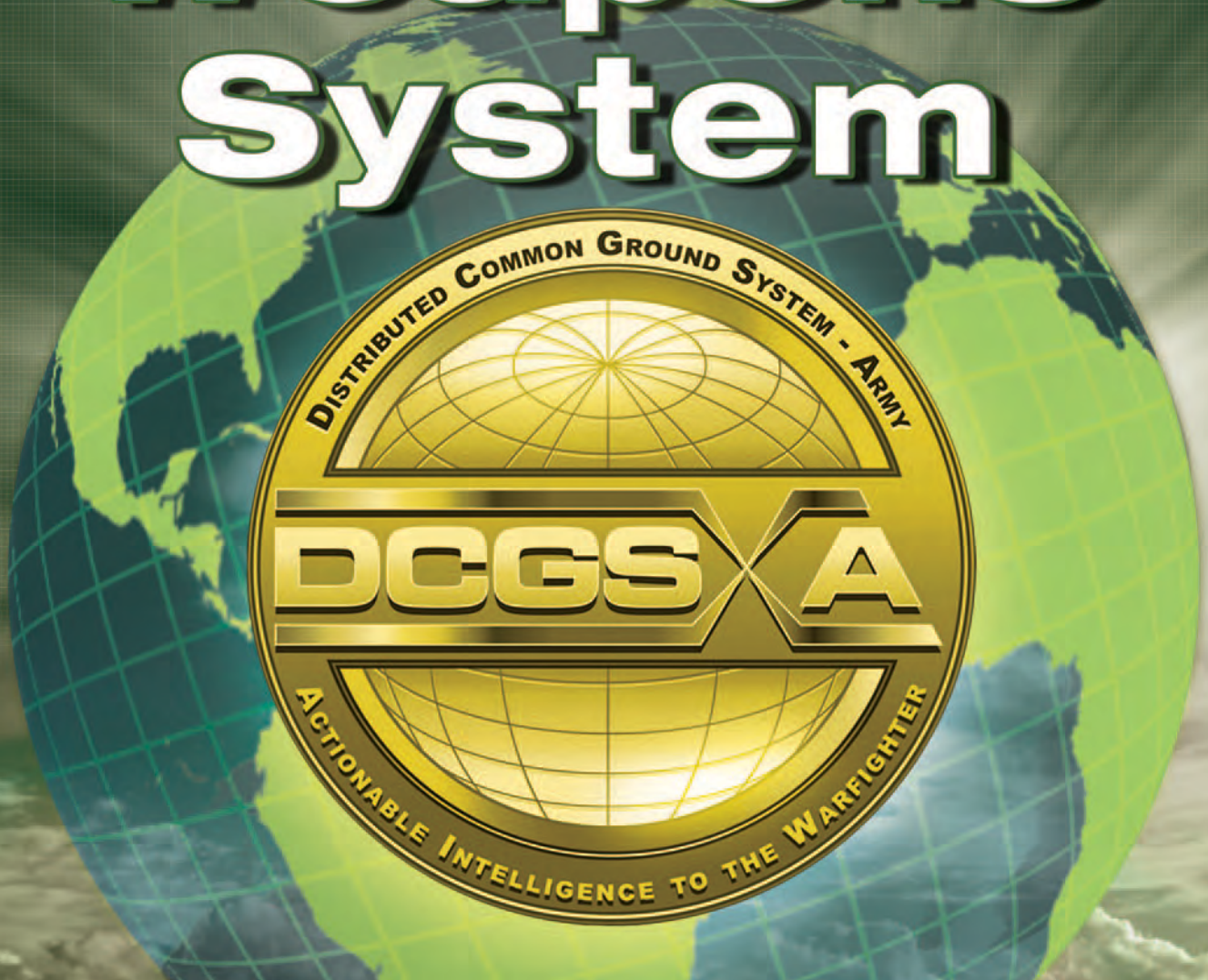
MI Professional Bulletin
October - December 2016
PB 34-16-4

Leveraging DCGS-A: Our Primary Weapons System



Subscriptions: Free unit subscriptions are available by emailing the Editor at usarmy.huachuca.icoe.mbx.doctrine@mail.mil. Include the complete mailing address (unit name, street address, and building number) and the number of copies per issue.

Don't forget to email the Editor when your unit moves, deploys, or redeploys to ensure continual receipt of the Bulletin.

Our mailing address: MIPB, USAICoE, Box 2001, Bldg. 51005, Ft. Huachuca, AZ, 85613

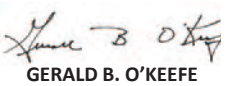
Issue photographs and graphics: Courtesy of the U.S. Army, DCGS-A Public Affairs and issue authors.

Purpose: The U.S. Army Intelligence Center of Excellence publishes the **Military Intelligence Professional Bulletin** (**MIPB**) quarterly under the provisions of **AR 25-30**. **MIPB** presents information designed to keep intelligence professionals informed of current and emerging developments within the field and provides an open forum in which ideas; concepts; tactics, techniques, and procedures; historical perspectives; problems and solutions, etc., can be exchanged and discussed for purposes of professional development

By order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:



GERALD B. O'KEEFE
Administrative Assistant to the
to the Secretary of the Army

1626003

From the Editor

As the new Editor, I would like to bid farewell to Sterilla Smith and thank her for her dedication to this bulletin.

MIPB is on the open (public) front page of IKN at https://www.ikn.army.mil/ and the site has undergone revision. Current and archive issues are again accessible. Archive access requires CAC login.

The following themes and deadlines are established for:

April – June 2017, BCT S-2 Operations, deadline for submissions is 30 December 2016.

July – September 2017, Division and Corps Intelligence Operations, deadline for submissions is 7 April 2017.

Articles from the field will remain important to the success of MIPB as a professional bulletin. Please continue to submit them. Even if the topic of your article may differ from an issue's theme, do not hesitate to submit it. Most issues will contain theme articles as well as articles on other topics. We seriously review and consider all submissions that add to the professional knowledge of the MI Corps and the intelligence community.

Please call or email me with any questions regarding your article or any other aspects of MIPB.

Tracey Remus

Editor

MI Professional Bulletin
October - December 2016
PB 34-16-4
Volume 42 Number 4

10

20

FEATURES

The views expressed in the following articles are those of the authors and do not necessarily reflect the official policy or position of the Departments of the Army or Defense, or the U.S. Government. Article content is not authenticated Army information and does not supercede information in any other Army publication.

DCGS-A: Our Primary Weapons System

DEPARTMENTS

Inside back cover: DCGS-A Situational Awareness Graphic

Always Out Front

by Major General Scott D. Berrier
Commanding General
U.S. Army Intelligence Center of Excellence

In the last issue of MIPB we explored megacities and their implications in future warfare. As U.S. technology and capabilities continue to improve, the enemy will progressively conduct operations in megacities and dense urban areas to mitigate our technological advantages. To win in complex operating environments like megacities, the Army developed the Army Operating Concept (AOC). The AOC describes how the Army will operate across multiple domains as part of joint, interorganizational, and multinational teams. According to the AOC the Army must deploy and transition rapidly, present multiple dilemmas to the enemy, operate dispersed while maintaining mutual support, and consolidate gains. These key tenets of the AOC place significant demands on ground commanders, who then turn to their intelligence professionals for real-time detailed intelligence. To answer these challenging commander requirements, the Department of Defense created the Distributed Common Ground System (DCGS) and the Army developed its variant: DCGS-Army (DCGS-A).

Army intelligence professionals use DCGS-A, their primary intelligence weapon system, to answer intelligence requirements rapidly and accurately. This edition of MIPB is focused on fully realizing the potential of our program of record, DCGS-A, and how it assists Military Intelligence (MI) professionals in improving fusion and analytic efforts. DCGS-A provides commanders with real-time intelligence while receiving and sharing information across the intelligence enterprise.

After the events of 9/11, in the infancy of operations in Iraq and Afghanistan, demand for intelligence, collection, analysis, and fusion skyrocketed. Unfortunately, many units and intelligence professionals, particularly those deployed to combat zones, found it nearly impossible to receive and share actionable intelligence in a timely, efficient manner. This inability to share was due to incompatible intelligence systems and platforms, most of which stovepiped information at each level of analysis and fusion. There was no single system or information sharing structure for units from the battalion to the joint task force level to receive and disseminate tactical to national level intelligence. The intelligence community began sustained efforts to build a system capable of tactical to national level access to data, collaboration, production, and dissemination. In 2007, the Army implemented the DCGS-A program of record.

DCGS-A is the realization of an Army "system of systems" that connects our forces to information and intelligence across the intelligence enterprise. Instead of individual collection sensors and platforms using separate, disjointed systems for production and dissemination, all analysis and production now falls under the DCGS-A umbrella. DCGS-A brings together multiple intelligence functions into a single system allowing units at all echelons to fuse information and intelligence from multiple sources across all intelligence disciplines. DCGS-A allows analysts to access intelligence across all classification levels, and contains many tools the analyst can use to produce better intelligence. These analysts use DCGS-A to provide commanders with actionable intelligence.

DCGS-A is critical to intelligence operations and is, therefore, one of our top priorities. We must tailor and operate DCGS-A to support commanders in fixed, reachback, and expeditionary operations. DCGS-A is a robust system, but its capabilities can only be fully achieved if our Soldiers know how to use it. We have to build and maintain proficiency with our main intelligence weapon system to optimize its many capabilities. I encourage you and your Soldiers to build and maintain proficiency with your intelligence weapon system. The juice is definitely worth the squeeze. There are currently initiatives in place to reduce the complexity of the DCGS-A system at the battalion level, as well as configuring a DCGS-A laptop as a server for use at the battalion level. Off-the-shelf capabilities are also being assessed for simplifying the use of DCGS-A programs. We all play an important role in ensuring that the force is fully trained and ready to employ DCGS-A while in garrison so that using DCGS-A is second nature during operations.

Our uncertain future poses significant challenges to MI professionals and the Army. DCGS-A is the MI professional's flagship system to answer intelligence requirements and disseminate intelligence products across all echelons. However, systems and technology do not solve all of our challenges. The strength of our profession resides with our Soldiers and Civilians. Increasingly reliable and technologically advanced systems do not provide us with the advantage to win without technically skilled users. Therefore, we must continue to build competent and adaptive Soldiers and leaders; MI professionals who are hungry to learn, think critically, and are proficient on their assigned intelligence systems. As General George S. Patton famously said, "A pint of sweat saves a gallon of blood."

"Always out Front and Army Strong!"

CSM FORUM

by Command Sergeant Major Thomas J. Latter
U.S. Army Intelligence Center of Excellence

DCGS-A: It Will Get Better, Use What You Have Now to the Best of Your Ability

Bottom Line Up Front: Distributed Common Ground System–Army (DCGS-A) will get better in the future, but you need to be proficient in the system you have available today.

What exactly does it mean when everyone keep saying DCGS is a program of record (POR)? It means the program is recorded in the present and Future Years Defense Program. In other words it is not going away. DCGS-A will be the intelligence weapon for the U.S. Army for the next 20 to 30 years. Let's look at this in comparison to the M16 Rifle which was fielded in Vietnam in 1965. Feel free to do some research on your own, but you will find that the original model of the M16 fielded in the 1960s did not fully meet the needs of the Army, especially in the environment in which we were utilizing it. There were multiple issues, some of which were addressed through increased maintenance and individual training on the weapon, and some of which were fixed through design improvements, which led to the M16 A1; and years later the M16 A2, and years after that the M4, which we see in widespread use today. By the way, the M4 is based on a Special Forces version of the original M16 designed in the 1960s. So you have the same weapons system updated and still in use 50 years after inception, that is a POR. What does this have to do with DCGS-A? You need to look at your current version of DCGS-A as the original M16.

This "system of systems" was designed on-the-go over the past decade to meet the changing needs of our Army to provide intelligence to the warfighting maneuver commander with access to strategic level intelligence to guide operational and tactical level missions. This original version was designed to support brigade and above headquarters, but mission has forced modifications to it, and in some cases due to overseas contingency operations extremely modify it to meet the needs of battalion and below formations, especially in the Special Operations Community.

First, let us address design improvements. Increment Two scheduled to be fielded in 2020 will address most of the major issues identified since the initial fielding in 2007 and address compatibility issues between systems. By Increment Two, contractual language will require additional developments to be able to plug and play with the system of record and allow for greater toggle-on and -off capabilities based on the echelon of system use. This is something that was not fully addressed or enforced in the past when the priority was to get the latest developments into the hands of the warfighters at the earliest opportunity. But we cannot wait until 2020 to get better.

Plug it in and use it. DCGS-A is not just about the analytical tools that reside on the system. It is also about getting "sets and reps" on employing the architecture; physically setting it up and verifying that your reporting is going through the system to publish on the Command Post of the Future system. If the commander is not seeing the intelligence as part of his overall operational picture he or she is not making an informed decision. If you are still running from the "2" shop to the Operations area and "fat fingering" the data, you are wasting time, critical in a decisive action training environment.

Unit level sustainment training means getting your multifunction work station talking to the Army Battle Command System. It may be hard to get the architecture right, but you need to use the systems while training so that they work during a deployment. Repetition, repetition, repetition…Try to go to the field every time your supported maneuver elements do and ensure you are jumping with the tactical operations center/tactical command post so your Soldiers become proficient at tearing down and setting up the architecture. Master this intelligence warfighting function by making it competitive among your personnel to stress speed of employment and develop the best practices for your organization. Share those best practices with your peers at other MI companies, battalion/brigade S2 sections, and division G2 and analysis and control elements.

If you polled units across the entire Army, including the Guard and Reserves, you will not find everyone has the M4, some units still have M16 A2 and some M16 A1s, so don't expect everyone to have the latest edition of the DCGS-A system. However, that is no excuse for not being proficient on your version of the system. Going back to the M16 analogy–if I provide Soldier "A" with an original M16 and give them 12 hours a day to train, seven days a week, in all weather conditions and times of the day with unlimited ammunition; and Soldier "B" with a M4, but only 200 rounds of ammunition and limit his/her training to 4 hours a month during day time and clear skies; Soldier "A" will consistently outperform Soldier "B" on the battlefield,

(Continued on page 9)

Technical Perspective

Chief Warrant Officer Five Matthew R. Martin
U.S. Army Intelligence Center of Excellence

In this edition of MIPB, we focus on the Distributed Common Ground System–Army (DCGS-A) family of systems. The primary purpose is to highlight some of the creative ways the system has been employed, valuable lessons learned, and the collective efforts of our intelligence professionals to improve education and training. Our enduring DCGS-A efforts are meant to ensure the Military Intelligence (MI) Corps continues to be postured to execute its core competencies *(intelligence synchronization, intelligence operations, and intelligence analysis)* in support of mission command.

In order to remain always out front, the Soldiers of the MI Corps must remain committed to seeking new and improved methods to train, implement, and deploy our intelligence systems. We must fully realize and enable our Soldiers to leverage technology and maintain pace with near-peer adversaries that strive to achieve overmatch. Through our collective efforts we can achieve the Chief of Staff of the Army's #1 priority "Readiness."

There is no better example of this enabling effort than the DCGS-A Initiatives Group (DIG). The DIG was formed in 2016 as part of a joint U.S. Army Intelligence Center of Excellence (USAICoE) and the U.S. Army Forces Command (FORSCOM) effort as a means to examine and propose solutions to the most complex challenges regarding training, employment, and functions associated with the DCGS-A family of systems. The 25 warrant officers selected to serve as members of the DIG are all expert trainers and proven DCGS-A practitioners who have demonstrated a strong desire to find solutions to technical and training shortfalls that allow the Army to maximize its investment in DCGS-A.

They are representative of the entire Army, including FORSCOM, the U.S. Intelligence and Security Command, USAICoE, TCM-Foundation and the Program Manager's Office, and unquestionably represent the greatest collection of DCGS-A talent the Army has collected into a singular body. The DIG has already made significant gains towards improving Army readiness with the development and execution of additional education and training initiatives and future requirements development. Their continued efforts ensure we have the opportunity to make revolutionary long-term gains in our Soldiers readiness at all echelons.

The complexity of DCGS-A is widely recognized and acknowledged. Despite the complexity of the system, our intelligence professionals across the Army regularly prove that, when paired with fully trained and proficient operators, we are capable of leveraging the full power of the DCGS-A family of systems to produce timely and accurate doctrinal intelligence products. However, lessons learned consistently illustrate that as a warfighting function, we currently lack uniform skills and knowledge to plan and develop an executable intelligence framework or architecture that is configured to meet mission requirements. This gap led the FORSCOM Commander to direct the creation of the Digital Intelligence Systems Master Gunner Course (DISMGC). The DISMGC is a collaborative effort providing a training and educational opportunity to further develop competent DCGS-A operators with an ability to plan, execute, and supervise the integration of a customizable intelligence architecture capable of meeting the demands of mission command.

The MI Warrant Officer Training Branch (WOTB) has also made significant gains towards optimizing DCGS-A and intelligence architecture knowledge through the development of a phased plan that leverages the Intelligence Electronic Warfare Tactical Proficiency Trainer to facilitate a decisive action end of course exam. Students will plan and configure a functional intelligence architecture and use DCGS-A components to provide intelligence support to the military decision making process. These ground breaking efforts will allow the WOTB to integrate existing professional military education into an overarching DCGS-A training strategy that will challenge future students' abilities while developing greater trust and confidence in our MI systems.

The Army will continue to be challenged by reduced operating budgets, and a move towards a smaller force–optimized to fight a wide-ranging array of threats. In order to ensure we are adequately prepared, the MI Corps must continue its efforts to maximize training opportunities and master our existing intelligence systems even as we embrace new and developing technologies. We will increasingly be counted on to provide the same level of quality intelligence support commanders are accustomed to–with reduced resources. This effort requires result-oriented leaders who are creative, adaptive, and willing to invest the time and effort necessary to truly master their craft.

"Always out Front and Army Strong!"

Tailoring Existing Capability in DCGS-A to Meet Emerging Demands

by Major Brandon L. Van Orden and Mr. Robert S. Coon

"The DCGS Enterprise…has one overarching objective–deliver intelligence to the decision maker. To achieve this objective three key enabling concepts exist to support this effort: Data and Service Standards, Enterprise Wide Data Management, and Integrated Analysis and Analytics…"
–DCGS Enterprise CONOP, 2016-2019

Introduction

In June 2014, the self-proclaimed Islamic State (IS) occupied Mosul and took control of the city. After subsequent events in Ramadi and Fallujah, and feeling the continued effects of a protracted civil war in neighboring Syria, the Government of Iraq requested U.S. military assistance.[1] As a result, U.S. Army Central (USARCENT) deployed a command post to Baghdad and ordered the 513th Military Intelligence Brigade (Theater) (513th MIB(T)) to support quickly evolving operations assisting host nation security forces in the defense of Iraq, efforts later designated as Operation Inherent Resolve (OIR).[2] The brigade deployed a tailored multidiscipline intelligence support element with a complement of tactical Distributed Common Ground System–Army (DCGS-A) program of record systems.

While U.S. and international civilian leaders had not yet fully defined the political, legal, and military implications of OIR, USARCENT and the 513th MIB(T) faced the challenge of having to deliver capability to forces committed to theater with a reliance on distributed analytical, systems integration, and intelligence sustainment. The brigade, with assistance from the U.S. Army Intelligence and Security Command (INSCOM) G3, quickly identified the need to tailor existing capabilities inside DCGS-A to a more responsive, flexible, and agile threat visualization and reporting tool suite. This was in response to intensively managed Force Manning Level constraints, the distributed nature of mission responsibilities, and the extensive participation of multinational partners.

The Problem: Trading Capability for Governance

The 513th MIB(T) deployed DCGS-A systems included Portable–Multifunction Workstations (P-MFWS), an Intelligence Fusion Server (IFS), and a Geospatial Intelligence Workstation. These tactical systems are designed to provide deployed forces access to the Army and larger Intelligence Community's intelligence enterprise. When employed correctly DCGS-A provides analysts access to over 700 historical and dynamic (live) threat associated sources harvested by one of the five MIB(T)'s DCGS-A Fusion Brains.[3] It can connect multiple analytical centers and share intelligence products through a federated system of servers regardless of geographic location or network domain.[4]

The tremendous capability DCGS-A provides comes at a cost. The amount of organizational energy units must commit to the technical, integration, and maintenance requirements of the system can be burdensome and can, at times, become too much for a unit to sustain. Challenges are varied, but include: connecting to local, tactical, or strategic networks; ports, protocols, and security management; coordinating between Army, joint, and interagency partners that host data required for ingestion; and extensive, long term training programs required at the unit level beyond initial operator certification. Most challenges can be traced back to the requirement for intensive governance–governance of data, governance of systems, and governance of training.[5] As units shift limited resources to governance, they must ensure they do not degrade support to analytical production, exploitation, or intelligence fusion.[6]

DCGS-A is based on a nodal hierarchy where each echelon maintains similar capability, with capacity (e.g., storage and processing) increasing as one moves up the hierarchy.

For example, units can configure a P-MFWS to operate, on a limited scale, as a standalone server. An IFS, when configured can provide some of the same data query and discoverability capabilities as the Fusion Brain.[7] Again, these configuration changes require extensive training, familiarization, and proficiency by the operators, integrators, and officers in charge.

A major node at the tactical level is the IFS. The IFS' significant components include the Application Server, Message Database, Meta-data Catalog, Interoperability Server, Ozone, and the Spatial Database Engine.[8] The Spatial Database Engine houses geospatial (e.g., imagery-maps, points, lines, and polygons) data. The Ozone provides access to the DCGS Integrated Backbone that, in turn, makes queries that are federated through the Meta-data catalog discoverable to an end user. The Interoperability Server houses the associational data base, and the Application Server ties them all together for use through over 129 applications or tools provided in the DCGS-A suite.[9] In our opinion, units determined to successfully employ the IFS should focus on three components: the application server, the message database, and the interoperability server. All units should, however, engineer their priorities and applicable tools based on specific mission requirements identified through staff analysis.

Through the IFS, units can tailor the data feeds ingested into their local message database based on specific regional or functional intelligence requirements. Using the Interoperability Server, units can deploy an application to access this server called the Tactical Entity Database (TED). The TED is an associational database that can take a copy of pieces (e.g., entity tables and attributes) of the authoritative analytical database of record (the Modernized Integrated Database (MIDB)), and employ it for use to support a named military operation. At its base, an associational database "associates" messages with entities (e.g., units, people, places, things, events) and in turn can associate entities with each other (e.g., a piece of equipment can be associated with a unit and a unit can be associated with a facility).[10]

513th MIB(T) and USARCENT determined that to be successful, they must leverage the capabilities DCGS-A offered, but also had to navigate the challenges associated with integration and sustainment. As they prioritized people and equipment, they determined pushing extensive hardware into Baghdad would not achieve the intended results. The question remained–how would the MIB(T) deliver capability through reach without increasing resourcing requirements forward?

Photo by Fusion C-ISIL Database Team, July 2016.

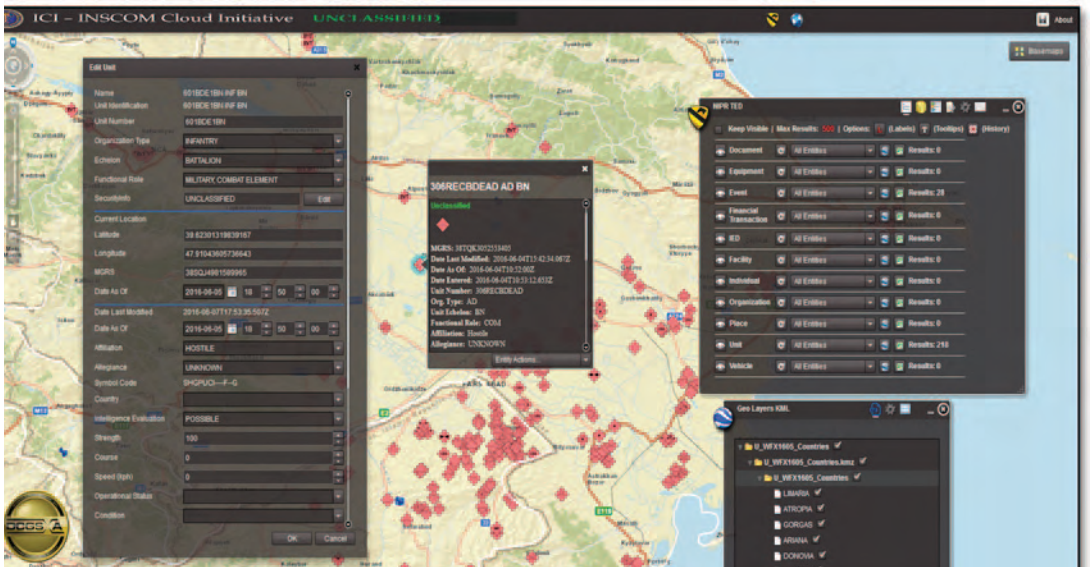
513th MIB(T) Soldiers Supporting from Reach.

Intensively Managed Force Management Level Constraints

Keen to keep the mission scope and responsibilities focused, the President of the United States, through the Secretary of Defense, limited the number and type of U.S. military forces authorized inside of Iraq.[11] Referred to as the Force Management Level, these constraints translated into small specialized teams, with limited capacity who were reliant on distributed support from outside of theater. Critical to the success of these specialized teams was the ability to deduce enemy intent through the fusion of disparate threat reporting. While not unique to operations in Iraq, significant challenges for OIR involved discerning relevant threat reporting from the irrelevant, and then ensuring the organization's digital intelligence systems were online, configured, and communicating with appropriate threat message (e.g., Multi-Media Message service) and operational relational databases (e.g., MIDB). The requirements associated with meeting the challenges above quickly outpaced the capability of the forward teams.[12]

Empowered by USARCENT, INSCOM and the 513th MIB(T) developed what would become known as the Counter–Islamic State in Iraq and the Levant (C-ISIL) TED, a data repository of relational entities and reporting. This repository, residing on DCGS-A hardware and software, formed the central physical node, or "publisher," of a strategy that distributed the exploitation of theater and national threat reporting in order to enable fusion forward.[13] This distributed exploitation agreement began in earnest in late 2014, with the 513th MIB(T), INSCOM G3 Operations and Training, and the Department of the Army Intelligence Information Services dividing responsibilities across functional intelligence types or sources, then creating object-oriented data

(e.g., units, people, places, things, events) in the C-ISIL repository for use by forces in theater. By removing/mitigating technical and operational overhead from forward units, the limited number of analysts 'at the edge' were able to focus on fusion, without having to spend valuable time and limited resources on exploiting hundreds or thousands of messages a day. Named for its founding participants, the INSCOM Cloud Initiative (ICI) delivered both traditional DCGS-A systems data and enterprise expertise, as well as web based services and tools accessible to all users inside and out of theater as part of a common framework.[14]



INSCOM, ICI Portal, 1CD Warfighter Exercise, May 2016.

The ICI took a major leap forward with INSCOM's partnership with the 82d Airborne Division's designation as the Combined Force Land Component Command–Iraq (CFLCC-I) and deployment in 2015. Through a series of deliberately planned pre-deployment engagements, the 82d assumed operational management responsibilities of evolving Mission Command using the overarching ICI strategy.[15]

Distributed Nature of Mission Responsibilities

As the partnership with the 82d Airborne Division expanded, so did the appreciation that each echelon operating in Iraq had very different mission responsibilities. The distributed nature of these responsibilities, and the inherent difference of type and periodicity of information required, amplified the need for responsive, web based applications where a distributed cloud could layer different types and sources of information based on disparate mission requirements within a common framework. Using DCGS-A derived intelligence information as its base, INSCOM developed a portal to deliver services from across the Intelligence Community without increasing configuration, bandwidth, or native storage requirements forward. Users now had the option of operating from their organic or theater provided DCGS-A hardware or the ICI portal independent of a specific technology platform (e.g., any computer with a connection to SIPRNET). Users could contribute, edit, save, and replicate their changes through a DCGS-A server federation spanning four countries and eight military organizations, all through web based tools. This expanded capability was critical in both assisting units in accomplishing their intelligence mission and capturing their unique information contributions for use to the larger Intelligence Community.[16]

These unique requirements changed at nearly every echelon, and yet it was critical to capture and share data with all parts of the federated strategy. Requirements for the CFLCC-I J2 section were often split between force protection and supporting Iraqi Security Force operations with dynamic targeting. Their data requirements were wholly different, but at times connected to the Combined Joint Task Force J2's requirements to support deliberate targeting at the operational and strategic levels. The brigade combat teams, deployed throughout Iraq, focused on building partnership capacity; their primary needs for intelligence information revolved around force protection and trainee/vendor vetting. The integration of Special Operations Forces became another complex layer, made easier through the ICI portal given its ability to integrate different programs of record and commercial systems in one intuitive environment.

By leveraging the distributed nature of the exploitation strategy, INSCOM could tailor capability quickly, responding to the varied and evolving requirements of each echelon by delivering new web based widgets or tools for use through the ICI Portal.

Extensive Participation of Multinational Partners

Throughout the first year of operations in Iraq, the challenges faced with data and intelligence integration, while difficult, all had one thing in common–they operated on secure U.S. only networks. As INSCOM, USARCENT, and the 513th MIB(T) became more efficient at the governance of data and integration of systems, they began to shift focus to the extensive number of nations participating in the coalition. The first, and simplest, was sharing with the integration of the commonwealth partners. Critical in this step was

a close partnership with the U.S. Central Command J2 staff. Following the practice of delivering services to the end user rather than hosting large amounts of data natively, INSCOM and the 513th MIB(T) leveraged existing cross-domain solutions, and proven industry standard business logic, to dynamically share intelligence reporting and object-oriented data between U.S. and partnered nations as appropriate.

As the coalition grew, new separate networks were established, forcing the 513th MIB(T) to host additional hardware and INSCOM to replicate the ICI strategy in a parallel environment. While again challenging, the lessons learned over the previous year and applied on the coalition network allowed for the initial capability launch in late winter 2015. These efforts, coupled with the great partnership between Army, joint, and multinational organizations, helped provide a similar capability to nearly all of the 29 countries participating in the coalition.[17] While the ICI as a strategy was developed out of the INSCOM and Army, care was taken to follow already established industry standard business practices and joint interoperability standards, thereby ensuring contributions made through the ICI portal could be shared throughout the intelligence community. By ensuring all contributions were ultimately written to the DCGS-A TED, the capability existed to publish those objects to other mission command and intelligence systems or databases. Just as the strategy takes relevant data from national and theater sources, the DCGS-A IFS can contribute unique objects to the community using established lines such as the Global Command and Control Systems–Joint or the U.S. Army Data Dissemination Service.[18,19]

Challenges Remain

Even with the success of the ICI as a strategy and its application as an intelligence architecture, there is still much work to be done. Governance across the enterprise requires consistent and intensive management. Every capability applied during INSCOM's build out of the ICI strategy was met with a unique set of circumstances each party involved had to navigate through. Configuration, bandwidth at some locations, and the disadvantage/disconnected user remain very real issues, as does balancing increased capability and sharing against very real cyber threats. Each opportunity must be exploited, and every challenge documented with the mitigation used that eventually will lead to success.

An example of success applied is the redeployment engagements between INSCOM, the MIB(T), and a deploying unit, such as the 82d Airborne. Applying the model developed prior to the 82d Airborne's deployment, INSCOM helped support division and brigade deployment validation exercises. These engagements introduced the deploying unit to INSCOM and MIB(T) capability, as well as offering an opportunity to delineate supported and supporting command responsibilities. To date, INSCOM and the 513th MIB(T) have supported, in addition to the 82d Airborne Division, the XVIII Airborne Corps, 101st Airborne Division, 1st Cavalry Division, and elements of 3rd Infantry Division's pre-deployment exercises. All of these units were scheduled to support operations in the USARCENT area of responsibility. Through these engagements, INSCOM and the MIB(T) were able to inform units of the unique characteristics of the operating environment as well as emerging capabilities applied in theater, such as the ICI strategy and portal.[20,21]

In conclusion, given the limited authorized force levels forward, the varied and distributed nature of each echelon's mission requirements, and the extensive number of multinational partners involved in OIR, INSCOM and the 513th MIB (T) designed a simple requirement based exploitation strategy. They tailored existing capabilities in DCGS-A, and delivered multiple web based services to build a responsive, flexible, and accessible threat visualization and reporting tool suite. This tool suite helped enable forward forces while not increasing technical, operational, or physical overhead.

Endnotes

1. Bill Roggio, "ISIS Takes Control of Mosul, Iraq's Second Largest City," *The Long War Journal*, 10 June 2014, at http://www.longwarjournal.org/archives/2014/06/isis_take_control_of.php. Accessed 11 July 2016.

