Federated Technical Control and Analysis Elements:
Setting the Theater for Cryptologic Warfighters

by Captain Thomas Mahoney

Strategic Context—Origins of a Federated System

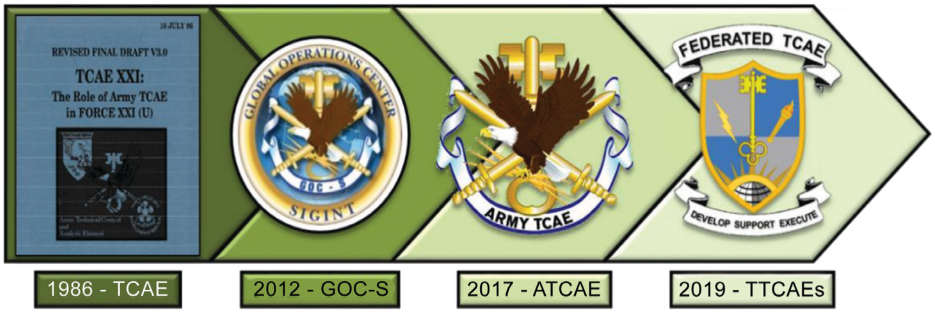
The 2018 National Defense Strategy describes "an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations."[1] Aggressive traditional powers, rogue regimes, proto-states, and violent extremist organizations threaten the post-World War II international order.[2] To address this increased complexity and uncertainty, the U.S. Army, as part of a joint force, postures itself to transition rapidly from a state of competition to armed conflict and then back to competition under enhanced and improved circumstances.[3] During periods of competition, the Army prepares the operational environment for potential transition to armed conflict by setting the theater.[4]

At the core of the intelligence warfighting function, the U.S. Army Intelligence and Security Command (INSCOM) and its subordinate military intelligence brigades-theater (MIB–Ts) set the globe and set the theater, respectively. This responsibility occurs in advance through a combination of preparatory intelligence activities and the establishment of authorities and permissions normally reserved for periods of conflict.[5] Posturing Army or joint forces to rapidly transition from competition to conflict necessitates that the intelligence warfighting function execute these analytic and administrative functions for each of the individual intelligence disciplines.

Within the signals intelligence (SIGINT) discipline, technical control and analysis elements (TCAEs) perform these critical functions. Currently, INSCOM maintains the Army technical control and analysis element (ATCAE) at the National Security Agency headquarters. In March 2019, the ATCAE hosted a forum to discuss how best to enable Army cryptologic forces to address the emerging challenges identified in the Army's multi-domain operating concept. As a direct result of the ATCAE forum, INSCOM is undertaking a major initiative to create a federated system of TCAEs, arrayed across echelons. The federated TCAEs will deliver the needed technical support to Army cryptologic forces around the globe, ensuring they possess the organizational agility and flexibility to answer any requirement, in any domain.

History and Authorities

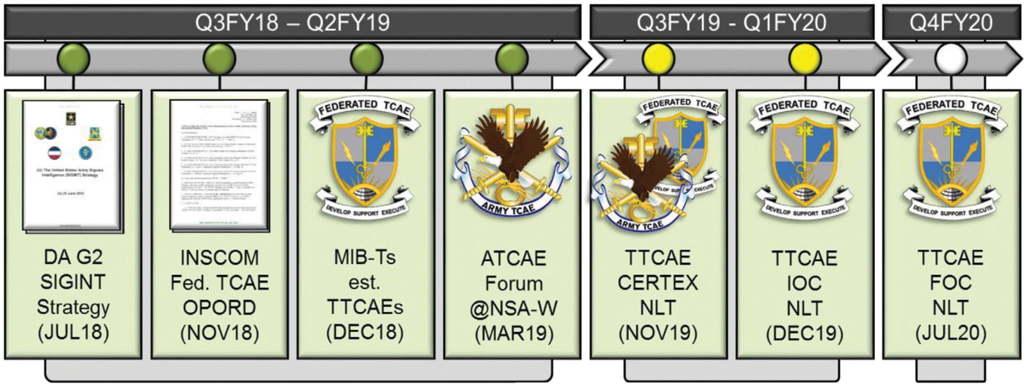
The ATCAE traces its origins back to the 1970s and 1980s, when the Deputy Chief of Staff for Intelligence directed its formation to "provide SIGINT operational support to tactical SIGINT units" in a response to merging the Army Security Agency into INSCOM. Over the decades, the roles and functions of the ATCAE adjusted to meet emerging requirements and needs. As shown in Figure 1, in 2012 the ATCAE disbanded and reorganized into the Global Operations Center–SIGINT. This reorganization was part of a broader INSCOM initiative to establish an overarching capability that was similar to an analysis and control element in support of deploying units. The system comprised Global Operations Centers for each intelligence discipline, answering to a prime Global Operations Center located at the National Ground Intelligence Center. As conditions changed and the Army and national focus shifted to a future fight executed across all domains, the need for TCAE roles and functionality to return became clear. To meet this requirement, INSCOM disbanded the Global Operations Center–SIGINT in 2017 and reconstituted the ATCAE in its place.[6]



