion and location of the reserve force. However, shortly thereafter, the analysts incorrectly determined that the unit had moved to a new location when the ground-truth was that the troops and equipment they were seeing belonged to another enemy unit. This resulted in a short-term confusion regarding the strength and location of the enemy reserve force. By the end of the test, however, the test unit analysts had correctly identified the reserve unit's location and disposition.

Vignette 4 Target Air Defense Radars

DOT&E did not find any indication that the test unit took any action to destroy enemy air-defense radars. It could be because the test unit's brigade commander and staff did not

¹⁶ Attica is a fictional host nation country created for the Attica scenario.

choose to act on them. It is also possible that the test unit took actions, but supporting evidence is buried in ATEC's large and mostly uncategorized test database, and DOT&E could not find the relevant data. When the test team designed the vignettes, they understood the test unit might decide not to engage the enemy air defense radars. The test data show that the tools mentioned in the vignette such as the Extended area of Interest (XOI) alerts, and 2D maps functioned as expected. The test data include reports that indicate the test unit knew about the air defense radar locations.

Vignette 7 Engage Enemy Reconnaissance

Data are insufficient to evaluate this vignette. The friendly and enemy units did not conduct the operation as envisioned by the vignette designers. The test team was aware that some vignettes would not happen because the test unit was conducting realistic operations with a live enemy force, and was not bound by the vignette design.

Vignette 8 Target Conventionally Equipped Insurgents

The test unit found and destroyed conventionally equipped insurgent forces. The only notable deviation from the expected actions was that the analyst chose to use text and voice rather than sending a Target Data (TIDAT) message from DCGS-A.

Vignettes 10 Target Enemy Invasion Force

The daily synch meeting discussions indicate the test unit successfully conducted the tasks necessary to track enemy movements. DOT&E could not find the actual products unit produced in the ATEC's large, uncategorized test database. This vignette was part of the pilot test, which occurred prior to the formal start of the FOT&E.

System Performance

The FOT&E demonstrated that a trained and experienced analyst can use the DCGS-A tools and applications to rapidly organize and analyze terabytes of intelligence data and reports and produce actionable intelligence. The DCGS-A Increment 1, Release 2 delivered incremental updates for applications supporting individual intelligence domains. The main advantage of the Release 2, however, is the updated database structure that enhanced intelligence fusion, and the addition of the Top Secret/Sensitive Compartmented Information (TS/SCI) enclave to Brigade Combat Teams (BCTs).

DCGS-A ingests intelligence feeds from more than 700 sources and consolidates the data into the Tactical Entity Database (TED), which organizes the intelligence feeds into a single database that is organized into 12 different entity types; Document, Equipment, Event, Facility, Financial Transaction, HUMINT Source, IED, Individual, Organization, Place, Unit, and Vehicle.¹⁷ Once intelligence information is parsed into the TED, analysts can use DCGS-A applications such as the time-wheel, link diagram, Querytree search, text extraction, and others

¹⁷ An entity is a discrete unit of intelligence information that is organized into one of the 12 types in the Tactical Entity Database (TED).

to search for, analyze and visualize the data, and populate the common operational picture without having to create or organize the database each time. This process turns an activity that could take days or weeks into one that takes only hours.

DCGS-A Release 2 includes TS/SCI enclaves in brigades. With the TS/SCI enclave in the BCT, analysts have the capability to see the in-depth TS/SCI intelligence information, rather than just summary information from higher headquarters. This gives BCT analysts more confidence with their analysis.

DCGS-A analysts do not have the responsibility or authority to directly task intelligence sensors such as cameras on UASs. However, DCGS-A is designed to consolidate sensor requirements and disseminate those requirements to the appropriate sensor owners. DCGS-A includes the Intelligence, Surveillance, and Reconnaissance (ISR) Synchronization Tool (IST), which is designed to consolidate the requests for sensor products and deliver to the owners of the sensors. Ideally, the IST should interface with tasking systems used by all U.S. military Services and agencies. This would allow any U.S. force equipped with DCGS-A to identify their sensor requirements and allocate them to any sensor.

A Defense Intelligence Agency application called Planning Tool for Resource Integration, Synchronization, and Management (PRISM) is the current tool to integrate the sensor resources owned by Services and agencies. The IST does not currently interface with the PRISM. It will require work from both the Defense Intelligence Agency and Army to integrate IST with PRISM.

At the beginning of the FOT&E, the Army mandated the test unit to use the IST. However, the unit reverted to using their old methods, using Intel Synch Matrix (Excel spreadsheet) and sharing through the Army battle command network. The unit used the Psi Jabber (DCGS-A chat tool) to communicate the request for collection and requests for information. Some of the users stated they did not use IST because it took too long and they were unable to see the advantages the tool was intended to provide. The Collection Manager stated the tool was overly complicated and was under the impression that the limited bandwidth made the tool unusable to the operator. The operators stated the process of creating a Primary Information Request and assigning assets took in excess of 1 hour using the IST, compared to minutes using the Intel Synch Matrix and Psi Jabber.

Intelligence Fusion

The fusion model used in the Department of Defense was developed by the Joint Directors of Laboratories in the 1980s. The model defines six levels of fusion (levels 0-5). The six levels, as applied to DCGS-A, are listed below. DCGS-A is designed to assist with levels 0 through 2a.

- Level 0: Pre-processing (Normalization)
 - Incoming data from the sensor or observer are converted to the format DCGS-A can use. The product is a “normalized” entity in the database (standardized lexicon)
- Level 1: Correlation of Data

- The first step is to identify entity type (Document, Equipment, Event, Facility, Financial Transaction, HUMINT Source, IED, Individual, Organization, Place, Unit, Vehicle)
- The second step is to determine if the entity is new or previously known, and merge duplicate information
- Level 2a: Relationship Analysis (Association)
 - Establishes operational and functional relationships between entities by:
 - Connecting common attributes
 - Matching templates and models of expected relationships
- Level 2b: Event and Activity Analysis
 - Correlates the base set of events and then aggregates them into associated clusters (called activities), then analyzes patterns for normalcy or abnormality
- Level 2c: Course of Action (COA) Hypothesis
 - Develop a set of hypothetical COAs, with a measure of the plausibility for each
- Level 3: COA Analysis
 - Project the hypothesized current enemy COA and the friendly actions
 - Draw inferences on threat and vulnerabilities for both
 - Assess projections of intent and strategy for both
- Level 4: Feedback Loop that monitors how levels 0-3 are functioning (tools and processes) and what shortfalls exist
- Level 5: Visualize and interact with the fusion products; use experience to assess the situations to refine solutions or identify knowledge gaps

The DOT&E-approved test plan included plans to collect, reduce, and analyze the data in accordance with the approved design of experiment. This design would have provided sufficient data to evaluate the specific and quantifiable data for DCGS-A's ability to process the level 0, 1, and 2a fusion in accordance with its requirements. The test database delivered after the FOT&E did not contain sufficient data to execute that analysis. However, the success of the link diagrams and situational assessment as evidenced in the vignette execution indicates that normalization, correlation, and association worked well enough to support the test unit's missions.

Although DCGS-A is required to provide assistance with up to level 2a fusion, the test unit used the system effectively to assist with levels 3, 4, and 5 fusion. The actual intelligence products that show the higher level fusion during the FOT&E are classified. However, a few generic examples of DCGS-A displays used for training are provided in Figures 3-1 through 3-6 below. These examples show both the analysis tools the analysts used to assist COA

development and analysis, and the displays that visualized intelligence information in tactical contexts.



Figure 3-1. Example DCGS-A Threat Graphics Tool Display



TARGET: MUMAR MAJAK			UNCLASSIFIED (EXAMPLE)		4/1 ID	
NUMBER: UN4522		AREA: ABU T'SHIR	MUHALLA: 810	STREET:	HOUSE:	
Targeted By: 4-1 ID		Battle Space Owner: TF 2-2		Trigger: HUMINT		
DOI: 05 JAN 2008	TASK: DETAIN	GRID: 38S MB 1234 5678		PHYSICAL DESCRIPTION		
Last given bed down grid (38SMB123456) for Mumar Majak is from 11 SEP 07 from DMR-1CD-12-345-67-8910				Sex: Male Age: 50 +/- Height: 6'2" Body Comp: Heavy Eyes: Blue Hair: Gray Other details: Large ears, normally wears glasses, limp on right leg. Western style clothing		
		TARGET INFORMATION				
		Target Category: Criminal Mastermind				
		Impact: Disrupts international crime syndicate				
		Possible Aliases: UNK				
		Known Movements: UNK				
STATUS:		Affiliations: Usual suspects Family: UNK Vehicles: UNK Religion: Shia				
PID: <input checked="" type="checkbox"/>	Target Summary: Mumar Majak is an international criminal mastermind in international narcotic production and smuggling, weapon smuggling, murder, extortion, racketeering, and other evil.					
Source: <input checked="" type="checkbox"/>						
Location: <input checked="" type="checkbox"/>						
Intel Cost: <input checked="" type="checkbox"/>						
Evidence: <input checked="" type="checkbox"/>						
Trigger: <input checked="" type="checkbox"/>	UNCLASSIFIED (EXAMPLE)		Source: HUMINT			
				Last updated with HUMINT		

Figure 3-3. Example DCGS-A Threat Characterization Workstation Display



Figure 3-4. Example DCGS-A Line-of-Sight Tool Display

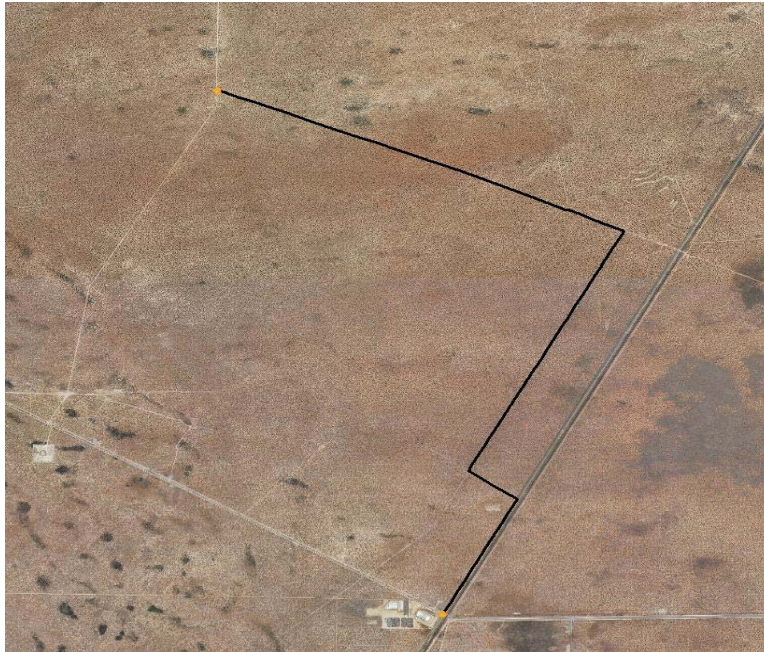


Figure 3-5. Example DCGS-A Route Time Speed Tool Display

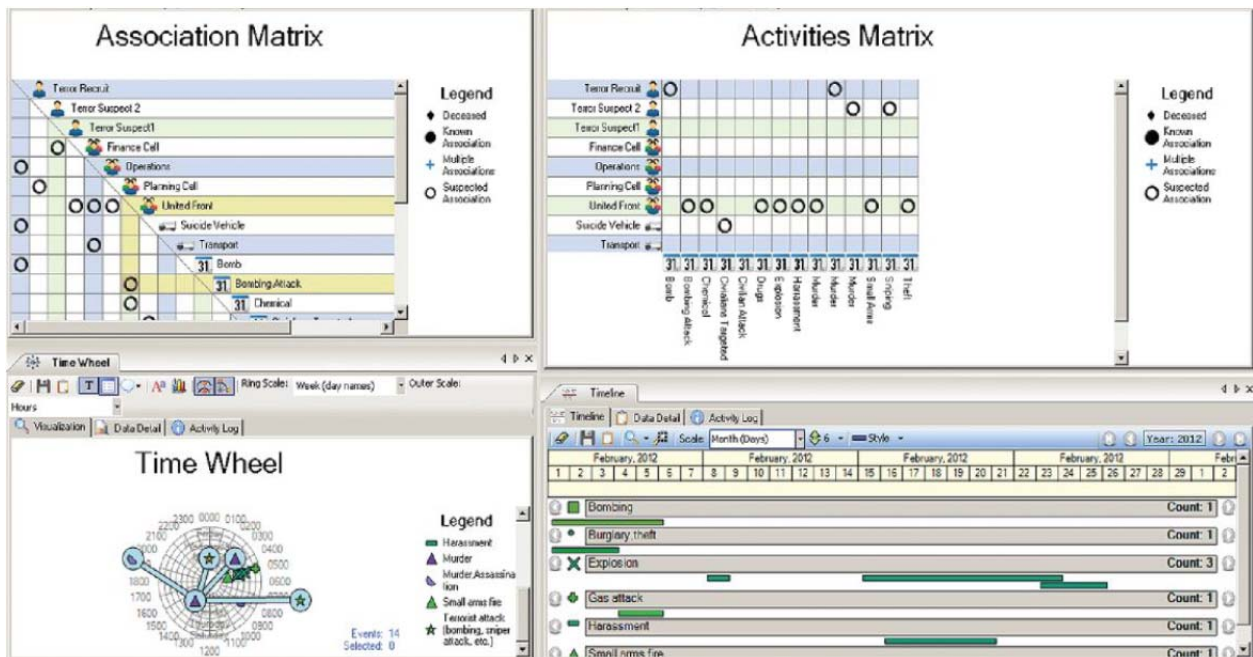


Figure 3-6. Examples of Selected Other DCGS-A Displays

Targeting Nomination

DCGS-A targeting functionality involves four steps.

1. Ingest information from intelligence sources. DCGS-A converts all received information to latitude and longitude for storage in the TED.
2. Update TED entities and compare with targeting criteria to identify potential targets.

3. Nominate targets by creating a Target Intelligence Data (TIDAT) message that includes descriptions and locations of the nominated targets—the default target location error for DCGS-A TIDATs is 500 meters. For nominated targets, the DCGS-A converts the stored latitude-longitude information to military grid reference system in the TIDAT. Only 10 of the 41 test records provided by ATEC contain information to compare the TIDAT location with the entity location stored in the TED. Nine of the 10 records have TED and TIDAT locations within the default target location error of 500 meters. ATEC provided insufficient information to determine why one record has a location difference of greater than 500 meters for the TED and the TIDAT.
4. Send the TIDAT to the Advanced Field Artillery Tactical Data System (AFATDS) for execution. Twenty-nine of forty-one of ATEC's test records contain information to compare the AFATDS targeted location with the location in the TIDAT message. Twenty-five of twenty-nine (86 percent) records have differences within the default target location error. Insufficient information is available to determine why four records have location differences greater than 500-meter differences.

The test unit believed that the target locations provided from DCGS-A to AFATDS were inaccurate. The data, although of very limited sample size, indicate that DCGS-A itself and its interoperability with AFATDS are not the inherent causes of the inaccuracies. Targeting data recovered by Program Management Office from brigade's server and message information from the simulation indicate that delay in the time from message ingest by DCGS-A and transmission of the TIDAT to AFATDS is a possible cause. For 91 analyzable records the median time between message ingest and TIDAT transmission was approximately 30 minutes. For moving targets, a delay of 30 minutes would make the TIDAT location inaccurate compared to the actual location. However, ATEC did not provide the necessary ground truth locations for all entities from the simulation to confirm this hypothesis. Another possible cause is that reported entity locations in simulated messages often differed from the actual locations in the simulation. From between 30,000 and 500,000 messages per day, the daily median differences in ground truth and reported locations were between 1 and 2 kilometers. ATEC's database was not complete enough for DOT&E to determine the cause of these differences.