2. Paul P. Reese, *"ARCENT Transition to Combined Joint Task Force-Operation Inherent Resolve, Initial Impressions Report,"* Center for Army Lessons Learned (CALL) No 16-10, March 2016, Fort Leavenworth, KS, 25.

3. Stephen Morton, *"DCGS-A Program Update,"* Presentation, Department of the Army Program Update, 19 May 2015, 2.

4. "DCGS-A Commander's Handbook," TRADOC Capability Manager Sensor Processing, Fort Huachuca, AZ, 2-3, 7.

5. Robert S. Coon, "Tactical Intelligence Operations Concept–Back to Basics in Support of Mission Command," Whitepaper, 7 July 2015, Headquarters INSCOM (Fort Belvoir, MD), 3.

6. Brandon L. Van Orden, *"The Role of a Data Manager in the Successful Employment of the Distributed Common Ground System–Army (DCGS-A),"* U.S. Army Command and General Staff College, 2014, Fort Leavenworth, KS, 52-53.

7. Charles A. Wells, *"DCGS-A Program Overview,"* Presentation, AFCEA Aberdeen Chapter Function, 14 March 2012, Aberdeen Proving Ground, MD, 4.

8. DCGS-A Commander's Handbook, 10-13.

9. Robert Collins, *"DCGS-A Program, Increment 2 Acquisition Construct and General Observations,"* Presentation, 2015 Army INTEL Industry Day, Aberdeen Proving Ground, MD, 4.

10. Robert Coon, *"Joint Operations Access Exercise Update 2,"* 66th Military Intelligence Brigade, Wiesbaden Army Airfield, Wiesbaden Germany, March 2013.

11. Patricia Zengerle, "Obama Seeks Some limits on Ground Troops for Islamic State Fight," *Reuters*, 15 February 2015, at http://www.reuters.com. Accessed 11 July 2016.

12. Department of Defense, *"Modernized Integrated Database (MIDB) Joint Interoperability Certificate Status,"* At http://jitc.fhu.disa.mil/index.html. Accessed 13 July 2016.

13. Brandon Van Orden, *"OIR CIP Dissemination,"* Systems Architecture and Data Integration SOP, as of 15 June 2016.

14. Robert S. Coon, Narada Overton, Nicholas Rife, *"Evolving DCGS-A Cloud Capabilities in the Operational Environment-Lessons Learned from the CJFLCC-I J2 and INSCOM G3,"* Information Paper, 27 October 2015, Fort Bragg, NC, 1, 2.

15. Nicholas Rife, *"Theater Intelligence Brigade Anchor Point Concept Supporting Distributed Common Ground System–Army,"* 29 June 2015. At https://www.army.mil. Accessed July 14 2016.

16. Robert Coon, *"Operation Inherent Resolve (OIR) COTS Pilot,"* Presentation, 24 May 2016, Fort Belvoir, MD.

17. Brandon Van Orden, *"Distributed Common Ground Station–Army (DCGS-A) Capability on the Coalition Network, Battlefield Collection and Exploitation (BICES),"* 7 March 2016, Information Paper, Fort Gordon, GA.

18. Defense Information Systems Agency, "Global Command and Control System–Joint (GCCS-J)." At http://www.disa.mil/mission-support/command-and-control/GCCS-J. Accessed July 18 2016.

19. Sam Easterling, "U.S. Army Tactical C2 Interoperability Services: Publish and Subscribe Server (PASS) and Data Dissemination Service (DDS)," Presentation, 2 December 2009, Army PM Battle Command.

20. "513th MIB (T) Anchor Point CONOP," 9 December 2015, Fort Gordon, GA, 1-3.

21. INSCOM, "Theater Intelligence Brigade as an Anchor Point," Information Paper, 11 September 2014, Fort Belvoir, MD, 1-4.

MAJ Brandon L. Van Orden is the former executive officer and operations officer for the 297th MI Battalion (Operations), 513th MIB(T) at Fort Gordon, Georgia.

Mr. Robert S. Coon is the senior operational requirements integration officer in the INSCOM G3 Office and is responsible for regionally aligned and globally responsive forces. He is stationed at Fort Bragg, North Carolina.

CSM Forum

(Continued from page 3)

not because they have the superior weapon, but because they have mastered their weapon. Remember the greatest intelligence asset the Army has is the trained intelligence professional–you. So get out there on whatever DCGS-A system you have and learn everything you can about it to maximize your ability to support your commander. When you do have recommendations for improvements to the system, ensure you push them up your chain of command. Do not assume something is obvious, or that someone else will fix something. Become part of the solution by making this intelligence warfighter weapon the best it can be in the coming decades.

"Always Out Front and Army Strong!"

MI History Trivia

On 6 March 1970, the Secretary of Defense announced that the US Army Intelligence School at Fort Holabird, Maryland, would move to its new home at Fort Huachuca. What other locations were considered for the new "Home of MI"?

A. Fort Meade, Maryland
B. Fort Riley, Kansas
C. Fort Lewis, Washington
D. Fort Bliss, Texas

Retreat Ceremony, Fort Holabird

See answer on page 31.

Synergize: Leveraging DCGS-A in Corps Intelligence Reachback Operations

by Major Jennifer Harlan and Chief Warrant Officer Three Brian Myhre

Introduction

With a shrinking and fully tasked force operating in a fiscally constrained environment, leveraging Distributed Common Ground System-Army (DCGS-A) to execute intelligence reach supports priority operations, enables training, and sets units on the path to successful home station mission command. In addition to employing intelligence reach during contingency and combat operations, I Corps G-2 relies on intelligence reach to maximize intelligence warfighting function capabilities during major bilateral and multinational Indo-Asia-Pacific operations. These include Ulchi Freedom Guardian in the Republic of Korea and Talisman Saber in Australia.

During these operations, I Corps G-2 forward deploys an average of 32 to 45 intelligence leaders, collection managers, and all-source analysts to provide immediate responsiveness to the I Corps Commander, enhance the Corps staff's understanding of the current enemy situation, and offer dynamic support to targeting and current operations. In addition, I Corps G-2 utilizes 35 to 45 Soldiers for intelligence reach to process single source message traffic, manage the intelligence database, produce the enemy common operating picture (ECOP), identify targets, and conduct longer term analysis. DCGS-A forms the backbone of intelligence reach operations.

Photo by SFC Kevin P. Bell

Capitalizing on DCGS-A in intelligence reach also enables integration of the joint, multi-component force. During Talisman Saber 15, I Corps' Total Force partner, the 34th Infantry Division (ID) (Minnesota Army National Guard), embedded a 20 Soldier analysis and control element (ACE) in the Joint Base Lewis-McChord intelligence operations facility. 34th ID utilized I Corps Intelligence Fusion Servers (IFS) to connect to the Corps intelligence architecture and contribute to the development of the ECOP. During the same exercise, two U.S. Navy analysts augmented I Corps in intelligence reach and employed DCGS-A to provide strategic maritime analysis.

For I Corps, the three primary functions of DCGS-A in intelligence reach include: establishing and maintaining the ECOP, providing support to targeting, and conducting in-depth and longer term analysis.

Developing the ECOP

The majority of the I Corps ECOP is created and managed by the intelligence reach element at home station. Notably, the forward G-2 team conducts operational collaboration and may modify the ECOP to capture significant activity, especially near the forward-line-of-own-troops. The logic path in Figure 1 provides a way to achieve data flow, production, and distribution of the ECOP in intelligence reach for DCGS-A version 3.1.7.3. *Numbers 1-6 below the figure correspond to a yellow gumball within Figure 1.*

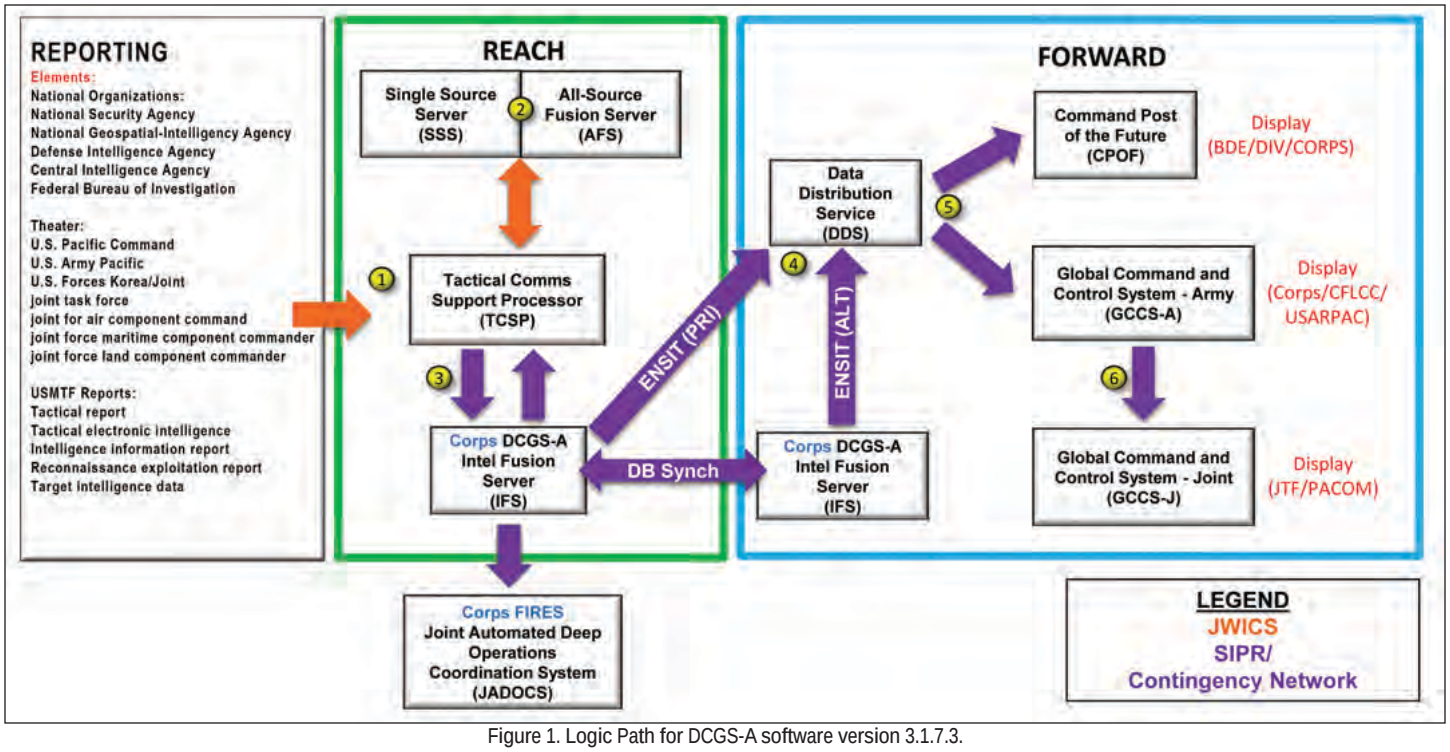


Figure 1. Logic Path for DCGS-A software version 3.1.7.3.

1. U.S. message text format (USMTF) data flows from national, theater, and Corps organic assets into the I Corps G-2 via a complex array of antennae and communications platforms. From there it reaches the I Corps DCGS-A Tactical Communications Support Processor (TCSP).
2. Corps analysts verify that reporting addresses the commander's priority intelligence requirements (PIR) and inject priority reports into the All Source Correlated Data Base on the All Source Fusion Server of the ACE Block II.
3. All Source analysts push the correlated data base from the ACE Block II to the DCGS-A IFS on the contingency network (e.g., SIPRNET, CENTRIX) through the TCSP.
4. The ECOP is then published to the Data Distribution Service (DDS) on the Battle Command Server and disseminated to adjacent and subordinate units' database.
5. From the DDS, all Corps and below Command Post of the Future and Global Command and Control System-Army (GCCS-A) can subscribe to the ECOP.
6. I Corps' GCCS-A provides the ground ECOP to the joint task force-level GCCS-Joint, where it is combined with the air and maritime enemy situation layers for display as the joint task force ECOP.

Support to Targeting

By providing near-real time vetting of thousands of reports per hour based on analyst-selected input, DCGS-A enables the intelligence reach element to pass prioritized targets to the fire support coordinator for action based on the high payoff target list. DCGS-A facilitates the initial vetting of targets and provides redundant options to pass targets, including:

1. Sending target intelligence data from ACE BLOCK II to Joint Automated Deep Operations Coordination System (JADOCS).
2. Passing targets from the analyst to Corps fires via chat.
3. Publishing targeting data directly from the IFS to JADOCS.
4. Passing tactical electronic intelligence through the Advanced Miniature Data Acquisition System Dissemination Vehicle TOMCATS to JADOCS.

Deep Dive Analysis

Corps analysts leverage DCGS-A in intelligence reach to provide more extensive "deep dive" and longer term analysis than is possible within the constraints of forward force strength and capacity. This bolsters the G-2's ability to answer the commander's PIR and enhances decision making. DCGS-A driven deep dive products focus predominately on intelligence support to wide area security and deep shaping.

DCGS-A in Intelligence Reach

Successfully leveraging DCGS-A in intelligence reach requires access to a robust and mature network, intra-staff communication, outreach to joint and combined units, and coordination with G-6 to address firewalls and manage DDS subscriptions. Most importantly, DCGS-A enabled units must build relationships and establish trust before conducting intelligence reach operations to better facilitate information sharing.

The benefits of leveraging DCGS-A in intelligence reach are multifold. DCGS-A supports primary, alternate, contingency, and emergency communications considerations and enables flexibility and redundancy at both the top and bottom of the architecture (e.g., multiple ACE BLOCK II and IFS configurations, information inject points, and potential web-enabled work arounds). Intelligence reach allows for continued support to home station mission command. Intelligence reach maximizes force capacity, reduces overhead, and enables Total Force integration. Intelligence reach reduces the forward footprint, poses less physical risk to Soldiers, reduces time away from home, and provides increased flexibility to the commander.

Nonetheless, intelligence reach has some limitations. It does not test or train the expeditionary capability of the full ACE, and depends on robust and reliable communications links. Intelligence reach support can be distracted by home station mission requirements and hindered by different time zones. Closed network exercises also pose a challenge for intelligence reach operations when home station infrastructure is not equipped to tie in.

The Way Ahead

Intelligence reach support extends the training base to home station and offers training opportunities to Soldiers and units restricted by funding. It replicates "troop cap" scenarios and effectively allows the Corps to train as a unit only separated by space. Intelligence reach represents the best method to practice theater integration at home station. Intelligence reach demonstrates sanctuary support to partner countries, and serves as a model as they build similar capabilities in their armies. This further enhances the I Corps effort to "Set the Theater" for the U.S. Army Pacific Commander.

DCGS-A is the essential ingredient in I Corps' ability to operate dynamically in a complex and fiscally constrained environment. In addition to producing the ECOP and conducting support to targeting from sanctuary, DCGS-A will be integrated into an array of Corps home station mission command operations. These include daily regionally aligned intelligence production, open source intelligence analysis, and federated intelligence production. Ultimately, the I Corps Live Wire initiative, which reinforces digital sustainment and seeks to leverage the system beyond intelligence reach, will serve to validate DCGS-A training and connectivity and encourage DCGS-A utilization in support of real world operations.

MAJ Harlan is the I Corps G-2 ACE All-Source Officer-in-Charge. She previously served in the White House Situation Room. Her next assignment is as an Army Fellow at the Asia-Pacific Center for Security Studies.

CW3 Myhre is the I Corps SIGINT Advisor. He previously served at the National Security Agency. His next assignment is as a SIGINT Analysis Technician instructor for the Warrant Officer Basic Course at Fort Huachuca, Arizona.

Photo by SGT Jennifer Spiker

by Lieutenant Colonel Thomas J. McCarthy

The Impetus for Change

Lieutenant General Charles T. Cleveland (Ret.), former commander of the U.S. Army Special Operations Command (USASOC), officially introduced *ARSOF 2022* in April 2013. The newly presented operating concept, which had been under development for many years, involved a multi-decade blueprint for change that was intended to prepare Army Special Operations Forces (ARSOF) to thrive in a future operating environment (FOE) characterized by uncertainty.[1] Improvements upon human capital investment, SOF-Conventional Force Interoperability, Integration and Interdependence, and Mission Command represent a few of the challenges discussed in *ARSOF 2022*, which would become more complex within the new FOE. Army SOF, and the intelligence apparatus supporting it, realized the need to evolve and adapt to the ever-growing and complex landscape that loomed ahead.

The ability for intelligence Soldiers to provide unimpeded support to operators around the globe became more pronounced upon continued evaluation of the FOE. Success was predicated on the ability to act simply, yet effectively, within austere locations–and with an ability to leverage both service and joint intelligence enterprises. The USASOC G2 was already on its way to achieving this goal when it began co-ordination with the Department of the Army G2, DCGS-A Program Manager (PM) and Raytheon in September 2012 to initiate, under a pilot program, development of the DCGS-A Lite capability.

What is DCGS-A Lite?

The full DCGS-A Lite suite includes Intelligence Fusion Servers (IFS) and streamlined Multi-Functional Workstations (MFWS), which allow personnel the capability to pull data from, and provide information to, conventional and SOF intelligence enterprises–in connected, limited, and disconnected environments. No additional equipment procurement is necessary, as the modified laptops and IFS originate from the unit's DCGS-A Basis of Issue Plan. DCGS-A Lite represents a new software load, vice new equipment procurement. While the DCGS-A Lite Basic Analyst Laptop (BAL) retains 80 percent of the software resident within the DCGS-A MFWS, it derives its true strength from the utilization of three primary, interconnected tools: Hyperion Entity Query; Analyst Notebook; and Vega 4D Spatial Analysis Application.[2] DCGS-A Lite full compatibility with all components of the Army Battle Command System has not yet been achieved; however, the system's data can be retrieved via the DCGS-A Integrated Backbone (DIB).

The system is fielded as a quick reaction capability. Administrative management resides with the DCGS-A PM, but operational execution is controlled by the USASOC G2. In special circumstances, units have been fielded equipment following submission and validation of operational needs statements to support overseas contingency operations. Funding for procurement of licenses to convert the backside processing operability of unit laptops and servers must be accounted for within organizational budgets. Field Service Engineer (FSE) support must be coordinated with the DCGS-A PM. The base software image is also unclassified, which supports applicability within the unclassified domain.

Why DCGS-A Lite?

USASOC forces are typically challenged with the ability to operate and query networked intelligence sources in bandwidth-challenged environments. Consequently, this limits the users' ability to leverage existing intelligence and to generate new intelligence as they perform special missions. DCGS-A Lite addresses this intelligence gap by operating within tactical communications networks and in a limited or disconnected "stand-alone mode." The system works by saving the latest data available before going into disconnect mode. Soldiers isolate the operational area and focus the search to ensure that only relevant data is made

available for review. New visualization techniques enable viewing of this data using any desired map form. Once a network connection is re-established, DCGS-A Lite transmits user-generated data and reports created while in disconnect mode and receives data cached from more than 780 data sources within the DIB to update the situational awareness. Because DCGS-A Lite is agnostic to the communications network with which it interfaces, it gives forward-deployed forces the ability to transmit and receive data over all network nodes from tactical radio to local area networks.[3]

Key evolutionary attributes for DCGS-A Lite include a simplified user interface (UI), streamlined training to manageable and retainable instruction, assured access to the DIB, and integration with both the DCGS-SOF Program of Record (PoR) and the Joint SOF Information Environment (SIE).[4] Access to the SIE network allows integration into the U.S. Special Operations Command's (USSOCOM) repository of data, which is managed under their DCGS-SOF PoR.

DCGS-A Lite's "core" capabilities includes enhanced link analysis, entity creation, and database query from both Hyperion and geospatial displays (maps), increased mapping and 4D visualization tools, and Semantic Fusion Service (SFS). The SFS supports advanced analytics by scrapping data within available repositories, and auto-tagging and recommending entities based on user-defined parameters. The scaled-down and tailored suite of functions enables ease of use and ease of training. DCGS-A Lite also employs the MarkLogic operating system, vice Oracle, which enables improved and increased processor speed for unstructured data, efficiency at the user level, and the capability to operate in disconnected, intermittent, or low-bandwidth (DIL) environments. The DCGS-A Lite's primary features include the following characteristics:

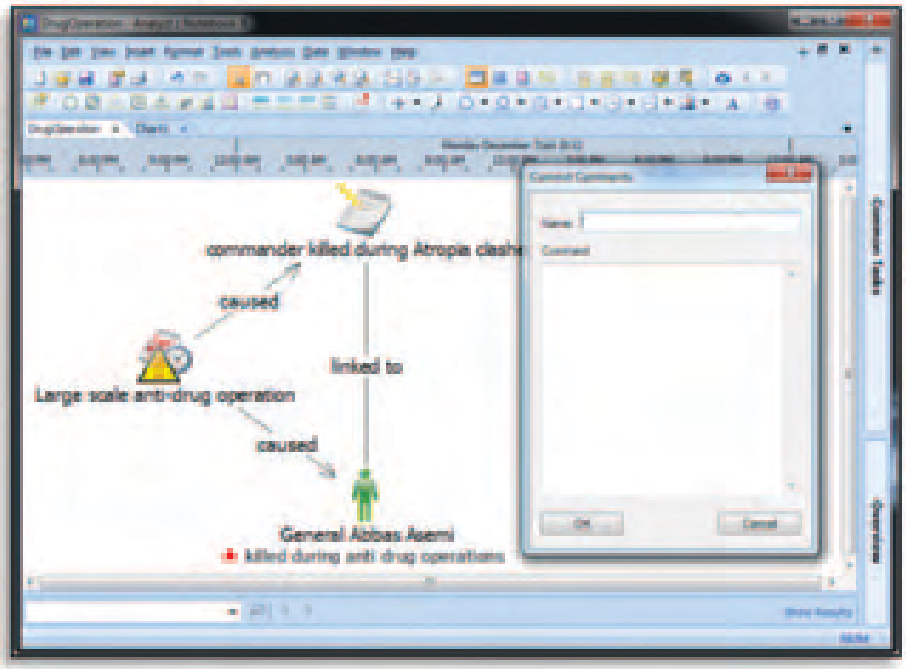
DCGS-A Lite Core Tools

Hyperion. Hyperion is a data mining and management tool with search capabilities as well as entity creation and management features. Primary features work while connected or disconnected from the network. Hyperion has access to multiple data sources, or repositories of intelligence data, integrated with analyst tools. These databases include a shared database (SDB) and personal database (PDB). The SDB is used when connected to the network and is populated with information filtered specific to a particular mission. The SDB data is managed through a standing query set up by an admin. The PDB stores data locally for offline access and is populated through offline setup with a subset of data from the SDB.

Analyst's Notebook. Analyst's Notebook is the industry standard link analysis tool for in-depth, complex network mapping problems. DCGS-A Lite provides tools that make it easy for an intelligence analyst to publish data for sharing, and import for further analysis.

Vega. Vega is a web-based, thin client application used for visualizing and working with data in a four dimensional space. The application can be deployed as an Ozone Widget or as a standalone web application and runs in modern web browsers without the need for a plug-in. Vega was created by Raytheon under contract support to DCGS-A as a prototype for use of emerging HTML 5 and WebGL web standards. Vega is fully government open source software, leveraging open source frameworks, with a focus on user experience as a platform for collaborative capability development with a stable application programming interface.

- Ease of Use: A streamlined UI focused on delivery of applications most used by intelligence analysts, integrating interoperable Query/Data Mining capability, Analyst's Notebook, and 4D Mapping. The UI provides the analyst with a "learnable" structure and enhanced data discovery, enabling network-wide collaboration.
- Ease of Training: The learnable UI is capable of supporting self-training in under two days utilizing the system's embedded video tutorials.
- Limited Mode: This functionality automatically activates if the network quality supporting DCGS-A Lite degrades (falls below a threshold of either 20 percent packet loss or latency of 1500+ milliseconds). While in limited mode, database synchronization will be disabled to conserve bandwidth, but users can still perform queries.
- Disconnected Capability: This feature allows users to operate the system in



Analyst's Notebook.

Vega.

austere environments with pre-downloaded query results, providing the operator flexibility for intelligence gathering and analysis. Once reconnected to the network, the system automatically synchs (i.e., uploads new information and downloads updates) with the DIB, allowing interoperability with the DCGS-A Enterprise, USSOCOM, and the greater Intelligence Community.

Simplicity and Application

The DCGS-A Lite Program of Instruction developed by Raytheon, with input from USASOC subject matter experts (SMEs) and system users, is built upon numerous enabling learning objectives which requires six academic hours to complete. The six blocks of instruction include an Introduction to the program, an Introduction to the DIB and Data Sources, Hyperion, Analyst's Notebook, Vega, and Semantic Tool Suite involving GeoTime, ArcGIS, GeoRover, and SOCET GXP.[5] Training is provided by a combination of Raytheon contracted instructors, the USASOC G2 fielding team, and FSEs and Military Occupational Specialty (MOS) 35T MI System Maintainer/Integrators. Raytheon also supports a 40-hour Administrator training course for FSEs and MOS 35Ts at their facility in Garland, Texas. The USASOC's Special Operations Mission Training Center (SOMTC) also provides DCGS-A Lite training year-round within a classroom setting. The SOMTC supports all USSOCOM elements and all requesting organizations external to the command.

Operational testing and evaluation for DCGS-A Lite has been performed over the years by numerous elements across the force. The 82nd Airborne Division employed the capability during its Joint Forcible Entry Vulnerability 14 Exercise. Feedback reflects optimal DIL performance following intentional network disconnection and utilization of the Personal Database, as well as low-bandwidth functionality via remote connection using the Global Response Intelligence Terminal. Moreover, auto-synchronization of database entities was observed following re-establishing connection to the local IFS.[6]

The DCGS-A Lite fielding team also deployed and tested the system over a two-month period in Afghanistan between November 2013 and January 2014. Fifteen demonstrations in both connected and disconnected mode were provided to more than 25 individuals encompassing MOS 18F SF Intelligence Sergeant, Army intelligence Soldiers, Department of Defense contractors (intelligence analysts), Navy Seals, Air Force intelligence analysts, Signals Intelligence (SIGINT) and Human Intelligence Analysts, U.S. Drug Enforcement Administration field agents, and Operation Enduring Freedom DCGS leads.[7] The system's user friendly interface, Hyperion search function, disconnected capability, and polygon search capability within Vega were lauded. Recommendations for improvement, which has informed development over time, includes the addition of an alert capability for reporting, communication with intelligence, surveillance, and reconnaissance assets, incorporation of SIGINT tools, and integration of a social media analysis capability.[8]

Within USASOC, 7th Special Forces Group (Airborne) has employed the system within its area of responsibility (AOR) since 2013. Interoperability across the force via application of common tools, DIL functionality, intuitive UI, and ease of use are benefits highlighted by users. Full conventional forces/SOF I3 and growth of resident DCGS-A Lite SMEs within formations are noted as areas requiring continued development.

The DCGS-A Lite system is currently deployed by multiple SOF and conventional organizations across various geographic combatant commands. Laptops and server nodes are currently in use and established at Fort Bragg, North Carolina; Eglin AFB, Florida; Iraq; Kuwait; Qatar, and South America. Data resident within these IFS are accessible via the DIB using either the DCGS-A MFWS or DCGS-A Lite BAL. USASOC is also developing a web-based application called Lite Zero that will

allow users to access the data via any SIPR terminal. DCGS-A Lite has retained an Authority to Operate from the Defense Information Systems Agency, received an Authority to Connect and Operate on the SIE, and has received a Letter of Introduction for the USCENTCOM AOR.

Hyperion.

Transformation Objective

The USASOC G2 began with the primary goal of developing a system that provides mission-enhancing tools and intelligence information as far forward as possible in the hands of an MOS18F on an Operational Detachment Alpha and 35-series Intelligence personnel assigned at the team, company, or battalion level. Sustainment of ease of use and training drives continued application of the system's three primary and interconnected tools. Development beyond these functionalities is certainly achievable, but not a critical goal for the command at this time.

Achievement of an initial operational capability (IOC) within all five active component Special Forces Groups (SFG) by the end of the calendar year remains achievable. Additional procurement above IOC, and fielding beyond the SFGs, is contingent upon findings from the DCGS-A PM's work to evaluate and deliver a battalion-and-below solution, as well as USSOCOM's work on the Union Dagger component of its DCGS-SOF PoR.[9] Research within both of these programs will inform the way ahead for attainment of full operational capability across the command. Until results from these efforts are made available, USASOC remains committed to refining the DCGS-A Lite system and expanding its utilization across all network domains. Personnel with interest about this program may contact the DCGS-A PM or the USASOC G2 for additional information.

Endnotes

1. LTG (R) Charles T. Cleveland, "ARSOF 2022," *Special Warfare*, April-June 2013, Volume 26, Issue 2, 3.

2. Michael W. Boardman (Director, Doctrine, Concepts, Experimentation and Lessons Learned DCELL), Memorandum for Director, Capabilities Development Integration (CDI) Directorate, "Lessons Learned (LL) Observations DCGS-A Lite," 14 May 2014.

3. USASOC G2, *DCGS-A Lite: Value of Mobile Intelligence*, 25 September 2014.

4. DCGS-SOF is comprised of four separate elements, none of which include any component of Army's DCGS-A PoR. These four elements include the DCGS-SOF Enterprise, Guardian Dagger (FMV PED), Silent Dagger (SIGINT PED), and Union Dagger (All Source Intelligence Fusion-ASIF).

5. Raytheon Company, *DCGS-A Lite Program of Instruction (POI)* v.416-83104B, 2015.

6. 82nd Airborne Division, *DCGS-A Lite Capabilities Demonstration*, 18 March 2014.

7. COL (R) Barry Harris, Memorandum for Record, "USASOC G2 DCGS-A Lite Operational Test Findings," 28 January 2014.

8. Ibid.

9. Union Dagger is a *prototype* software solution managed by Program Executive Office Special Reconnaissance, Surveillance, and Exploitation (PEO SRSE) DCGS-SOF that provides data search capability for the forward-deployed warfighter. (PEO SRSE DCGS-SOF, *Union Dagger*, 3 December 2015).

LTC McCarthy currently serves as the Intelligence Operations Division Chief within the G2, USASOC, and has more than 20 years of experience within both SOF and conventional organizations. Previous assignments include Intelligence Planner in JSOC, XO and Operations Officer for the 319th MI Battalion, and Experimentation Chief for the Mounted Maneuver Battle Lab. He has three deployments to Afghanistan and two deployments to Iraq. LTC McCarthy holds an MS in Strategic Intelligence from the National Defense Intelligence College and graduated from West Virginia State University in 1997.

Digital Intelligence Systems Master Gunner Course

by Chief Warrant Officer Five Andrew Maykovich
and Chief Warrant Officer Two Nick Rife

The Distributed Common Ground System–Army (DCGS-A) is a collection of systems, services, and capabilities that, when correctly employed, gives intelligence Soldiers access to, and the ability to, process intelligence information with unprecedented speed and accuracy. The well-documented complexity of the system necessitates a comprehensive, cradle-to-grave training strategy that emphasizes career-long growth that eventually results in all intelligence Soldiers mastering the fundamentals of their weapon system. Despite considerable resources dedicated to training Soldiers in the application of DCGS-A systems at the U.S. Army Intelligence Center of Excellence (USAICoE), Foundry courses, New Equipment Training and Tactical Engagement Teams, significant knowledge gaps remain across the Army. These knowledge gaps create systemic and persistent frustration among intelligence Soldiers, preventing the effective employment of the DCGS-A family of systems and limiting intelligence readiness across the force.

Readiness is the #1 priority, ...and there is no other #1.
–GEN Mark Miley, CSA
January 2016

To address these knowledge gaps, in October 2015, the U.S. Army Forces Command (FORSCOM) G2, directed the creation of the Digital Intelligence Systems Master Gunner Course (DISMGC). It quickly became clear that to successfully create such a course would require a collaborative approach leveraging expertise from across the intelligence enterprise. Over the next four months, FORSCOM, in partnership with the U.S. Army Intelligence and Security Command (INSCOM), USAICoE, and the Joint Forces Headquarters Indiana Intelligence Center, recruited 25 intelligence warrant officers who are recognized experts and innovative practitioners with the DCGS-A family of systems. These warrant officers collaborated to construct a comprehensive program of instruction (POI) that is adaptable to cover the full spectrum of DCGS-A enabled operations, and academically rigorous to justify the Master designation.

The three week POI prepares Military Intelligence (MI) Military Occupational Specialty (MOS) immaterial Active Component/Reserve Component/Army National Guard senior noncommissioned officers, junior, and mid-grade warrant officers and officers to assist in planning and developing a customizable unit intelligence framework to support mission requirements, as well as supervise and inspect DCGS-A related training plans within their unit footprint.