Situation Assessment and Order of Battle

The Threat Characteristics WorkCenter is a new tool in Release 2 to assist the unit with forming enemy order of battle and tracking enemy unit strength. The test unit found the tool technically immature. When updating enemy unit strength, a design flaw in the tool showed enemy attrition of some units as greater than 100 percent, which is physically impossible. Updates to the TED deleted the order of battle for enemy units in the WorkCenter, forcing analysts to re-create the enemy order of battle, something that happened often. Analysts were better at tracking insurgent group hierarchy than they were at establishing conventional enemy unit order of battle and strength. This indicates that analysts may need more training at intelligence analysis for conventional operations. One user suggested that aids such as threat template libraries would help.

Database Synchronization

The test unit reported problems with data synchronization. Reported problems included synchronizations not finishing, losing filter information when making changes, and battalions losing information from their database when accepting updates from the brigade that included merged data from other battalions. The FOT&E data were insufficient to characterize the performance and determine causes.

At the request of DOT&E, in September 2015, the DCGS-A Program Management Office conducted a data synchronization test in its Ground Station Integration Facility to explore the problems reported from the FOT&E. The test used a WIN-T emulator to simulate a stable tactical network with varying bandwidths and time delays. The test compared four methods for synchronizing the data:

- Ad-Hoc synchronization using the Datamover application (the test unit used this method during the FOT&E)
- Interchange File Format (IFF) Remote Package Archive (RPA) files
- Virtual Cabinet (VCAB)
- Datamover application in scheduled job mode

Factors in the experimental design were: number of entities, file size, and network bandwidth. The time to complete the synchronization was the response variable. The bandwidth of the connection between the two DCGS-A systems was varied to match the following three bandwidths utilized during NIE 15.2:

- 1) Low Bandwidth: 1024 kilobits per second (kbps)
- 2) Medium Bandwidth: 2048 kbps
- 3) High Bandwidth: 4096 kbps

The test team selected representative files from the FOT&E database. The test files are described in Table 3-2 below: they include high, medium, and low numbers of entities. Each entity could contain different size files, such as a pre-formatted message (4 kilobits) or a full motion video (15,000 kilobits). The test team selected representative files that contained small, medium and large sized files.

Table 3-2. Test Input Data Files

Index	Original File Name	# of Entities	File Size (kb)	Category	
				# of Entities	File Size
1	1918.07.192Z.iff	5	4	Small	Small
2	0833.52.984Z.iff	7	1700	Small	Medium
3	1823.47.335Z.iff	5	15000	Small	Large
4	0722.47.866Z.iff	330	92	Medium	Small
5	0748.48.945Z.iff	408	1994	Medium	Medium
6	0604.32.940Z.iff	416	15538	Medium	Large
7	0451.14.400Z.iff	951	276	Large	Small
8	0723.12.543Z.iff	874	2300	Large	Medium
9	1843.57.961Z.iff	891	15000	Large	Large

Figures 3-7 and 3-8 below summarize the findings. The figure 3-7 plots show data synchronization times for various file sizes over high, medium, and low bandwidth. Each data synchronization method is plotted on separate lines. The plots show using Ad-Hoc Datamovers will take about 3,000 seconds (50 minutes) consistently regardless of the file size or bandwidth, whereas the same task can be completed within 1,000 seconds (17 minutes) using any other method.

Figure 3-8 plots present the synchronization time for large, medium, and small numbers of entities. It shows that time requirement increases in direct relation to the number of entities when the Ad-Hoc Datamover method is used, but not when any other methods are chosen.

Table 3-3 shows the correlation factors. As the highlighted items show, the correlation is relatively low for all four methods for bandwidth and file sizes. In other words, the bandwidth and files sizes had no discernable influence on the synchronization time. The correlation between the time and number of entities are above 0.9 for all four methods, indicating that the number of entities is the dominant determinant for time for data synchronization. This means that the number of entities will influence the synchronization time regardless of the method chosen. However, all three right-hand side plots Figure 12 show that slope is steep for Ad-Hoc Datamover but very flat for all the others. This means that the number of entities will have much more influence on the time for Ad-Hoc Datamover than for any other method.

The explanation for the correlation between the time and number of entities can be found in the data synchronization protocols. For Ad-Hoc Datamover, each entity is treated as a separate file item, requiring the link to be established between the sending and receiving terminals before each entity is transferred. To move a file containing 951 entities, the network has to establish the linkage 951 times. In contrast, all other methods transfer the entire database

once the link is established. Thus, the sending and receiving terminals need to establish the linkage only once, regardless of the number of entities in the database.

The Ad-Hoc Datamover was designed for cases where the user has to send a quick update. The test unit chose to use this method because they did not want to be bound to a pre-set schedule and they wanted to perform data synchronization when other activities were at low level. This is fine as long as the unit uses the Ad-Hoc Datamover to move a quick update involving only a few entities. When synchronizing a large database with hundreds of entities, the user can “schedule” individual Datamover synchronization for a minute or two in the future. This will allow the users to choose when they want to synchronize each time without the time delay of the Ad-Hoc Datamover method.

In summary, the data synchronization test excursion provided these insights:

- The method the test unit used, Ad-Hoc DataMover, is significantly slower than any other method when synchronizing a large number of entities.
- Even low bandwidth (1024 kbps) is not a limiting factor for data synchronization; there is no significant difference between time and bandwidth when the bandwidth is 1024 kbps or higher.
- File sizes do not make significant difference to the data synchronization time.
- Although the number of entities directly correlate with the synchronization time regardless of the synchronization method, the time requirement increases rapidly with the number of entities only with the Ad-Hoc Datamover method.

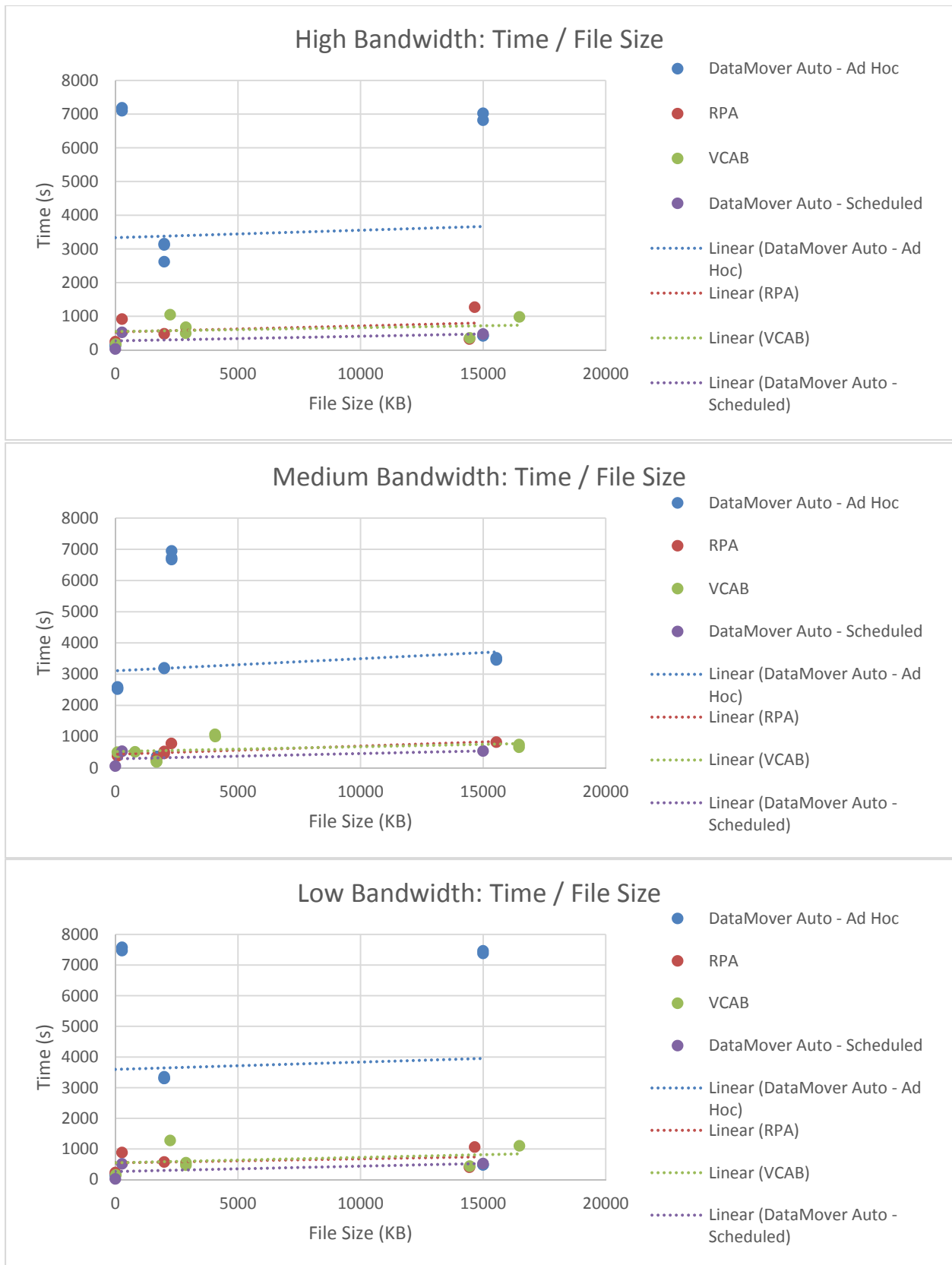


Figure 3-7. Overall Results of the Data Synchronization Test, Time vs File Size

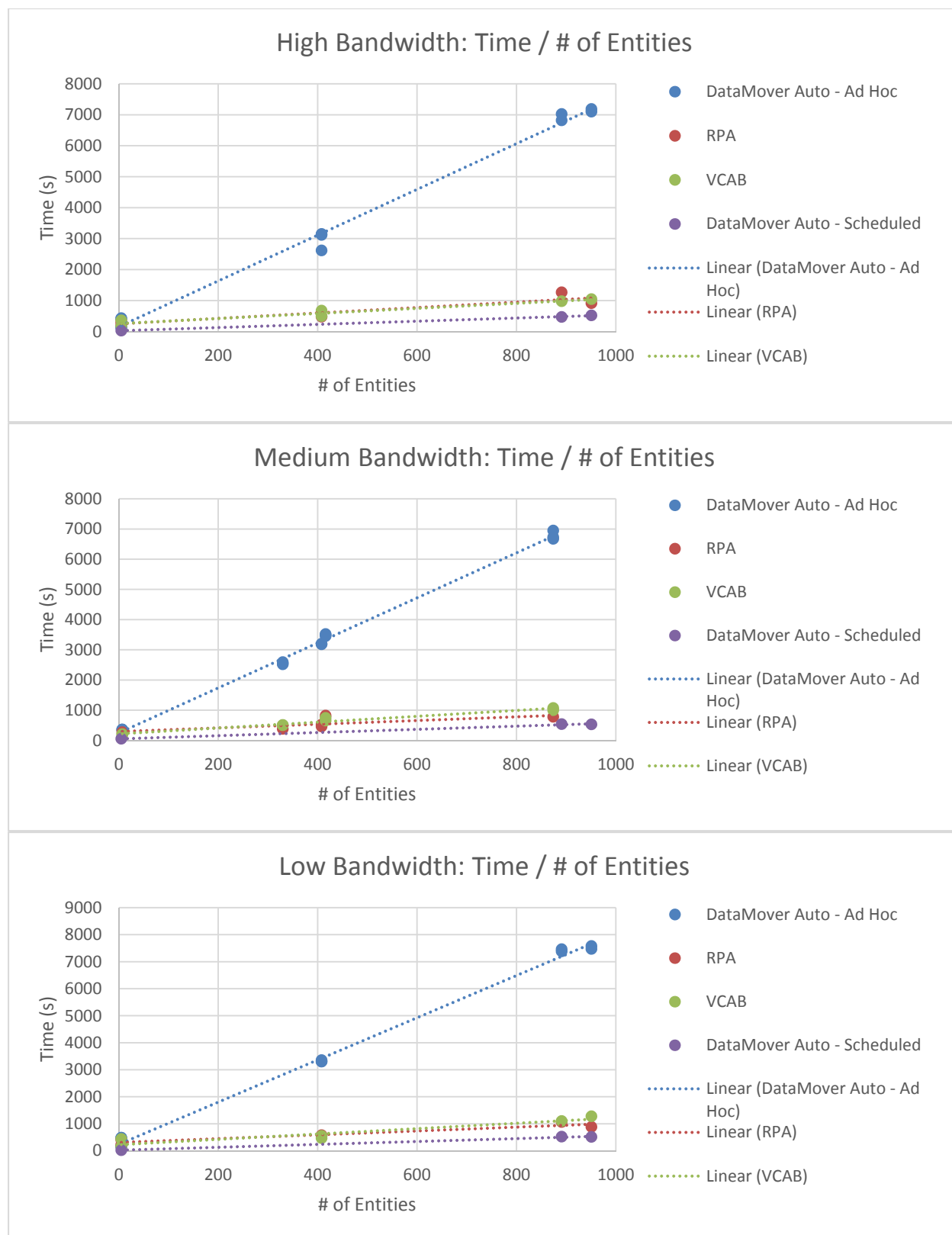


Figure 3-8. Overall Results of the Data Synchronization Test, Time vs Number of Entities

Table 3-3. The Summary of the Data Synchronization Correlation

Method	Variable	by Variable	Correlation	Lower 95%	Upper 95%
Ad-Hoc DataMover	File Size (kB)	Bandwidth (Mbit/s)	0.03	-0.29	0.35
Ad-Hoc DataMover	Number of Entities	Bandwidth (Mbit/s)	0.03	-0.30	0.34
Ad-Hoc DataMover	Number of Entities	File Size (kB)	0.06	-0.26	0.37
Ad-Hoc DataMover	Total Time (s)	Bandwidth (Mbit/s)	-0.01	-0.33	0.31
Ad-Hoc DataMover	Total Time (s)	File Size (kB)	0.10	-0.22	0.41
Ad-Hoc DataMover	Total Time (s)	Number of Entities	0.99	0.99	0.99
IFF RPA	File Size (kB)	Bandwidth (Mbit/s)	0.04	-0.47	0.52
IFF RPA	Number of Entities	Bandwidth (Mbit/s)	0.01	-0.49	0.50
IFF RPA	Number of Entities	File Size (kB)	0.02	-0.48	0.51
IFF RPA	Total Time (s)	Bandwidth (Mbit/s)	0.03	-0.47	0.52
IFF RPA	Total Time (s)	File Size (kB)	0.38	-0.14	0.74
IFF RPA	Total Time (s)	Number of Entities	0.91	0.77	0.97
Scheduled DataMover	File Size (kB)	Bandwidth (Mbit/s)	0.16	-0.52	0.72
Scheduled DataMover	Number of Entities	Bandwidth (Mbit/s)	0.08	-0.58	0.67
Scheduled DataMover	Number of Entities	File Size (kB)	0.50	-0.20	0.86
Scheduled DataMover	Total Time (s)	Bandwidth (Mbit/s)	0.07	-0.59	0.67
Scheduled DataMover	Total Time (s)	File Size (kB)	0.53	-0.15	0.87
Scheduled DataMover	Total Time (s)	Number of Entities	0.99	0.98	0.99
VCAB	File Size (kB)	Bandwidth (Mbit/s)	0.04	-0.41	0.48
VCAB	Number of Entities	Bandwidth (Mbit/s)	0.01	-0.43	0.45
VCAB	Number of Entities	File Size (kB)	0.05	-0.40	0.48
VCAB	Total Time (s)	Bandwidth (Mbit/s)	-0.04	-0.48	0.41
VCAB	Total Time (s)	File Size (kB)	0.20	-0.27	0.59
VCAB	Total Time (s)	Number of Entities	0.96	0.91	0.99

Human Intelligence (HUMINT)

The Human Domain (HD) tool failed multiple times during the pilot test and caused a large amount of data to be irretrievably lost (estimated ~130 hours of work lost from two incidents). After those incidents, the test unit's HUMINT analysts lost confidence in the HD plug-in and asked permission to use the Counterintelligence HUMINT Automated Reporting and Collection System (CHARCS) and Advanced Tactical HUMINT Nexus-Army (ATHENA) to

support operations—the test team agreed with the request. CHARCS is a separate acquisition program that helps collection and reporting of HUMINT and ATHENA is a HUMINT tool delivered with the DCGS-A Release 2, with fewer functions than the HD. The HUMINT analysts did not see much need for the added functionality the HD delivers, and considers the combination of CHARCS and ATHENA to be adequate to conduct their mission.

Dissemination of Intelligence Information

DCGS-A successfully posted information to, and received information from, the Data Dissemination Service (DDS). The DDS allows sharing data among any system that is part of the Army Battle Command System, such as Command Post of Future and AFATDS.

DCGS-A enabled users to exchange information with the larger intelligence enterprise via the DCGS Integration Backbone (DIB). The DIB facilitated collaboration and sharing among Service and Agency systems such as Air Force DCGS, DCGS – Navy, National Geospatial Agency, National Security Agency (NSA), and others.

The test unit used the DIB extensively to post and retrieve data and products (the test unit posted 5,600 products on the DIB over the 14-day test). While the unit was successful in using the DIB to share information, they had challenges with finding relevant results from DIB searches. Successful DIB search requires use of the metadata catalog managed by the DIB management office (outside of the DCGS-A system). A metadata is a searchable description of data, and users across the military Services and agencies must use common metadata tagging methods to facilitate an effective DIB search. Users also complained about the inability to update or remove products posted by others. During shift changes, the incoming Soldier must copy the DCGS-A products of the outgoing Soldier and repost them, rather than continuing work on the same product. This wastes time and results in many versions of same DCGS-A products.

Supporting the Current Operations

The test brigade commander and staff were very enthusiastic about the DCGS-A's ability to help managing the battle, but comments from battalion commanders and staff indicated they did not consider DCGS-A to be very helpful for the fight on the ground. They stated that once the battle starts, it is very difficult to update DCGS-A while also tracking the battle. As a workaround, some battalion analysts resorted to tracking the battle using pencil and paper and updated DCGS databases once the battle was over.

Weather

The Staff Weather Officer (SWO) noticed the weather tool produced inaccurate weather predictions when using the DCGS-A provided tools. The SWO had to rely on the Air Force weather website to get the right weather predictions. The contractors later identified a software logic fault in the weather tool; the DCGS-A cannot process the three-letter location station code the Air Force sends, as it is designed to accept only four-letter code.

This page intentionally left blank.

Section Four

Operational Suitability

DCGS-A Increment 1, Release 2 is operationally suitable, provided the Army intensively trains DCGS-A users and provides continued refresher training to units in garrison. DCGS-A is a complex system and the skills required to use it are perishable; partly because of the complexity of the system, the analysts stated they cannot maintain high level of skills without constantly using the system. DCGS-A Release 2 operational suitability improved over the previous release, but the usability and reliability still need improvements. System usability as measured with the System Usability Scale (SUS) during the FOT&E was low-marginal.¹⁸ Training improved significantly compared with the previous release. The FOT&E training included three training periods from September 2014 through April 2015. The extensive collective and unit-level training improved the unit's ability to integrate the DCGS-A capabilities with the unit's mission. The operational availability (A_o) of DCGS-A remains high at all echelons, and reliability improved from a major failure on average once every 16 hours during IOT&E to once every 28 hours during FOT&E. The system achieved a maximum time to repair of one hour 85 percent of the time, compared to the required 90 percent.

Training

The training for FOT&E included the New Equipment Training (NET) conducted January through February 2015 plus three collective events (CEs). CE1 was conducted from September through October 2014, CE2 in February 2015 right after the NET, and CE3 was conducted at the same time as the validation exercise for NIE 15.2. The test unit completed the entire cycle of the Army's 8-step training model (Figure 4-1) before the FOT&E.

To effectively operate DCGS-A, the unit not only needs to teach the operators and analysts skills necessary to use the DCGS-A tools and applications, but needs to develop and train operators on standard operating procedures (SOPs) and tactics, training, and procedures (TTP). The CEs provided this intensive training to the FOT&E test brigade. Although the Army provided comprehensive and effective DCGS-A training to the test unit, the FOT&E revealed areas which requires improvement:

- a. Battalion users complained that they send intelligence information to brigade for consolidation, but brigade analysts override the battalion information without informing the battalion analysts. When the battalion gets the database back, they have no quick and easy way to tell what items changed, and therefore, have to spend time going back through the database to check what was changed. The Army should develop TTPs or material solutions for better coordination of changes in the TED.
- b. The Army should teach DCGS-A operators the TTPs and SOPs for interfacing with the other battle command sections and the systems that support them; i.e., what

¹⁸ System Usability Scale (SUS) is a ten-item attitude Likert scale giving a global view of subjective assessments of usability. It was developed by John Brooke in 1986.

information to push to the Data Dissemination Service, and when, and how to disseminate the information on the DIB.¹⁹

In addition to receiving the training for the NIE 15.2, the majority of the users in the test unit were trained on DCGS-A during the NIE 15.1. The two cycles equate roughly about 18 to 24 months of training for the average unit. This amount of training roughly compares to the number of training hours for the average tank crew. The test unit intelligence officers felt that operating DCGS-A requires a similar type of training regimen as a tank crew.



Figure 4-1. The Army's 8-Step Training Model²⁰

Usability

Users completed the SUS three times, once during the pilot test and twice during the record test. The all-source analysts provided the majority of the responses (11/23 during pilot, 15/18 for the first record survey, and 28/40 for the second record survey). Mean scores from the three surveys are between 49 and 50 while 70 or higher is considered acceptable in commercial industry. These scores represent low-marginal usability.

Figure 4-2 below shows that the usability scores are statistically the same in all three assessments, indicating the possibility that experience did not make a significant difference in the perception of usability.

¹⁹ The Data Dissemination Service enables data sharing across the Army Battle Command Systems located in the same Tactical Operations Center.

²⁰ Acronym used in Figure 4-1: After Action Review (AAR).

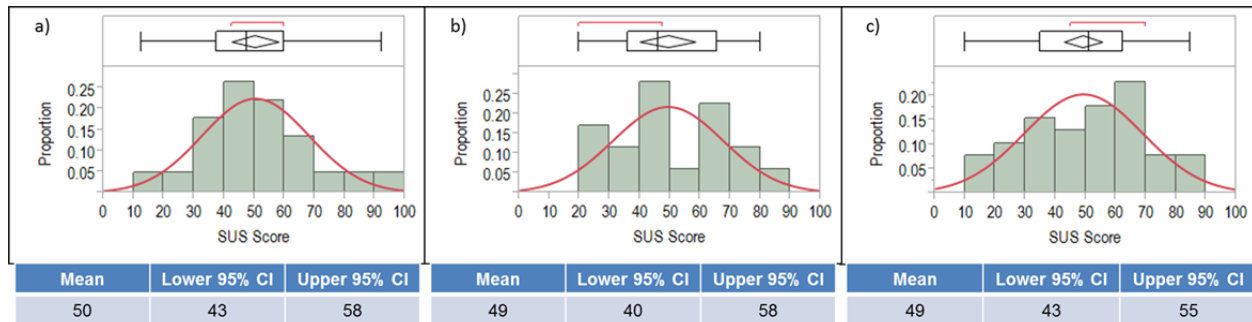


Figure 4-2. DCGS-A System Usability Scale (SUS) Scores from the (a) Pilot Test, (b) First Survey Period during the Record Test, and (c) Second Survey Period during the Record Test

Surveys and interviews during FOT&E indicated that brigade users were generally more positive about the DCGS-A than battalion users, but Figure 4-3 below indicates that two groups had no statistically significant differences in their perception of the usability. One possible explanation is that while both groups saw similar perceptions regarding with the DCGS-A usability, some of the battalion dissatisfaction came from other factors such as workload.

The battalion's intelligence analysts expressed frustration with the amount of time they had to spend working on the database. They complained that it can take hours to synchronize databases. The later data synchronization excursion revealed that the method the test unit used (Ad-Hoc Datamover) required significantly longer time for data synchronization compared to three other methods available to the users. Using other methods, the same database synchronization that took 2 hours could have been completed within 15 minutes.

Battalion analysts also complained about the time units spent reviewing the data for accuracy. After the battalion updates their database, the analysts at the brigade TOC consolidates input from all sources, and post the fused product back on the TED. The battalion analysts were not notified of the changes or the rationale for them. The battalion users were frustrated when their input was modified without them being in the loop. They suggested that either the brigade analysts need to inform them of the changes, or the system should highlight changed items so that they do not have to review each item in the TED to see which ones changed, and why.

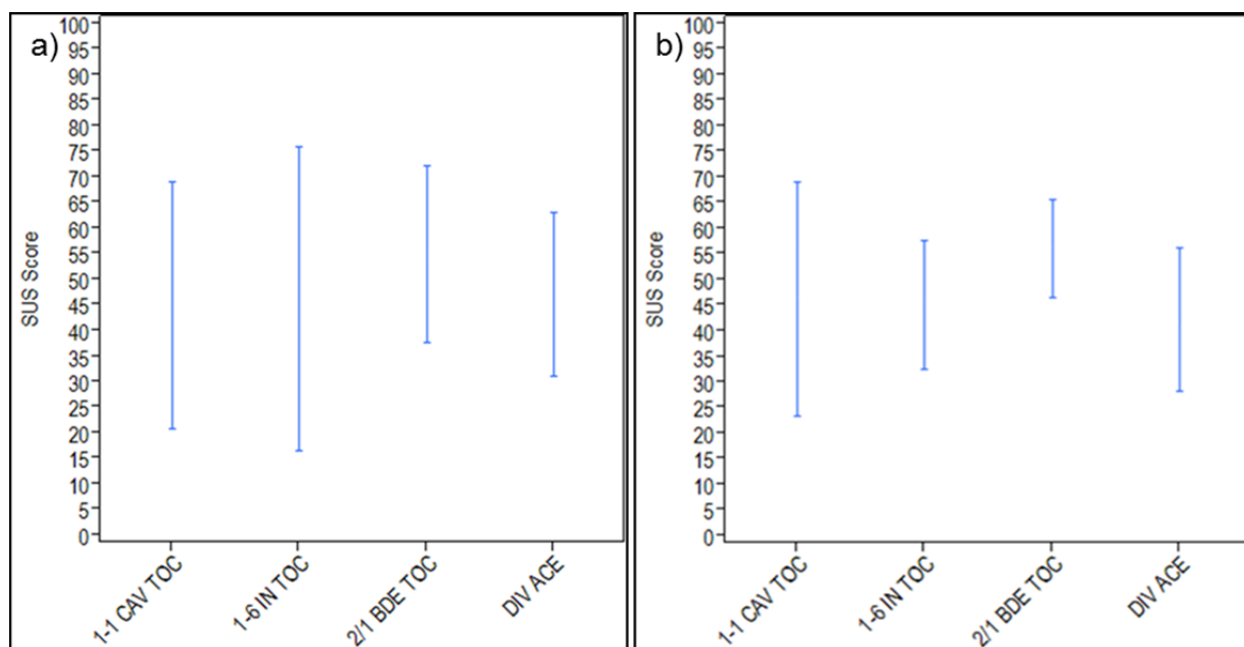


Figure 4-3. Bars Representing 95% Confidence Intervals about the Mean SUS Scores²¹
 (The left side shows the first and the right side shows the second survey period during Record Test.)

Availability

Operational Availability (A_o) is a measure of the probability that a system will be operating or capable of operation when required. The DCGS-A system achieved an A_o of 0.99, satisfying the requirement of 0.90. Table 4-1 shows the A_o values for only the DCGS-A and the system-of-systems. The system-of-systems availability estimates the probability of all systems required for intelligence mission being operational. The data indicate that the users were able to execute the intelligence missions 97 percent of time, with all essential services working.

²¹ Division Analysis and Control Element (ACE) is organic to the Headquarters, Headquarters and Operations Company (HHOC) of the divisional Military Intelligence battalion.

Table 4-1. DCGS-A Operational Availability (A_o) during the FOT&E

		Operating Hours	System Failure Down Time (Hours)	Operational Availability (A_o)	95% Confidence Interval ¹
Brigade TOC	DCGS-A	224	3.18	0.99	0.96–0.99
	System of Systems ²		6.87	0.97	0.93–0.98
Brigade TAC	DCGS-A	218	No System Failures	1.0	No System Failures
	System of Systems				
1-6 Battalion	DCGS-A	247	No System Failures	1.0	No System Failures
	System of Systems				
1-1 Battalion	DCGS-A	275	0.50	0.99	1.00–0.98
	System of Systems		0.78	0.99	1.00–0.97

Notes:

¹ Confidence intervals obtained by assuming time to failure and time to repair are distributed exponentially.

² System of systems availability includes down time caused by unit support equipment failure and failures in equipment external to DCGS-A. System Failure includes systems aborts and rapidly recoverable events that were system aborts.

TOC – Tactical Operations Center; TAC – Tactical Action Center

Reliability

Mean Time Between System Failures

Table 4-2 shows the Mean Time Between System Failure (MTBSF) for the servers located in the brigade and battalion operations centers. DCGS-A achieved a point estimate MTBSF of 28 hours in the brigade and 137.5 hours in the battalion. The DCGS-A has no requirement for system reliability because the Army Requirements Oversight Council removed the requirement of 160-hours MTBSF after the IOT&E.

Table 4-2. DCGS-A Mean Time Between System Failure (MTBSF)

DCGS-A Intelligence Fusion Server (IFS) Location	Operating Hours	System Failure Events ¹	Failure Functional Area	Point Estimate (Hours)	95% Confidence Interval ² (Hours)
Brigade TOC	223.7	8	All Functional Areas	28	14–65
Brigade TAC	217.8	None	No Failures	No Failures	(No Failures)
1-6 Battalion	247.0	None	No Failures	No Failures	(No Failures)
1-1 Battalion	275.0	2	All Functional Areas	138	38–1135
NOTES: ¹ System failure events affect all attached workstations. During a system abort event, workstations only have access to locally stored data. Server resident data and applications are not accessible until the server is repaired. ² Confidence Intervals calculated assuming time to failure is exponentially distributed. TOC – Tactical Operations Center; Tactical Action Center					

Mean Time Between System Failure (MTBSF) for Intelligence Functional Areas

Table 4-3 shows the observed failure events by the affected intelligence functional areas. The figure shows the total number of events for each system, the operating hours, and the number of failures affecting all and specific functional areas.

The point estimate for MTBSF for an area is the sum of failures affecting all areas and those affecting the specific area. For example, the fire support functional area in the brigade TOC experienced 14 failures—9 failures that affected all areas and 5 failures that only affected fire support. While rebooting the system, server or workstation corrected the majority of failures, some of the failures caused unsaved work to be lost. During the FOT&E, the 9 server failures caused 9 hours and 3 minutes of lost work. The lost work accounts for both the repair time and the time the users spent to recover their work.