The vision and intent is to place a minimum of one DISMG at USAICoE, the Joint Indiana Intelligence Center, at each division, corps, and MI brigade-theater by the end of Fiscal Year 2017. The eventual goal places a minimum of one DISMG at each brigade combat team, and multiple DISMGs at echelons above brigade. Reaching that goal requires a combination of careful talent management and a restructured training strategy that focuses on career-long education and development of every MI Soldier.

The goal of the DISMGC is not to create a single point of excellence within an organization, nor is it to create an individual whose sole focus is DCGS-A. Rather, the objective is to develop an individual who is capable of designing an intelligence architecture that supports the specific unit mission. A graduate of the DISMGC will be capable of planning and supervising the integration of automated intelligence systems supporting intelligence operations, sharing best practices within their unit, and supervising DCGS-A systems architecture training.

Additionally, the DISMG will ensure that unit automated intelligence systems are functional and utilized to their fullest extent. They will review standard operating procedures and training documentation to accurately report the training status within the unit to their senior intelligence officers (SIOs). This capability will allow SIOs to better understand DCGS-A training resources available throughout the intelligence enterprise, as well as individual and unit level DCGS-A training needs.

Finally, the DISMG will have a limited capability to troubleshoot DCGS-A systems related issues, filling the current knowledge gap that exists between operator level and the MOS 35/353T MI System Maintainer/Intregrator. The DISMG will not have administrative privileges, or the knowledge set necessary to perform the functions of an MOS 35/353T or a field service engineer/field service representative.

The DISMGC is designed as three one-week modules that align with the decisive action phases of unified land operations. It is taught using a combination of classroom presentation, lectures, practical exercises, student presentations, and weekly written examinations, as well as a comprehensive final exam. The course requires significant class participation from students, and from guest instructors from multiple units across the enterprise to support specific blocks of instruction. Although currently taught only at Fort Bragg, North Carolina, each corps level Foundry site as well as the Joint Indiana Intelligence Center will eventually become certifying facilities.

Photo courtesy of U.S. Army

Students at DCGS-A Master Gunner Course, Fort Bragg, NC.

The first week (Shape and Deter) focuses on systems capabilities to ensure all students are operating on a common baseline. During this week, students are required to demonstrate the ability to develop and evaluate a unit level DCGS-A training strategy, demonstrate knowledge of various intelligence data feeds, and data replication versus federation. The concept of home station mission command is critical to this phase of training. Students receive several interactive presentations from appropriate industry representatives including engineers from the Systems Integration Laboratory and senior leads at the DCGS-A Field Office Fort Hood, Texas. Maintaining industry support provides DISMGs with an understanding of what advocates exist, and conversely provides industry partners with invaluable direct feedback from highly qualified and experienced users. Each student is also assigned a DCGS-A Master Gunner instructional topic which they must develop and present to the class for evaluation later in the course.

The second week (Seize the Initiative, Dominate) focuses on operating in a joint, interagency, and multinational environment, and aligning assets to deliberately introduce capabilities into the environment. During this week of instruction, students develop and establish an intelligence architecture for use in a deployed environment, develop a Primary, Alternate, Contingency and Emergency (PACE) plan, and virtually examine DCGS-A interoperability with other Mission Command Systems at the Fort Bragg Mission Training Center. Students will learn to leverage national assets while maximizing their organic capability in a distributed environment. Students also develop redundant data acquisition measures, and gain a better understanding of how to distribute capability in order to reduce their vulnerability.

The third and final week of the course (Stabilize, Enable Civil Authority) focuses on planning exercise simulation as well as technical diagnostics. Additionally, students plan and brief a functional "fixed FWD" and exercise environment architecture, two frameworks that loosely align with phases four and five of decisive action. Each student is required to teach their designated instructional block, where they will be graded primarily on the technical content and their demonstrated ability to answer instructors' questions. Students also participate in problem solving sessions where they offer potential solutions to systemic problems faced in employing the DCGS-A family of systems. At the end of the third week, students are required to complete a comprehensive final exam that covers all of the material presented during the course.

The DISMGC POI was designed as an academically rigorous course, suitable for intelligence professionals with extensive DCGS-A experience. It allows experienced MI professionals an opportunity to collaborate with peers from across the U.S. Army, develop solutions to systemic intelligence systems related problems, and improve their units' intelligence readiness. Although there are no prerequisite courses required to attend DISMGC, students are required to pass the DISMGC pre-test, and must have the endorsement of their division or corps SIO or equivalent. The ideal candidate has significant experience establishing intelligence frameworks, a firm understanding of the DCGS-A family of systems, and a mind open to learning multiple methods for maximizing their capabilities. The course is currently open to warrant officers (WO1 through CW3), but will open to all MI personnel between the ranks of E5 and O4 in Fiscal Year 2017.

CW5 Andrew Maykovich is currently assigned as the Senior Warrant Officer Advisor to the G2, FORSCOM. Previously, CW5 Maykovich served as the OIC of the Special Forces Intelligence Sergeants Course, and deployed multiple times as the Senior Analyst for the XVIII Airborne Corps.

CW2 Nick Rife is currently assigned as the DISMGC OIC, INSCOM G3. Previously, he served as 82nd Airborne Division G2 Fusion Chief, FBNC and CJFLCC-I, as well as 4th BDE, 82nd Airborne Division Fusion Chief, FBNC and Kandahar Afghanistan.

Enhancing DCGS-A NET/DTT through the Integration of IEWTPT

by Captain Jared S. Doucet

Introduction

The Distributed Common Ground System-Army (DCGS-A) provides critical contributions to support the commander's understanding of the area of operations (AO). Intelligence Soldiers using the DCGS-A system acquire information on the threat, weather, and terrain to facilitate visualization of the environment's unique attributes enhancing tactical maneuver, maximizing combat effectiveness, and improving the unit's ability to operate in unpredictable and changing surroundings throughout the operational spectrum.

As with any complicated system, units must understand how to leverage that asset. To facilitate mastering DCGS-A, the New Equipment Training/Doctrine and Tactics Training (NET/DTT) provides both formal and informal military intelligence (MI) and DCGS-A training on a continual basis. The New System Training Integration Directorate (NSTID) as a part of the U.S. Army Intelligence Center of Excellence at Fort Huachuca, Arizona is responsible for all training development for DCGS-A. NET/DTT trains Soldiers how to leverage DCGS-A's capabilities by using the Intelligence Electronic Warfare Tactical Proficiency Trainer (IEWTPT).

The IEWTPT is a non-system virtual training environment used to deliver scenario-based intelligence preparation of the battlefield (IPB)-driven situational training exercises (STX) within a decisive action training environment (DATE). Employing this training device to provide a realistic simulation of operations helps Soldiers go beyond the "buttonology" of DCGS-A and demonstrates the applicability of the system for all intelligence support functions.

DCGS-A Functions

DCGS-A contains an arsenal of tools to accomplish its core functions of search, map, report, and analyze. Additionally, DCGS-A can be used to perform the following:

- Task and control select Army sensor systems.
- Automate intelligence synchronization, specifically intelligence, surveillance, and reconnaissance (ISR) planning.
- Reconnaissance and surveillance integration and assessment processing.
- Fuse and exploit data and information.
- Support knowledge generation.
- Provide ground station capabilities.
- Provide automated support to intelligence product generation.
- Disseminate information and intelligence about the threat, weather, and terrain at all echelons.
- Support situational understanding as well as targeting and effects.
- Support the defense of civil authorities.

Commanders' desired mission outcomes are based on a clear understanding of the situation within their AO answering such questions as:

- What is/are the enemy's capabilities and likely courses of action?
- What are the characteristics of the environment?
- How much time is available?

DCGS-A as a Command Tool

DCGS-A mitigates risk by providing commanders improved situational awareness and access to real-time data. The DCGS-A Network/Enterprise retrieves, sends, and exploits information to increase the commander's overall situational awareness, and to create specific intelligence products using raw data from various databases. Some intelligence products include:

- Annex B (Intelligence).
- Battle update brief.
- Intelligence summary (INTSUM)/graphical INTSUM.
- Target package.
- Intelligence estimate/running estimate.
- Human Intelligence reports.
- Signals Intelligence reports.

DCGS-A Facilitates Planning and Sharing

DCGS-A provides the operating force a fully compatible ISR-processing system to enable collaborative planning and the sharing of threat, weather, and geospatial information

with joint and multinational partners through all phases of training and deployment. DCGS-A supports mission planning coordination and the synchronization of activities to enhance the development, communication, rehearsal, and execution of mission orders. It also facilitates the rapid planning, execution, and synchronization of all warfighting functions resulting in the current and future force's ability to operate within the enemy's decision cycle.

IEWTPT Provides Support

IEWTPT supports MI team, crew collective, and individual task training using live, virtual, and constructive capabilities as the program of record training device for home station MI training. It is intended to be a cost-effective means to virtually train by providing relevant critical tasks which place trainees in a realistic scenario using operational concepts and software toolsets.

The primary mechanism for the IEWTPT's scenario is the technical control cell which provides the power for several simulations by creating a virtual data environment for training multiple intelligence disciplines. The target signature array includes embedded MI system program managers or networked training capabilities to simulate unique MI system software for payload or sensor-specific training. The program is supported by three to four (site specific) technical support specialists who work directly with MI command staffs and trainers to support MI-focused training event creation and execution.

Begin a Training Event

A training event starts with a new materiel information brief via telephone conference between NSTID, the unit, and the program manager approximately 120 days before the training event. Mission Training Complex (MTC) and local IEWTPT personnel conduct their own briefings for those to receive training. This is followed by a key leader engagement between NSTID Soldiers, unit personnel, and MTC representatives.

Training Process/Timeline

NSTID personnel brief unit leadership on DCGS-A capabilities and the advantages of the new NET/DTT/IEWTPT simulation training event. Instructors facilitate intensive IPB-based training for students within 10 days of the DATE on DGCS-A capabilities as well as creating products associated with the four steps of IPB. This is followed by a 3-day STX simulated by IEWTPT to provide realistic, timely, and dynamic message drops, along with friendly/enemy positional information on the battlefield giving the unit a realistic and relevant training event.

Training Results

Unit leaders should, at a minimum, attend their Soldiers Mission Analysis Brief at the end of the STX (Day 13) to observe how Soldiers have improved their proficiency on using the DCGS-A equipment. This allows leaders to gain a good understanding of Soldiers' enhanced IPB and briefing skills, as well as learning how DCGS-A data is passed to the command post of the future. All training and exercise materials are left with the unit, the supporting IEWTPT team, and the MTC staff to allow other units to request the same training. After each event NSTID leads an after action review with both the unit receiving the training and MTC personnel to continuously improve training. Work is in progress on DCGS-A v3.2.x training to use the IEWTPT to support longer and more complex training events.

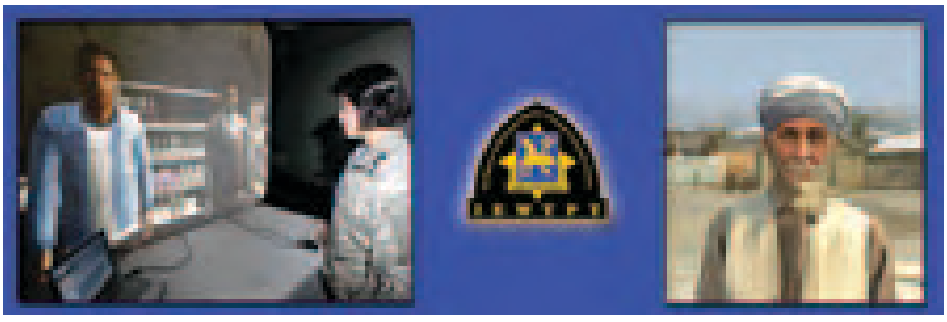
NSTID recently provided this training and scenario-based exercise to two separate organizations and the feedback has been favorable:

The 201st Expeditionary MI Brigade Executive Officer received his Soldiers' Mission Analysis Brief after Day Two of the STX, and was impressed how his Soldiers not only used DCGS-A in an IPB DATE scenario to create and brief products, but also how they pushed the red common operating picture to CPOF.

The 8th Military Information Support Group (Airborne) S2 was impressed with how his Soldiers were able to use DCGS-A to build their products and brief their analysis. Unit leadership identified how the training exercise was made more realistic using IEWTPT. They also commented on how their sustainment DCGS-A training will also improve due to the addition of IEWTPT. They understood that now their units could request the same training exercise further into their training cycle, keeping their analysts proficient.

For training questions contact the New Systems Training and Integration Division at (520) 538-0706.

CPT Doucet is a NSTID Instructor/Course Writer. He holds a Bachelor's Degree in Aeronautical Science from Embry-Riddle Aeronautical University.



DCGS-A Supports CJTF–HOA's Intelligence Operations

by Mr. Douglas Harris

Introduction

Through unified action with U.S. and international partners in East Africa, the Combined Joint Task Force Horn of Africa (CJTF-HOA) conducts security force assistance, executes military engagement, provides force protection, and provides military support to regional counter-violent extremist organization operations in order to support aligned regional efforts, ensuring regional access and freedom of movement, and protecting U.S. interests.[1]

The CJTF-HOA Intelligence Directorate (J-2) has a dynamic mission in providing intelligence support and all source intelligence products focusing on ten countries within the area of operations (AO) and 11 countries within its area of interest (AI). These countries include: Burundi, Djibouti, Eritrea, Ethiopia, Kenya, Rwanda, Seychelles, Somalia, Tanzania, Uganda, Yemen, and South Sudan. The Distributed Common Ground Systems-Army (DCGS-A) plays a critical role in providing analysts a means to process, exploit, and disseminate actionable intelligence products.

Photo by Douglas Harris

CJTF-HOA Intelligence Analysts receiving DCGS-A training.

DCGS-A Supporting Intelligence Operations

Due to the unique mission requirements, products focusing on political, military, economic, social, information and infrastructure (PMESII) are produced on a daily basis. CJTF-HOA intelligence analysts utilize DCGS-A to retrieve raw intelligence data to build all source intelligence products that are used to support the decision making process. Intelligence reports are routinely data-mined via Query Tree, analyzed, and then disseminated to both higher and lower echelons to maintain situational awareness within the area of responsibility. To support upcoming mission requirements, the DCGS-A team has requested additional data sources and recently obtained Combined Information Data Network Exchange information. Deep dive products focusing on historical significant activities (SIGACTS) within the AO/AI will use this information. The final deep dive product entails a graphical depiction of SIGACTS within the AO/AI on a map created via ArcMap. Additional spatial analysis is conducted by creating a density to identify known and unknown "hotspots" of violent extremist activity.

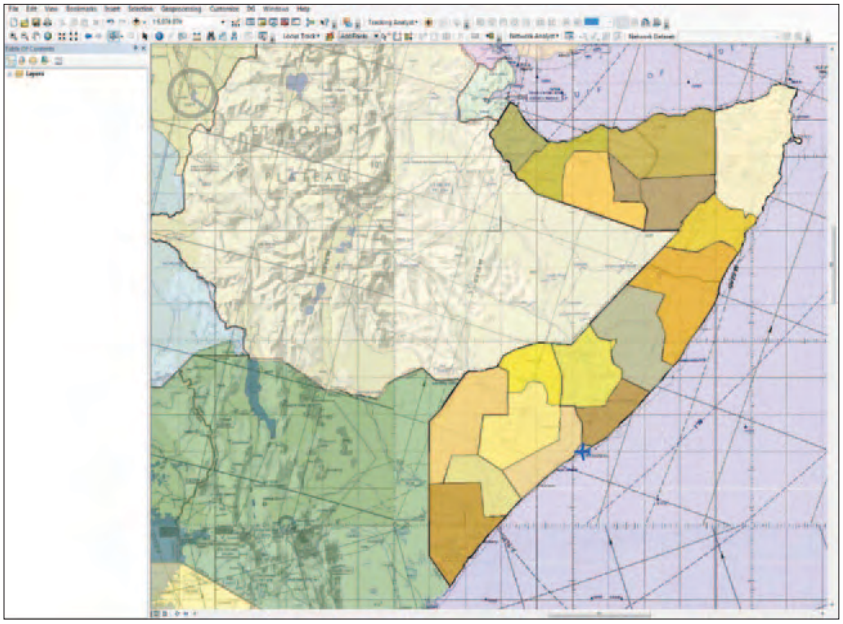
Network Analysis of Violent Extremist Organizations

DCGS-A's Link Diagram program within the Multi-Function Workstation (MFWS) is used to depict the organizational structure and assessed linkages between key entities. Finished intelligence products produced by the J-2 often include network analysis products. They depict the organizational structure of violent extremist organizations, orders of battle, and political parties.

Due to the constant rotation of J-2 personnel, network analysis products created from Link Diagram are saved to the Tactical Entity Database (TED) within MFWS. The ability to save products to the TED has two significant advantages. Saving link diagrams and entities assists analysts with conducting a turnover with new analysts by providing a snapshot of key leaders, groups, and activities that the J-2 has focused on. Additionally, the TED enables analysts to continuously update the attributes of entities with current intelligence by appropriately tagging information obtained from sources such as intelligence information reports.

Sharing Information

The task organization of Camp Lemonnier/CJTF-HOA forces includes multiple Army and joint units, and national



ArcMap 10.0 is routinely used for product development.

intelligence agency assets, each with a specific mission requirement that contributes to the J-2 mission. Geographic dispersion of units throughout the camp creates the requirement to share information. The current DCGS-A architecture involves each Portable MFWS "pointing" back to a local Intelligence Fusion Server. This allows analysts at their respective unit access to information created or updated by a separate unit.

Operations are positively impacted by allowing analysts to see the most current information saved within the TED. Analysts across all echelons–from CJTF-HOA to USAFRICOM–are able to view and update information providing a common operational picture of violent extremist activity within the AO/AI.

The Way Ahead

Continuous DCGS-A training and information technology support is necessary due to the steady rotation of analysts within the J-2 and supporting organizations–often 10 to 15 percent each month. Furthermore, continuous training is necessary to baseline and integrate the Active and Reserve Component joint Service members not familiar with DCGS-A. CJTF-HOA J-2 will meet this challenge by conducting thorough turnovers and by incorporating best practices that are a part of the J-2's standard operating procedures.

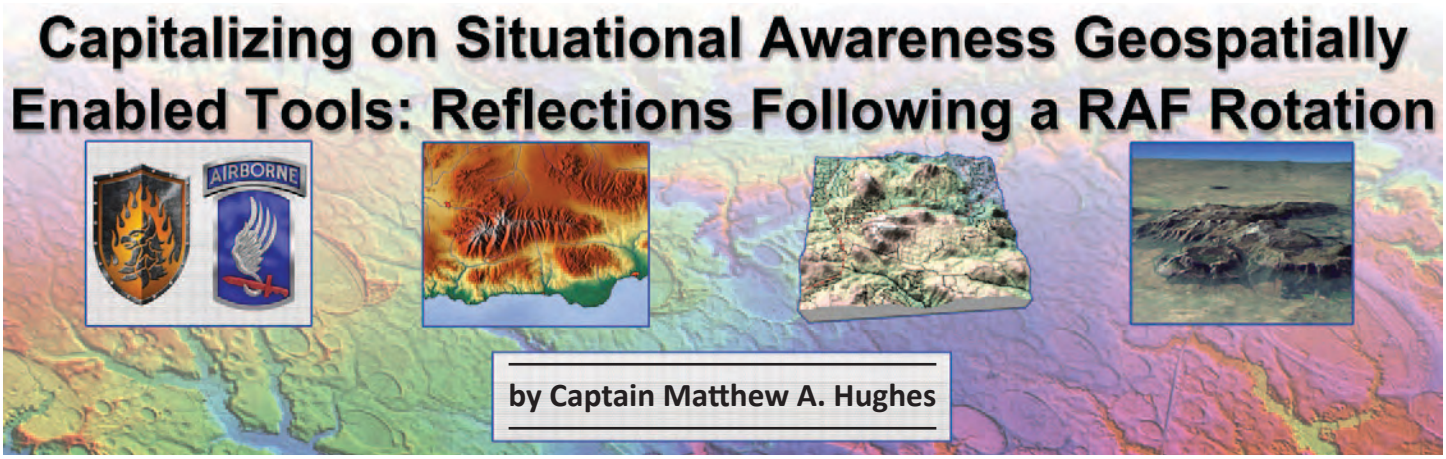
CJTF-HOA's operations prevent violent extremist organizations from threatening the U.S., ensuring the protection of the homeland, U.S. citizens, and U.S. interests. The processing, exploitation and dissemination cycle drives the intelligence mission. DCGS-A is the backbone of maintaining a continuous intelligence cycle and satisfying priority intelligence requirements.

Endnotes

1. http://www.hoa.africom.mil/about, 15 April 2016.

Doug Harris is currently the Distributed Common Ground Systems- Army (DCGS-A) Embedded Trainer attached to Combined Joint Task Force-Horn of Africa's J-2. He has provided DCGS-A training and support to several units deployed within CENTCOM, PACOM and AFRICOM's area of responsibility since joining the DCGS-A program in 2008. Prior to joining the DCGS-A program, he was an Intelligence Officer with the United States Marine Corps.

Capitalizing on Situational Awareness Geospatially Enabled Tools: Reflections Following a RAF Rotation



by Captain Matthew A. Hughes

What is a Situational Awareness Geospatially Enabled Tool?

Situational Awareness Geospatially Enabled (SAGE) is an extension tool for use on ArcGIS designed by the U.S. Army Corps of Engineers' Geospatial Research Laboratory to simplify and expedite generating geospatial layers and analysis products. Users download foundation data from the Army Geospatial Center's Common Map Background portal online, which become inputs for SAGE.[1] These include elevation data (i.e., Shuttle Radar Topography Mission, Digital Terrain Elevation Data, and digital surface or terrain models) and landcover layers (i.e., GeoCover or VISNAV datasets). Through a series of seventeen steps, Soldiers can use SAGE to transform this foundation data into a comprehensive mission folder for a region.[2] The complete folder includes a series of layers for cross-country mobility, mobility corridors, slope degree and more, facilitating intelligence preparation of the battlefield (IPB) and geospatial analysis associated with friendly and enemy courses of action.

SAGE received Project Manager Distributed Common Ground System Army (DCGS-A) authorization for use on DCGS-A systems on March 18, 2014.[3] The program is Unclassified//FOUO, so a unit may install SAGE on a standalone system with ArcGIS, as it does not have a certificate of networthiness for use on NIPRNET systems. Units may request SAGE training in the form of a standard 40-hour block or remotely through other means, using developed training modules or new material tailored to mission needs.

Familiarization and Preparation for Deployment

A geospatial engineer in a sister brigade first introduced me to SAGE when he hosted a 40-hour training block at Fort Hood, Texas. I sent our all-source analyst with a DCGS-A workstation to this training. Following the course, the analyst described the toolsets and new capabilities to our intelligence cell and we began to incorporate SAGE into analysis projects. We applied SAGE during a field training exercise at Fort Hood in August 2015. Throughout the exercise, members of my team benefitted from additional one-on-one training with SAGE developers and trainers. We created several analysis products that enhanced mission planning during the exercise, demonstrating the program's versatility to battalion and company leaders.

In the remaining weeks leading up to deployment, we further gained familiarization as our intelligence cell created SAGE mission folders for 11 countries, requiring over 200 hours of computing. We mastered the process of finding foundation data and transforming it into a mission folder with detailed geospatial data, readily available for additional analysis or incorporation into a brief. We constantly used these folders throughout the deployment to generate detailed analysis products, often with very little prior notice, throughout the area comprising Operation Atlantic Resolve.

Advent of SAGE in Europe

We invited our organic pilots and analysts from the 173rd Infantry Brigade Combat Team, 12th Combat Aviation Brigade, and 60th Geospatial Planning Cell Detachment to a 40-hour SAGE training block we hosted in Germany, in November 2015. This training marked the advent of SAGE in Europe; spearheading its implementation from company to theater levels in training and contingency operations. For the 40-hour block, we used a mission folder for Hohenfels Training Area (HTA), Germany containing light detection and ranging (LIDAR) data in a series of practical exercises in preparation for two pending rotations at Hohenfels.

In one exercise, I provided the enemy situation for a friendly air assault mission in Raversdorf Village. Pilots then plotted enemy air ambush teams and used SAGE to assess suitability of flight paths using linear viewshed features, exposing any areas where enemy elements could see and engage helicopters along templated flight paths. The pilots then flew their chosen flight paths in a flight simulator with

(Clockwise) In November 2015, CW2 Deuel flew the UH-60 flight simulator at Illesheim, Germany along a route he templated for HTA, Germany using SAGE. He modeled air ambush teams' radial line-of-sight and generated a linear viewshed along his flight path to determine visual detection probability along the route.

programmed enemy weapons systems at the chosen grids to gauge the usefulness and accuracy of SAGE for mission analysis.

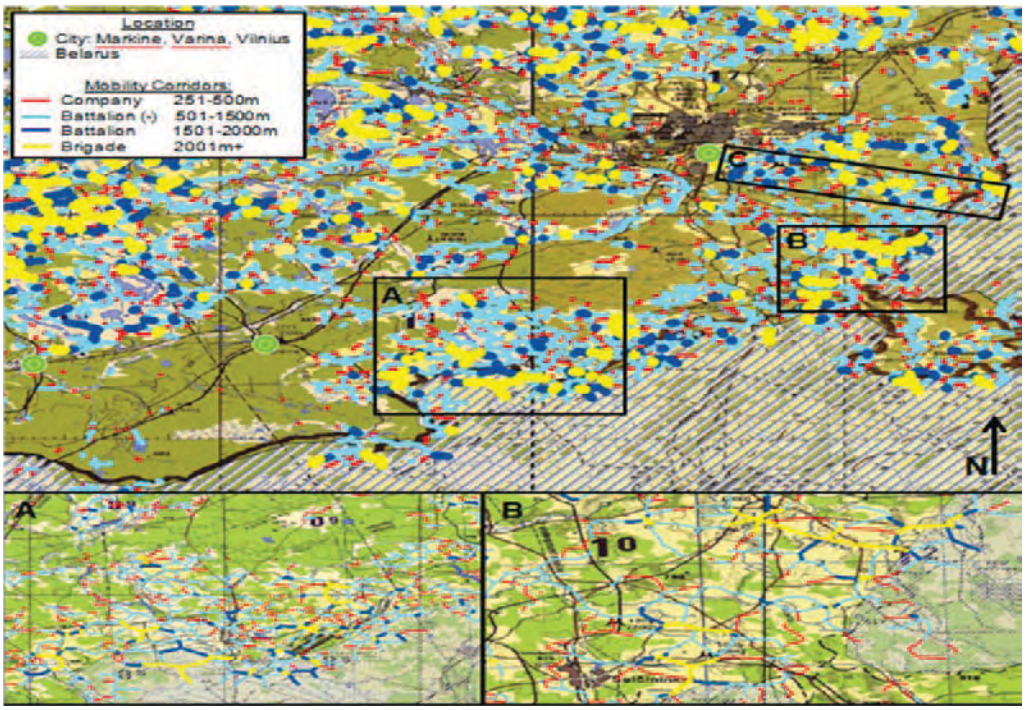
SAGE Expedites and Enhances Intelligence Preparation of the Battlefield

Following this 40-hour block, our intelligence cell completed IPB for HTA in December 2015. This is a lengthy process, requiring extensive research and detailed analysis, but SAGE greatly expedited Steps 1 and 2 of IPB by generating a digital modified combined obstacle overlay. We exported and briefed images of different layers generated using SAGE, such as landcover, hydrology, and mobility corridors. We then created sample products relevant to aviation operations using SAGE tools. We made a slope degree layer for the entire training area and a mounted brushfire modeling in different colors of the time required for a Downed Aircraft Response Team (DART) to reach a helicopter at any point on the map. This greatly reduces time required for analysis in the event of a downed aircraft. Similar tools can generate a cross-country mobility model for 12 types of NATO vehicles or an overlay modeling time required for a quick response force (QRF) to reach any area on the map.

In December 2015, we also conducted rapid IPB in support of a mission flying Lithuanian military leaders in a UH-60 Blackhawk, near the southeastern border to assess feasibility of adversarial border crossings. We used SAGE to model mobility corridors along the border, compare surrounding land cover, assess cross-country mobility for armor and wheeled assets, and construct a linear viewshed for the UH-60 flight path to model if they would be able to see these potential border crossings or if they would need to adjust their altitude or route.

Revolutionizing Analysis and Autonomy at the Battalion Level

In April 2015, several months prior to our deployment to Germany, we conducted a rotation at the National Training Center in Fort Irwin, California. We cancelled one air assault mission due to risk management as we could not get the dynamic and continuous geospatial support needed to provide



In December 2015, analysts used SAGE to identify and analyze avenues of approach in border regions of southeast Lithuania for a Lithuanian aerial leader's recon of the border.

slope analysis on changing landing zones. If we had SAGE tools during that training rotation, we would have had all the slope analysis tools readily available to make that mission a success. During our rotational deployment to Europe, SAGE gave our battalion S-2 cell unprecedented autonomy, granting flexibility and efficiency by enabling us to generate geospatial products we would have previously requested from higher echelons or specialized intelligence cells.

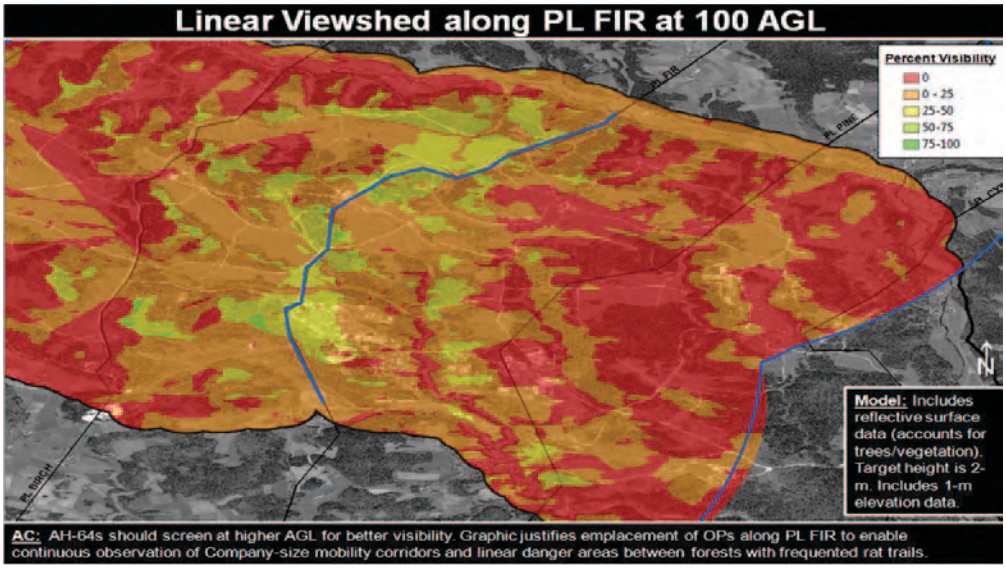
During a January 2016 training rotation, our unit supported the Italian Garibaldi Brigade at the Joint Multinational Readiness Center (JMRC), HTA, Germany. SAGE played a pivotal role in the success of the unit's mission. The topographic cell of our higher headquarters had shut down one-month prior as part of downsizing, and the Italian unit was unable to provide the same geospatial support we would expect from a U.S. brigade S-2 cell. We had a similar experience using Sage during another training rotation at JMRC in April 2016.

At Hohenfels, we utilized SAGE to create a variety of products, including:

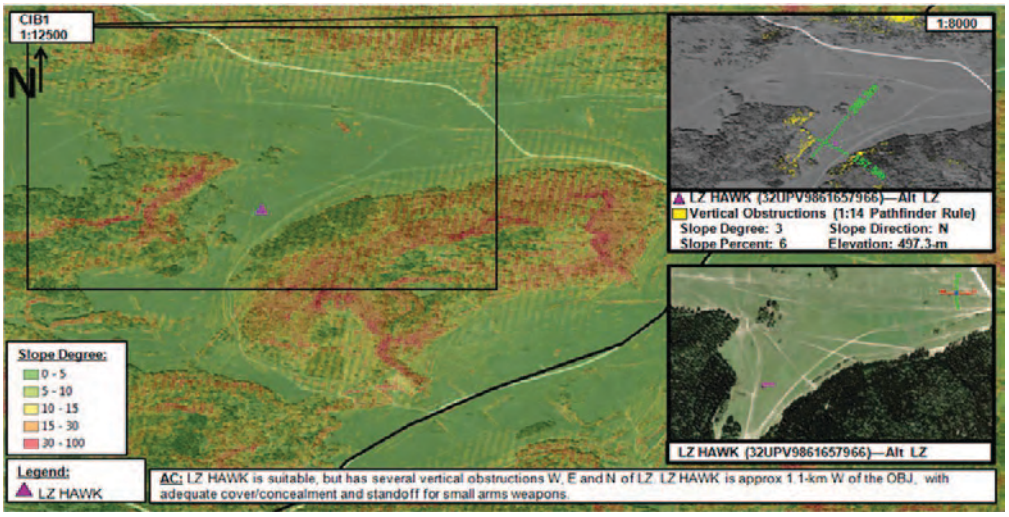
- Enemy Integrated Air Defense System coverage areas for helicopters flying at varied above ground levels (AGLs).
- Helicopter landing zone (HLZ) analysis (including slope degree, slope aspect, and vertical obstructions using the 1:14 pathfinder rule).
- Visibility for AH-64 Apache screen line at varying AGLs.
- Mounted brushfires for DART and QRF showing travel time to areas on map.
- Mobility corridors overlay for echelons platoon(-) to brigade.
- Cross-country mobility overlays for 12 types of NATO vehicles and dismounted troops (contributed to analysis for friendly evasion and escape or enemy infiltrate/exfiltrate).
- Likely enemy observer post and air ambush team locations, based on visibility.
- Force protection assessments for airfield and forward arming and refueling point.

Interoperability with Google Earth, Quick Terrain Modeler, and other programs also enabled us to build 3-dimensional vantage points to gauge suitability of attack-by-fire positions for AH-64s and observer posts (OPs) for scouts prior to missions using radial line-of-sight tools with reflective surface data.

In June 2016, our battalion traveled to Poland to support Operation Anakonda, a multinational training operation throughout Poland. Using SAGE, we assessed the suitability of flight paths for an air assault mission consisting of 32 helicopters. Toolsets assisted in determining optimal vantage points for enemy scouts, flight path sections most vulnerable to enemy weapons systems, potential masking terrain, and HLZ suitability.



S-2 cell utilized SAGE to reflect visible areas for AH-64s screening at 100 AGL during a training rotation at HTA, Germany in January 2016. Analysts used graphic to argue in favor of OP insertions along PL FIR due to poor coverage of AH-64 screen.



S-2 cell used SAGE to assess the suitability of LZ HAWK during a multinational air assault in April 2016 at HTA, Germany.

The Way Forward

An emphasis on LIDAR data collection in Europe can greatly enhance utility of SAGE among intelligence cells. NATO recently announced plans to "deploy four multinational battalions to Estonia, Latvia, Lithuania and Poland" in a deterrence role."[4] This will include U.S. troops and will likely increase the number of training exercises in Poland and the Baltic States. Unfortunately, geospatial databases such as the Army Geospatial Center Portal and the Geospatial Repository and Data Management System contain only 30-meter elevation data for these areas, as opposed to the LIDAR available for Hohenfels. Units should submit requests for LIDAR data collection of training areas and border regions in Poland and the Baltic States to enhance the efficacy and precision of analysis using SAGE.

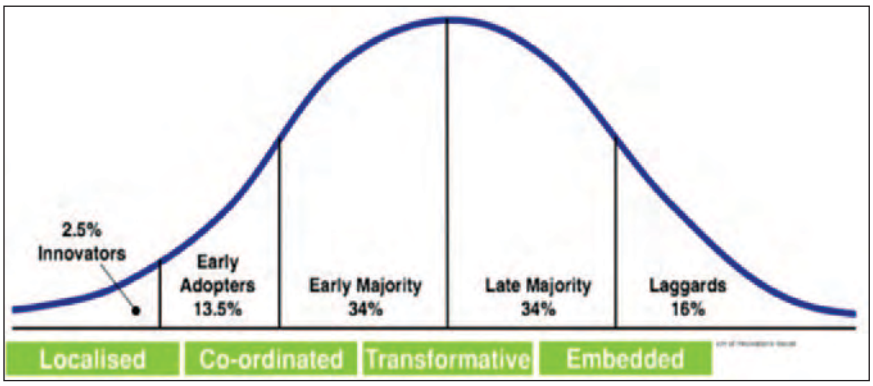


Figure 1. The Diffusion of Innovations Theory Model illustrates that over time, a population will adopt an innovation in distinct phases based on a variety of conditions.[7]

The U.S. Army Intelligence Center of Excellence can play a significant role in spreading awareness of SAGE tools by incorporating demonstrations and training on SAGE into the curriculum for enlisted, warrant officer, and officer ranks. According to the Diffusion of Innovations Theory, introduced by French sociologist Gabriel Tarde in 1903 and further developed by E. M. Rogers in 1995, certain conditions can "increase or decrease the likelihood that a new idea will be adopted by members of a given culture."[5] Following this model, the diffusion of SAGE in the Army is currently in the "early adopter" phase (See Figure 1). Relatively few units are applying SAGE in training or real-world missions, mostly due to a lack of awareness. Exposure to SAGE during institutional training periods can contribute to awareness and implementation.

Additionally, SAGE does not come pre-installed onto DCGS-A workstations when fielded or during updates as some applications. Those wishing to use SAGE acquire a file from a current user or from a SAGE trainer and personally install it on a workstation. Since most battalion S-2s have a DCGS-A workstation in their Modified Table of Organization and Equipment, DCGS-A mentors should periodically acquire SAGE updates and install SAGE when they update units' DCGS-A workstations. Intelligence analysts with SAGE experience should host training for sister units to demonstrate SAGE applications and distribute digital files. This can be especially effective in preparing for a rotation at a combat training center with other units, facilitating information sharing, and collaboration on IPB. Such efforts can bring about institutional change in battalion and brigade S-2 cells across the Army and propel the diffusion of SAGE beyond the "early adopters" phase for maximum benefit.[6]

Endnotes

1. U.S. Army Geospatial Center CMB Online, accessed 4 June 2016. At https://agcwfs.agc.army.mil/CMB_Online/default.aspx.

2. Michael Rainey, "SAGE Quick Start Guide–Creating and Visualizing Foundation Products," 23 July 2015, 6.

3. Charles A. Wells, Memorandum for Record, 18 March 2014, Program Executive Office: Intelligence, Electronic Warfare and Sensors, Authorization for Use of SAGE tools on DCGS-A workstations, Department of the Army.

4. Ryan Browne, "NATO Chief: 4 Battalions to Eastern Europe amid Tensions with Russia," *CNN Politics*, 13 June 2016, accessed 24 June 2016. At http://edition.cnn.com/2016/06/13/politics/nato-battalions-poland-baltics-russia/.

5. Diffusion of Innovations Theory, University of Twente, accessed May 28, 2016. At https://www.utwente.nl/cw/theorieenoverzicht/Theory%20clusters/Communication%20and%20Information%20Technology/Diffusion_of_Innovations_Theory/.

6. Ibid.

7. Clive Young, "Enabling Innovation and Change–Part 1," University College London, 24 June 2012, accessed 24 June 2016. At https://blogs.ucl.ac.uk/the-digital-department/2012/06/24/enabling-innovation-and-change-part-1/.

CPT Hughes is an All-Source and Signals Intelligence Officer currently serving as the S-2 for the 3-227 Assault Helicopter Battalion, 1st Air Cavalry Brigade at Fort Hood. He earned a BS in Arabic/Spanish and minored in Terrorism Studies at the United States Military Academy. He is currently completing an MA in Intelligence Studies through American Military University.

How Should DCGS-A Approach Its Big Data Challenges?

by Lieutenant Colonel (Ret.) Jake Crawford

The views expressed in the following article are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. Listing the products and services in this article does not imply any endorsement by the U.S. Army, the U.S. Army Intelligence Center of Excellence, or any U.S. government agency.

The U.S. Army's Distributed Common Ground System-Army (DCGS-A) enables Army units to collect and consolidate data from each unit's internal sources, plus over 700 external sources.[1] DCGS-A then merges and fuses the data, thus establishing relationships between the data to help leaders make decisions. During this process each Army unit employing DCGS-A may process terabytes (TB), if not petabytes (PB) of data during a military operation. How then should DCGS-A approach the challenges of dealing with a potentially unmanageable amount of data? Big Data is one of DCGS-A's core functions insofar as it directly impacts mission success or failure, life or death, and victory or defeat.

Terabyte - A terabyte (TB) is a large allocation of data storage capacity applied most often to hard disk drives. Hard disk drives are essential to computer systems, as they store the operating system, programs, files and data necessary to make the computer work. Depending on what type of storage is being measured, it can be equal to either 1,000 gigabytes (GB) or 1,024 GB. Disk storage is usually measured as the first, while processor storage as the second.

Petabyte – A petabyte (PB) is an even larger allocation of data storage capacity. As with terabytes (TB), depending on what type of storage is being measured, a PB can be equal to either 1,000 TB or 1,024 TB.

This article examines DCGS-A's Big Data challenges. It starts with an overview of the DCGS-A system and its intended use, and then continues by defining Big Data in the context of the DCGS-A program. Next, the article analyzes the DCGS-A Big Data strengths, weakness, opportunities, and threats. The article then concludes with an exploration of possible big data solutions for DCGS-A, to include, but not limited to: hardware and software tools, data storage and analysis service, and non-materiel solutions as prescribed by the Army (doctrine, organization, training, leadership, personnel and facilities).

What is DCGS-A?

The DCGS-A Public Affairs Office website characterizes DCGS-A as a system that consolidates battlefield data obtained by Soldiers and sensors from national, theater, and tactical level assets. It then analyzes these vast amounts of data and provides decision makers an enhanced picture of the enemy and battlefield conditions. This "picture" (consisting of graphic, image, and text products) is commonly referred to as a common operational picture (COP). It provides leaders with situational awareness and enables Army units to "see first, understand first, act first, and finish decisively".

The DCGS-A Program Manager (PM), in cooperation with the Training and Doctrine Command's Capability Manager–Foundation, is responsible for designing, developing, fielding, and sustaining DCGS-A. The PM's strategy separates DCGS-A into two increments. Increment 1 (the current system) is comprised of:

- *Fixed nodes* in sanctuary locations not on the battlefield, providing data and services to the mobile nodes.
- *Mobile nodes* embedded with units on the battlefield, consisting of servers and workstations utilized in tents and/or vehicles (see Figure 1), that receive data and access services to process data.
- *The Army network* that interconnects the fixed and mobile nodes.

Increment 2 (the future system) will build upon Increment 1 by adding more services, as well as the Cloud-based network architecture (depicted in Figure 2), that provides users access to data and services from anywhere in the world.

Figure 1. DCGS-A Mobile Node Configuration.[2]

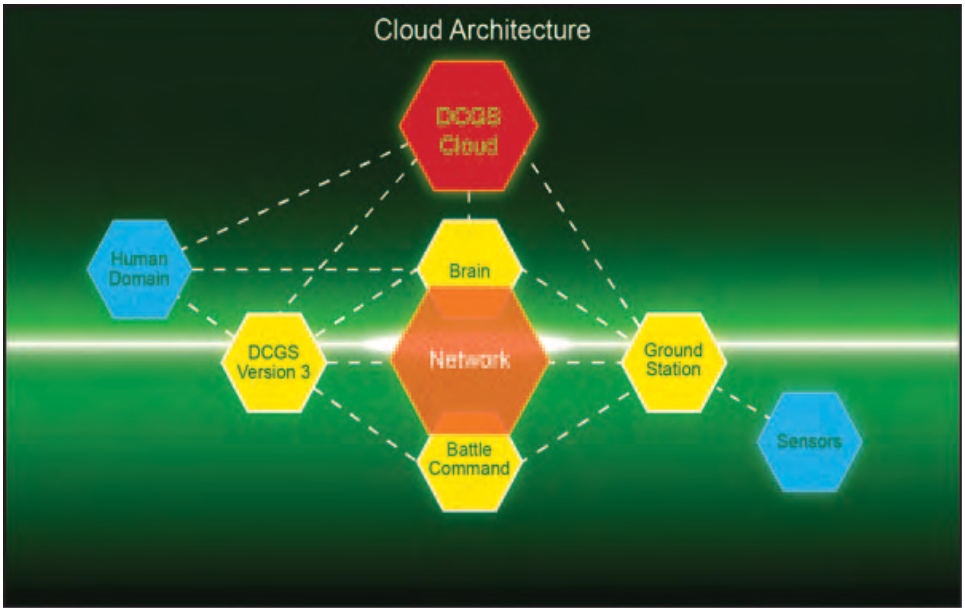


Figure 2. DCGS-A Cloud-based Network Architecture.[3]

What is Big Data in the Context of DCGS-A?

Big Data is a massive amount of organized and/or unorganized data.[4] Big Data is characterized by its volume, velocity, variety, value, and veracity.[5,6] Army units (using the DCGS-A) receive data from their internal and location specific sources in addition to over 700 external sources.[7] This equates to data *volumes* ranging from terabytes to petabytes during a military operation. Furthermore, military operations often have a high operational tempo meaning the *velocity* of data received for analysis will likewise increase exponentially. This data will include a wide *variety* of structured data (such as pre-formatted reports that are readily incorporated into a database) and unstructured data (e.g., images and graphics).

Along with the volume, velocity, and variety of data, Army units must possess the ability to discern the *veracity* (e.g., accuracy, usefulness, and reliability) of the information. In other words, which items are "garbage in" as they will invariably produce "garbage out" results. Finally, the *value* of the collective data is influenced by each of the previous attributes, and derived from each unit's utilization of DCGS-A to analyze the data. For the Army, value is ultimately determined by the extent to which data provides situational awareness and facilitates decision making.

How Does Big Data Impact the DCGS-A Program?

The volume, velocity, variety, plus veracity variance of data processed by Army units highlight some of DCGS-A's internal strengths and weaknesses. They also present DCGS-A with various external opportunities and threats. Figure 3 summarizes the DCGS-A strengths, weaknesses, opportunities, and threats (SWOT).

The first Big Data strength for DCGS-A Increment 2 is its status as a "new start" program. Increment 2 possesses the flexibility to incorporate new technologies and operating procedures into the system, to include advances in Cloud Computing and Big Data management and analysis. This dovetails well with the first opportunity, the availability of new/upgraded Big Data and Cloud Computing technologies that were not available to Increment 1. The combination of this strength and opportunity will enable DCGS-A Increment 2 to address some of its Big Data challenges.

The second strength, availability of terabytes to petabytes of data, will provide units exponentially more data from which to draw conclusions. However, this can also lead to the Big Data weakness of data overload, resulting in units receiving more data than they can process in a given time period. Army and Department of Defense investments and technological advances in sensors that increase the volume, variety, and velocity of data received by Army units further compounds the weakness of data overload. This paradigm shift is a proverbial double-edged sword for DCGS-A. Increases in data provide units with more historical and real-time data that improves the fidelity of their trend analysis; conversely, more data elevates the "messiness" of each unit's overall data set.

"Messy" data includes errors and "inexactitudes" of data.[8] For example, two separate sensors may report on (supposedly) the same entity within a short time of one another. Any deltas in the sensors' reporting are errors (e.g., sensors are looking at different entities) or inexactitudes (e.g., sensors are reporting on the same entity, but from different perspectives, thus producing somewhat differing reports). However, authors Mayer Schonberger and Cukier (see Endnote 8) believe that despite the risk of elevated messiness, more data is always better.

For DCGS-A this is true when conducting trend analysis in an effort to predict what an opponent will do in the future. More data increases the confidence in the correlation between indicators (shaping actions) that precede major events (decisive actions). As Mayer-Schonberger and Cukier point out, for predictions it is less important to understand why an opponent does something, and more important to understand what indicators the opponent will display prior to conducting decisive action.

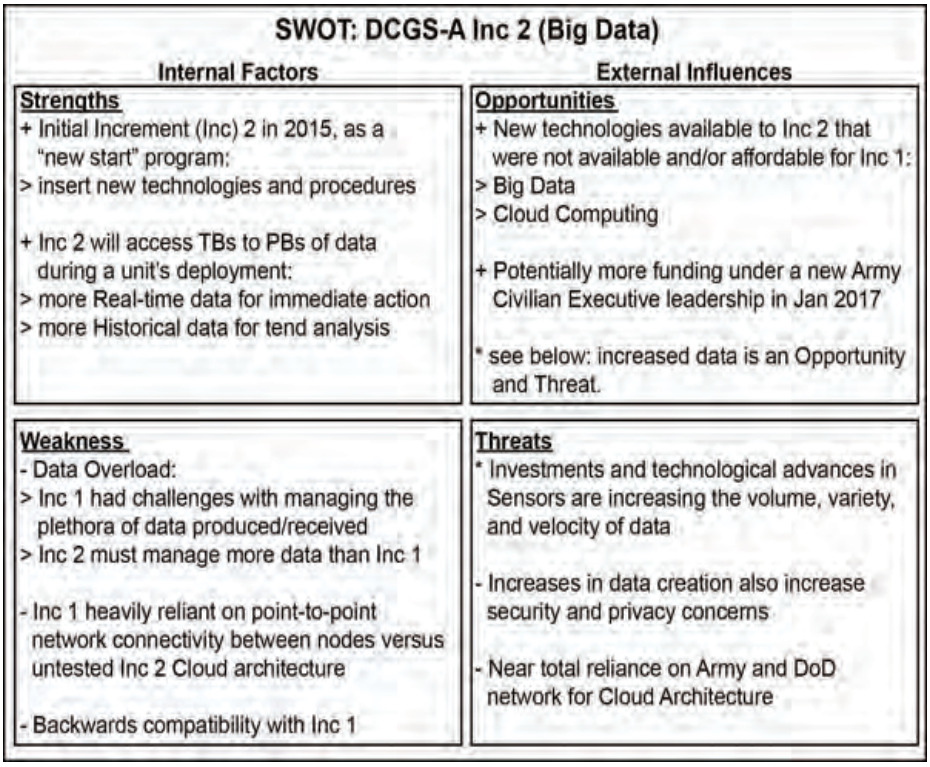


Figure 3. DCGS-A SWOT Matrix.

On the other hand, messy data can introduce an unacceptable level of risk. Military operations frequently include life-or-death situations; thus, making critical decisions based upon data considered "messy" is generally not acceptable. These situations require higher fidelity (e.g., "eyes on") real-time data, confirmed by multiple sources, prior to taking action. For example, before sending troops to take an objective by force, units (utilizing their access to real-time data) can obtain confirmation (and reconfirmation) of their opponent's status via multiple independent sources. This is one of the great benefits of Big Data for Army units, and DCGS-A Increment 2 will further enhance this capability by sorting through the "messy" data.

How Will DCGS-A Handle its Big Data Challenges and Threats?

The DCGS-A PM Office, plus Army units utilizing the system, can exercise various steps to maximize DCGS-A Increment 2's strengths and opportunities, while simultaneously minimizing its weaknesses and threats. First, as previously mentioned, the PM Office can insert new and/or enhanced Big Data technology into the system. For instance:

- ✦ Simultaneous transaction processing (user interaction) and analytic processing (trend discovery and pattern identification) using the same system. For DCGS-A this could reduce the number of workstations required in each unit by combining multiple functions into a single integrated platform.
- ✦ Search and interactive analysis of structured data through a new visualization interface. For DCGS-A the visualization interface could enhance the human-to-machine interface and make it easier for users and decision makers to understand the data and results of analysis.
- ✦ A query approach that enables analysis of unstructured data on systems, such as Hadoop. ("Hadoop is a free, Java-based programming framework that supports the processing of large data sets in a distributed computing environment.")[9] This tool could enhance DCGS-A's ability to process the plethora of unstructured data it receives, such as images and graphics.
- ✦ Visualization and exploration of Big Data that samples and profiles data automatically to create catalogs (organized listing of metadata). This solution could bolster DCGS-A's organization of data, especially unstructured data, and increase user's ability to find, understand, and utilize data.

The second step for the DCGS-A program concerns cloud computing. With the proper cybersecurity protections, this could enhance DCGS-A's data storage capacity as well as Army units' access to analytical services. Cloud computing is examined in more depth in a separate article.

Army units and users must also take actions that, under Army parlance, are non-materiel solutions including changes in doctrine, organization, training, leadership, personnel, and facilities. A paramount priority is to establish full-time, dedicated, and properly trained knowledge managers who are responsible for ensuring that the data DCGS-A uses, as well as the results and application of DCGS-A's analysis (i.e., information and knowledge), are properly managed (e.g., metadata-tagged, discoverable, and accessible).

Furthermore, but of no less importance, units must create, adopt, and enforce cybersecurity policies and procedures to protect data from hostile forces. Finally, Army leaders and decision makers must understand what Big Data and its analysis can and cannot deliver, especially in real-time life and death situations.

Conclusion

Big Data is critical to the U. S. Army. Data are the building blocks for the DCGS-A, and DCGS-A Increment 2 will provide Army units the tools to manage the complexities of Big Data. These complexities include messy vs. unmessy data,

structured vs. unstructured data, and the five "Vs" of Big Data: volume, velocity, variety, and veracity; all of which collectively affect a unit's ability to draw value from the internal, local, and externally produced terabytes to petabytes of data that a unit must handle during a military operation.

DCGS-A Increment 2 will require both materiel and non-materiel capabilities in order to effectively and efficiently manage Big Data. For materiel solutions, the system will require data handling and analysis capabilities by Oracle: Oracle 12c, Oracle Business Intelligence Enterprise Edition, Big Data SQL, Big Data Discovery, and Business Intelligence Cloud Service. For the non-materiel solutions, the Army should institute knowledge managers for each unit employing DCGS-A, establish and enforce cybersecurity policies and procedures to protect data, and promote a firm understanding of the benefits and limitations of Big Data.

Using DCGS-A Increment 2, Army units will have the ability to differentiate the vital data from the interesting but less (or not) relevant data, connect-the-dots between the volumes of Big Data at their disposal, and form a picture of the operational battlefield environment and activities that convey a shared understanding of the situation. This COP is the key product of the DCGS-A data analysis, the situational understanding it provides is the goal, and enhancing leaders' decision making capacity is the ultimate objective.

Endnotes

1. Colonel Robert M. Collins, "DCGS-A Inc 2: The Evolving Environment and Transition to Open Competition," 2014. At http://www.afcea.org/events/armyintel/14/documents/COL_Collins_2014.pdf, 3.

2. "FY 2014 Annual Report: Distributed Common Ground System-Army (DCGS-A)", Office of the Director, Operational Test & Evaluation, 20 January 2015. At http://www.dote.osd.mil/index.html.

3. "DCGS-A", DCGS-A Public Affairs Office, 7 May 2014. At http://dcgsa.apg.army.mil.

4. Efraim Turban, Linda Volonino, and Gregory R. Wood, *Information Technology for Management: Advancing Sustainable, Profitable Business Growth* (9th ed.) (Hoboken: John Wiley & Sons, Inc., 2013), 7.

5. "About Big Data", University of Maryland University College, 2015. At http://www.umuc.edu/analytics/about/big-data.cfm.

6. Paulo B. Goes, "Big Data and IS Research," *MIS Quarterly* 38(3) (2014): iii-viii.

7. Collins, 3.

8. Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live, Work, and Think* (New York: Houghton Mifflin Harcourt Publishing Company, 2013).

9. "Definition–Hadoop", TechTarget.com. (n.d.). At http://searchcloudcomputing.techtarget.com/definition/Hadoop.

LTC (Ret.) Crawford served 23 years on active duty in the Army Acquisition, Military Intelligence, and Adjutant General Corps, and deployed to Iraq and Afghanistan. For his final assignment he was the Army Test and Evaluation Command System Team Chair for DCGS-A, responsible for the developmental and operational test and evaluation of the DCGS-A Increment 1 system. He is a graduate of the U.S. Military Academy at West Point, earned an MBA and is currently enrolled in an MS program for Information Technology and Systems Engineering.

MI History Trivia

On 6 March 1970, the Secretary of Defense announced that the US Army Intelligence School at Fort Holabird, Maryland, would move to its new home at Fort Huachuca. What other locations were considered for the new "Home of MI"?

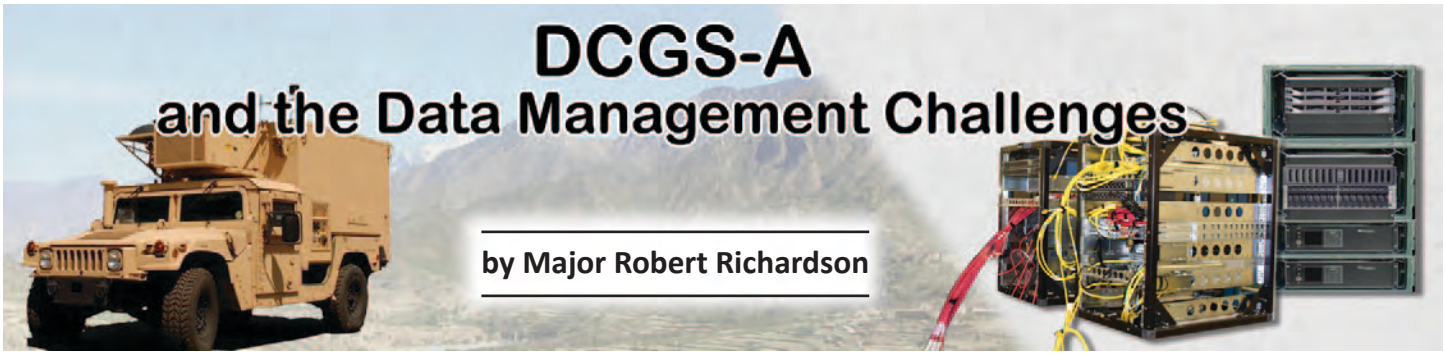
A. Fort Meade, Maryland
B. Fort Riley, Kansas
C. Fort Lewis, Washington
D. Fort Bliss, Texas

US Army Intelligence Center and School, early 1970s

On 4 May 1971, the colors of the new USAICS were ceremonially unfurled by COL Charles Allen, the last commandant of the school at Fort Holabird and the first at Fort Huachuca.

From question on page 9.

*Correct answers in **RED***



DCGS-A and the Data Management Challenges

by Major Robert Richardson

Introduction

There are many real, current and future advantages to utilizing Distributed Common Ground Station-Army (DCGS-A). DCGS-A is our primary intelligence weapon system, a system of systems forming our foundational layer, which allows access across the intelligence enterprise. The system provides access to a myriad of sensor reports and analytic products, from space to mud. The many different analytic reports are processed into a machine language (e.g., United States Message Text Format and Variable Message Format). Those reports can then be passed to every Intelligence Fusion Server (IFS) at every battalion through corps. This creates a network of shared intelligence that can quickly and efficiently be processed within, and updated, by DCGS-A. The resulting intelligence can then be combined with reports from that user's own unit to create an incredibly detailed intelligence portion of the common operating picture. This is a gross oversimplification of the intelligence foundation layer, but is intended to convey the power of DCGS-A.

However, as with any system, there are challenges both real, and in some cases, misperceptions. For example, DCGS-A requires continuous training with leader oversight in order to maintain proficiency on its myriad functions and applications. Another major challenge is database management. Imagine the power a single unified database would bring to DCGS-A. This database would be replicated at echelons across an entire theater, where intelligence is transmitted and updated at the speed of digits and tied to other Mission Command Systems. This capability would exponentially increase the value of the intelligence warfighting system. This article focuses on the database management challenges for DCGS-A. Database management is, and will continue to be, a major challenge for all current versions of DCGS-A, the next version, and future versions beyond that.

Background

What constitutes a DCGS-A database? Principally, DCGS-A has two primary means of holding data. The first is the Tactical Entity Database (TED). The TED uses a Relational Database Management System data structure. Imagine an Excel spreadsheet that goes off nearly into infinity. An entity (a person, place, thing, event, etc.) can either be manually created, or digitally generated from a sensor. An entity has attributes that augment the original entity database entry. For example, a tank battalion, can have attributes like time observed, location, nomenclature of vehicle, quantity, etc. A high value individual can have attributes like identifying information, and can have relevant reporting linked to the entity. Every SALUTE (size, activity, location, time, and event) report, improvised explosive device, or even routine patrol reporting, can be input into the TED along with the thousands upon thousands of digitally reported tactical reports. This capability provides a method of archiving data that is searchable and more importantly sharable. Through a means of transfer called a "data mover", or a variety of other methods, the database is sharable to other IFS in the foundation layer.

The second means of holding, archiving, and sharing data is the DCGS-A Integrated Backbone (DIB). The DIB is a repository for holding and sharing finished intelligence products. It is comparable to an intelligence only SharePoint where intelligence Soldiers will post their Microsoft Office type files as well as other file types. The DIB is the preferred method of sharing finished intelligence products such as intelligence summaries, intelligence information reports, target folders, and other intelligence product. The strength of the DIB resides in its federation. Networked users can see and data mine the files in other federated DIBs. Intelligence professionals are not limited to using SharePoint or email to distribute intelligence products and reports, and therefore, are no longer relegated only to what they send out manually.

Disadvantaged users, those that do not have access to a Portable Multi-Functional Workstation, can still access both the TED and DIB, as well as other tools, through another DCGS-A information sharing utility called the OZONE Widget Framework. Often referred to as a series of "apps", the OZONE is more accurately a series of tools and utilities that are accessed through the web via a URL. The TED, DIB, and OZONE Widget Famework are all designed to be used

with each other to bring out the full potential of DCGS-A. Many OZONE widgets have "light" versions of functions like mapping, TED editors, and DIB upload tools. These widgets augment any user authorized in the DCGS-A's network active directory by the system administrator.

Data Management Challenges

Sensors are operational throughout a theater at all times, and many organizations rely on the finished intelligence products provided by a sensor processor ground station from a higher or adjacent organization. Those organizations that know how to integrate sensor generated entities from the rest of the intelligence enterprise have the potential to have incredible situational awareness. However, those organizations must currently integrate or "merge" those entities as reports come in. For example, imagine three observers; a dismounted observation post, a mounted scout, and an airborne electronics collection platform, all report on the same threat tank platoon. If unmanaged, those three reports of tank platoons would all be in about the same location, at about the same time, and potentially, the three reports could be confused for as much as a company of tanks. The challenge is further exacerbated when multiple echelons are tracking the same tanks and those entities are shared across the foundation layer.

Data management is difficult, but it is addressed in New Equipment Training and the newly developed DCGS-A Master Gunner Course. DCGS-A does have tools that are designed to reconcile multiple reporting. DCGS-A version 3.2.4 and beyond have a fusion function that accepts new entities and measures the variation in the attributes between the new entities and existing entities already in the local TED. This function is unique to newer versions of DCGS-A. The system measures and reconciles similar reports with the tolerance set in the correlators.

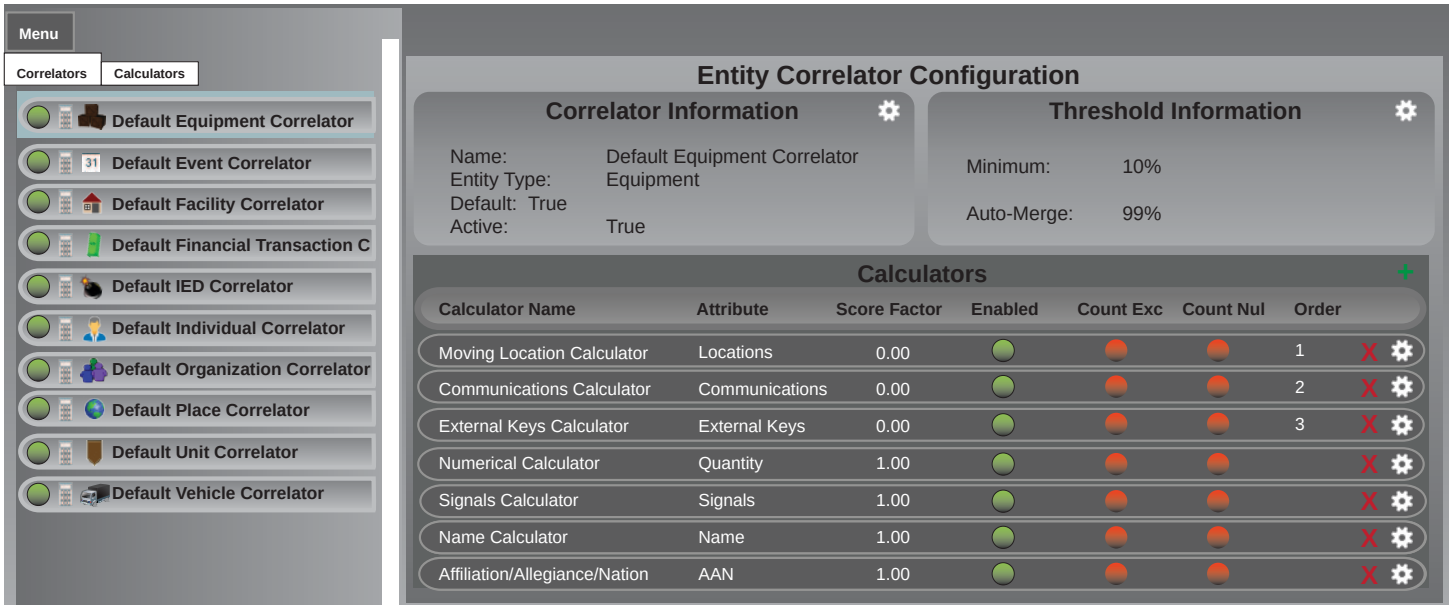


Figure 1. Entity Correlator Configuration. This screenshot was graphically reproduced and may have slight variations from the actual correlation tool.