The MTBSF data also indicate that the busier users incurred more frequent failures. For example, the fire support analyst at brigade TOC experienced five failures on their module in addition to the nine server failures that affected everyone in the TOC. Thus, the fire support analyst experienced 14 failure events in 224 hours, or about every 16 hours. The 95 percent confidence interval is between 9 and 29, indicating that the long-term reliability in terms of MTBSF for a fire support analyst is not likely to exceed 29 hours. While this may not cause mission to fail, the frequency of reliability failures may have contributed to the low-marginal SUS score.

Table 4-3. MTBSF by Functions

System	Operating Hours	Failure Events	Failures Affecting each Functional Area	Point Estimate (Hours)	95% Confidence Interval ¹ (Hours)
Brigade TOC IFS	224	20	9 affected All Functional Areas 5 affected only Fire Support 2 affected only Data Manager 2 affected only Folder Manager 2 affected only Weather	25 16 20 20 20	13–54 9–29 11–40 11–40 11–40
Brigade TAC IFS	218	1	1 affected only Fire Support	218	3–8,602
1-6 Battalion IFS	247	5	5 affected All Functional Areas	50	21–152
1-1 Battalion IFS	275	4	3 affected All Functional Areas 1 affected only All-Source	92 68	31–444 26.9–252
Workstations	5,768	55	16 affected All Functional Areas 27 affected only All-Source 5 affected only Fire Support 4 affected only Weather 1 affected only GEOINT 1 affected only TGS 1 affected only SIGINT	360 137 274 288 339 339 339	222–630 101–190 179–443 186–472 212–582 212–582 212–582
NOTE: Confidence Intervals calculated assuming time to failure is exponentially distributed. TOC – Tactical Operations Center; IFS - Intelligence Fusion Server; TAC – Tactical Action Center					

Failure Mode/Chargeability Analysis

Failure modes for the DCGS-A system include:

- One network switch failed due to excessive heat. The field service representative turned the air conditioner off while performing maintenance on the Intelligence Processing Center-2 and failed to turn the air conditioner back on. This caused the network switch to fail over and connectivity was lost.
- The folder manager services were corrupted in several instances and restarted the services on the interoperability server.
- The Multi-Function Workstation (MFWS) experienced numerous occurrences of service failures that required restarting on either the workstation or the server. MFWS lost connectivity and required rebooting to regain connectivity to either the server or network. Individual MFWS reboots only affected the workstation, but restarting the service on the server caused all MFWSs to lose the service.

Maintainability

Maintenance personnel completed 85 percent (73 of 86) of maintenance actions in less than one hour and did not meet the requirement of 90 percent (see Figure 4-4). This is not significant since operations were able to continue in all but one failure event, when an overheated router caused a disruption in network services.

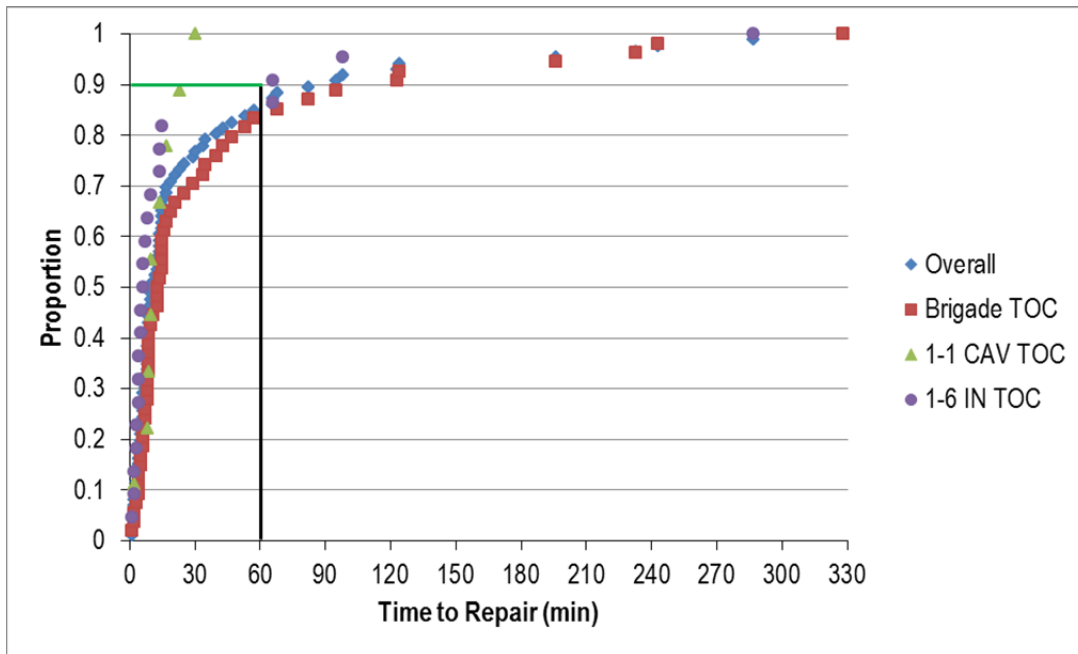


Figure 4-4. Cumulative Distribution of Repair Times during the 2015 DCGS-A FOT&E

Figure 4-5 identifies the typical, planned, DCGS-A hardware and software maintenance support flow chart. The operator generally provided the first level of maintenance. If the operator was not able to resolve the failure, the operator generated a trouble ticket elevating the failure to subsequent levels of maintenance until the failure was resolved. This flow was modified during FOT&E and field service representatives were the primary source of maintenance. Six field service representatives were embedded in the brigade and battalions during the exercise; two at division, two at brigade, and one at each of the battalions. Embedded field service representatives and offsite field support engineers provided hardware and software maintenance operations and repair parts support. Military Intelligence Systems Maintainers/Integrators (35Ts) received system administration and maintenance training and are expected to provide first line unit level maintenance (see Figure 4-5), but during the test were relegated to providing operator level subject matter expertise and unit maintenance trouble ticket management. Battalion staff officers from 1-1 Cavalry and 1-6 Infantry expressed a desire to have 35Ts provide primary maintenance support, with field service representatives minimally embedded and field service engineers available for additional support.

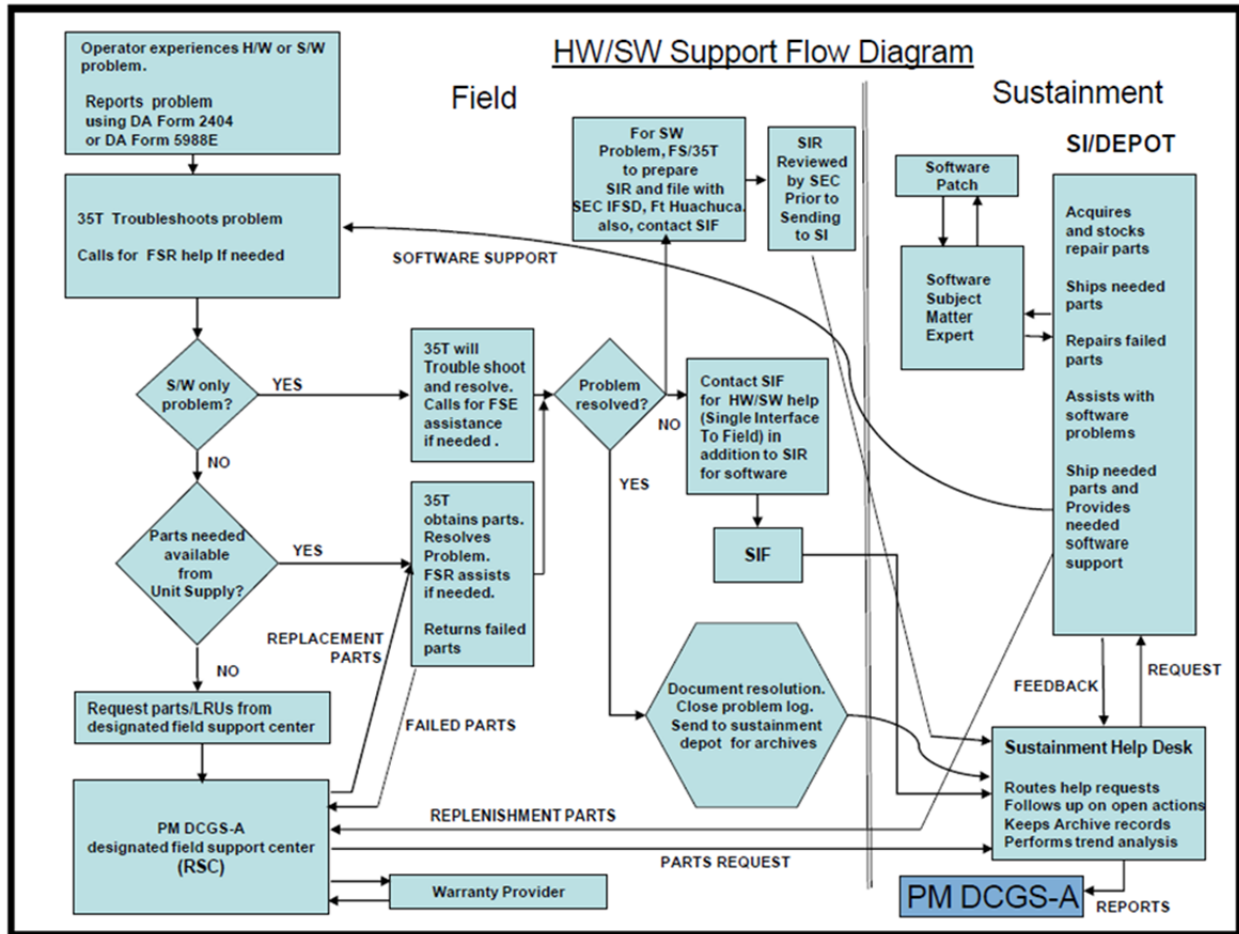


Figure 4-5. Typical Planned DCGS-A Family of Systems Maintenance and Software Support Flow^{22,23}

²² Life Cycle Sustainment Plan, DCGS-A Increment 1, Version 1.1, Production and Deployment and Operations and Support, dated April 10, 2015.

²³ Acronyms on this figure: Hardware (H/W), Software (S/W), Field Service Representative (FSR), Line Replaceable Unit (LRU) Regional Support Center (RSC); Army Occupation Specialty for Military Intelligence Systems Maintainer/Integrator (MOS 35T), System Integrator (SI), System Integration Facility (SIF); Software Incident Report (SIR), Software engineering Center (SEC), Intelligence Fusion Systems Division (IFSD).

This page intentionally left blank.

Section Five Survivability

Cybersecurity testing confirmed that the DCGS-A program manager improved the cybersecurity of DCGS-A Release 2 compared with Release 1, but cybersecurity test teams still found less critical vulnerabilities requiring remediation. The greater concern is that vulnerabilities inherited from the Army's interfacing systems and tactical networks degrades the cybersecurity status of DCGS-A as well as other programs of record on the tactical networks. The classified annex B to this report provides details of the cybersecurity testing.

This page intentionally left blank.

Section Six Recommendations

DOT&E recommends the Army take the following actions:

- Institutionalize the training provided to the FOT&E test unit so that all DCGS-A equipped units receive intensive, scenario-driven, collective training.
- Improve DCGS-A training to include standard procedures for:
 - Coordinating TED changes among the DCGS-A users at different TOCs, such as between brigade and battalions.
 - Metadata tagging for data posted on the DIB.
- Maintain DCGS-A unit readiness via continuous use of DCGS-A in garrison.
- Train the users about the pros and cons of each method of data synchronization.
- Improve reliability by tracking and correcting software faults.
- Improve the cybersecurity posture in all Army tactical networks.

ATEC should resolve systematic shortfalls with data collection, reduction, and analysis during testing.

- Demonstrate the end-to-end process of collecting, reducing, and analyzing the data before an operational test.
- Conduct a developmental test with operationally representative networks and the operational test instrumentation before an operational test of complex networked systems.
- Attribute all performance anomalies to system performance, test process, or data collection and reduction before the test ends.
- Analyze data sufficiently to identify and resolve anomalies and inconsistencies during the test.

This page intentionally left blank.

Appendix A: Details Regarding the Vignettes

Table A-1. The Time Lines for the 10 Vignettes

	Vignette	Who	26	27	28 APR–1May	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th	13th	14th		
			Sun	Mon	Tue–Fri	Sat	Sun	Mon	Tue	Wed	Thur	Fri	Sat	Sun	Mon	Tues	Wed	Thur		
Target Insurgent Leader	1	1-1 CAV			Target Insurgent Leader															
Target IED Factory	2a	1-6 IN	TGT IED Factory																	
Target IED Factory	2b	1-6 IN										TGT IED Factory								
Target IED Factory	2c	1-6 IN											TGT IED Factory							
Target Reserve Forces	3	2/1 AD & 1-1 CAV						Target Reserve Force												
Target Air Defense Radars	4	1 AD & 2/1 AD			Target ADA Radars															
Disrupt SVBIED Attack	5	2/1 BCT						Disrupt SVBIED Attack												
Disrupt Assassination Plot	6	1-6 IN	Disrupt Assassination Plot																	
Engage Enemy Recon	7	1 AD & 1-1 CAV	Engage Enemy Recon																	
Target Heavy Insurgents	8	1-1 CAV	Target Heavy Insurgents																	
Target Rogue ANA Leader	9	1-1 CAV	ANA Ldr																	
Target Ellisian Invasion	10	1 AD	Invasion																	

IED – Improvised Explosive Device; SVBIED – Suicide Vehicle-Borne Improvised Explosive Device; ANA – Attica National Army; CAV – Cavalry; IN – Infantry; AD – Armored Division; BCT – Brigade Combat Team; TGT –Target

To evaluate the overall operational value of DCGS-A, the test team developed and injected 10 pre-determined vignettes and supporting intelligence data into the test database. The goal was to evaluate if the unit could discover the intelligence data and exploit them.

The test database is composed of baseline data from the Army Training and Doctrine Command's (TRADOC) Training Brain Operations Center (TBOC), which contains hundreds of thousands of intelligence data records, including data from combat theaters. TRADOC uses TBOC for operationally realistic Soldier and leader training.

Five of the ten vignettes (1, 2, 5, 6, and 9) replicated Wide Area Security (WAS) story lines, while the other five vignettes (3, 4, 7, 8 and 10) emulated Combined Arms Maneuver (CAM) storylines. The vignette 2 was played three times (2a, 2b, and 2c) because the test unit found and destroyed the improvised explosive device (IED) factory much quicker than expected (2a), and the enemy set up a second location, which the test unit found and destroyed again (2b). The enemy set up a third location, and the test unit found it, and was planning to destroy that location when the test ended (2c).

Figures A-1 through A-14 show more details about the vignettes. The acronyms used in the figures are listed at the end of this appendix. Figure A-1 shows design and execution for the first vignette, replicating a story line involving finding and neutralizing an insurgent leader. The top line on the chart (Search Big Data, Create and Manage Entity, signals intelligence collection...) shows top-level activities the test unit is expected to perform under the Army doctrine and training. The bullets below provide more details. The white test boxes indicate the actual actions the test unit took during the test.