Correlators measure and control the variance in entities. If within tolerance, the Fusion Exploitation Framework will automatically merge reports. Referring to the previous example, if multiple observers report on the same target, and the correlators are set appropriately, then the system will merge the reports and all associated media into a single entity. Correlators and the associated merging function work for any entity (person, place, event, etc.) that is input into the TED or shared among TEDs.

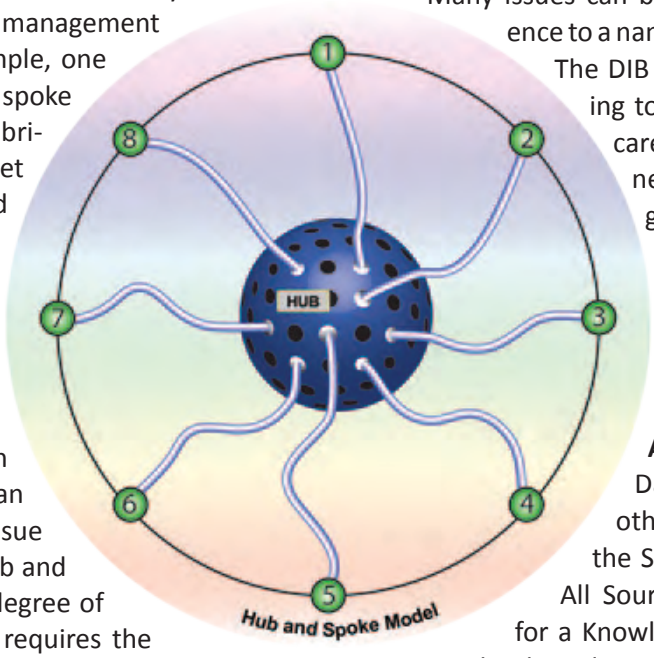
Another advantage of the DCGS-A version 3.2.4 is that the Cross Domain Solution Suite allows entities, message traffic, and finished products to be moved among the high side and collateral enclaves. However, currently the only DCGS-A capability for data basing entities from an all-source perspective resides with the Analysis Control Element Block II.

A Way Ahead

So how then does the intelligence warfighting function of the future manage a nearly infinite amount of information in all its variations without getting buried? Future intelligence handoff lines should be more than just lines on the map. Imagine a force where the IFS at all echelons from the battalion, brigade, and division, both forward and in sanctuary, can contribute to the total intelligence picture. In striving for that goal, one of the most significant challenges is establishing

rules on how the data is managed. Even though most elements can have the same entities, nearly every element may have modified them in some way. One solution is to use intelligence handoff lines as the basis to conduct database management. Units that are battlespace owners will naturally gravitate toward using geographic boundaries as the basis for database management. Another way to manage the data is by assigning management responsibilities based on different functions by echelon. Establishing rules as to which echelons conduct data movers, merge, or link media to an entity will be critical to the future of intelligence information management.

Geographic filters are helpful in developing boundaries that enable the operator to prioritize his entity management, but rules for database management can also be designated. For example, one technique is to use a hub and spoke method of data distribution. The brigade database manager can set up a data pull "data mover," and pull all the subordinate units updates per a predesignated time hack. For example, the data pull could occur every 12 or 24 hours in conjunction with the intelligence cut off for developing the latest intelligence summary. Then the brigade database manager can reconcile the database and re-issue it to all subordinate units. This hub and spoke method allows for a high degree of control at the brigade level, but requires the subordinate units to trust the new data. An alternate method is to require the battalions to reconcile data within the TED at their level, and then push the updated TED to the brigade for consolidation. This method puts the requirement on the battalion to maintain not just a database but a trained database manager. While this is still a form of hub and spoke, it puts more responsibility on the subordinate units to maintain themselves.



Hub and Spoke Model

Another method is a web as opposed to a hub and spoke. In the event that the network is not a constraint, it is possible to allow all IFS in the architecture to constantly update one another. The most important decision in this instance would be the settings of the correlators, timing of the data movers, and at what echelon the final reconsolidation authority resides. All correlators would ideally be set identically among all IFS in the network in order to reduce the number of conflicts the database manager needs to manually reconcile.

Lessons Learned

There is no universal solution to database management. However, there are many ways to do it wrong. Successful database management is dependent on the health and status of the network, the number and type of domains included, and the extent of the organization's digital capacity. Other factors include the following:

A good standard operating procedure (SOP). Without near draconian adherence to a digital SOP, multiple copies of old files and repeats of entities will cause the TED and DIB to get cluttered and unusable. While there are multiple ways to change or delete a file, there are database management challenges associated with those changes and deletions. Many issues can be mitigated with a strict adherence to a naming convention and style sheets. The DIB and TED are designed to be living tools, but they must be managed carefully. Understand that it may be necessary to default to the intelligence battlespace owner's methodology in order to synchronize databases. Look to the combatant command or the military intelligence brigade (theater) for guidance.

A good Knowledge Manager. Database management is yet another "out of hide" function that the S2 needs to resource. The senior All Source Technician is a good choice for a Knowledge Manager, but may lack an in-depth understanding of the system to balance both intelligence production and digital discipline. Like other "out of hide" functions, the database manager is typically personality driven. Sometimes the right person for the job is not necessarily the most senior or experienced person. When choosing the database manager, you may want to consider those Soldiers who excel during the fusion and data mover segments of New Equipment Training or a graduate of the DCGS-A Master Gunner Course. Another alternative is to turn database management over to a reach element/external organization. This method would require considerable trust, and the reach element would require an intimate knowledge of the local network status.

Reliable system administrator support. Part of properly managing the DIB involves the system administrator. There are some challenges that should be considered when planning the use of DCGS-A at brigades and especially battalions. There are two systems administrators involved in the

use of DCGS-A. The overall DCGS-A systems administrator is the MOS 35T/353T, MI System Maintainer/Integrator; the Digital Domain Server (DDS) systems administrator is the MOS 25-series communications Soldier. DDS is a part of the IFS along with the Cross Communication Interface and the Active Directory. The DDS is the virtual messaging system that allows DCGS-A to communicate with the rest of the Mission Command Systems. However, there are not enough MOS 35T/353T to afford one per maneuver battalion. Maybe it is time to consider the use of MOS 35F, Intelligence Analyst as system administrators at battalion level. In order to be a system administrator the user requires Security+ and Network+ certifications. Allowing a MOS 35F to act as a system administrator at the battalion level would alleviate the shortage of intelligence system maintainers.

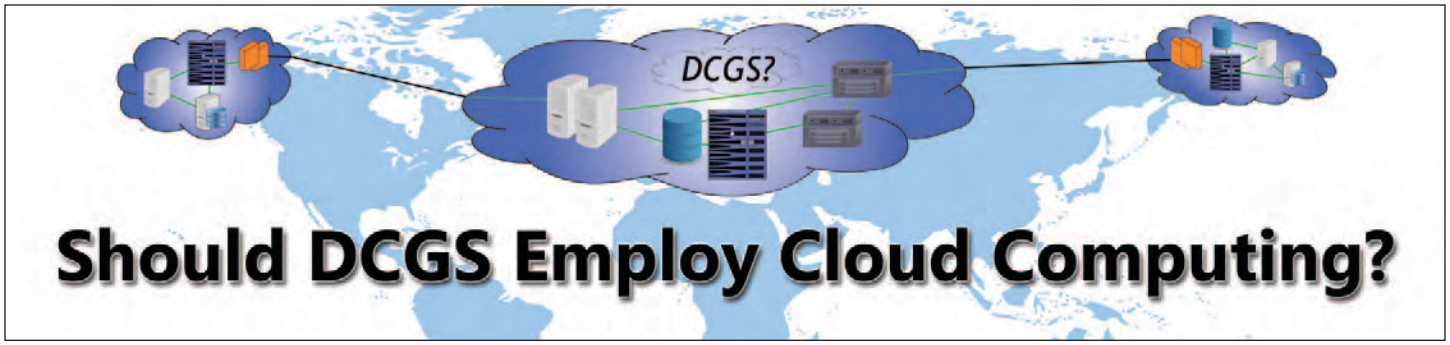
A complete understanding of the network. The senior intelligence officer needs to know the network almost as well as the senior communications officer. For example, it is important to know when to move data, and how much can affect the status of the network. A smart S2 doesn't try to move data during the commander's update brief. The decision to use a hub and spoke or a web for data distribution should be based on a complete understanding of the network. The solution will differ if the organization is on a fiber optic backbone or a satellite based communications architecture. A few of the many aspects of database management that should be addressed include:

- Aspects of entity management; such as rules covering who and what echelon has override authority on entities.
- Delineation of administrative privileges and trust levels.
- Selection of those involved in database management across echelons.
- Dictating the specifications associated with naming conventions and style sheets.
- The unique set of training requirements.

Conclusion

There are significant advantages to employing DCGS-A 3.2.4 and beyond at all echelons, and the juice is worth the squeeze. If done right, effective database management can be the difference between successful and unsuccessful intelligence support. Effective database management will result in every sensor, report, and digital product anywhere from any echelon being at the disposal of any intelligence professional in the theater. However, without significant digital discipline the intelligence community could easily create unique digital problems and fail to provide timely and relevant intelligence support. The devil is in the details. Functions, roles, and responsibilities should be delineated as part of intelligence handoff lines. Carefully crafted SOPs covering all aspects of database management are crucial. It is critical that the intelligence community takes the time to get database management right.

MAJ Robert Richardson enlisted in the Army in 1992 where he served as an infantryman and signalier before transitioning to the Officer Corps in 1997. He deployed to OEF 04-05, OIF 06-07 and OEF 09-10 serving in positions as a Platoon Leader, Brigade S-2, and Brigade AS2 respectively. MAJ Richardson later served as a test officer under the Army's Test and Evaluation Command at Ft Bliss, Texas. MAJ Richardson's civilian and military education includes a BA in Government and World Affairs from the University of Tampa and an MS in Strategic Intelligence from the National Intelligence University.



Should DCGS Employ Cloud Computing?

by Lieutenant Colonel (Ret.) Jake Crawford

The views expressed in the following article are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. Listing the products and services in this article does not imply any endorsement by the U.S. Army, the U.S. Army Intelligence Center of Excellence, or any U.S. government agency.

Introduction

The U.S. Department of Defense (DoD) Distributed Common Ground System (DCGS) is a family of systems (FoS) consisting of an Army (DCGS-A), Air Force (DCGS-AF), Navy (DCGS-N), and Marine Corps (DCGS-MC) component. The DCGS FoS is intended to provide all four Branches of the Armed Forces with core functionality that includes: data sharing, real-time data access, data storage and redundancy (backup), access to software applications and other services, and information security.[1] In addition, the four Branch specific DCGS systems provide data visualization and reporting capabilities unique to each Branch.

Given the required core capabilities of the DCGS FoS, as well as the Branch specific requirements, is cloud computing a suitable option for the DCGS FoS? This article begins with an overview of the DCGS requirements and architecture. It then describes cloud computing and analyzes its benefits and risks as applied to the DCGS FoS. Finally, the article examines various cloud computing solutions for possible implementation by the DoD for the DCGS materiel capability.

What is DCGS?

According to the Under Secretary of Defense for Intelligence, the DCGS enterprise is a collection of tenets that forms the foundation for partner organizations to share data and services associated with intelligence, surveillance, and reconnaissance (ISR).[2] The DCGS FoS encompasses the hardware, software, personnel, and processes through which the tenets are implemented.

The DCGS FoS provides users the ability to task sensors, process data collected from sensors, exploit the data via analysis, and disseminate the products developed from the analysis.[3] The DCGS enterprise provides the DCGS FoS with core functionality, to include user access control (login) and security; user global access; survivability (works when connected and/or disconnected from the network); affordability (falls within the Branches' fiscal budgets); agility (Branches can rapidly deploy or reconfigure components), and intelligence (supports advanced analysis).[4]

Although it is the DoD's intention that DCGS FoS continues to work when disconnected from a telecommunications network, it is nonetheless highly reliant upon network connectivity for data sharing, continuity of operations (COOP) with remote site data storage (backup), and many of the ISR specific services. As illustrated in the following figures, DCGS shares data and services (via a telecommunications network) among a plethora of stakeholders (Figure 1), as well as between multiple echelons (several having only limited network bandwidth) within each military Branch (Figure 2).

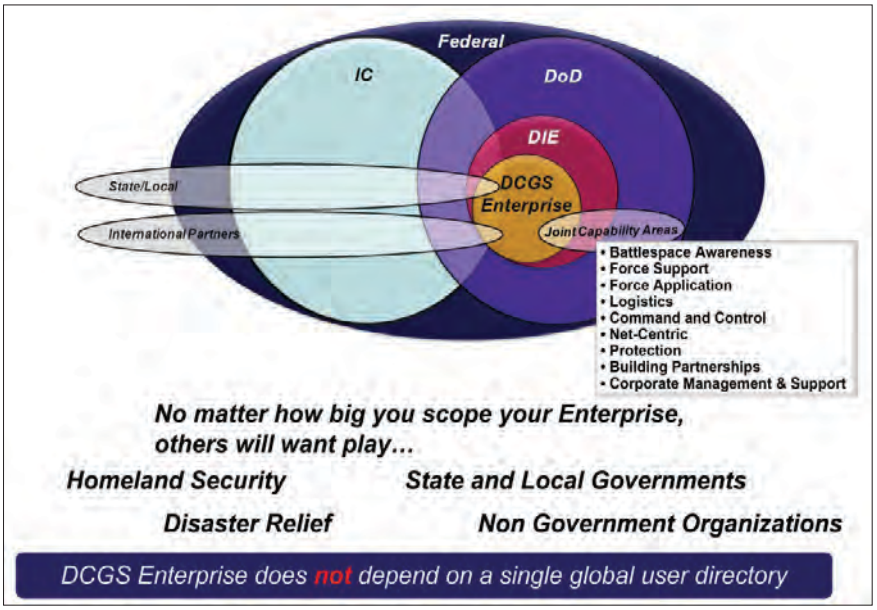


Figure 1. DCGS Horizontal Reach: Stakeholder/Partner Organizations.[5]

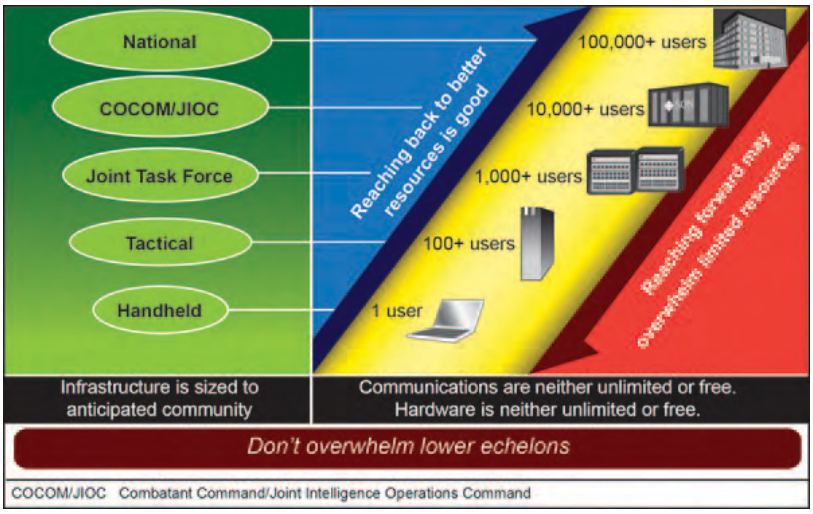


Figure 2. DCGS Vertical Echelons: from National Satellites to Tactical Handheld.[6]

In order to facilitate connectivity and interoperability among each of the Branch's DCGS systems, the DoD tasked the Air Force to develop the DCGS Integration Backbone (DIB). The DIB establishes a common architecture, interface standards, core tools, and documentation to guide all of the Branches as they develop their DCGS variants.[7] The DIB is the optimum component of the DCGS enterprise architecture for the DoD to apply cloud computing tenets and technical solutions to guide and improve the overall DCGS program.

What is Cloud Computing?

Many nations have established varying levels of release authorization for their national intelligence products and procedures. This ranges from information that nations readily share with the world, to information that remains tightly controlled, to information that nations guard closely and only share among trusted individuals. Like national intelligence, cloud computing encompasses a variety of techniques for organizing and sharing resources.

Cloud computing involves the use of rented, leased, or owned infrastructures that utilize the Internet and private networks to provide convenient and on-demand access to data and shared resources.[8] Via the cloud, users retrieve and store data, utilize software programs, and access other services, all of which reside on remote servers/computers instead of the user's computer (desktop, laptop, smartphone, etc.)

There are four major categories of services (SaaS, PaaS, IaaS, dSaaS) provided via cloud computing, as well as the cloud architecture (application layer, platform layer, infrastructure layer, and hardware layer) upon which each service category depends. The first three services are:

1. "Software as a Service" (SaaS) provides applications that run on a server, but render results to a client. Processing of data takes place entirely on the server, or is divided between the server and client.[9] SaaS decreases software costs by eliminating the requirement to purchase and maintain software and/or site licenses for each client. SaaS also increases agility by enabling rapid changes in software applications that are immediately and simultaneously available to all clients.

2. "Platform as a Service" (PaaS) provides access to resources that enable users to develop their own web pages and software applications. These tools include software development tools, web servers, and operating system application program interfaces.

3. "Infrastructure as a Service" (IaaS) entails virtual machines (hardware emulation) that provide users with processing capabilities, storage, and networking capabilities. It is the foundation upon which the SaaS and PaaS services run.

The final category is "Data Storage as a Service" (dSaaS). This service is a derivative of IaaS, and focuses on providing secure, sustained, omnipresent, and flexible storage. Service providers, such as the Amazon Simple Storage Service, offer customized storage ranging from frequent use, to general use, to long-term archive storage services. [10]

In addition, there are four common types of clouds: "public," "private," "community," and "hybrid." In the case of public clouds, a service provider (not the customer/user), owns and/or manages the remote servers, as well as many of the services.[11] Some notable public cloud computing examples include Google Drive, DropBox, UConnect, OneDrive, and Box. Public cloud providers can be compared to utility companies who offer their services to the public on a "pay-per-usage fee."[12]

Private clouds are described as being typically owned by large companies or government agencies that are dispersed over multiple geographic locations.[13] These organizations implement private clouds (generally hosted on servers and networks that are owned and/or managed by the organization) in order to achieve a higher level of security and data confidentiality than expected on a public cloud. Private cloud owners utilize private networks (e.g., fiber, Ethernet, wireless), firewalls, and other technical and procedural means to limit access to, and increase the security of their data and services. In this paradigm, only authorized users are allowed to access services (e.g., company servers), as opposed to public clouds via which any user may access services (e.g., Google Drive).

Community clouds are similar to private clouds insofar as only authorized users may access them. However, instead of a single private cloud for a single organization, a community cloud provides a shared private cloud for use by multiple cooperating organizations.[14] Each organization participating in a community cloud must agree on what resources (e.g., data, services, networks, etc.) they will share. The members may select from various governance models for managing their shared resources. This includes (but is not limited to): outsourcing control to a neutral party; appointing one member to control all resources; allowing each member to control their individual resources; or appointing members as executive agents to manage each class of pooled resources (e.g., data manager, network manager, service "A" manager, service "B" manager, etc.) By combining resources, the cost to each community member decreases. However, each member also assumes the risks and security issues inherited from the other community members.

Hybrid is the last type of cloud. Under this configuration individual clouds (public, private, and community) maintain their independence while establishing (at a minimum) a private-to-public cloud interface.[15] Via this connection, organizations gain access to resources (e.g., data and services) that are otherwise not available in their cloud. At the same time, cloud partners maintain the benefits of their organic cloud architecture (i.e., security of data maintained in a private cloud) while benefiting from the capabilities of the partner cloud (i.e., ubiquitous access to data in a public cloud).

However, this type of partnership also exposes each party, in varying degrees, to the risks associated with each of the interfacing clouds. A simplified example of a hybrid cloud is the creation and storage of this article. I created this paper via a public cloud (Google Apps hosted on Google Drive); however, I maintained backup files on my private "home" cloud (instantiated on personally owned computers, storage devices, and local area network, with access limited to "home" users only). Via the interface between the public cloud (Google Drive) and private cloud ("home"), I was able to work on this article from anywhere with Internet access, while ensuring the backup files remained secure regardless of public cloud and Internet security issues.

How Can Cloud Computing Assist DCGS?

Cloud computing could assist the DCGS program by providing users the DCGS core capabilities (data sharing, real-time data access, data storage and redundancy (backup), access to software applications and other services, and information security) to all users, regardless of their Branch. Each of the cloud computing options would provide DCGS the following benefits:

- Reduced software costs and increased flexibility (ability to add/delete/change applications).
- Increased mobility via the ability to access services and data from anywhere with connectivity to the Internet (public cloud) and/or private network (private cloud).
- Data backup and continuity of operations (rapid ability to relocate operations to an alternate site if the primary location is compromised).
- Access to all publicly available data and services (private clouds may limit this option to only privately available resources).

However, DCGS also assumes the following risks with cloud implementations:

1. Cost to convert from a non-cloud to a cloud-based architecture, to include lost productivity during the changeover.
2. Network availability of Internet and/or private networks.
3. Security concerns stemming from increased vulnerability to network cyberattacks and exposure to threats via external service providers.

Table 1 summarizes the benefits and risks associated with the four cloud computing instantiations (public, private, community, and hybrid). Following Table 1 is an explanation of each benefit and risk as applicable to the DCGS program.

Table 1. DCGS Implementation of Cloud Computing: Benefits vs. Risks

	Benefits (Pros)	Risks (Cons)
Public Cloud	*Cost:* reduced via shared services (SaaS, PaaS, IaaS, dSaaS) *Flexibility:* expand or consolidate capabilities/services *Mobility:* ubiquitous access to data and services via Internet Data backup and COOP *Data/Services (**D/S**):* access to all publically available data & services	*Cost:* conversion to Cloud network (**NW**): dependence on Internet *Security and privacy* (**S/P**): decreased control of data transmitted via the Internet and handled by an outside service provider
Private Cloud [Benefits/Risks beyond Public Cloud]	*S/P:* increased control of data and services *NW:* less susceptible to Internet related issues (i.e., DoS and QoS)	*D/S:* limited to private resources *Cost:* increased infrastructure (procure and maintain servers and/or networks)
Community [Benefits/Risks beyond Public and Private Cloud]	*Cost:* shared among community members *D/S:* access to more resources within the community *S/P:* more secure than Public	*Cost:* higher than Public *D/S:* shared management/control of resources between members *S/P:* vulnerabilities and insider threats from community members
Hybrid [Benefits/Risks beyond Public, Private, and Community Cloud]	*Cost:* less than Private *S/P:* more than Public *D/S:* agility–can add, delete, change, and make resources ubiquitously available (via Public)	*Cost:* more than Public *S/P:* less than Private *D/S:* exposes shared resources to more attacks and less privacy (via Public)

Public clouds afford all of the benefits, and expose users to all of the risks, as previously described. Implementing a private cloud would provide DCGS increased control of its data and services by keeping theses resources "in-house," while also eliminating exposure to Internet related cyber vulnerabilities, and quality of service and denial of service risks. On the other hand, a private cloud solution restricts DCGS's access to publicly available resources, and necessitates additional infrastructure for maintaining a private network (however, since the DoD already owns private networks, this last point is a minor concern).

A community cloud, hosted within the DoD, would enable each DCGS stakeholder (Army, Air Force, Navy, Marines, and other organizations as depicted in Figure 1) to consolidate their resources (data, services, networks) into a single communal environment. When compared to each stakeholder establishing its own private cloud, this solution facilitates the sharing of resources among all community members, thus reducing each member's individual costs. A community cloud also provides superior security, versus a public cloud, by restricting access to the community members only. However, this solution requires a greater level of cooperation and coordination among the members for managing the data and services, ensuring security, and controlling any pooled network capabilities. Thus, it is more expensive than a public cloud.

Finally, DCGS could establish a hybrid cloud solution. This approach entails a combination of public clouds and private clouds (individual organizations and/or communities). Hybrid clouds are more expensive than public clouds insofar as the need to procure and maintain privately owned resources (e.g., services and networks), but they could prove less expensive and more effective (than a strictly private cloud) for sharing data and services. A hybrid cloud (via the ability to protect resources on the private cloud side) provides more security than a public cloud; however, a hybrid cloud is less secure than a private cloud due to its inherited public cloud security risks.

What Cloud Computing Solutions Are Best For DCGS?

Based upon the above analysis, DCGS should implement a hybrid cloud computing architecture as depicted in Figure 3.

This hybrid solution allows each Branch (as well as specific stakeholders) to retain individual private clouds, while establishing separate community and public clouds for all stakeholders' collective use.

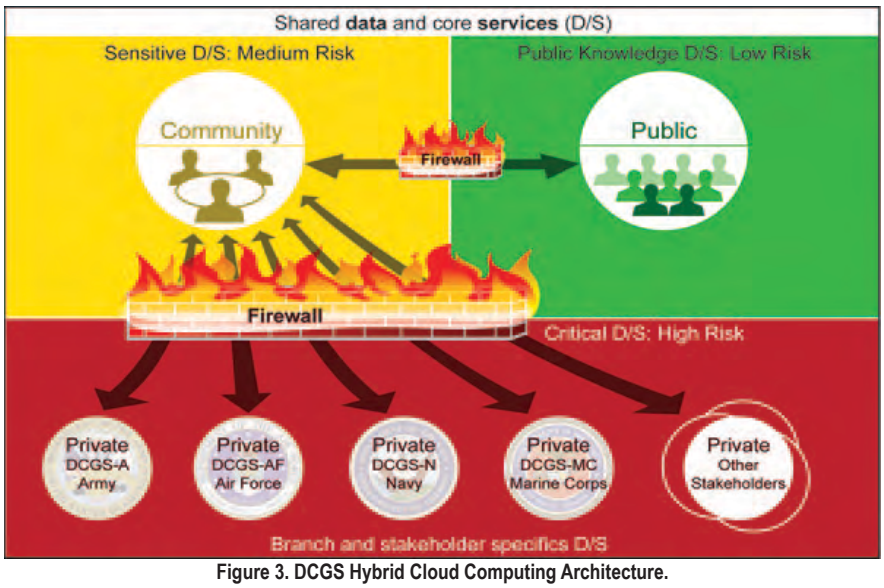


Figure 3. DCGS Hybrid Cloud Computing Architecture.

The private clouds provide the following benefits:

- Allows each Branch to retain its specific functionality on their Branch, organization and/or unit servers and networks, thus providing them at least limited capability during DoD network downtimes.
- Maximizes the security of each stakeholder's critical data.

The community cloud, residing on DoD private networks and servers:

- Facilitates the sharing of core services and data.
- Provides a greater level of security as compared to the public cloud.
- Evenly spreads the costs for maintenance and distribution of core data and services across each of the Branches.

Lastly, the public cloud benefits DoD users having limited access to DoD/Branch networks and/or utilizing mobile devices. The public cloud provides these users access to DoD/Branch low risk data and services (as well as publicly available data and services) from anywhere on Earth with Internet connectivity.

Conclusion

This article described the DoD's DCGS program, consisting of an enterprise architecture and Branch specific systems for each of the four Branches of the Armed Forces. The four cloud computing models (public, private, community, and hybrid) were examined and the benefits and risks associated with each approach were analyzed as they applied to DCGS. Finally, a recommendation for employing a hybrid cloud computing solution for the DCGS program that maximizes the aforementioned benefits while minimizing the risks was proposed.

As the DoD evaluates potential cloud vendors and products, to assist in creating and/or maintaining its hybrid cloud computing architecture, it should consider the following five key points:

Technology neutrality. The DoD should not limit itself to any specific vendor's proprietary materiel solution. Instead, the architecture must retain the flexibility to select the best technology (i.e., hardware and software) available that satisfies the DoD's requirements.

Ecosystem support. Since the best solutions for the DoD will likely not all come from the same source, vendors must provide products that integrate with solutions from other companies.

Ability to customize. Vendors must possess the willingness and capacity to customize their products to satisfy the DoD's unique requirements.

Secure solutions. Vendor products and processes must adhere to industry, as well as DoD, security and privacy specifications.

Expertise. Vendors should possess the experienced and skilled personnel, executable and sustainable processes, and requisite resources to deliver their advertised products and services.[16]

Endnotes

1. Raytheon, "Distributed Common Ground System (DCGS)," 19 November 2015. Retrieved from www.raytheon.com/capabilities/products/dcgs/.

2. Gerhard Beck, "Distributed Common Ground/Surface System (DCGS) Enterprise: DCGS Enterprise Overview," 5 December 2011. Retrieved from https://www.ise.gov/sites/default/files/Track3-GerhardBeck-WIS3-DCGSEnterpriseOverview.pdf.

3. Committee C4ISR for Future Naval Strike Groups, "C4ISR for Future Naval Strike Groups," The National Academies Press, 2006, 186. At http://dx.doi.org/10.17226/11605.

4. Beck.

5. Beck.

6. Beck.

7. C4ISR for Future Naval Strike Groups, 182.

8. Efraim Turban, Linda Volonino, L., and Gregory Wood, Information Technology for Management: Advancing Sustainable, Profitable Business Growth (9th ed.) (Hoboken, NJ: John Wiley & Sons, Inc., 2013), 47-50.

9. Irv Englander, The Architecture of Computer Hardware, Systems Software & Networking: An Information Technology Approach (5th ed.) (Hoboken, NJ: John Wiley & Sons, 2013).

Sumit Goyal, "Public vs Private vs Hybrid vs Community–Cloud Computing: A Critical Review," I.J. Computer Network and Information Security, 2014, 3, 20-29. http://dx.doi.org/10.5815/ijcnis.2014.03.03, and Turban.

10. Amazon S3. Retrieved from https://aws.amazon.com/s3/.

11. Turban.

12. Goyal.

13. Turban (2013, 47-50).

14. Goyal.

15. Goyal.

16. e.Republic, Inc., "5 Things to look for in a Cloud Computing Provider," Government Technology, 26(11), November 2013.

LTC (Ret.) Crawford served 23 years on active duty in the Army Acquisition, Military Intelligence, and Adjutant General Corps, and deployed to Iraq and Afghanistan. For his final assignment he was the Army Test and Evaluation Command System Team Chair for DCGS-A, responsible for the developmental and operational test and evaluation of the DCGS-A Increment 1 system. He is a graduate of the U.S. Military Academy at West Point, earned an MBA and is currently enrolled in an MS program for Information Technology and Systems Engineering.

ATEC's Contribution to DCGS-A for the Warfighter

by Stephen Conley

Introduction

The Distributed Common Ground System-Army (DCGS-A) platform underwent testing by the U.S. Army Test and Evaluation Command (ATEC) and the resulting report directly contributed to the DCGS-A Program Manager's modernization plan. Operating units could potentially receive an improved system in 2017. The testing and evaluation (T&E) report initiated discussion between the Department of the Army Deputy Chief of Staff G-2 and the Intelligence Community to align testing and training requirements and create better training environments for individual and collective training.

Avoiding a Catastrophic Failure

An effectiveness, suitability, and survivability evaluation provides findings and conclusions that inform decision makers of operational capabilities and limitations at critical times throughout the acquisition lifecycle of any program. A poorly designed test event may lead to insufficient data for analysis and produce inaccurate reporting. Decisions based on inaccurate reporting may contribute to "catastrophic failures," where an effective capability does not get to Soldiers. ATEC's Army Evaluation Center developed a *Management, Mechanics, and Math (M3)* methodology as a deliberate approach to create a testing environment that fosters effective analysis and evaluation, incorporating both the science of testing and the art of a military exercise.