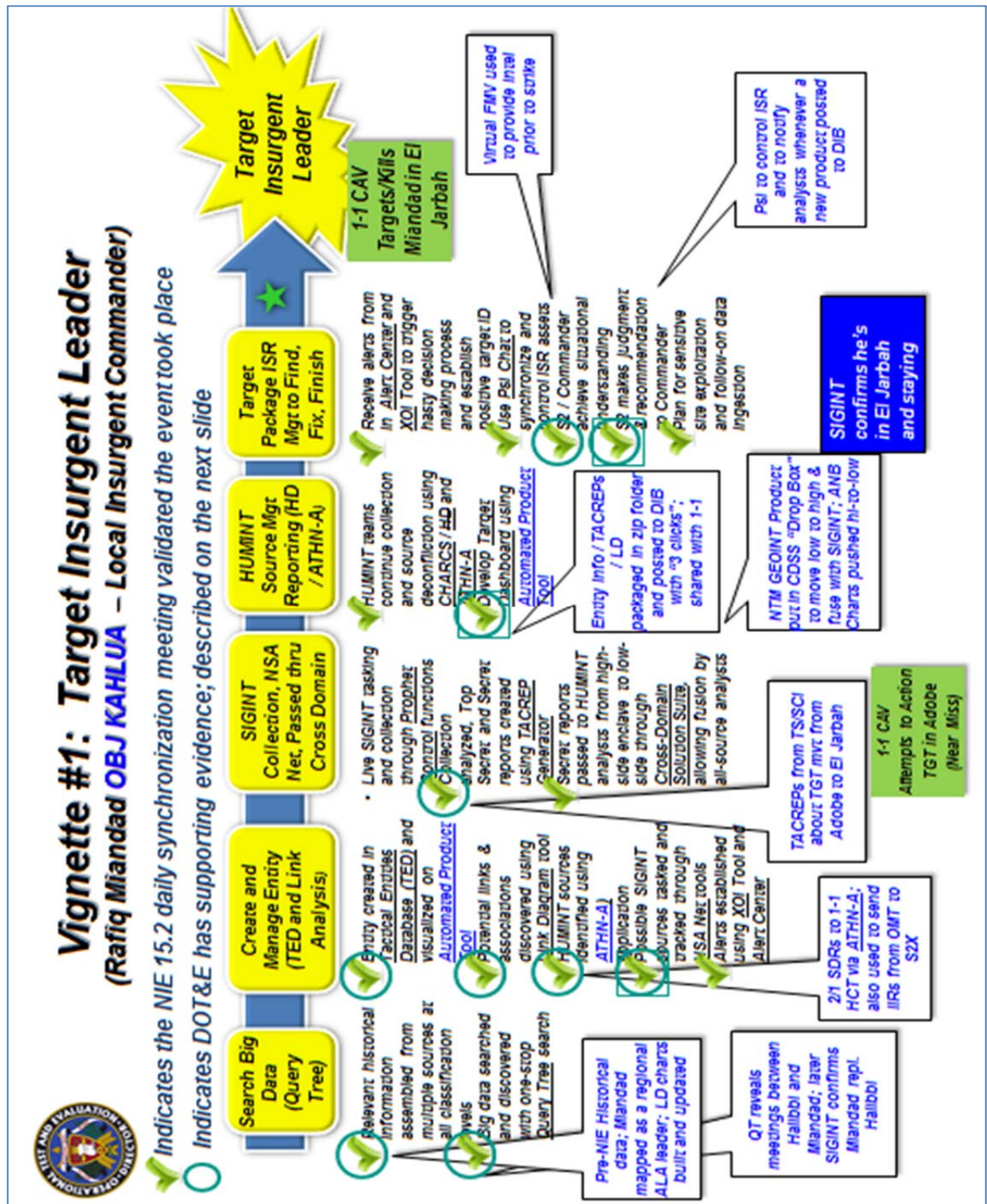


Figure A-1. The Actions Anticipated in the Vignette 1 Story Lines and Supporting Tools the Unit Was Expected To Use²⁴

²⁴ The acronyms used in the Figures A1 through A-14 are listed at the end of this appendix.

As indicated on the top of the chart, the daily synchronization meeting—composed of members from the Brigade Modernization Command (BMC), the Army Test and Evaluation Center (ATEC), and DOT&E—reviewed each day’s activities and put a check mark when the test unit conducted the expected activities. After the test, DOT&E added a circle when it located supporting evidence in the test database. In many cases, DOT&E did not find supporting evidence, but that does not indicate the evidence was not there. It simply means that DOT&E did not have sufficient manpower and time to search through the 275 folders containing 6,090 files that ATEC provided to locate the appropriate evidence.

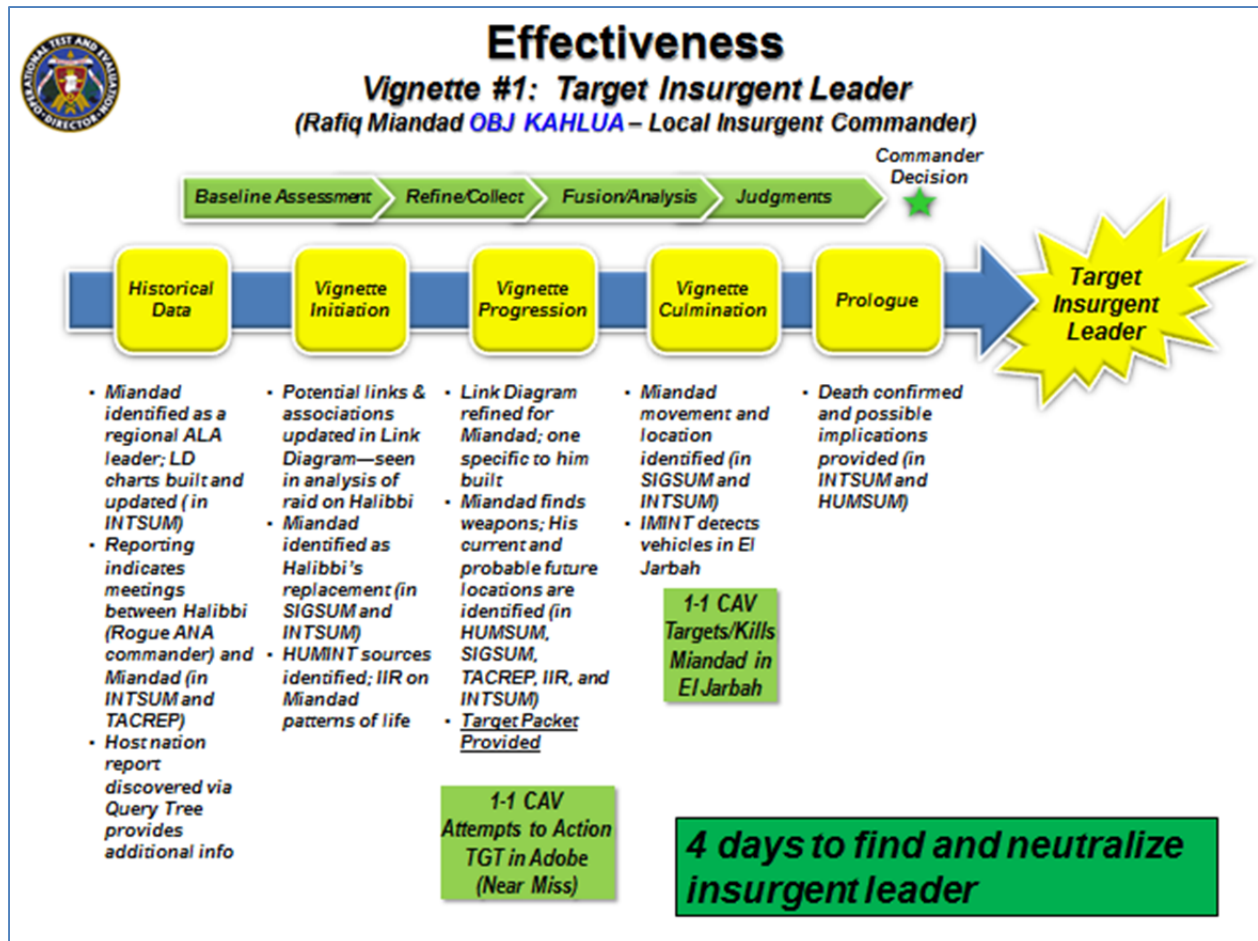


Figure A-2. Evidence DOT&E Found in Support of Vignette 1

Figure A-2 shows more details on the evidence DOT&E found regarding vignette 1. As described in the bullets, the test unit used Query Tree tools to locate relevant information and link diagram to identify associates, confirming that a character named Rafiq Miandad is a regional insurgent leader, and that he has replaced the previous leader, Halibbi. The test unit found and killed Halibbi, the previous leader, during the pilot test. The supporting evidence clearly shows that the test unit quickly found the suspect, confirmed the identity, located and nominated the target, and then confirmed the kill.

Figures A-3 through A-5 shows the test unit’s three consecutive successes to find, confirm the location and intent, and nominate the target of IED manufacturing facilities.

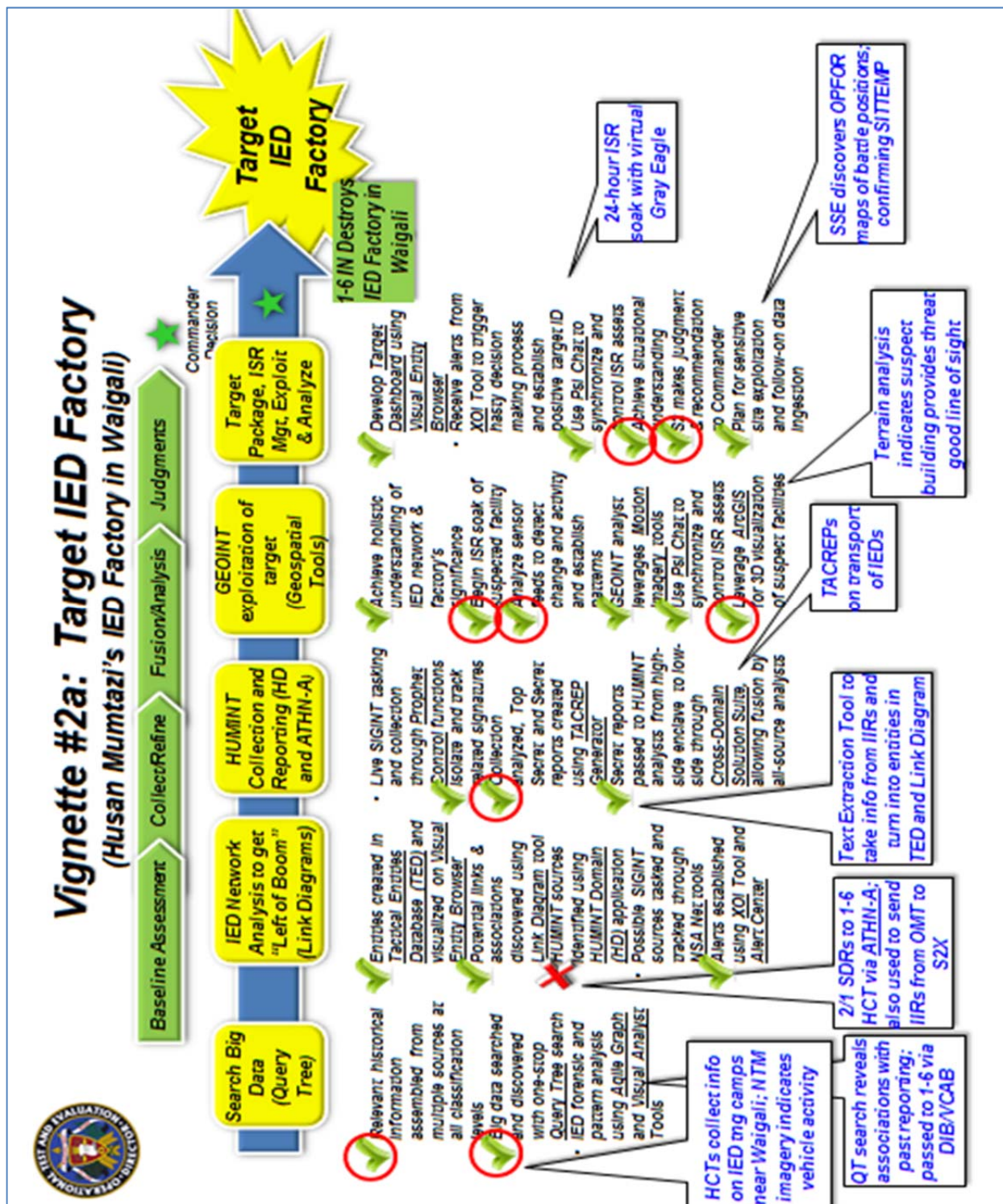


Figure A-3. The Actions Anticipated in the Vignette 2a Story Lines and Supporting Tools the Unit Was Expected to Use

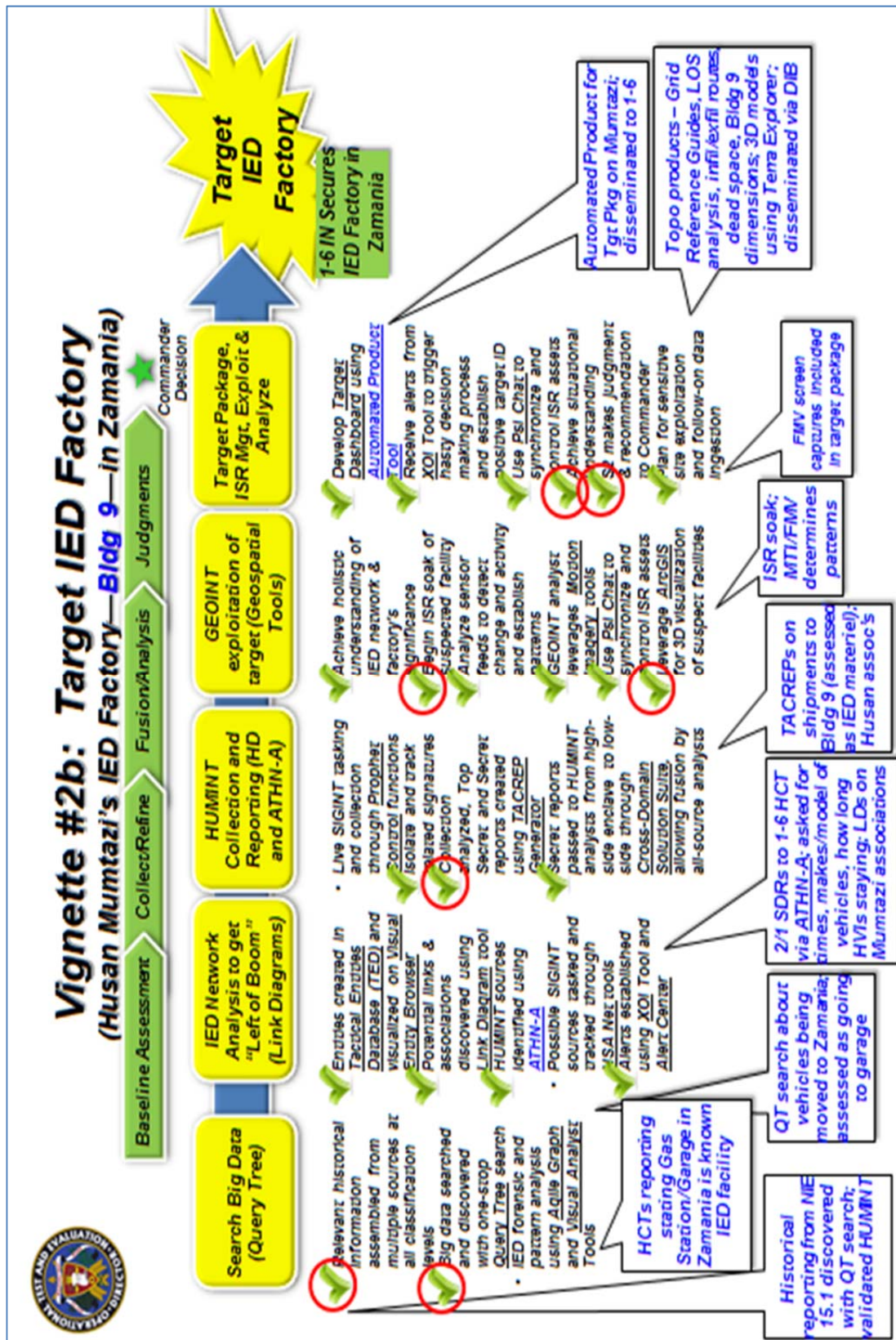


Figure A-4. The Actions Anticipated in the Vignette 2b Story Lines and Supporting Tools the Unit Was Expected to Use

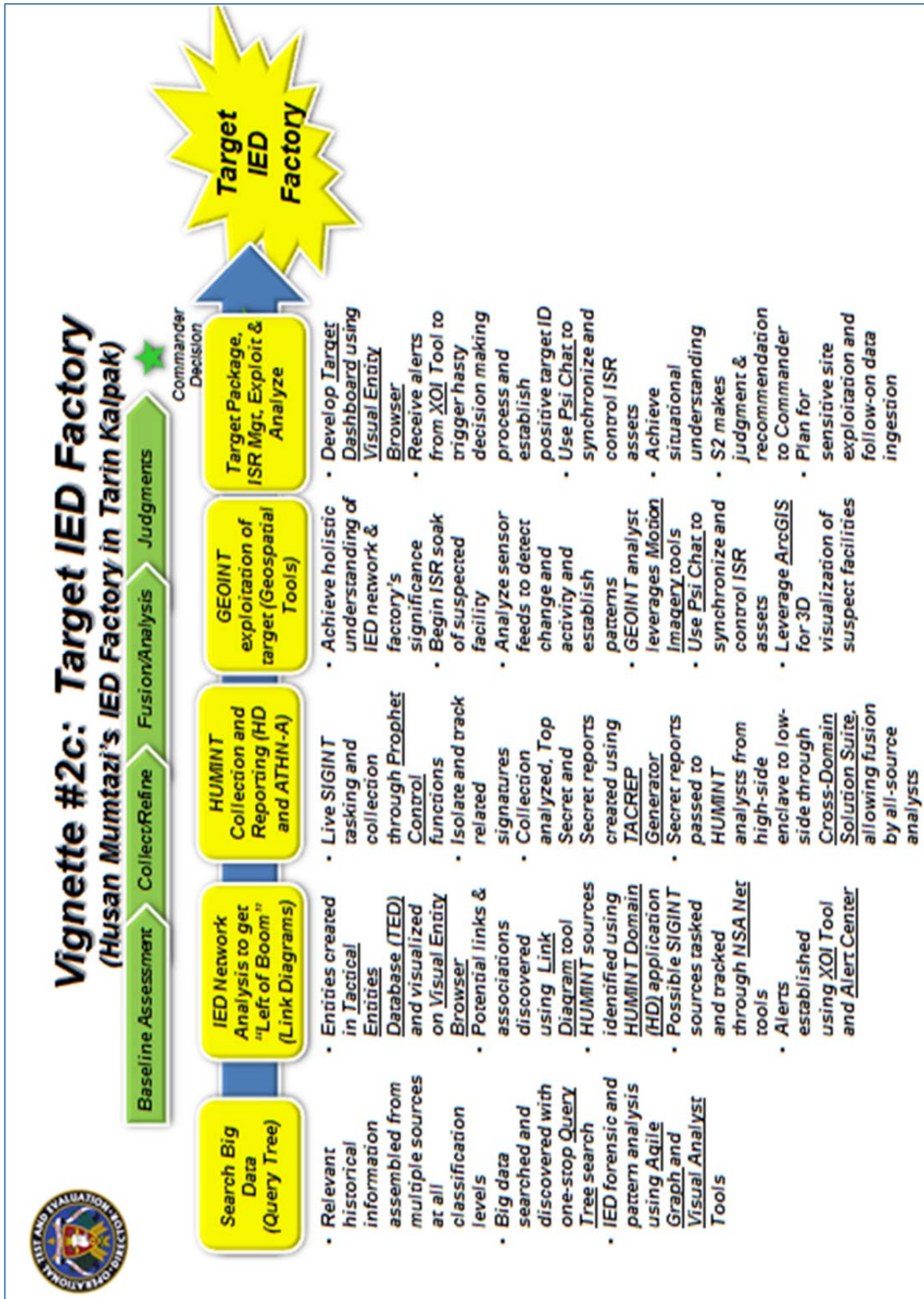


Figure A-5. The Actions Anticipated in the Vignette 2c Story Lines and Supporting Tools the Unit Was Expected to Use

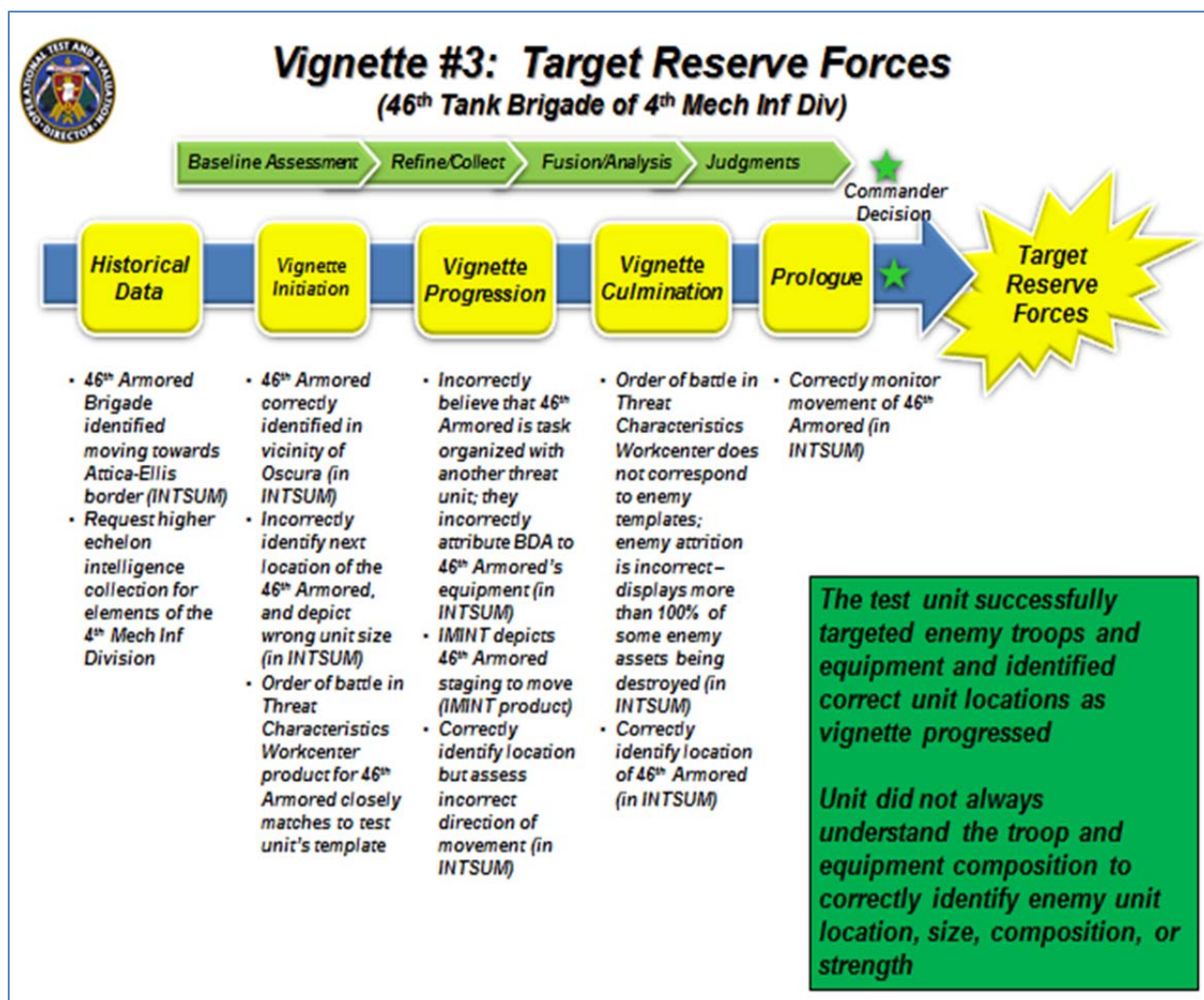


Figure A-6. The Actions Anticipated in the Vignette 3 Story Lines and Supporting Tools the Unit Was Expected to Use

Figure A-6 demonstrates the challenges with a vignettes-based operational test. In order to preserve the operational realism and fairness of evaluation, both live and simulated units, friendly and foe, were free to make decisions regarding their actions. The test team did not inform the test units about the vignettes, other than making them aware that they were collecting data on previously-injected story lines.

The daily test team synchronization meetings kept track of test progress, and made adjustments to vignettes where possible. Those adjustments worked very well for the Wide Area Security (WAS) scenarios, and thus, DOT&E found significant supporting evidence for them. For the Combined Arms Maneuver (CAM) vignettes such as vignette 3, it was more difficult.

The test unit identified enemy units moving toward the border as expected in vignette 3, and requested higher echelon intelligence collection for the enemy unit and order of battle. The test unit accurately tracked the enemy troop and equipment, but incorrectly associated the equipment with the wrong enemy unit. Figure A-7 below shows the details of the actions the test unit took regarding vignette 3.

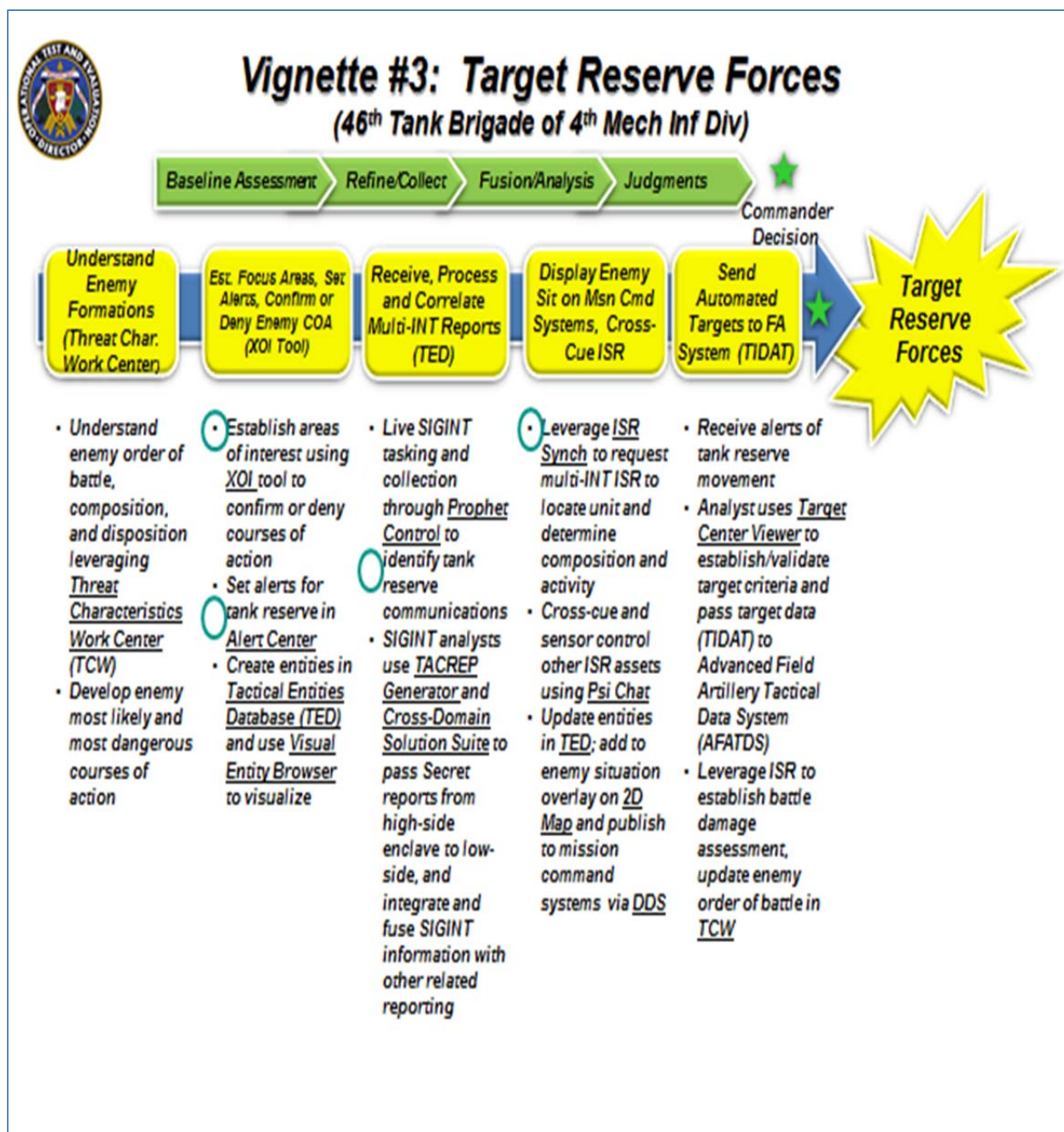


Figure A-7. DOT&E Assessment of Vignette 3

As described in the detail steps, the test unit did not correctly identify the enemy order of battle, resulting in a mistaken conclusion about which enemy unit they were fighting. The FOT&E was only 12 days. The unit would likely have had a much better appreciation for the enemy order of battle in a longer fight because of the accumulation of intelligence. Even with this shortfall, the unit identified and tracked the enemy unit and took steps to neutralize them.