This methodology employed a complex live, virtual, and constructive (LVC) simulation to conduct the operational test of DCGS-A Increment 1, Release 2. As a base, the LVC environment assisted the development of a division warfighter-like event spanning the full spectrum of military operations. This enabled ATEC to collect, evaluate, and understand data regarding system and user (man-machine interface) by increasing control of a chaotic complex operational environment (OE). Soldiers are direct beneficiaries of such robust testing, which also facilitated the analysis and evaluation of DCGS-A's intended technical and operational capabilities.

T&E Used Both Art and Science

The science of the M3 methodology accounts for capturing all data, records, and reports including, but not limited to: system log files, execution logs, test director notes, user and operator assessments and surveys, while allowing Soldiers the greatest freedom to practice the art of intelligence.

DCGS-A testing in a realistic environment presented a challenge to the T&E community. Evaluators needed to see DCGS-A in an OE to fully enable the evaluation and support T&E analysis of an intricate IT system. Soldiers depend on information systems that effectively automate cognitive functions to achieve their assigned mission. Therefore, the data produced from the LVC testing environment not only had to support analysis of the technical and performance specifications, but also assess a warfighting unit's ability to support the commander's intent. DCGS-A must provide the user, staff, and commanders with effective products (timely, correct information or product) in an efficient manner and with a quantifiable output.

Photo by WO1 Jamie Garcia, MI TRP, 2CR

The ease-of-use enables Soldiers to meet these metrics enhancing mission success. Time, in this context, is defined as latest time information is of value. These products provide the commander with situational understanding within the OE and an improved ability to quickly determine the intent of hostile or unknown entities.

Testing must produce data that can be ordered and analyzed. Evaluation requires a testing environment that provides an understanding of the impact the system has with respect to overall mission requirements of both the Soldier and the operational unit. Testing DCGS-A via the M3 methodology implements military exercise management

Photo ccourtesy of US Army , DCGS-A Public Affairs

and mechanics principles, garnering the supporting data necessary for the math behind an evaluation. DCGS-A testing via M3 methodology allows the Soldier and unit the freedom to operate seemingly unencumbered by test requirements.

The test aligned the mechanics of a military exercise with the testing requirements of message counting, reporting, and tracking of vignettes embedded in a free-play command post exercise. The test conditions employed a scenario-driven simulation with a white cell working with friendly forces (or Blue Forces) and enemy forces (or Opposing Forces). The test team ensured key missions and event threads were exercised within the parameters of a controlled but flexible event. The test storylines or vignettes were built to create specific scenarios that can be tracked (such as rolling up an improvised explosive device factory, working terror cell linkages, etc.) The exercise allows the friendly and enemy commanders to act as the catalysts that drive their decisions.

T&E Provides Positive Results for the Soldier

T&E of DCGS-A produced numerous benefits to the Soldier. Three immediate benefits are enumerated below.

1. The M3 methodology led to distinctive operational outcomes. For example, the brigade reported that DCGS-A capabilities allowed their S-2 section to be more timely and operationally effective, although battalions felt that certain technical functions were not used at their level. This feedback allowed the Program Management Office (PMO) to develop a scalable solution. The U.S. Army Intelligence Center of Excellence develops intelligence requirements by echelon and the PMO deploys them based on capabilities and dependent upon echelon requirements. The near future holds a potential DCGS-A Battalion Solution Capability projected for Fiscal Year 2017 prior to possible fielding to the force.

2. This test codified some of the usability concerns heard from the field. Usability is a key system attribute for DCGS-A Increment 2. As such, the PMO included a usability focus from the start, and created a Human Systems Interface style guide which describes user interface design methods and style recommendations for the DCGS-A program. The usability guide will drive each tool or widget to have a similar look and feel.

3. The LVC testing environment that made the operational test in Fiscal Year 2015 a success can also support excellent individual and collective training. As an example, for an individual task:

> ***The trainer selects the task to develop a "baseball card" for a specific high value individual (HVI). The condition is to use the information provided during the 30-minute exercise scenario to develop baseball cards of specific persons of interest based on a given the commander's priority intelligence requirement. The standard is 90 percent accuracy. The trainer simulates sending 300 pieces of information to the trainee, of which 30 pieces are "truth data" about a specific HVI. The injection method (Signals, Human, and Measurement and Signature Intelligence, etc.) used will be determined by the exercise Master Scenario Events List. At the end of the training session one can determine the ratio, the amount of information the analyst has on the baseball card over the 30 known pieces of information. Anything less than 90 percent (or less than 27 pieces does not receive a passing score or grade.)***

The capability goes one step farther. It lets the trainer know which three pieces of information were not listed and drives a discussion with the user to determine why those pieces were not listed. Did the user not think they were important? Did the user miss something because of a substandard query or narrow search? The result is knowing exactly what the user did resulting in failure, and then being able to focus re-training on a particular topic. The process and M3 methodology can be expanded to collective training for an entire battalion or brigade S-2 shop preparing a combat training center rotation.

Conclusion

The M3 methodology blends the "Art of War," typically found in the execution of military exercises, with the "science" of testing and data collection that enables the arith-

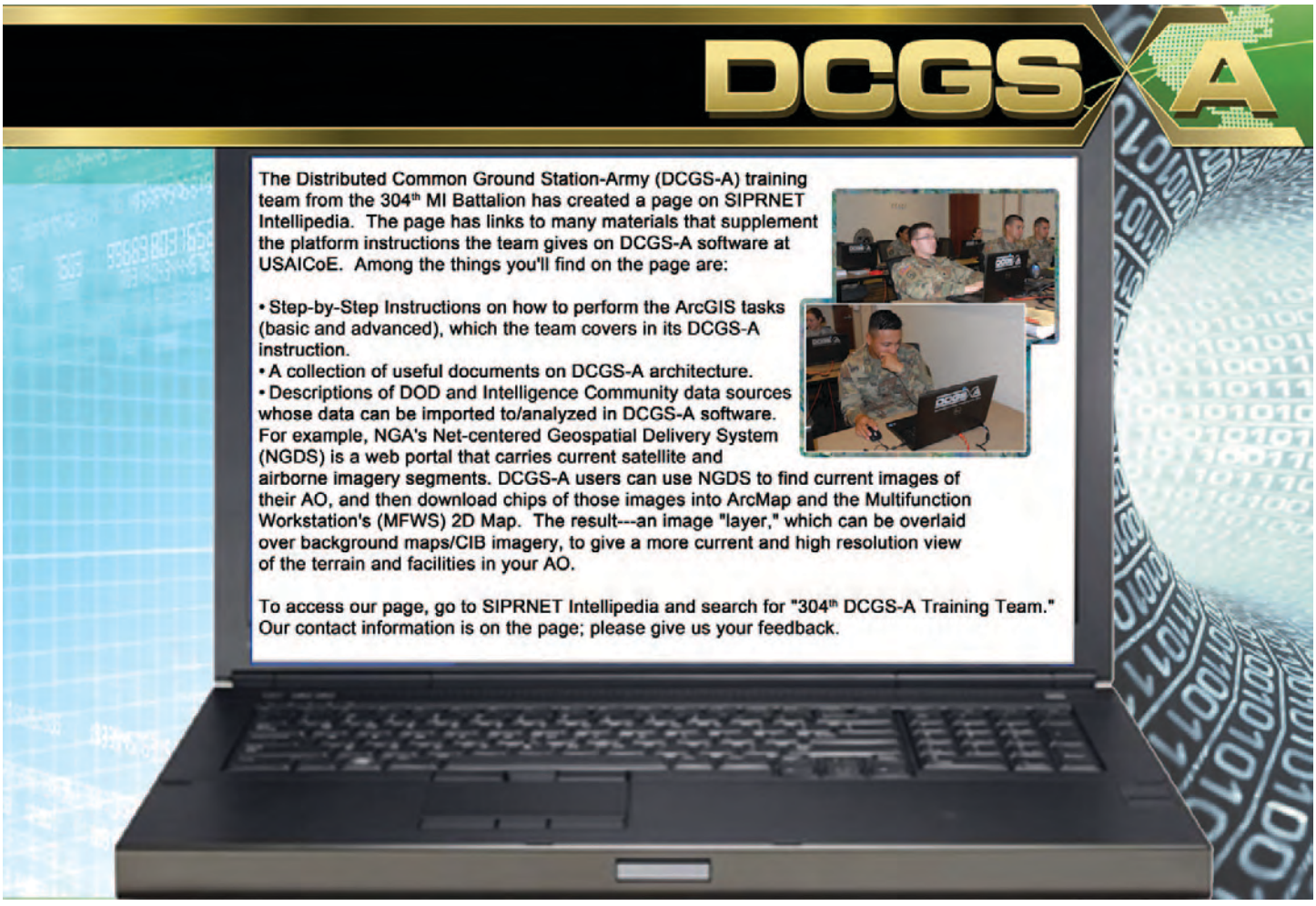
metic to evaluate complex information systems like DCGS-A. The use of military exercise principles coupled with the fidelity and control of testing enabled the T&E community to provide valuable insights to DCGS-A which helps the Program Office better shape the man-machine interface for Soldiers and units using DCGS-A. It created dialogue with Department of the Army on the potential to require test simulation to develop a training environment that supports training of individual and collective tasks. This is no different than determining a Soldier's proficiency with his/her individual weapon and how effectively he/she operates within the squad on a movement to contact. This capability could grow with the DCGS-A program and support both the training and testing communities. What does all this really mean? Intelligence Soldiers from battalion through brigade to echelons above corps in theater intelligence brigades all receive a better toolset to provide accurate, timely, and relevant intelligence to commanders at all levels from garrison to theater.

Acknowledgements

• John Diem, Director, ATEC, Operational Test Command, Test Technology Directorate

• Jennie Lenig-Schreffler, ATEC, U.S. Army Evaluation Center, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Evaluation Directorate, Aberdeen Proving Ground, Maryland.

Mr. Conley is a senior evaluator and a retired U.S. Army Officer who has worked for ATEC since 2003. He evaluated the Future Combat Systems Network; has been a test technologist; led the Army Evaluation Center effort for the Army's Agile Process and Network Integration Evaluation, and managed the DCGS-A evaluation. He holds a bachelor's degree in Industrial Engineering from Lafayette College and an MBA in Information Systems from City University. He is a graduate of the Army's Command and General Staff College, is a Harvard Senior Executive Fellow, and is attending the Defense Acquisition University Senior Service College Fellowship Program.

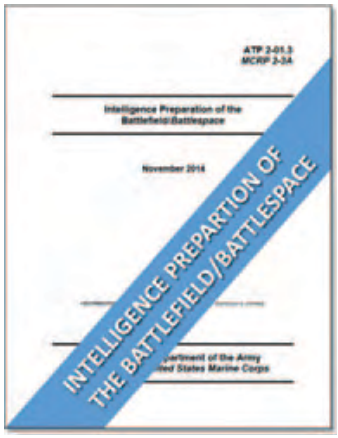


Training the S-2/G-2 for IPB Success

by Jennifer Dunn

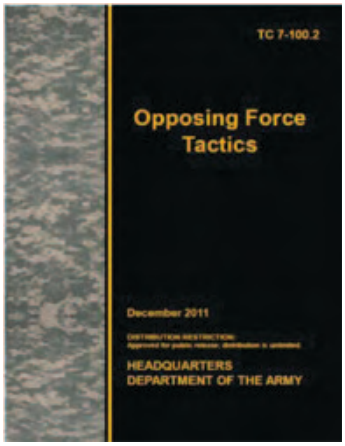
Introduction

The U.S. Army Training and Doctrine Command (TRADOC) G-2 has played an integral role in developing the military intelligence (MI) profession, augmenting MI training curriculum, and improving MI doctrine. In 2014, the U.S. Army Intelligence Center of Excellence (USAICoE) transitioned its Field Manual 2-01.3, Intelligence Preparation of the Battlefield, to the Army Techniques Publication (ATP) format. The new ATP 2-01.3, Intelligence Preparation of the Battlefield/Battlespace (IPB), includes updated concepts developed by the TRADOC G-2.



TRADOC G-2's small, but vital, role in the update to the IPB manual enabled the manual to provide MI analysts with new tools to assess threats in a way other than traditional templating.

TRADOC G-2 ACE Threats Integration (ACE-TI), the organization that worked directly with USAICoE for the IPB doctrine update, serves as the Army lead for designing, documenting, and integrating threat and operational environment conditions in support of all Army training, education, and leader development programs.[1] In order to execute this assigned task, ACE-TI is an organization comprised of intelligence specialists and military analysts trained to study and analyze threat actors from around the world in order to ensure proper depiction of threats in these areas. This mission has resulted in the creation of two foundational concepts: *functional tactics and functional analysis*. Functional tactics "describes a tactical action according to the role each actor and element has in bringing about success and does so using a common language and necessary and sufficient battlefield functions."[2] This concept allows students of threat tactics to understand that *all* tactical actions, no matter what threat organization is the focus of analysis, can be reduced to three primary functions: action, enabling, and support. These functions and discussion on how threats employ them can be found in detail in Training Circular (TC) 7-100.2, Opposing Force Tactics.



The detailed examination of threat tactics that resulted in the concept of functional tactics created a unique perspective for analysts in ACE-TI. It allowed analysts to not only see how threat organizations will organize and tactically act for offensive and defensive missions, a threat perspective, it also provided analysts with the key indicators needed to analyze a threat's actions in order to formulate the best picture of a threat course of action (COA), an analytical perspective. This is, in essence, functional analysis.

Functional Analysis

Functional Analysis
An intelligence analysis methodology that uses the concepts of *functional tactics* to predict probable and/or possible enemy courses of action.

Functional Tactics
The idea that threat tactical action is best understood and described by the functions each force, element, or actor performs in order to bring about mission accomplishment.

Functional analysis is an intelligence analytical methodology that uses the principles of functional tactics to predict threat COAs. This methodology is designed to result in a graphical depiction (which shows disposition and actions) of how a threat may use its capabilities to conduct operations to accomplish its objectives. Functional analysis and the idea of functional tactics were first developed conceptually by ACE-TI to support its mission to improve Army training. Since the development of these concepts, ACE-TI has actively worked to disseminate them throughout the Army, and of late has worked very closely with USAICoE to augment current MI training and doctrine. The first big success of this effort is the collaboration between USAICoE and ACE-TI for ATP 2-01.3, the IPB manual. ACE-TI's largest contribution to this manual can be found in Appendix B, Functional Analysis.

ACE-TI's efforts at propagating the concept of functional analysis has not ended with the publication of the newest IPB manual. It works daily both through its collaborative efforts with USAICoE and through its own independent teaching efforts to share functional tactics and functional analysis with the Army.

ACE-TI Teaching MI Professionals

In May 2016, the Director of ACE-TI visited Fort Huachuca, Arizona to observe a capstone exercise for the MI Captain's Career Course. This visit served as an opportunity for ACE-TI and USAICoE to continue their collaborative efforts and identify what else can be done jointly to further improve MI training in the Army. It was identified at this meeting that ACE-TI could support USAICoE by pursuing a number of initiatives, all of which ACE-TI has taken before its leadership for consideration.

These initiatives include drafting a publication that assists S-2/G-2s in expressing enemy COAs in maneuver language (as opposed to 'threat language' found in the TC 7-100 series), providing a catalog of threat models for use in IPB execution, and exploring options for MI officers' and noncommissioned officers' attendance at ACE-TI's Threat Tactics Course (TTC), and/or integration of TTC material into the USAICoE curriculum.

ACE-TI's Threat Tactics Course

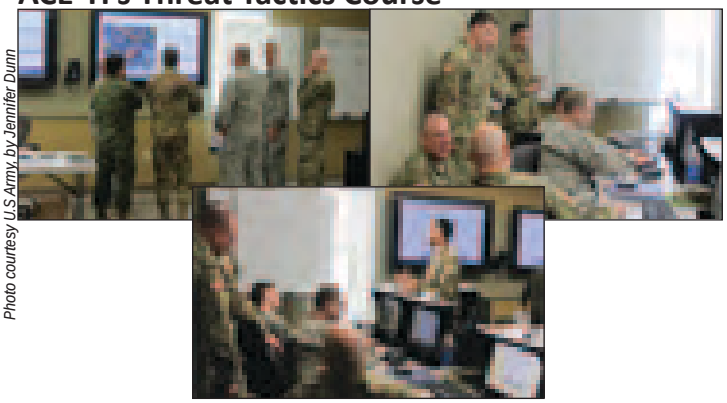


Photo courtesy U.S.Army by Jennifer Dunn

Soldiers at March 2016 Threat Tactics Course.

ACE-TI has taught a course on threat tactics at Fort Leavenworth, Kansas, for approximately 16 years. Over the years the course has changed names (formerly known as the "Hybrid Threat Train the Trainer") and the content has shifted to meet the Army's need for tactics based instruction. The course started as an annual event targeting members of the opposing force (OPFOR) program at the various training centers throughout the Army, but has greatly expanded since then. Students now range from the traditional OPFOR practitioners, to intelligence observer controller trainers, to intelligence analysts assigned to battalions, brigades, and even intelligence centers such as the National Ground Intelligence Center.

Students now have the option to either attend one of the bi-annual resident course offerings at Fort Leavenworth (typically in March and August) or use a mobile training team (MTT) option that is conducted on an 'as requested' basis. The primary purpose of the course is to teach the concept of functional tactics, and all the classes that make up the course curriculum facilitate this effort, including functional analysis. If any readers are interested in attending the next resident course, please call the ACE Threats Integration Point of Contact at (913) 684-7922. For any readers interested in learning more about the MTT offering, call (913) 684-7962.

USAICoE Support to Fort Leavenworth Training

One final note on ACE-TI's involvement in training MI professionals: USAICoE recently decided to send a lieutenant colonel to Fort Leavenworth for the purpose of teaching a short refresher course on IPB to incoming majors assigned to the Command and General Staff College (CGSC). This MI officer is assigned to TRADOC G-2 Leavenworth and will work daily with the analysts in ACE-TI. This physical co-location will further develop the collaboration between TRADOC G-2 and USAICoE by allowing ACE-TI to assist the officer in teaching IPB at CGSC and enabling the MI officer to assist TRADOC G-2 in the development of its initiatives to provide additional support to USAICoE.

MI Professional Development

MI professional development does not end when one leaves Fort Huachuca, nor does it only occur while attending courses at USAICoE. There are opportunities for development throughout the Army, and TRADOC G-2 has made it a part of its mission to assist the Army MI community in this endeavor. A variety of entities in TRADOC G-2 are actively working intelligence issues, and the ACE-TI/USAICoE collaboration highlights what only one organizational element is doing.

Endnotes

1. TRADOC Regulation 10-5-1 Organization and Functions, Headquarters, U.S. Army Training and Doctrine Command, 20 July 2010.

2. Jon Cleaves, "Director's Corner: Thoughts for Training Readiness," TRADOC G2 *Red Diamond* Newsletter, April 2014.

Jennifer Dunn is a civilian intelligence specialist currently assigned to the TRADOC G-2. She is the Deputy Director for one element of the G-2, ACE Threats Integration, and specializes in threat representation in Army training, education and leader development, and capabilities development programs. Her office is responsible for helping TRADOC describe the strategic environment and developing a composite threat model to be incorporated into Army training. As a member of the Army intelligence community, her office also specializes in assisting the Army with training MI professionals.

The Unseen Target: What Trucks and Fishbones Can Teach Us About Intelligence Analysis

by First Lieutenant Jeff Yao

This article does not imply any endorsement by the U.S. Army, the U.S. Army Intelligence Center of Excellence, or any U.S. government agency.

Talent hits a target no one else can hit;
Genius hits a target no one else can see.
–Arthur Schopenhauer

The human brain is hard-wired to react. The truly innovative, the undeniably original, the deep thinkers and lofty dreamers of this world are the exception rather than the rule. Most of us still react to threats rather than anticipate them, driven by a relentless, deeply ingrained tendency to let our heuristics control us rather than the other way around. Even within the intelligence community, we are not immune to the subconscious shortcuts that serve us so well in day-to-day life, but fail us so spectacularly when the stakes are highest.

In the spring of 2015, 1st Battalion, 8th Infantry Regiment, left the shadow of Pike's Peak just as the snows around Fort Carson began to melt, landing at Camp As Sayliyah in the deserts of Qatar. Now, this deployment was not one characterized by the ubiquitous dread of an improvised explosive device (IED) detonation on the next patrol down the streets of Mosul, or the headaches of maintaining ground lines of communication stretched thin across the punishing wadis of Kandahar, but that's not to say it was a complete cakewalk. Qatar presented its own challenges. In a region with porous borders, international threats, and close alliances, the security of your neighboring nations is inextricably tied to that of your own. Furthermore, our regional responsibility competed with our local focus as we attempted to tip-toe around a diplomatically sensitive intelligence environment, foster strong relationships with an unfamiliar higher headquarters, and clearly define the purpose and identity of a deployment that, at first blush, seemed suspiciously like a garrison environment.

Our staff rose to meet these challenges, but just as we began to hit our stride, the terrorist group formerly known as ISIS declared a "month of disaster" during Ramadan, and the world was shocked by near-simultaneous terror attacks across three separate continents on what has been dubbed Bloody Friday, 26 June 2015. In the flurry of activity following this event, I had my first look at analytical target fixation.

One of the attacks was the suicide bombing of a Shia mosque in Kuwait City not far from the installation to which our parent brigade deployed. Following the incident, several Emergency Action Committees were called, and during one of these, in the scramble to make sense of the events, some analysts latched on to Shia mosques as targets. Other parties unquestioningly followed suit; analysis quickly began on nearby Shia mosques, their proximity to locales frequented by our Soldiers, and precautionary measures to take. Whether or not Shia mosques represented a true threat is unimportant–they very well may have been the most attractive targets for Sunni extremists, and could have been a valid point of focus. However, the tunnel vision reactivity to a solitary event and the group-think that took place, insidiously as always, is of concern.

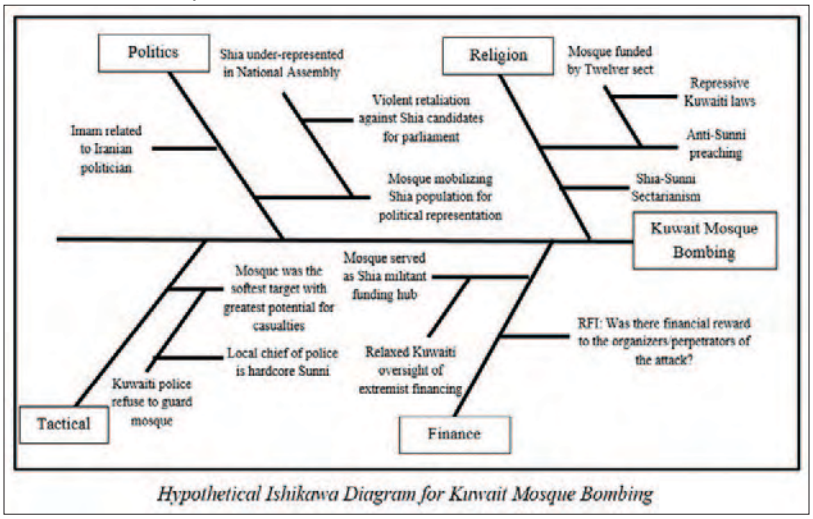
As analysts, our job is not solely to excavate meaning from historical data, but also to forecast for our commanders the threats of tomorrow, as protean as they may be. So how did this group of analysts, rigorously trained, dangerously intelligent, and with over 50 years of experience between them, fall victim to some of the most basic biases as laid out by Kahneman, Tversky, and others?[1] Furthermore, how do we prevent it?

The answer to the first question is covered extensively in Kahneman's treatise *"Thinking, Fast and Slow."*[2] In short, heuristics and cognitive biases are critical to daily functioning, and they invisibly affect our decision making whether we like it or not. The answer to the second question, however, is much more interesting and useful to us. There is already a glut of literature on analytical techniques. Richards Heuer in particular has formalized a wealth of structured techniques, while several authors have provided intriguing multidisciplinary elaborations on his work.[3,4] However, I sought something simpler, something that could be immediately and generally applied to examination of events "right of boom." This method had to be foolproof; it had to be implementable with few to no resources, and it had to

offer insights substantially better than those resulting from the unguided (albeit generally well-informed) discussion that is all too common in intelligence work. And that's when I found the 5 Whys, a strategy known for its use by Toyota Motor Corporation.

It's unclear who codified the 5 Whys. A press statement released by Toyota itself states that Taiichi Ohno pioneered the technique, while other sources attribute its development to Sakichi Toyoda.[5,6] Regardless of its source, its utility to the company is without question. Ohno wrote that the method formed "the basis of Toyota's scientific approach," and the technique has been co-opted into other corporate methodologies, such as Six Sigma and lean manufacturing.[7] The approach is beautifully Japanese in its elegance and simplicity: When confronted with a problem, ask "Why?" Then ask "why" again. Then again. This iteration of causal back-tracking leads the analyst inexorably towards the root cause of the issue. Five times is a guideline; more or less may be required. In some cases, asking five times leads to a nonsensically reductive answer, while in others, deeper digging may be required. As simple as this solution may sound, its power should not be underestimated.

In implementation, a method detailed by Toyota Production System teacher Karn G. Bulsuk would be particularly effective for a complex task such as intelligence analysis.[8] Bulsuk recommends an Ishikawa diagram, also known as "fishbone diagram" or, whimsically, "Fishikawa diagram," a fictional example of which is below.



Hypothetical Ishikawa Diagram for Kuwait Mosque Bombing

The problem is placed on the right end of a fishbone structure. In this instance, our problem is a suicide bombing on a mosque in Kuwait City. We ask ourselves the first why: Why did ISIS bomb this mosque? Along the spines of the fishbone, we answer this question by developing several causal categories. Religion is almost certainly a factor, given the target of the bombing. Political agenda, financing, and tactical considerations are potentially others. Focusing on one causal category, we ask: Why did religion motivate ISIS to bomb the mosque? From this query, we can identify second-order causes, or, in the case we encounter an intelligence gap, we write ourselves a request for information (RFI). "ISIS, a Sunni, and potentially Salafi, extremist group harbors enmity for Shia apostates" seems like an obvious answer, but are there other religious motives at play?

From this point, we deviate into a hypothetical situation for the sake of explanation. Say there were reports that the imam at the mosque preached an anti-ISIS or anti-Sunni message. Upon responding to this finding with "Why?" we discover that Iranian Twelver organizations provided funding for the construction of the mosque. And once more, "Why?" This persistent investigation leads us ultimately to find that the political atmosphere in Kuwait marginalizes Shia citizens and organizations, leading to radicalization funded by foreign entities with a vested interest. These causes or RFIs branch off of the causal category, and are themselves stems for deeper cause branches. We continue to ask "why?" in response to our answers, eventually creating a rich, granular, and holistic tabulation of the potential causes and contributing factors to our problem.

In his discussion of the 5 Whys, Ivan Fantin elaborates that the eventual root cause(s) must be a process that is in some way broken.[9] In a context other than the industrial, the root cause must be something over which we have some level of control. If the root cause for our failure to detect an IED before it occurred was a lack of time, resources, or manpower, then the utility of our analysis is limited. These problems cannot be easily fixed, nor is their resolution within the lane of the intelligence warfighting function. Similarly, if the root cause we arrive at through iteration in the mosque bombing example is that the Sunnis despise Shias due to contentions over the Prophet Muhammad's succession in 632AD, our ability to solve millennia of animosity is a dubious proposition at best. Instead, we must direct the questioning toward potentially solvable issues. If the root cause for a failure to detect an IED was because we didn't conduct route reconnaissance, or the convoy plan was miscommunicated to the route clearance package, or our Soldiers were not vigilant due to an unsustainable operational tempo, then the 5 Whys have yielded concrete recommendations for our commander.

This technique's strength lies in its simplicity. Nothing is needed other than paper and pen for participants who desire visual representation. The discussion is natural–

hypothetical narratives don't need to be constructed from limited understanding of complex situations. Instead, the attempt to answer the question "Why?" drives the analysis from the concrete immediacy of the event toward the abstraction of the causes, writing intelligence requirements along the way when confronted with uncertainty. Additionally, the very act of questioning, of inquisitive challenging, breaks down the bandwagon, and creates a healthy competitive environment that fosters criticism and defense of ideas as opposed to abject concurrence. Finally, the method is robust; there are virtually no situations in which a deeper understanding of contributing factors would be insignificant to analysis, and this formalized method ensures at least some degree of that depth for almost any given problem set.

As powerful as the "5 Whys" technique is, it is not meant to serve as the sole analytical technique used. Common techniques such as challenging assumptions are still useful. Was it really ISIS that bombed the mosque, or were they claiming credit for a successful but unrelated lone wolf attack? So too is the Analysis of Competing Hypotheses; the branching theories of root causes lend themselves particularly well to comparison using Heuer's venerated system. However, used in conjunction with, or as a basis for other techniques, this system provides an efficiently structured method of creating narratives useful to development of practical recommendations that otherwise may never have been considered. Therein lies the genius, identified decades ago by a company that makes trucks. By illuminating the invisible, and short-circuiting our mental shortcuts, the "5 Whys" helps intelligence analysts hit the targets that no one else can see.

Endnotes

1. Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science*, New Series, Vol. 185, No. 4157. (Sep. 27, 1974), 1124-1131.

2. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus, and Giroux, 2011).

3. Richards J. Heuer, *Psychology of Intelligence Analysis* (Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency, 1999). At https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf.

4. Valtorta et al. propose a synthesis of Heuer's Analysis of Competing Hypotheses with Bayesian networks, while Pope and Jøsang utilize subjective logic calculus to attempt to address perceived shortcomings in human reasoning.

5. Taiichi Ohno, *"Ask 'Why' Five Times about Every Matter,"* March 2006. At http://www.toyota-global.com/company/toyota_traditions/quality/mar_apr_2006.html.

6. Olivier Serrat, "The Five Whys Technique," *Knowledge Solutions*, February 2009, 30-32. At http://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1200&context=intl.

7. Taiichi Ohno, *"Toyota Production System: Beyond Large-scale Production,"* 1978. At http://www.ce.berkeley.edu/~tommelein/lci/tps_ono.pdf.

8. Karn Bulsuk, "Using a Fishbone (or Ishikawa) Diagram to Perform 5-why Analysis." At http://www.bulsuk.com/2009/08/using-fishbone-diagram-to-perform-5-why.html.

9. Ivan Fantin, *Applied Problem Solving: Method, Applications, Root Causes, Countermeasures, Poka-Yoke* and A3, 92-110.

1LT Yao is currently the Collection Manager, HHC, 3rd ABCT, 4th Infantry Division, Fort Carson, Colorado. Previous assignments include Battalion Assistant Intelligence Officer, HHC, 1-8IN, 3ABCT, 4ID, Fort Carson. He is a graduate of the U.S. Military Academy with a BS in Economics and the MI BOLC, Fort Huachuca, Arizona.

Red Diamond
Threats Newsletter
TRADOC G-2 Operational Environment Enterprise
ACE Threats Integration
Fort Leavenworth, KS Volume 7, Issue 03 MAR 2016

Modeling Violent Extremist Organizations Using Existing Doctrinal Threat Models

by MAJ Jay Hunt and Jerry England (DAC), TRADOC G-2 ACE Threats Integration

During one of the discussions in the December 2015 Decisive Action Training Environment (DATE) 3.0 Working Group meeting, several of the attendees voiced a need for a threat model that mirrored the Islamic State of Iraq and the Levant (ISIL). Their main objection to the existing hybrid threat models depicted in the Training Circular (TC) 7-100 series was that they were either purely guerrilla forces or purely insurgent. The working group expressed a desire to create a doctrinal model for a new "thing like ISIL."

The Hybrid Threat (HT) Force Structure is a composite model of threat capabilities that can be used for training and developmental purposes. This collection of models is the foundation of the military forces in DATE and is used across the Army as a consistent and doctrinally-aligned training tool. The very nature of the HT presents unique challenges for commanders that want to train their forces against current and emerging threats. This is particularly evident as exercise designers grapple with integrating the characteristics of violent extremist organizations (VEOs) such as ISIL.

Initial Steps: ACE-TI Approaches to the Hybrid Threat

The first order of business by ACE Threats Integration (ACE-TI) was to review the existing approved doctrine publications—primarily the TC 7-100 series. The desired organization required by users was similar to parts of both the guerrilla and insurgent models. These two organizations would serve as the base unit. To minimize the reinvention of the wheel, a modified guerrilla/insurgent model would streamline doctrinal approval and adoption.

One of the explicitly-stated needs by the users was an organization that included improvised explosive devices (IEDs) as a primary weapon in its structure and tactics. The cells within the HT local insurgent organization do not include a specific IED cell, but there are direct action and multi-functional cells that could serve this purpose. Further reading in the description of these elements' tactics explicitly includes their use of IEDs.