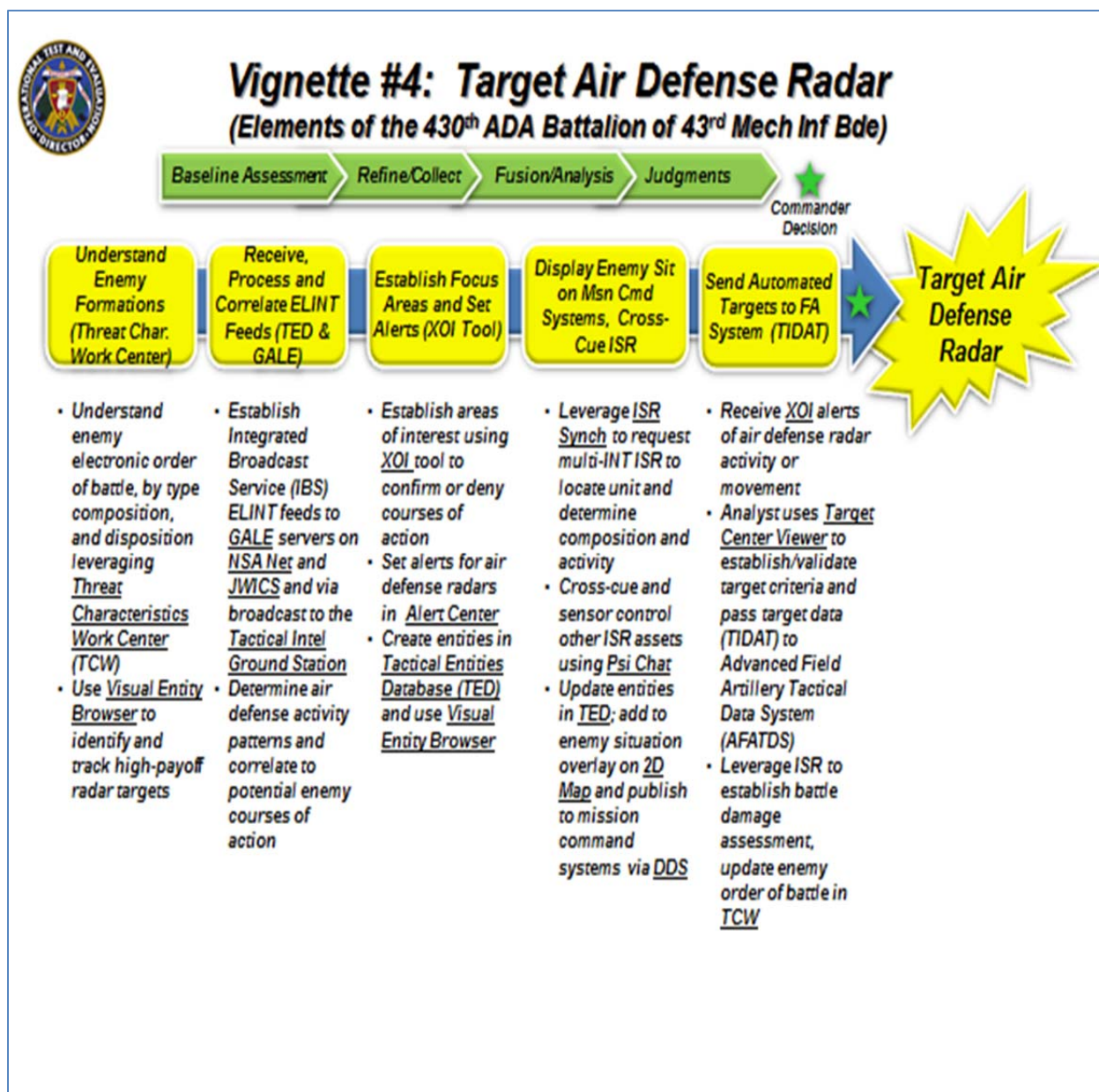


Figure A-8. The Actions Anticipated in the Vignette 4 Story Lines and Supporting Tools the Unit Was Expected to Use

Vignette 4 involved enemy air defense radars. DOT&E did not find any indication that the test unit took any action to destroy enemy air-defense radars. One possibility is that the commander and staff did not choose to act on them. It is also possible that the unit took actions, but supporting evidence is buried in the ATEC test database, and the test team did not find the relevant data. When the test team designed the vignettes, they understood the test unit may not choose to act against the enemy air defense radar. The test data show that the tools mentioned in the vignette, such as the Extended Area of Interest (XOI) alerts and 2D maps, functioned as expected. The test data include reports that indicate the test unit knew the air defense radar locations.

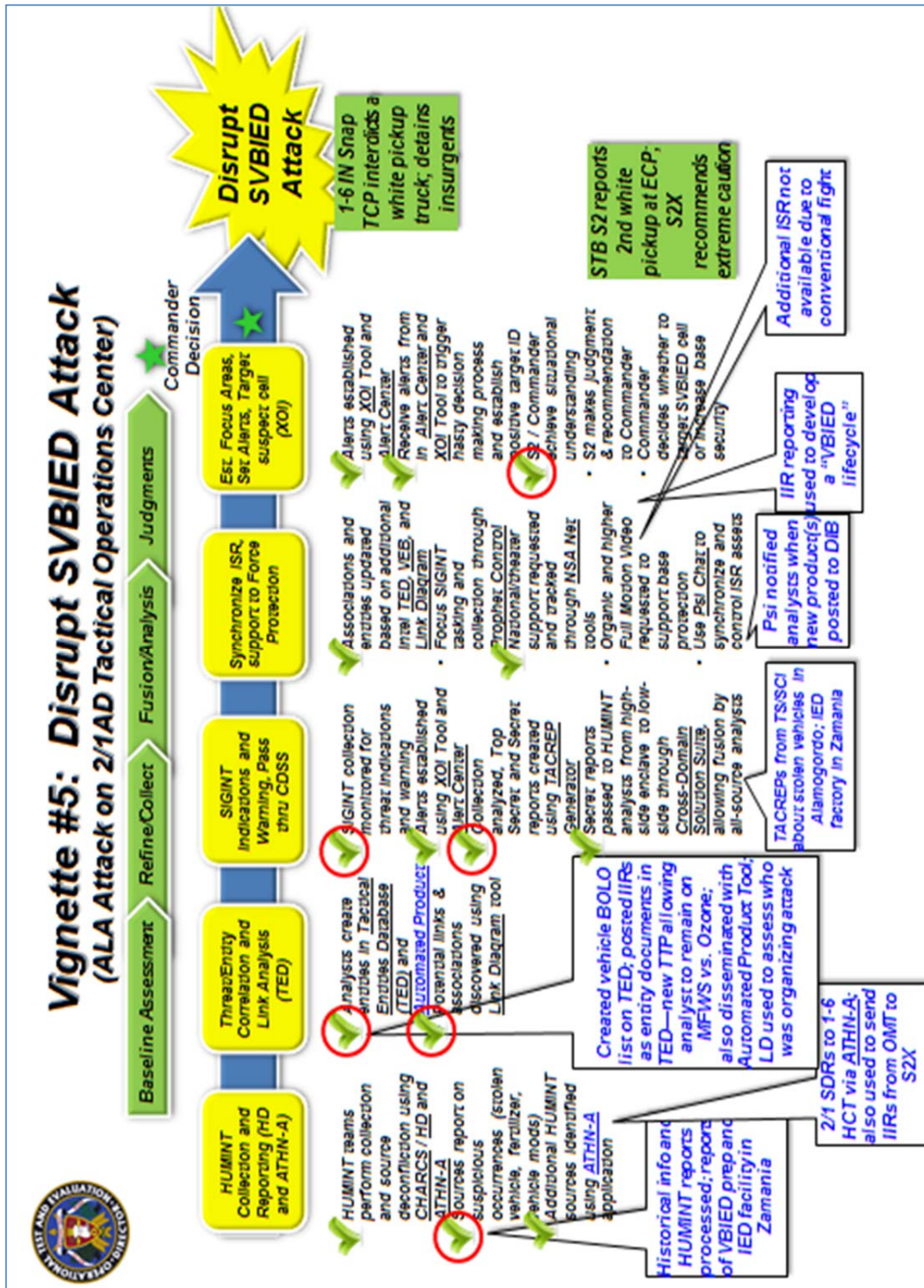


Figure A-9. The Actions Anticipated in the Vignette 5 Story Lines and Supporting Tools the Unit Was Expected to Use

In vignette 5, DCGS-A enabled the unit to determine indications of an impending vehicle borne improvised explosive device (VBIED) attack. Historical information and HUMINT reports indicated VBIED preparation in vicinity of Zamania. Analysts noticed increased enemy reconnaissance near a friendly force headquarters, and received HUMINT reports of insurgents planning VBIED activities. The DCGS-A analyst created vehicle be-on-the-look-out list on the TED, and disseminated the intelligence with the Automated product tool. The analyst received reports via the DCGS-A about stolen vehicles near IED factory in Zamania. The all source analyst used DCGS-A Link Diagram to assess the organization preparing the attack. GEOINT Intelligence identified a vehicle at a known IED factory. The HUMINT analysts identified the VBIED vehicle and driver. GEOINT products showed that a VBIED was at a known IED factory, and a HUMINT analyst later reported that the vehicle had left. The analysts advised guards to exercise extreme caution when the vehicle was reported at the entry control point. The test unit stopped the vehicle and detained insurgents.

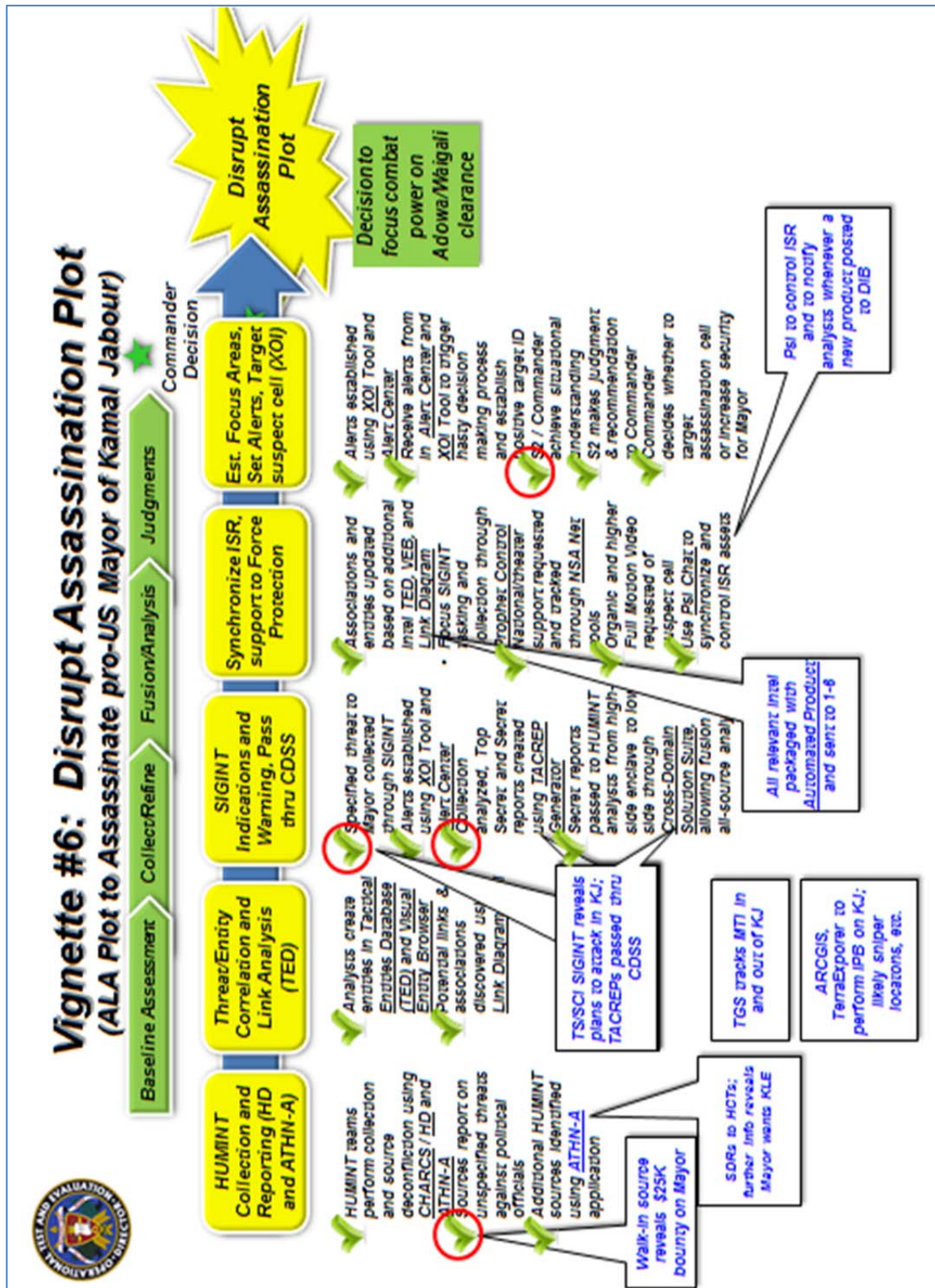


Figure A-10. The Actions Anticipated in the Vignette 6 Story Lines and Supporting Tools the Unit Was Expected to Use

In vignette 6, DCGS-A helped the unit determine the existence of an assassination plot against a local mayor. An intelligence summary and link diagram confirm that analysts were aware of the historical precedent for insurgent assassinations in the mayor's village. The HUMINT sources indicated that the mayor might be the target of an assassination attempt, and the unit placed the mayor on the list of individuals to protect. Analysts used GEOINT to evaluate sightlines in the mayor's village. HUMINT and signals intelligence (SIGINT) revealed insurgents had placed a bounty on the mayor, and that assailants were on standby. The mayor announced a press conference, but insurgents kidnapped him before the conference. Insurgents planned to bring the mayor to his press conference and execute him. Even though the unit knew the plot, the commander chose to counter the enemy attack to the weak side of the friendly unit and did not intervene to prevent the assassination. DOT&E considers the vignette as a success for the intelligence analysts using DCGS-A because the analysts provided appropriate intelligence for the commander to make the decision.

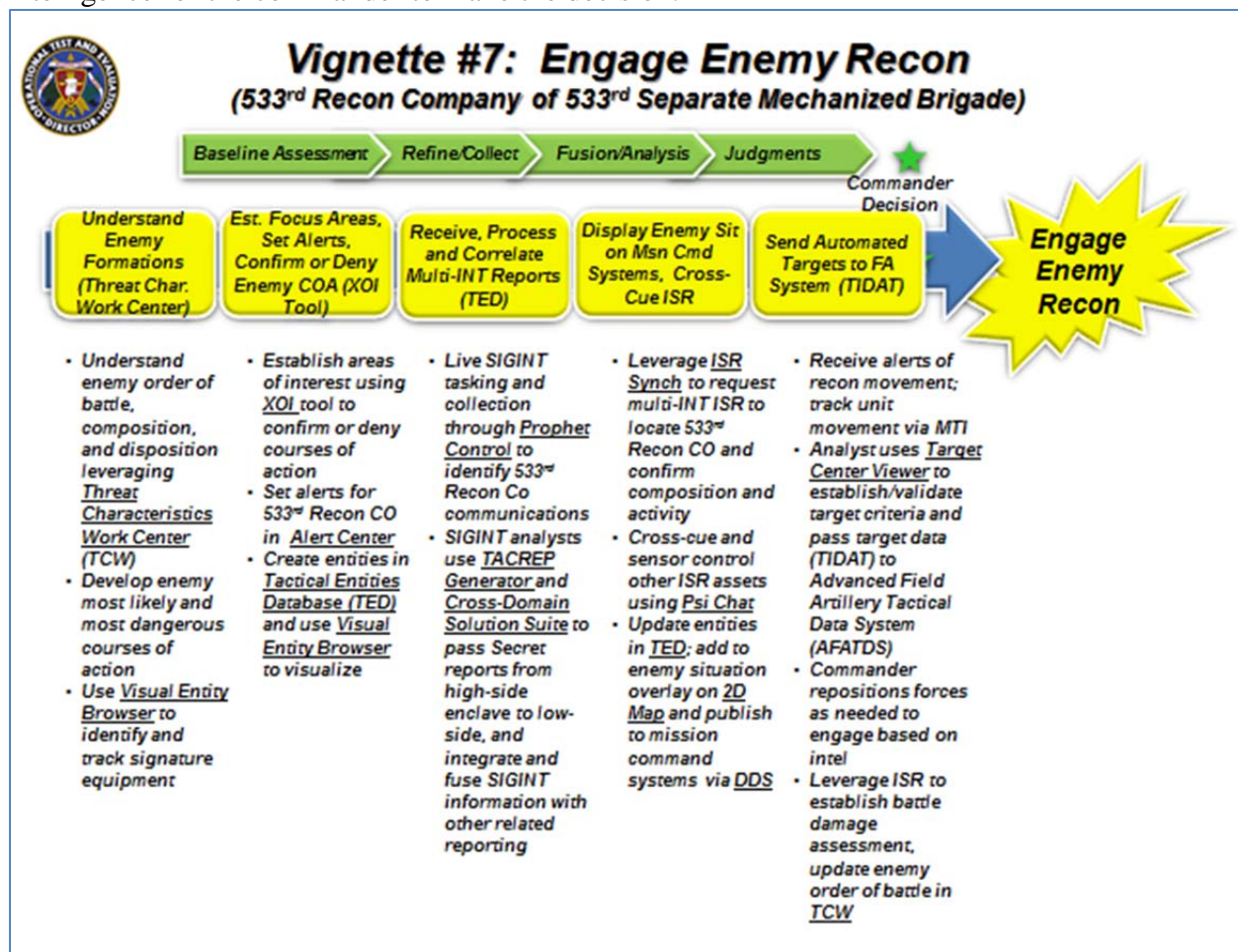


Figure A-11. The Actions Anticipated in the Vignette 7 Story Lines and Supporting Tools the Unit Was Expected to Use

Due to the free play nature of the FOT&E, neither the enemy nor the friendly units conducted the fight as envisioned by the designers of vignette 7. Hence, this vignette was not relevant for evaluation.



Vignette #8: Target Heavy Insurgents (Conventionally-Equipped ALA in Anthony-Vado Gap)

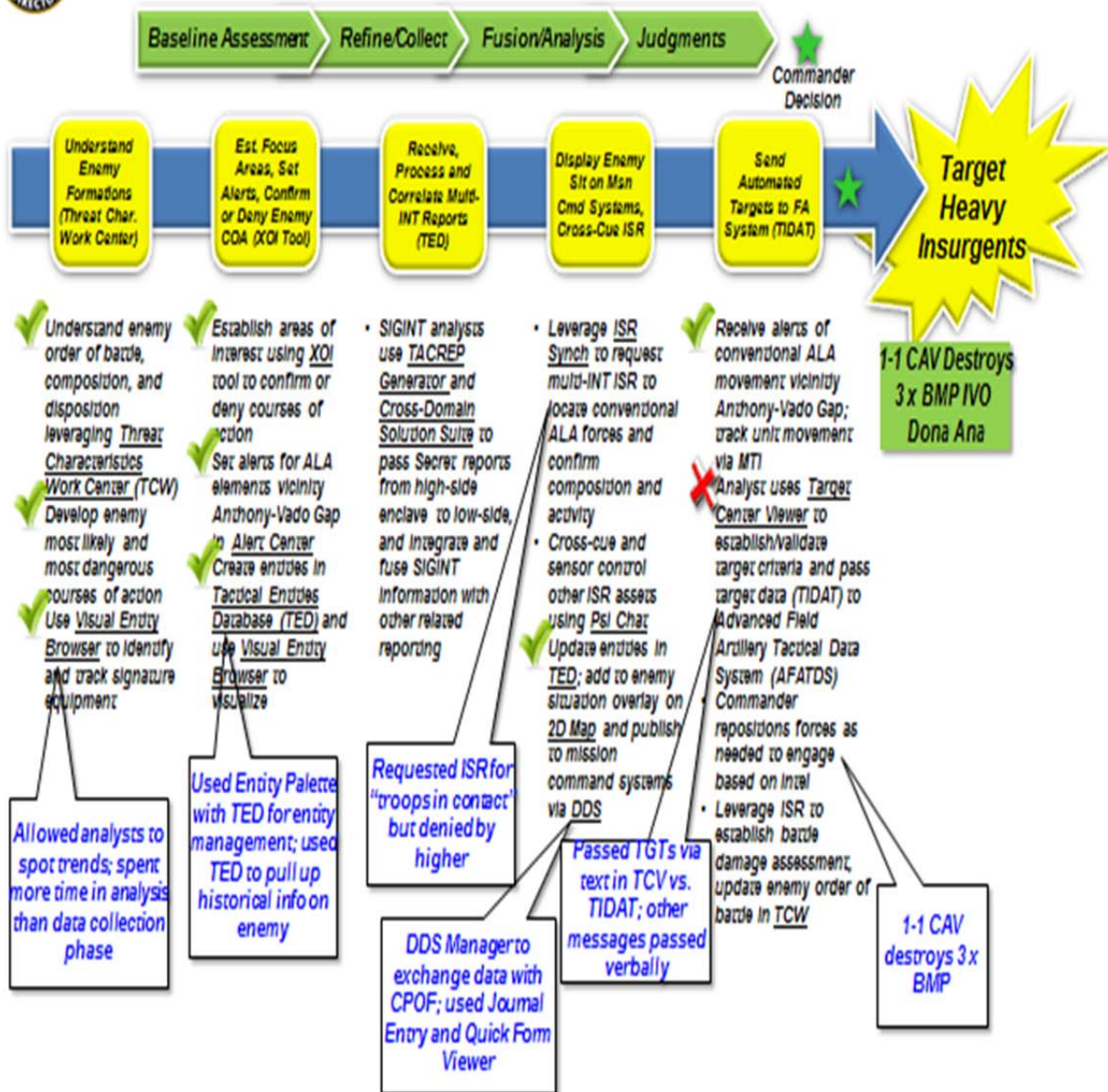


Figure A-12. The Actions Anticipated in the Vignette 8 Story Lines and Supporting Tools the Unit Was Expected to Use

Figure A-12 shows story line for finding and destroying a conventionally equipped insurgent force. The only deviation from the expected action of vignette 8 is that the analyst chose to use text and voice rather than sending a Target Data (TIDAT).

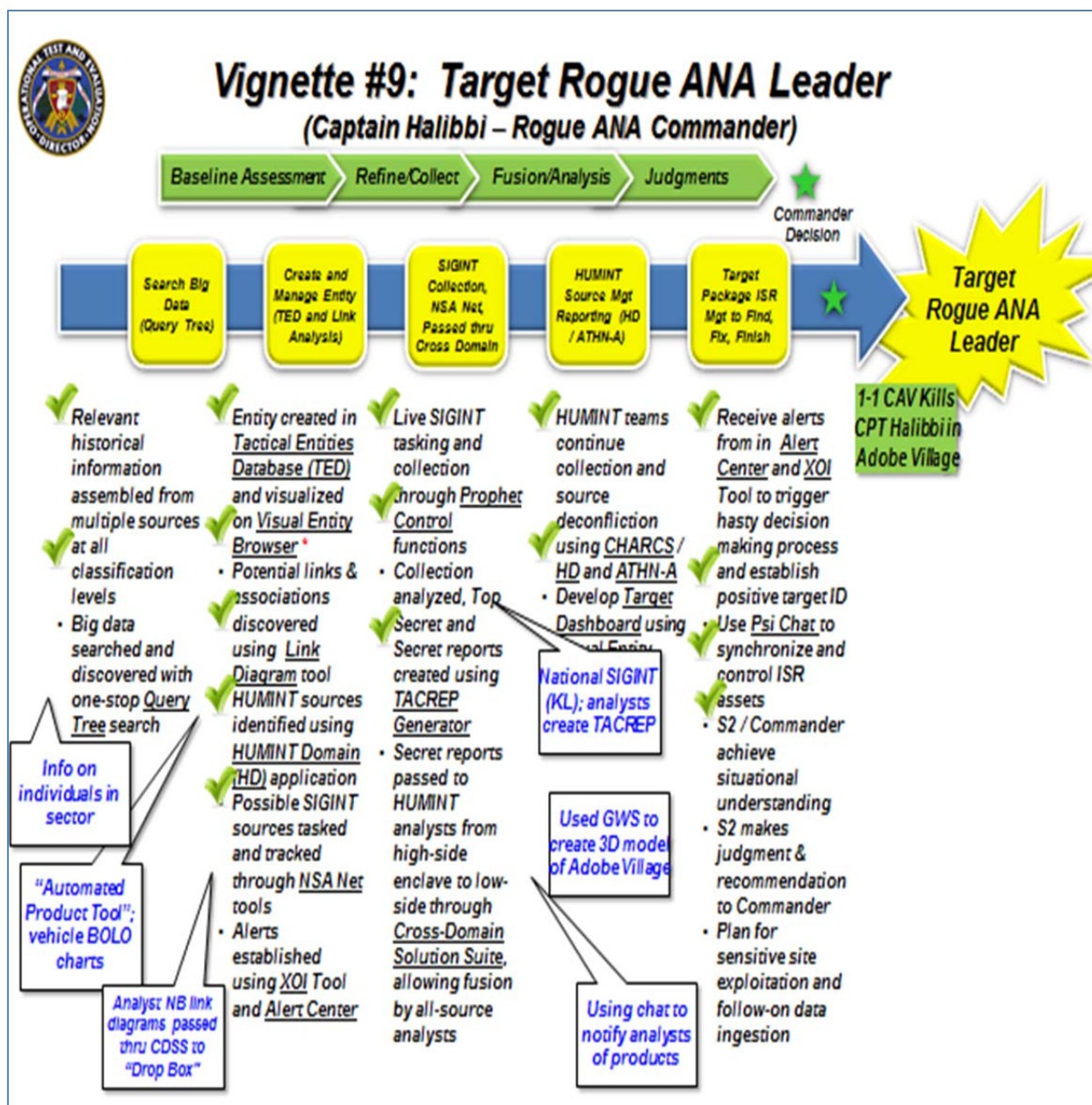


Figure A-13. The Actions Anticipated in the Vignette 9 Story Lines and Supporting Tools the Unit Was Expected to Use

In vignette 9, the test unit successfully found and neutralized an insurgent leader. Analysts used historical information to identify associations and learned that the leader was smuggling weapons. Analysts then discovered intelligence that revealed meetings between the rogue leader, his associates, and regional members of an insurgency. The GEOINT found the smuggling operations. The test unit used multiple intelligence sources to monitor the rogue leader's movement and made the rogue leader their top priority target on the high value individuals target list. Using intelligence that the insurgents and rogue leader were causing increased enemy activity in a local village, the unit targeted and eliminated the rogue leader.

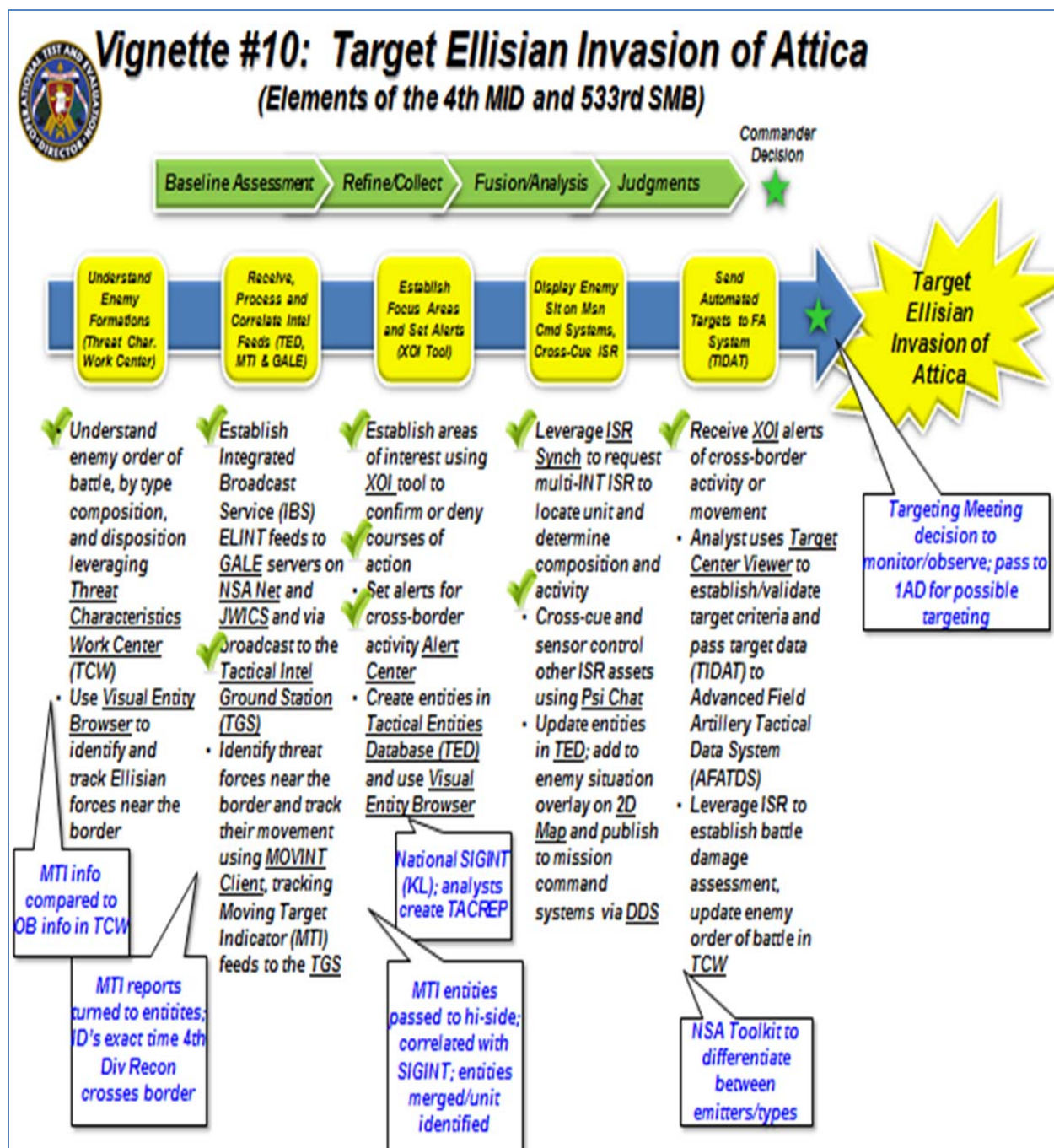


Figure A-14. The Actions Anticipated in the Vignette 10 Story Lines and Supporting Tools the Unit Was Expected to Use

The daily test team synchronization meeting discussions indicate the unit successfully executed the tasks necessary to track enemy movements in vignette 10. DOT&E did not find the actual products the unit produced for vignette 10 in the test database. This vignette was part of the pilot test, not the formal record part of FOT&E.

Acronyms used in Figures A-1 through A-14

AFATDS: Advanced Field Artillery Tactical Data System
ALA: Attica Liberation Army (Fictional insurgence force)
ANA: Attican National Army
ATHN-A: Advanced Tactical HUMINT Nexus-Army
BMP: Boyevaya Mashina Pekhoty (Soviet Amphibious Infantry Fighting Vehicle)
BOLO: Be On the Look-Out
CAV: Cavalry
CDSS: Cross-Domain Solution Suite
CHARCS: Counterintelligence HUMINT Automated Reporting and Collection System
CPOF: Command Post of Future
DDS: Data Dissemination Service
DIB: DCGS Integration Backbone
ECP: Entry Control Point
ELINT: Electronic Intelligence
FMV: Full Motion Video
GALE: Generic Area Limitation Environment
GEOINT: Geospatial Intelligence
GWS: Geospatial Intelligence Workstation
HCT: Human Intelligence Collection Team
HD: Human Domain
HUMINT: Human Intelligence
HUMSUM: Human Intelligence Summary
IBS: Integrated Broadcast Service
ID: Identification
IED: Improvised Explosion Device
IIR: Intelligence Information Report
IN: Infantry
INTSUM: Intelligence Summary
ISR: Intelligence, Surveillance, and Reconnaissance
IVO: In vicinity Of
KL: Klieg Light
LD: Link Diagram
Mgt: Management
MOVINT: Movement Intelligence
MTI: Moving Target Indicator
NIE: Network Integration Evaluation

NTM: National Technical Means
NSA: National Security Agency
OBJ: Objective
OPFOR: Opposing Force
OMT: Operational Management Team
QT: Query Tree
S2: Intelligence Officer
S2X: Staff element subordinate to the S2 (staff intelligence officer), coordinates Human intelligence and Counter Intelligence
SIGINT: Signal Intelligence
SIGSUM: Signal Intelligence Summary
SDR: Surveillance Detection Routes
SITTEMP: Situation Template
STB: Special Troops Battalion
SVBIED: Suicide Vehicle Borne Improvised Explosive Device
TACREP: Tactical Report
TCP: Traffic Control Point
TCW: Threat Characterization Work Center
TED: Tactical Entity Database
TIDAT: Target Data
TGS: Tactical Intelligence Ground Station
TGT: Target
TS/SCI: Top Secret / Sensitive Compartmented Information
VCAB: Virtual Cabinet
XOI: Extended area of Interest