What Questions Need to be Answered?

As with most user requests, the requirement was intended to address specific unanswered questions. Agreements about the application of a newly-designed threat force structure for training should be clearly understood by both the user and ACE-TI to meet the requesting entity's intent.

Consensus among the working group participants revealed the following distinguishing characteristics that would best describe a VEO like ISIL:

- The VEO functions like a local insurgency, but is managed and enabled like a franchise of a larger enterprise in respect to direction, identity, and specialized capabilities,
- The VEO operates a military element that is capable of projecting significant, mostly-conventional elements; this armed force can appear to change from near-invisibility to juggernaut and back almost magically,

- ✦ Combat losses cause little apparent effects, and
- ✦ Local populace acceptance and/or participation levels creates few problems for the VEO.

The DATE 3.0 Working Group initially appeared to be correct in its belief that the HT did not effectively portray a VEO similar to ISIL. The questions by the participants about the structure and behavior of this organization were similar to those expressed about ISIL by military and civilian analysts. Analysis of open sources provided ample material on its high-level leadership organization. Most of the writings included obligatory line and block charts and contained a high degree of certitude about their conclusions. The other bulk of writings leaned toward the tactical end of the spectrum, with a range of details and horror stories of invincibility.

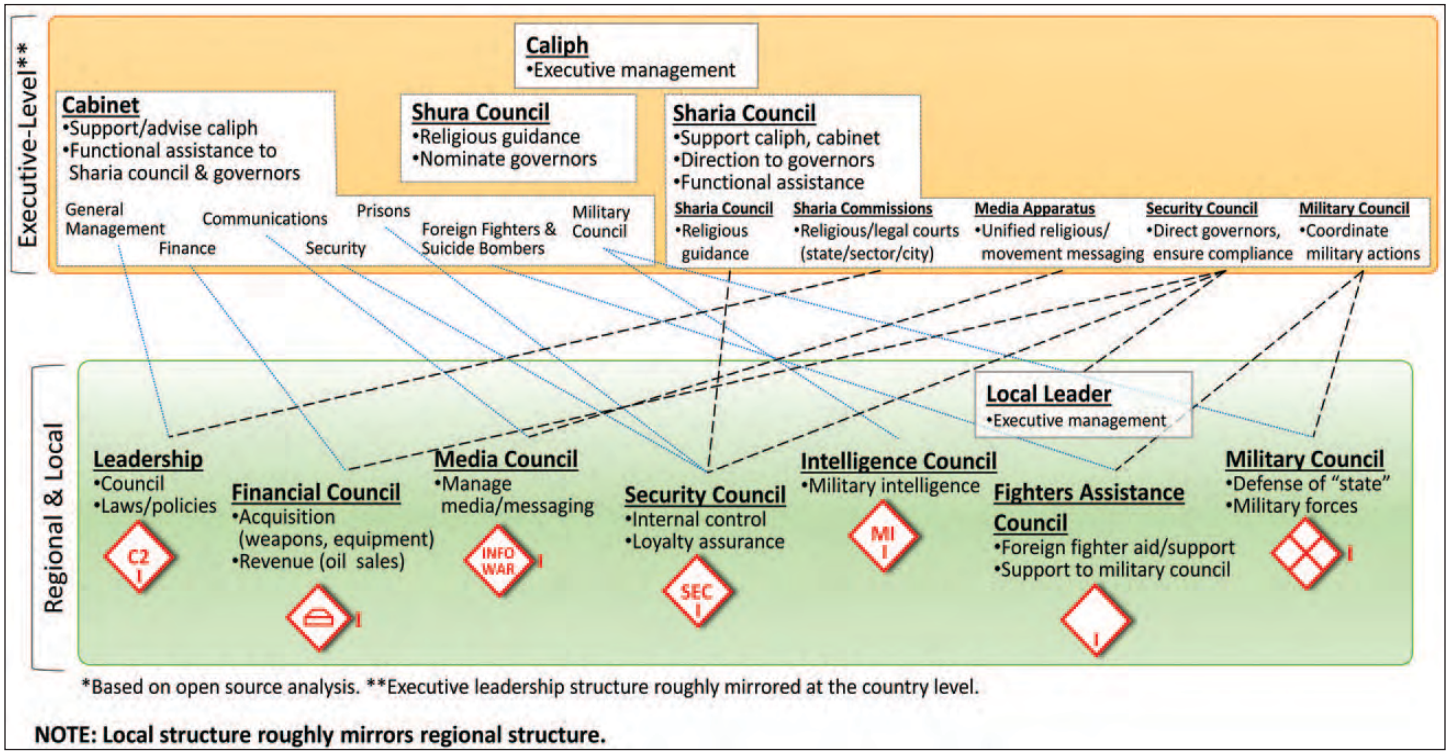


Figure 1. Notional functional leadership of higher-affiliated violent extremist organization.

The key task was not to exactly replicate ISIL, but to create an organization that possessed similar organizational and capability characteristics that could be used within the DATE environment and other approved training mechanisms. Any insights ACE-TI gained through the development of this organization would be added-value.

For the purposes of modeling the HT in a training environment, ACE-TI narrowed the questions it needed to answer to three:

1. How does this VEO function locally, regionally, and even nationally or trans-nationally?
2. How does the VEO convince the populace to tolerate or support it?
3. How does the VEO create armies from almost nothing, deploy them in large numbers, and then have the force disappear?

Mapping HT Force Structures as a Method

The main HT structures that were initially examined were the local insurgent organization and the guerrilla battalion. Detailed analysis concluded these organizations contained most of the capabilities inherent in ISIL organizations that were needed in the HT.

These organizations portray many of the force projection and direct action capabilities needed at the local levels, but lack the necessary enabling capabilities found in VEOs like ISIL. The influence and specialized capabilities of the higher insurgent organization were needed in the new VEO model. Below is an example of a possible VEO organization. It fields a variety of local forces, aligned and enabled by the leadership, and features specialized capabilities of the higher insurgent organization:

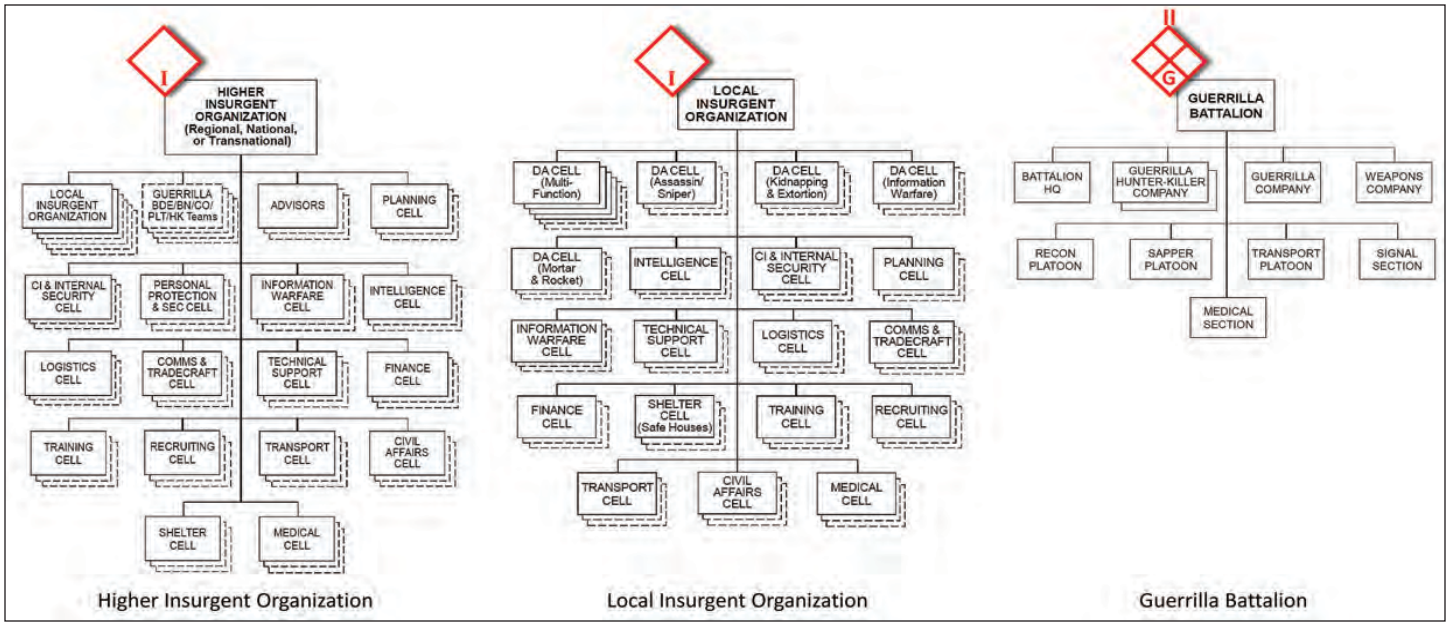


Figure 2. Relevant doctrinal OPFOR models.

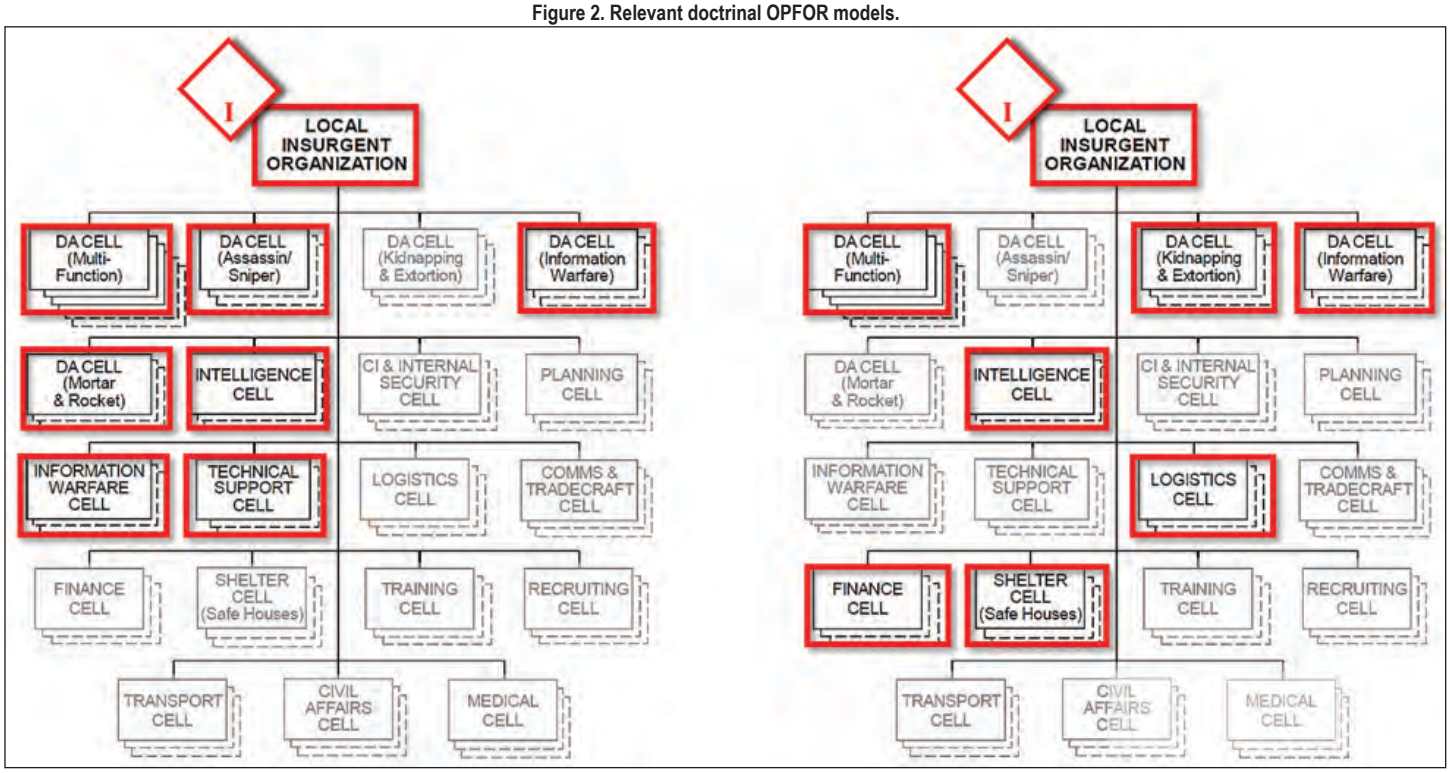


Figure 3. Example modular structure mapping of doctrinal OPFOR models.

This collection of existing threat models meets the requirement of an external leadership and enabling element that leverages ideological adoption and force capabilities of local elements for its own purposes. This is not actually a new organization, but a modular task organization of the structures described in TC 7-100.3, Irregular Opposing Forces, paragraph 2-21. The modularity allows for consistency and on-demand support for the local elements, while the allegiance and readiness of the local franchises supports the parent organization's perception management and force projection needs.

Aligned and Enabled. One of the major differences between ISIL and al-Qaeda is ISIL's ability to maintain control of invaded areas. Conquering is easier than ruling. ISIL's ability to seize and then hold terrain has been, so far, essential to its staying power. The combination of propaganda, influence maneuvering, and normalizing its presence keeps the populace just under its reaction threshold and facilitates positive control of the civilians. The higher organization, through its apparatus of internal intelligence and control, is able to identify and supply where it needs additional controls. This enabling function is key. Some locales may need technical assistance. Others may need additional forces to motivate a local militia.

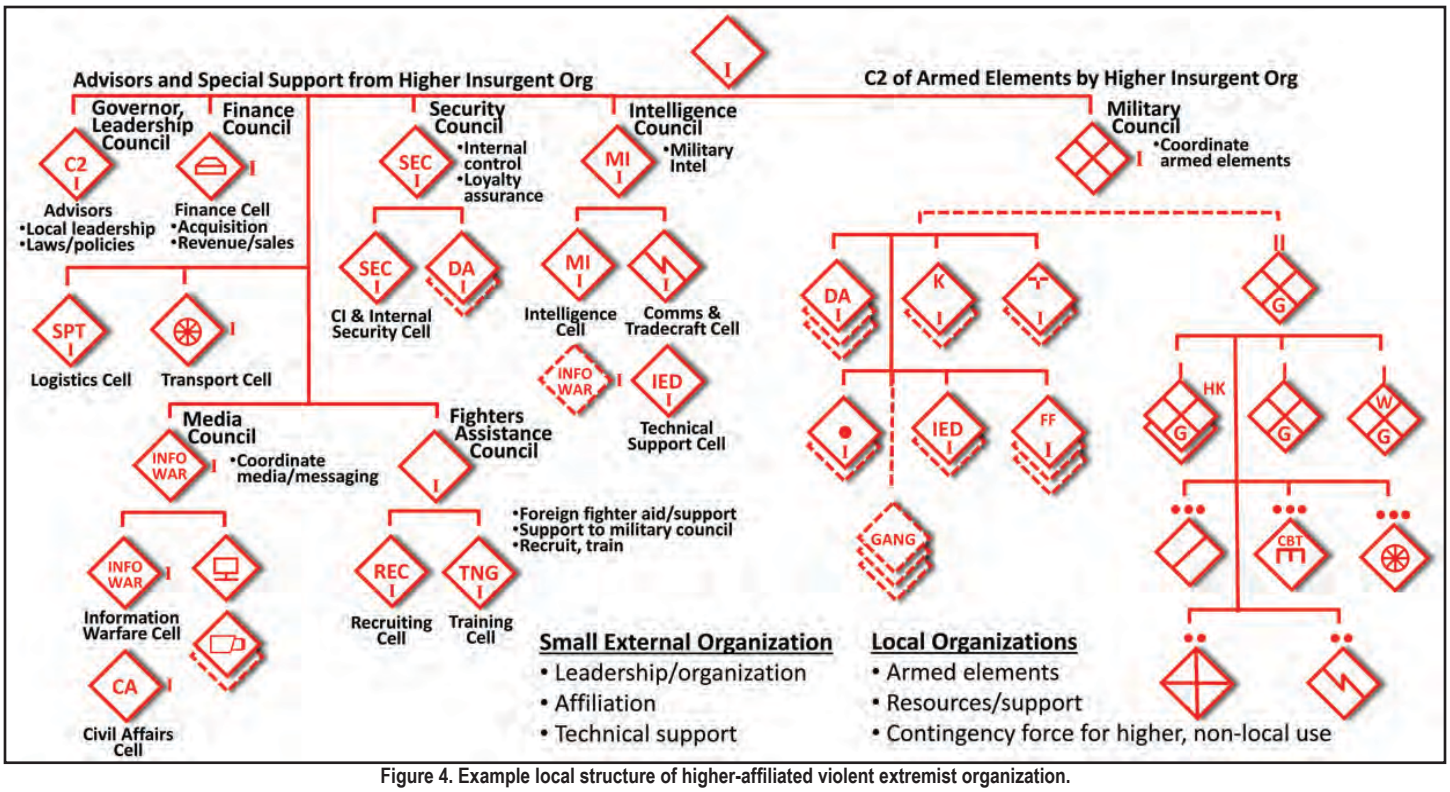


Figure 4. Example local structure of higher-affiliated violent extremist organization.

Still others may need assistance for civil control and management. Fighting as an insurgency while operating as an enterprise has been a key differentiator for ISIL.

Local Insinuation. ISIL appears to have a significant and long-term internal-control and loyalty-assurance process. Over a period of months—sometimes years—ISIL infiltrates, insinuates, and integrates itself into local life through intentional low-reaction activities such as marriages and participation in community groups, mosques, and local armed groups. ISIL operatives normalize their presence and identify potential allies and enemies. The VEO can then effectively maneuver, groom, corrupt, motivate, or kill its way into actionable positions of influence. By the time the local population starts realizing ISIL is in its midst, it is too late for the civilian populace or local government to resist.

Ghost Army. One of the most difficult issues was how could this VEO deploy a combat force in the thousands, take casualties, and then disappear. If the VEO masses in significant numbers for very long, the group becomes a target for conventional forces on the other side. The ACE-TI solution was to make the parent organization use the local affiliates as expeditionary forces. Militias and other local armed groups would receive orders to temporarily deploy alongside similar elements from other locales. Consistent uniforms, flags, and symbols give the impression of a singular force. As with the ancient Persian Immortals, these forces could take significant casualties with little noticeable degradation.[1] When the mission objectives are sufficiently achieved, the elements return to their home locales.

Armed elements deployed for a common purpose and directed from the parent organization may fight alongside each other, but may be unlikely to integrate with each other. Equipment and tactics may be unique to a particular formation or area. This might facilitate identification of individual groups and possible vulnerable divisions between the various groups for tactical exploitation by the VEO's opponents.

A sophisticated propaganda campaign enables ISIL to multiply the effects of its brutality. Beheadings, mass executions, and parades of armored vehicles in action gives the impression of tactical progress to ISIL fighters on the ground, potential recruits, and donors. The images in social media do not necessarily reflect events throughout the groups' territory, but support the narrative of a comprehensive system that is in control and ready to deal with dissent.

End State

The end state of this process was an organization that roughly mirrors a real-world threat and leverages the existing HT force structures. This model answers the original questions posed by the DATE 3.0 Working Group without creating a completely new structure.

This model is a work in progress, but it does illustrate the idea that exercise designers can modify existing HT force structures to model specific real-world threat actors. The doctrinal threat models are only a toolbox. Trainers and developers possess some flexibility, but should always try to use organizations that already exist in the HT force structure. The use of standard force structures improves consistency between training exercises, maintains alignment with DATE, and simplifies integration with the simulations community. A more refined and detailed version of this VEO will likely be incorporated into the next version of DATE and related exercise mechanisms. In DATE-speak, it may become the foundation of an "Atropian Caliphate."

References

Barrett, Richard. "The Islamic State." The Soufan Group. November 2014.

Engel, Pamela and Michael B Kelly. "ISIS Commander Reveals How The 'Caliph' Radicalized Under American Detention In Iraq." Business Insider. 11 December 2014.

Glenn, Cameron. "Al Qaeda v ISIS: Leaders & Structure." The Wilson Center. 28 September 2015.

Headquarters, Department of the Army. Army Doctrine Reference Publication 1-02, Terms and Military Symbols. 2 February 2015.

Headquarters, Department of the Army. Training Circular 7-100.3, Irregular Opposing Forces. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 24 January 2014.

Headquarters, Department of the Army. Training Circular 7-100.4, HT Force Structure Organization Guide. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 4 June 2015.

Ingram, Haroro, "Why we keep getting snared in Islamic State's propaganda trap." The Conversation. 21 January 2016.

Raqqawi, Abu Ibrahim. "How Can ISIS Continue Achieving its Slogan 'Stay and Expand'." Raqqa is Being Slaughtered Silently. 30 June 2015.

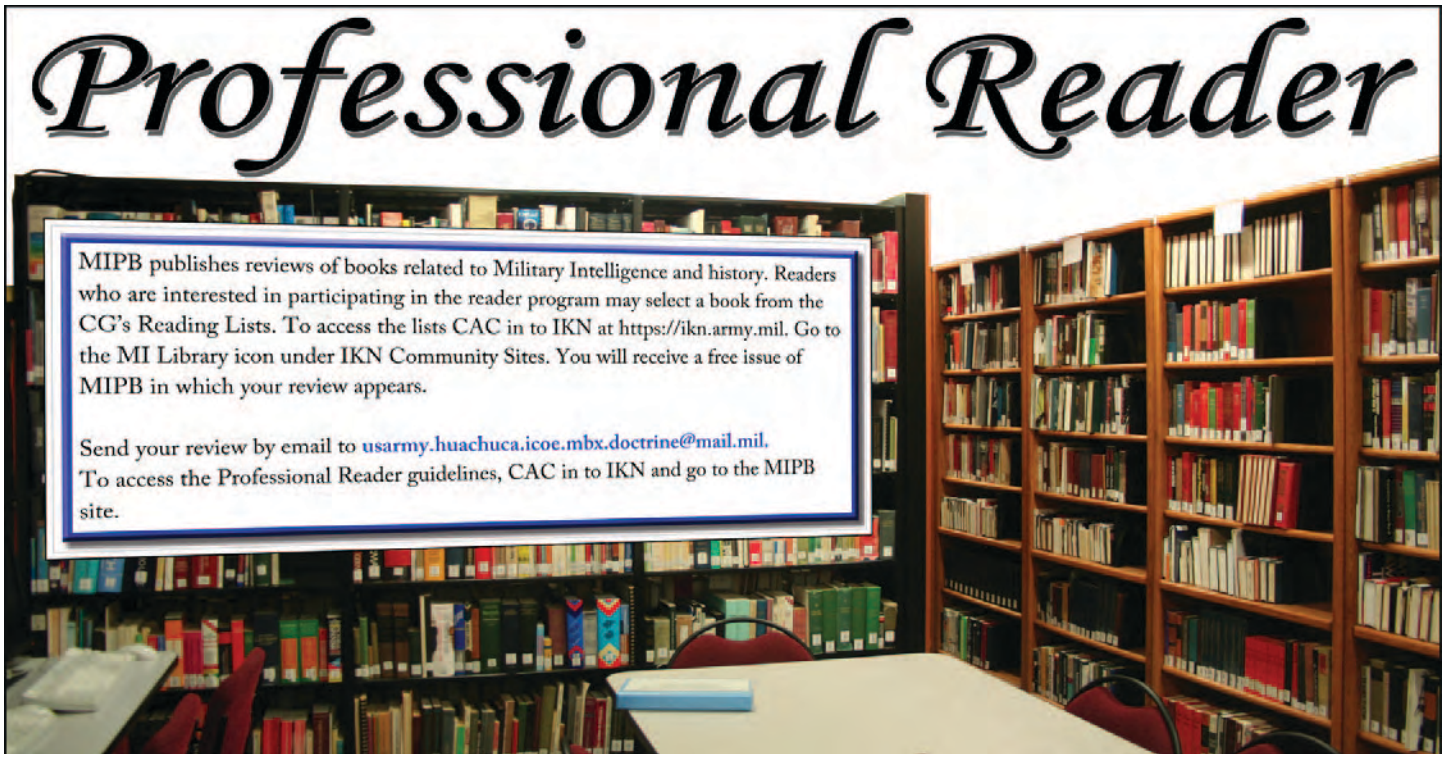
Thompson, Nick and Atika Shubert. "The anatomy of ISIS: How the 'Islamic State' is run, from oil to beheadings." CNN. 14 January 2015.

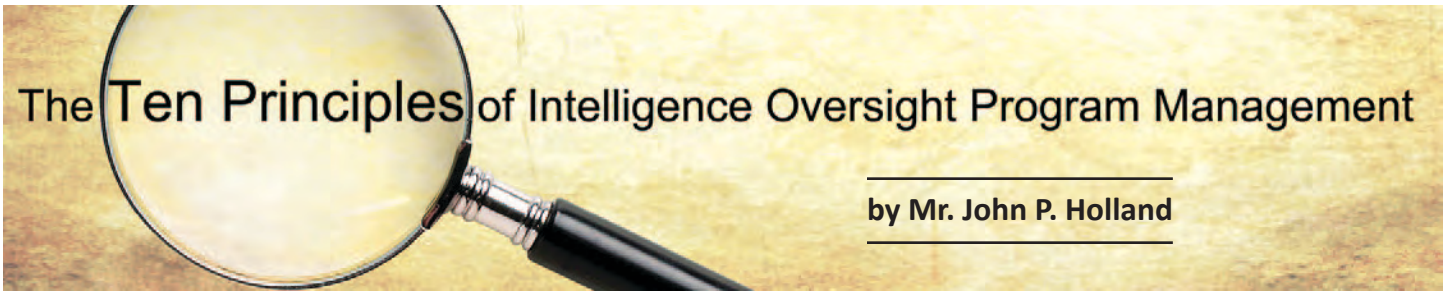
Endnotes

1. M.R. Reese. "The Immortals: An elite army of the Persian Empire that never grew weak." Ancient Origins. 13 November 2014.

MAJ James (Jay) Hunt is a strategic intelligence officer currently on temporary assignment to TRADOC from CENTCOM ARE Detachment 7. His more than 26 years in service spans assignments from intelligence analyst in active duty maneuver units to national-level intelligence organizations.

Jerry England has been an Intelligence specialist with the TRADOC G-2 since 2008. His specialty is in threat information warfare and order of battle analysis for Army training.





The Ten Principles of Intelligence Oversight Program Management

by Mr. John P. Holland

1. Take assigned responsibilities seriously. While there is a range of additional duties from Safety to Equal Opportunity begging for the attention of the command, only one has two Presidential oversight boards and sub-committees in the U.S. Senate and U.S. House of Representatives, and is unique to Military Intelligence (MI) units–Intelligence Oversight (IO). IO has been the focus of numerous investigations and inquiries from simple command level inquiries to national level with Congressional implications. All questionable intelligence activities (QIA) find their way to the Army Inspector General (IG) who personally reads them all. Needless to say, take it seriously –there is a lot at stake here.

2. Do not appoint the brand new second lieutenant (2LT) as the unit Intelligence Oversight Officer (IOO). It is common practice to groom junior officers by giving them additional duties. It is a great way to teach them the myriad duties necessary to run a unit. It places them in positions to lead, demonstrate initiative, and grow as officers. However, Intelligence Oversight is not one of those developmental opportunities. *Army Regulation 381-10 Intelligence Oversight*, requires commanders to appoint "an experienced MI professional" as the unit IO officer. The problem is that a 2LT is not "experienced." It simply takes years of directing intelligence collection efforts, reading the ensuing intelligence reports to correctly apply the rules under Procedure 2 and 3 and make dissemination determinations under Procedure 4. This is particularly difficult in sensitive open source platforms and in signals intelligence (SIGINT). There is a reason that the National Security Agency requires all employees complete rigorous IO training and possess years of experience before the employee is certified as an IO officer. A new 2LT, not yet familiar with the collection power in an MI unit and how to assess the U.S. Person information it may include, is not the best choice when there are experienced warrant officers and U.S. Government civilians available. Appointing a senior military or a Department of the Army civilian experienced in their craft, preferably across a broad range of intelligence operations, will pay dividends. Additionally, IO is an inherently governmental function that cannot be performed by a contractor.

3. Foster a culture of compliance and oversight. Every MI unit has its own culture. It is a combination of many things: the unit's history, morale, recent deployments, mission, personnel turn-over, and leadership. Some units have a culture reticent to report any QIA or significant/highly sensitive incidents. The rational may be that unit leaders do not want any perceived mistakes on their watch. As a result they often do not report any QIA, or at the very least do not contact higher to discuss collection issues that have a high chance of U.S. Person data being included. This is contrary to intent of *DOD 5240-1R Procedures Governing the Activities of DOD Intelligence Components that Affect U.S. Persons.* Reporting QIA and significant/highly sensitive matters demonstrates a command's ability to self-regulate and handle the collection authorities it has been given. Fostering a climate of reporting is critical to protecting those mission authorities and can be used as justification for requesting additional collection authorities. Furthermore, IOOs have to often question the risk-to-reward ratio of new intelligence collection platforms. Many new open source intelligence (OSINT) platforms are expensive, redundant, and venture into areas that the public and policy makers have not fully codified their positions regarding the intelligence community's access. This requires someone to ask difficult and unpopular questions at a staff meeting regarding not only the information's value, but how it is to be collected.

4. Automate questionable activity reporting. AR 381-10 allows 5 days to report a QIA. Time is critical in reducing the impact of such incidents. Many units have an automated reporting tool using MS SharePoint on SIPRnet. Some units opt for a reporting tool that is an email alias to key staff members, the IOO and the Staff Judge Advocate (SJA). Regardless of the method, automating the reporting method speeds up the reporting process, increasing accuracy and accountability while providing an auditable process. Most importantly–it shows command involvement.

5. Tailor your training to unit mission and authorities. Simply using a canned set of PowerPoint IO training slides from another unit, briefing them, and checking the proverbial box complete is absolutely the wrong way to conduct IO training. Just like any other training, IO training should be tailored to reflect the unique intelligence processes within the unit, or more importantly how the unit actually conducts intelligence collection, processing, maintaining intel-

ligence databases, and the dissemination decision points. Training slides value increases when the unit's intelligence section real names (i.e., the "ACE" or "OSINT Shop") and the names of key positions (i.e., G2 Night Shift "Pit Boss" or ACE Chief) are used. Furthermore, IO training should include examples of potential QIA using examples drawn from the local collection platform capabilities. In short, training customization increases applicability of the lessons and hopefully the likelihood of recognizing a QIA and reporting it.

6. Read and study. No doubt reading a National Security Directive such as *PPD-28 Signals Intelligence Activities* will induce a near comatose nap. However, to be a true intelligence professional, it is crucial that you read, understand, and apply the rules. Simply put: if you don't read them–you won't know them. Start with *AR 10-87 Army Commands, Army Service Component Commands, and Direct Reporting Units*, and your unit's authorizing mission documents to determine if you are authorized to collect "raw" intelligence or merely read published intelligence reports. Read *EO 12333 U.S. Intelligence Activities*, and match its sections with corresponding sections in DOD 5240.1-R and then AR 381-10. Doing so will allow you to see the application and intent of each procedure as it has worked its way down from the President, through the Secretary of Defense to the Sectary of the Army. For SIGINT personnel, read EO *13587 Foreign Intelligence Surveillance Act*, and applicable U.S. SIGINT directives. For Human Intelligence, the readings should include Defense Intelligence Agency policies. Counterintelligence practitioners should read *AR 381-20 The Army Counterintelligence Program*.

7. Ensure access to unit operations orders, intelligence reports, and intelligence databases. Prior to execution, all operations orders should be reviewed by the unit IOO and the SJA. It is far better to prevent a QIA than to go through an investigation later. Too many MI unit IOOs do not routinely check the intelligence reports their units produce or question the dissemination of U.S. Person information their analysts are getting access to and retaining with no thought to the relevance to the unit's foreign intelligence or counterintelligence mission. Again, appointing a seasoned MI warrant officer with full access to the unit databases, intelligence reporting, and all intelligence platforms, to include special access programs can prevent QIAs. Special attention should be paid to open source programs. Remember, conducting the annual files review of unit databases is required by Army Regulation 381-10.

8. Request the Inspector General inspect your IO program. *AR 20-1 Inspector General Activities*, requires the command IG inspect intelligence unit's IO program every 2 years. Acting a disinterested third party, the IG can give an MI unit commander an honest assessment of his IO program and will share best practices learned from other MI units. MI unit commanders should ask to see the previous IG inspection report completed on their unit to determine if the recommendations and finding were implemented. The IG is a valuable asset in running an effective IO program.

9. Map out the intelligence reporting data flow. Data is best visualized like plumbing in a house. Like water, all that intelligence data is going somewhere and is contained in something. Chart the process by which intelligence is collected from the field, processed, analyzed, and the products created and disseminated. Identify where the control measures and internal review processes exist at all levels. Some IOOs have been amazed once they drew the intelligence data flow on a dry-erase board and saw all the intelligence "databases" that grew from a spreadsheet to a system of record. Simply drawing out the intelligence data feeds and following them through the unit's processes, and then out of the unit to customers and labeling the associated authorities at each collection point can be very telling.

10. Leave a legacy. Too frequently what were once very effective IO programs are now dead on arrival. What was the cause of death? The previous IOOs drove the program through the sheer force of rank or personality rather than institutionalizing the procedures of recognizing and following the rules and reporting QIAs. As a result, when they left the unit, the procedures were not modeled and passed on like a battle drill to the next group of Soldiers. Making IO part of the everyday operational considerations is the sure way to leave an endowment at every MI unit. IOOs should emphasize that QIA reporting is not punitive. The root cause may be with the policy that is inconsistent, incorrect, contradictory, or obsolete. The problem may reside in training (not done, incorrect, inconsistent, incomplete, not tailored enough to what Soldiers needed), or it may be communication (poor propagation of policies, incorrect command emphasis, failure to provide left/right limits). The issue may be with an individual who is willful, or negligent. The point is to review what went wrong, why it went wrong, and enact measure to prevent recidivism and foster a climate of continuous improvement.

Mr. Holland has served as the DOD Senior Intelligence Oversight Official since August 2015. His former DA civilian positon was Deputy Intelligence Oversight Advisor to the Commander, U.S. Army Intelligence and Security Command. He is a retired U.S. Army MI officer, having served in various staff and command positions for over 20 years and served in Operations DESERT SHIELD/STORM and with the JCIU, Afghanistan. He is graduate of CAS3, Command and General Staff College, and the Information Resources Management College, National Defense University. He holds graduate degrees from Webster University and Liberty University, and is a 1986 Distinguished Military Graduate of Elon College.

Doctrine Corner

by Martin C. Meadows

Identity Activities

Introduction

We are all familiar with using identification cards to verify people's identities. When credible identification cards are not available, we can use 'biometrics' to identify people. JP 2-0 Joint Intelligence, defines biometrics as "The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics." We have collected and compared specific physical characteristics, also called 'biometric modalities' (e.g., DNA, finger- and palmprints, iris images) for years and this capability has proven to be very reliable and beneficial. These specific modalities are selected in part to automate the collection and analysis of unique individual biometric signatures. In addition to those 'measurable' physical characteristics, identification attributes also includes observable physical characteristics (e.g. hair color, eye color, build, complexion), biographic, reputational information, and behavioral traits and characteristics.

Identity activities can be described as a collection of functions and actions that appropriately recognize and differentiate one individual from another to support decision making. These functions and actions include:

- Collection of biometric signatures and physical materials.
- Processing and exploitation of biometric signatures and physical materials.
- Inclusion of this information into all-source analytic efforts.
- Production of identity intelligence (I2) and Department of Defense (DOD) law enforcement criminal intelligence products.
- Dissemination of these products.

Identity products inform the command and staff, influence operational planning and assessment, strengthen precision targeting, and promote decisive action at the point of encounter. These functions and actions are integrated across joint, interagency, and multinational partners.

Identity activities are applicable across all warfighting functions. Most DOD service members, civilians, or contractors who come into direct contact with foreign nationals during the course of their duties may need to identify and characterize those encounters, enroll new encounters, or use identity information to support their missions. Identity activities are conducted to establish an unknown individual's identity or confirm a previously encountered individual's identity. Identity activities enhance many combat tasks across the warfighting functions, examples include, but are not limited to:

- Combat arms Soldiers manning checkpoints, performing cordon and searches, patrols, raids, personnel recovery operations, or distributing humanitarian relief.
- Military Police interacting with criminals, informants, victims, witnesses, detainees, internees, refugees, displaced persons, or evacuees.
- Military Intelligence personnel interacting with counterintelligence or human intelligence sources.
- Supply officers vetting local national and third party personnel hires or vendors.
- Medical or dental personnel tending to humanitarian assistance or disaster relief patients.
- Any Soldier performing guard duty to control access at forwardly deployed military facilities.

Applying Identity Activities to all Phases of Operations

Identity activities are also applicable across all phases of operations. Ideally, during phases zero and one, identity data sharing agreements are coordinated with other U.S. government agencies and multinational partners, and identity databases and supporting communication architectures are developed. At the same time, the conduct of identity activities during these phases can support U.S. and multinational military operations. It may also send a signal to potential adversary or enemy personnel that they will not be able to easily act against friendly forces' or our interests.

During phases three and four, conducting identity activities should make it harder for the enemy to traverse the area of operations (AO) without being identified by U.S and multinational forces, and help deny adversaries and enemies access to personnel, facilities, equipment, critical infrastructure, sensitive cultural sites, resources, and vulnerable populations. Identity activities bring attribution while they disrupt

deception and disinformation. They help to disrupt the enemy's ability to conduct sabotage, subversion, intimidation, coercion, and criminal activities within the AO. Adversaries who might have been able to act freely and with anonymity, may now have to spend additional time and resources to conduct their activities while at the same time trying to remain hidden. Their ability to easily form opposition groups and networks should be significantly curtailed. Conversely, identity activities can significantly increase friendly force targeting and detention activities.

During phase five operations, friendly forces can use identity activities to aid in the identification of key leaders who must be engaged to sustain their friendly disposition, or who can be swayed to remain neutral or become even friendlier. We can also use identity activities to assist in the identification of those threat personnel who might be influenced to cooperate with friendly forces.

Differentiating Groups of People

We can use identity activities to distinguish groups of people. During most biometric enrollment encounters, detailed biographical information is also collected. Collecting the religious or tribal association of biometrically enrolled individuals can help identify the larger group to which they may belong. As well, noting specific tattoos or other identifying body marks on specific locations of the body can be used to associate people of the same group to one another. Similarly, wearing specific articles of clothing in a particular manner and at a specific location and/or time can be used to identify individual persons as belonging to a larger group of people.

Identity Attributes

At the tactical and operational levels, we collect and exploit biometric signatures to help authenticate the identity of both friends and foes we encounter. The use of facial images may be the most common method. (Think of how many identification cards have photos of their bearer's face.) Fingerprint and iris images are also frequently used. Analysts can also use biographic, behavioral, and reputational information to help identity or confirm the identity of people. Biographical information can come from personal communications or from identification documents. Behavioral information has to be observed. Reputational information can come from a local tribal elder, neighbor, local civilian police, or employer to vouch for the person's identity, skills or training (capabilities), associates, ethics, or extremist leanings.

Physical. Physical characteristics are the defining traits or features of the body which differentiate one individual from another. Collecting, processing, and comparing these characteristics provides the most consistent and accurate validation of an individual from a previous encounter. Relying solely on these modalities to identify someone requires previously collected samples of their modalities in order to have data to compare against. Without these comparative data samples, all that can be said is that the individual is not someone who was previously biometrically enrolled.

Biographic. Biographic information refers to an individual's educational, life, and work histories. We can use a person's biographic information to help identify their associations with other people, locations, and events, and to support other analytical efforts. Biographic information includes, but is not limited to an individual's:

- Full name (and any other names they may have used).
- Date of birth.
- Family members (mother, father, siblings, extended family members, spouse, children, etc.).
- Friends and associates.
- Current and previous residences.
- Current and previous work addresses.
- Places where someone has travelled.
- Membership, participation, or support of organizations and/or events.

Behavioral. Behavioral information refers to an individual's mannerisms or how they speak, walk, sit, stand, or dress, all of which can be used to aid in their identification. An individual's preferences, such as what they eat and/or drink, what books they like to read, or what movies they like to watch are also behavioral information. The way someone interacts with other people, such as their peers, seniors, subordinates can also be used to aid in identifying them. (Note: most people act differently in public, or when they are being recorded, than they do in a private environment. Similarly, most people act differently in professional settings than those which are less formal.)

Reputational. Reputational information refers to a formal or informal assessment by other people or organizations. This assessment may be based on either investigation(s) or experience(s) by the people or organizations making the assessment. Reputational information can include statements attesting or vouching for a person.

Collecting Contextual Data

An important part of collecting identity information is the collection of contextual data related to the 'enrollment.' An enrollment encompasses the circumstances associated

with the occasion during which a person's biometric modalities are collected, and why the person was selected for enrollment. Contextual data can provide important insight and understanding into why a person was enrolled. It also describes the location in which an enrollment occurred, such as at a checkpoint or during a cordon and search, and when a person was enrolled. Additional data that can be included as contextual data is whether or not the individual was alone when enrolled. Contextual data includes not only the situational information associated with an enrollment, but can also include the biographical characteristics of the person being enrolled.

For detainees, contextual data can include what pocket litter was found on them, what weapons they had, what uniform they were wearing, what other clothes they had, and what equipment they had when they were captured. It also includes the event in which they were participating or what activity they were performing when they were detained. It might also include whether or not they attempted to resist capture or provide false information. It can also include any statements they made, what language they were speaking, and their general attitude and disposition. It can include their overall physical appearance (such as visible injuries and/or tattoos), and what aid, if any, was given to them.

Planning for Identity Activities

Since identity activities can be used to support many different operations, commanders and staffs must carefully consider how identity activities can be used to support each operation, and then plan how to integrate these activities into their operations. Some questions to ask are:

- What is the ultimate purpose of conducting identity activities? Is it to enable access control, population control, site exploitation, or distribution of aid or services?
- Who is the targeted population? Is it only military aged males, the entire population, or another subset of it?
- What biometric modalities are to be collected and what is the extent of the enrollment? Some examples–
  - If facial images are to be collected, do mission requirements require a full 180 degree set of photos of the face, or just a single front facial image?
  - Are iris images to be collected?
  - Are all ten fingers to be printed or are only the index fingers and/or thumbs?
  - Are flat slaps required?
  - Are palm prints required?
  - Is DNA to be collected?
  - Are voice prints to be collected?
- What kind of security is needed to protect personnel conducting identity activities? What are the risks associated with integrating identity activities into operations, not only to friendly forces, but to the greater population?
- What is the greater population's attitude toward the use of biometric collection and enrollment devices? Do they want more security, and are they willing to tolerate the inconvenience of being stopped, processed, and enrolled, or might they be ready to riot to yet another imposition on their daily lives?
- What are the cultural sensitivities to collecting identity information?
- How much biographic information needs to be collected to support the overarching mission or operation?
- Is linguist support necessary?
- Who conducts the enrollments? Partner nation security forces or U.S. forces?

When planning for the use of identity activities, in addition to resourcing for hand-held biometric collection devices, commanders and staffs must consider the importance of developing, establishing, and maintaining a robust and resilient communication architecture. The sending and receiving of numerous complete identity profiles, with associated photos, and contextual and biographical information can consume large amounts of bandwidth. Commanders need to ensure their Soldiers receive appropriate training in the use of the hand-held biometric collection devices and how to upload and download biometric information to the devices. Commanders must also allow time for training pertaining to accessing and using identity databases.

Identity Activities and I2

Identity activities and I2 are not interchangeable. As previously stated, identity activities can be described as a collection of functions and actions that appropriately recognize and differentiate one individual from another to support decision making. I2 is the product resulting from the analysis of identity data collected from the intelligence disciplines, other information collection operations, and from identity activities. Commanders and staffs at all levels use identity activities, and resulting identity information, as well as I2 and DOD law enforcement criminal intelligence products, to support planning, direction, execution, and assessment of operations.

I2 helps to identify unknown potential adversary or enemy personnel by associating these individuals to other persons, places, events, or materials. I2 further expands upon information collection or target development. I2 helps validate

foreign persons for positions of trust; aids in identifying friendly or neutral foreign personalities or groups for engagement; helps to distinguish friendly, neutral, enemy, and unknown personnel, and assists in identifying known or unknown threat networks.

Conclusion

The role of identity activities will continue to expand as a force multiplier in complex operating environments. Commanders and their staffs will continue to rely on identity activities to increase the effectiveness of combat tasks to accomplish their mission. In diverse theaters of operations, identity activities have proven useful in:

- Reducing tactical, operational, or strategic surprise.
- Restricting adversary and enemy mobility, hindering their ability to employ asymmetric tactics across the operational environment and beyond.
- Protecting personnel, facilities, and equipment.
- Denying adversary and enemy access to resources.
- Disrupting adversaries' and enemies' use of deception and disinformation tactics.
- Restricting adversaries' and enemies' access to personnel, facilities, equipment, critical infrastructures, and vulnerable populations.
- Managing foreign populations.
- Supporting stability tasks.

The dynamics of military operations are changing to meet the challenges of dense urban areas, more adaptive adversaries, adversaries who will likely be dispersed and often intermingled with the populace, adversaries who will likely employ asymmetric tactics, and a variety of actors across the operational environment possessing greater technological capabilities to challenge regional stability or U.S. and partner nations' interests. The importance of accurate, reliable, and timely information and intelligence on neutral and adversarial or enemy actors is critical. Fortunately, identity activities greatly enhance our ability to develop relevant information to satisfy this requirement.

Mr. Meadows works as a military intelligence doctrine writer and team lead at the U.S. Army Intelligence Center of Excellence. He is responsible for the development of U.S. Army doctrine on biometrics-enabled intelligence, document and media intelligence, and human intelligence. Previously, Mr. Meadows served in the U.S. Army as an interrogator and as a debriefer, and has taught at the Defense Strategic Debriefing Course, the U.S. Army's Interrogation Course, and the Joint Analyst-Interrogation Collaboration Course. Mr. Meadows has operational experience conducting interrogations in Iraq and debriefings in Germany.

Leveraging DCGS-A Best Practices

by Mr. Chet Brown, Chief, Lessons Learned Branch

This column introduces quite a few Distributed Common Ground Station-Army (DCGS-A) "Best Practices." Our primary intent in describing these best practices is to provide information for you to consider in improving your current, or in developing new, training plans, standard operating procedure (SOP) documents or leader development efforts.

Army Regulation 11-33 The Army Lessons Learned Program, defines a best practice as, "A change to how something is done that results in improved personal or unit performance or behavior but is not yet fully implemented across (the) force." Recent U.S. Army Intelligence Center of Excellence (USAICoE) Lessons Learned (LL) Team collection reports show a significant increase in observed DCGS-A best practices. The LL Team's most recent (at the time of writing) collection contained 12 observation topics; 5 of which were specific DCGS-A best practices. That report supports an emerging trend of best practices being employed more frequently and widespread than we have previously experienced or reported.

USAICoE LL Team members have documented this emerging trend evidenced by the increased inclusion of DCGS-A best practices in their respective collection reports. They, and others, have noticed a change in the expressed attitudes and explicit comments from Soldier's regarding DCGS-A. The evidence of a changing sentiment is anecdotal but still credible. Current general perception of DCGS-A is illustrated by the absence of previously frequent comments such as, "DCGS-A is broken" or "We don't use DCGS-A." USAICoE LL collectors are now receiving unsolicited affirmations of DCGS-A capabilities from Soldiers and leaders, "This is how we use DCGS-A to support …" and "We used DCGS-A to do this…"

While much of the noticeable change occurred within brigade combat team (BCT) elements, the LL Team observed positive changes in capitalizing on the system's capabilities at every echelon equipped with DCGS-A. The G-2 of a theater support command recently provided USAICoE LL with specific examples of DCGS-A products to support the unit's commander and dispersed and varied subordinate units. Many have offered their thoughts and opinions on the cause of this positive DCGS-A reporting trend. We'll avoid conjecture and simply provide the identified best practices for your consideration in four categories:

- Commander involvement.
- Leader knowledge and mentoring.
- Standard operating procedures (SOPs).
- Training.

If you regularly receive (and read) USAICoE LL Team products you may detect a correlation between these four categories and the content of our Top Ten Intelligence Training Lessons and Best Practices information paper (17 Nov 2015) available at https://army.deps.mil/Army/CMDS/USAUSAICoE_Other/LL/SitePages/Home.aspx.

Commander Involvement. As we sought to identify the themes common to each of the units demonstrating DCGS-A best practices we discovered a correlated best practice–BCT commanders directing their subordinate units/personnel to train, use, and integrate DGCS-A into operations. Commanders fully understand the value of intelligence information and products through their operational experiences. Commanders translate their high expectations of intelligence and overall mission command information support into their unit's training priorities and objectives. In the "Top Ten" paper mentioned above we identified, "… the Commander's oversight of planning, resourcing, conducting and assessing training results in superior performance."

The commander's role is also evident in units which successfully leverage the full range of DCGS-A capabilities and integrating DCGS-A products into the units' mission command information processes. A best practice for BCT commanders to ensure DCGS-A training priorities are enforced and the system is fully integrated into the BCT mission command architecture is to state their intent in an operations order (OPORD), concept of the operation (CONOP) description, or specifying in an SOP. Written references issued under the commander's authority underscores the importance of accomplishing individual and collective DCGS-A

training in order to fully support the BCT commander's intent. Including DCGS-A training events in an OPORD is a superior best practice as the order provides routine instructions identifying, or directs providing, resources and support required to conduct training.

Leader Knowledge and Mentoring. Leaders who are well-informed or proficient in applying DCGS-A capabilities and products are better able to serve as mentors than those less knowledgeable. LL results neither indicate, nor does this column advocate, leaders becoming DCGS-A operators as a best practice. There are three best practices linked to leader knowledge we have observed in units which employ DCGS-A well: DCGS-A products used to support intelligence preparation of the battlefield (IPB) in driving the military decision making process (MDMP), managing DCGS-A operator talent, and demonstrating competence in military intelligence (MI) skills (manual/analog environment) before transitioning to employing DCGS-A.

Leveraging the full power of DCGS-A depends upon one knowing what the system can provide or produce. An S-2 in a heavy (now armored) BCT, in collaboration with USAICoE's DCGS-A Tactical Engagement Team (TET), produced a spreadsheet which correlates IPB products to specific DCGS-A Tool capabilities and products. The spreadsheet also identifies which IPB or MDMP step the product supports. The spreadsheet and its associated Tactical SOP (TACSOP) book are Best Practices. The unit which developed the TACSOP granted permission to USAICoE–and actively encouraged us–to disseminate the reference to any who may benefit. Both are available on the USAICoE LL Home Page at the link provided earlier in this column.

Leaders must also know how best to task and supervise their subordinate DCGS-A operators to achieve the desired product or obtain the required information in the most efficient and accurate manner possible. It is sometimes a challenge for leaders to know which of their subordinates is the most capable in the myriad of available DCGS-A capabilities, tools, and outputs. The challenge is increased when the BCT intelligence cell and elements of the MI company combine to create the brigade intelligence support element (BISE). We'll come back to this condition later in this column when discussing DCGS-A training best practices.

Once one knows the full range of DCGS-A capabilities and is able to effectively direct the intelligence production tasks of DCGS-A operators (or their respective section leaders), the most critical hurdle to leveraging DGCS-A remains–integrating the system into the unit's mission command network. Even the most technically proficient and experienced personnel are often challenged in establishing DCGS-A on the tactical network and keeping the system fully operational. These challenges are not limited to DCGS-A. The operational variables also impact a unit's ability to employ all of the mission command systems. The U.S. Army Forces Command Commander's Fiscal Year 2017 Training Guidance emphasizes the challenge in using digital mission command systems as becoming increasingly more difficult as commanders are directed to, "… train to fight in a degraded cyber environment…(Warfighter Exercises and Combat Training Center(CTC)) rotations (will) include contested cyber and electromagnetic spectrum environments."

Inherent to integrating DCGS-A into the unit's tactical information network is keeping the system operational and interoperable with the mission command systems in the dynamic and complex operational environment. Even the highest-performing units employing DCGS-A are faced with unexpected challenges to network connectivity and continued interoperability. The adage that no plan survives first contact is proved by the frequency in which units have to solve unanticipated problems or impediments to network connectivity. Not every problem can be anticipated; however, providing a sequence of potential resolution strategies or mitigating measures have proven helpful to units and personnel who faced a wide range of issues.

SOPs. SOPs are a best practice. An SOP containing a DCGS-A primary, alternate, contingency, emergency (PACE) plan is a better practice. A superior practice occurs when personnel refer to their unit's DCGS-A PACE plan to overcome a variety of unexpected network or interoperability problems.

USAICoE LL has produced several products which describe and demonstrate the value of effective PACE plans in general. A component not addressed in previous USAICoE LL PACE commentary is, "How will information from (or products of) DCGS-A be transferred to the force as you progress in sequence when implementing your PACE plan?" PACE plans are frequently considered only to effect communications; simply relaying information in either analog or digital formats. DCGS-A PACE plans also address relaying information but requires a more thoughtful and detailed understanding of the information content and context which can (or must) be transmitted within each of the PACE plan measures.

DCGS-A PACE measures may have to (should) be aligned according to the unit's operational or planning phases. One must understand how to provide DCGS-A products to support MDMP, targeting, or answering priority intelligence requirements. Conversely, one must identify how to receive intelligence information or data normally fed to DCGS-A during network outages or system failures. It is better to de-

vote the time and study of critically important details required to develop a PACE plan for DCGS-A operations in the relative calm and environmentally stable garrison environment, instead of attempting to implement ad hoc solutions during the fast-paced dynamic environment at a CTC when dealing with multiple environmental and physical stressors. Understanding and applying the processing power and 'bandwidth' needed to transmit specific DCGS-A products within each PACE plan mechanism helps ensure effective support to the unit's processes (targeting, IPB, MDMP, etc.)

Additional impact on the unit's other mission command systems and/or 'bandwidth' should also be considered. A BCT best practice is to have the BCT S-2, BISE Chief, BCT S-6, and BCT Intelligence Systems Maintenance/Integration Technician validate the DCGS-A PACE plan CONOP before attempting to implement during operations or training. Unfortunately, there is not a single DCGS-A PACE plan solution available or suitable for general application. We can only offer the lessons and best practices others have implemented for you to consider during your individual or collective unit efforts.

Training. We mentioned a best practice arising from a unit benefitting from USAICoE's DCGS-A TET. LL reporting indicates the DCGS-A TET training is in itself a best practice for units to implement. The dictionary definition of synergy, not the oft-cited buzzword meaning, is achieved throughout the BCT intelligence warfighting function when applying the techniques and procedures trained by the DCGS-A TET.

We've observed more than a few DCGS-A training best practices; most are linked to the eleven unit training principles of effective collective training (Army Doctrine Publication 7-0, Training Units and Developing Leaders, August 2012). The remaining best practices presented in this column may also be applied to other crew-served or mission command systems; however, our intent is to highlight techniques specific to DGCS-A.

DCGS-A operator skills are highly perishable. Daily use of DCGS-A is a best practice. An associated additional best practice enabling daily DCGS-A use is to operate on the garrison network. There are many technical, security, policy, environmental, site and other issues a unit must address in order to place a tactical system on a garrison information technology network. The procedures and approvals are usually site (home station) specific and are not generalizable to the force. Seek guidance from the experts at your home station to identify the steps needed to put DCGS-A on your garrison's network.

Using DCGS-A every workday results in increased operator and leader familiarity and proficiency in intelligence production tasks. An ancillary benefit of daily DCGS-A use is the increased opportunity for operators to experience discovery learning; identifying on their own novel, improved, or more efficient techniques in applying DCGS-A tools and functions.

Cross training DCGS-A analysts in performing functions routinely assigned to one (or the same) analyst eliminates single points of failure should an analyst not be available or becomes a casualty. Single source, all source, high-side, and low-side analyst positions should be cross-trained as a best practice. Lessons learned mandates placing a spotlight on the DCGS-A database manager. Units routinely assign one analyst to perform as the DCGS-A database manager as a means to control information correlation. The unit's intelligence production is made vulnerable without a designated, trained, experienced or available alternate for the database manager and should be part of any PACE plan.

Training to maintain DCGS-A is a best practice. Every unit which employs DCGS-A understands the value and scarcity of MOS 35T, MI System Maintainer/Integrator, Soldiers and warrant officers. These are the personnel upon whom units most rely to ensure their DCGS-A components are operational and remain operational when in the operational environment. They too must be provided the opportunity to train and master maintenance skills specific to DCGS-A. Maintenance task training should be included in the units training plan and appropriately resourced. Having MOS 35T Soldiers standing by to address DCGS-A issues during other training events is not maintenance task training. Incorporating specific maintenance task training objectives and performance measures into existing DCGS-A training events is appropriate. The best resource LL has identified to integrate DCGS-A maintenance task training is your unit's Intelligence Systems Integration and Maintenance Technician.

Visit the USAICoE LL Homepage at https://army.deps.mil/Army/CMDS/USAUSAICoE_Other/CDID/Lessons%20Learned/SitePages/Home.asp or contact the LL Branch Chief at (520) 533-7516; DSN (314) 821-7516 for more information.

Moments In MI History

Gero Iwai:
First Japanese American Counterintelligence Agent in the U.S. Army

by Lori S. Tagg, Command Historian, USAICoE

In the early morning hours of December 7, 1941, the Japanese Air Force bombed the U.S. Naval fleet anchored in Pearl Harbor, Hawaii. According to the multi-volume *History of the Counter Intelligence Corps*, "During the first minutes of the raid, agents of the Corps of Intelligence Police (CIP), scattered throughout the island of Oahu, raced to CIP headquarters in the Dillingham Building in downtown Honolulu. A hurried 10-minute conference and the agents were out on their first assignment of the war. Following a previously arranged plan, they dispersed in teams. Their mission was to apprehend all pro-Japanese sympathizers." CIP agents began rounding up individuals on a "pickup list" compiled over the previous 10 years. Within days, more than 400 individuals had been arrested and confined at a makeshift detention camp. While many of those on the list were Japanese, pre-war investigations had confirmed that allegations of espionage among the Japanese American community in Hawaii were predominantly false.

Those investigations were largely the handiwork of Gero Iwai, a 36-year-old Hawaiian native and a 10-year veteran of the CIP. As one of the first Japanese Americans to pursue an ROTC course during his attendance at the University of Hawaii, he was appointed a 2nd Lieutenant, Infantry, in the Officers Reserve Corps upon graduation. However, on August 19, 1931, Iwai chose to enlist in the U.S. Army, was placed on the Detached Enlisted Men's List (DEML), and was assigned as a CIP Investigator in the Office of the Assistant Chief of Staff (ACoS), G-2, Hawaiian Department. [Note: the DEML was equivalent to today's "branch immaterial" assignments.] At the time, Iwai was the only Nisei (second generation Japanese American) employed in the G-2's counterintelligence office. For the first 10 years of his Army career, Iwai worked undercover, his true occupation unknown even to his own family. He monitored the activities of the Japanese community, surveilled the activities of the Japanese Consulate General, and established a network of informants among the Japanese Americans employed at the Consulate. Iwai and his fellow CIP agents painstakingly compiled the list of individuals they believed would be a threat to the U.S. should war with Japan occur.

On April 8, 1941, Iwai was honorably discharged from the Army and accepted an appointment as a Reserve officer serving as the Assistant to the ACoS, G-2, Hawaiian Department. In time, Iwai became the Officer in Charge of the Translation Section of the Counter Intelligence Detachment. The day after the Pearl Harbor attack, given his years of experience and knowledge of the Japanese culture and language, he was the natural choice for a special joint and interagency assignment.

Lt. Col. Gero Iwai, the U.S. Army's first Japanese American counterintelligence **agent, was posthumously inducted into the Military Intelligence Hall of Fame in 1995.**

Iwai and fellow Nisei, Douglas Wada, a Naval intelligence officer, were chosen to work with the Federal Bureau of Investigations to interrogate a captured Japanese officer. The first Japanese prisoner of the war, Ensign Kazuo Sakamaki, had commanded a Japanese midget submarine launched against targets in Pearl Harbor. Due to mechanical issues, his submarine had run aground miles from the harbor, and he had been captured by military police. Among Sakamaki's possessions was a navigational chart that, upon analysis by Iwai and Wada, was found to designate the berthing locations of all the major carriers and warships of the U.S. Navy. Furthermore, documents recovered from the Japanese Consulate and translated by Iwai and Wada provided further evidence of the staggering extent of Japanese pre-war espionage.

Throughout the war, Iwai continued to conduct counterintelligence work for the Counter Intelligence Corps (CIC), successor to the CIP. His personal crusade was to prove the Japanese Americans in Hawaii were loyal to the U.S.. His thorough investigation uncovered not a single subversive or hostile act against the U.S. on the part of Japanese Americans. His top-secret report to that effect reportedly swayed the opinions of military leaders, including Gen. Delos C. Emmons, commander of the U.S. Army in Hawaii, who subsequently proposed the formation of what would become the 100th Infantry Battalion, made up almost entirely of Japanese Americans from Hawaii.

Iwai remained in Honolulu with the 401st CIC Detachment until 1949, when he was assigned to the 441st CIC Detachment in Tokyo. He returned to the U.S. in 1954 and, after 26 years of honorable service, retired from military service as a Lieutenant Colonel in 1957. Ironically, Iwai's efforts to prove the loyalty of the Hawaiian Japanese Americans both before and during World War II had completely estranged him and his family from the community he sought to protect. Instead of living his final years in his beloved native Hawaii, Iwai settled in San Francisco, where he passed away in 1972.

Contact and Article
Submission Information

This is your professional bulletin. We need your support by writing and submitting articles for publication.

When writing an article, select a topic relevant to the Military Intelligence and Intelligence Communities.

Articles about current operations; TTPs; and equipment and training are always welcome as are lessons learned; historical perspectives; problems and solutions; and short "quick tips" on better employment or equipment and personnel. Our goals are to spark discussion and add to the professional knowledge of the MI Corps and the IC at large. Explain how your unit has broken new ground, give helpful advice on a specific topic, or discuss how new technology will change the way we operate.

When submitting articles to *MIPB*, please take the following into consideration:

- Feature articles, in most cases, should be under 3,000 words, double-spaced with normal margins without embedded graphics.
- We cannot guarantee we will publish all submitted articles and it may take up to a year to publish some articles.
- Although MIPB targets themes, you do not need to "write" to a theme.
- Please note that submissions become property of MIPB and may be released to other government agencies or nonprofit organizations for republication upon request.

What we need from you:

- A release signed by your unit or organization's information security officer/operations security officer/SSO stating that your article and any accompanying graphics and photos are unclassified, nonsensitive, and releasable in the public domain (IAW AR 380-5 DA Information Security Program). A sample security release format can be accessed at our website at https://ikn.army.mil.
- A cover letter (either hard copy or electronic) with your work or home email addresses, telephone number, and a comment stating your desire to have your article published.
- Your article in Word. Do not use special document templates.
- Any pictures, graphics, crests, or logos which are relevant to your topic. We need complete captions (the Who, What, Where, When), photographer credits, and the author's name on photos. Do not embed graphics or photos within the article. Send them as separate files such as .tif or .jpg and note where they should appear in the article. PowerPoint (not in .tif or .jpg format) is acceptable for graphs, etc. Photos should be at 300 dpi.
- The full name of each author in the byline and a short biography for each. The biography should include the author's current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications.

We will edit the articles and put them in a style and format appropriate for ***MIPB***. From time to time, we will contact you during the editing process to help us ensure a quality product. Please inform us of any changes in contact information.

Submit articles, graphics, or questions to the Editor at usarmy.huachuca.icoe.mbx.doctrine@mail.mil.

Our contact information:
Contact phone numbers: Commercial 520.538.0956
DSN 879.0956

Distributed Common Ground System-Army

U.S.ARMY

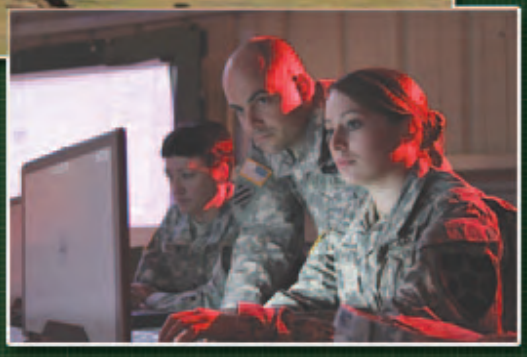
DCGS A

Improving SITUATIONAL AWARENESS *and* DECISION MAKING Across *the* Spectrum *of* Conflict

Find out more at
dcgsa.apg.army.mil

Providing Actionable Intelligence to the Warfighter

ATTN: MIPB (ATZS-CDI-DM)
BOX 2001
BLDG 51005
FORT HUACHUCA AZ 85613-7002



Headquarters, Department of the Army.
This publication is approved for public release.
Distribution unlimited.

PIN: 200811-000