ATCAE	Army TCAE	TCAE	tactical control and analysis element
GOC–S	Global Operations Center-SIGINT	TTCAE	theater TCAE
SIGINT	signals intelligence		

Figure 1. TCAE Reorganizations from 1986 to Present

TCAEs derive their roles and authorities from the INSCOM Commanding General, who functions as the principal Army Service cryptologic component.[7] The Director, National Security Agency/Chief, Central Security Service, as the responsible officer for all cryptologic activities, delegates the authority to conduct cryptologic operations to each of the Service cryptologic components. As the Army Service cryptologic component, the INSCOM Commanding General exercises his authority to set individual theaters for cryptologic operations by setting the globe for all Army units performing a SIGINT mission.[8] As the strategic environment evolves and the national focus shifts from counterterrorism and counterinsurgency to global competition and conflict, contested across all domains, INSCOM's federated TCAE initiative postures Army cryptologic forces to provide effective intelligence support to any operation or contingency.



ATCAE	Army TCAE	NLT	not later than
CERTEX	certification exercise	NSA–W	National Security Agency-West
DA G2	Department of the Army, Intelligence	OPORD	operation order
est.	established	Q1	1st quarter
Fed.	federated	Q2	2nd quarter
FOC	full operational capability	Q3	3rd quarter
FY	fiscal year	Q4	4th quarter
INSCOM	U.S. Army Intelligence and Security Command	SIGINT	signals intelligence
IOC	initial operational capability	TCAE	tactical control and analysis element
MIB–T	military intelligence brigade-theater	TTCAE	theater TCAE

Figure 2. Timeline for Federated TCAEs

Implementation of a Federated TCAE System

Department of the Army G-2's SIGINT strategy served as the catalyst for INSCOM's federated TCAE initiative.[9] Consideration of emerging requirements, resurgence of pacing threats, and a shift toward multi-domain operations drove the decision to distribute TCAE functionality across echelons by way of a federated system of TCAEs. INSCOM's federated system establishes TCAEs at the Army, theater, and operational level.[10] The ATCAE distributes technical control (administrative) and technical production (analytic) functions and responsibilities to the TCAEs at subordinate echelons, ensuring that Army cryptologic forces are properly enabled, regardless of location or mission.

Following guidance from the INSCOM Commanding General, MIB–Ts aligned to each theater reorganized their organic cryptologic personnel and resources to establish theater TCAEs (TTCAEs). Dedicated to enabling cryptologic operations within their theater, these TTCAEs set the foundations necessary to exercise TCAE functionality. In March 2019, the ATCAE hosted a forum at the National Security Agency-Washington to discuss the implementation of INSCOM's federated TCAE system initiative. The Commanding General reiterated the importance of the federated TCAE and issued instructions for MIB–Ts to establish TTCAEs and integrate them into the federated system. As shown in Figure 2, each TTCAE participates in a certification exercise to assess its initial operational capability and they should reach full operational capability by July 2020.

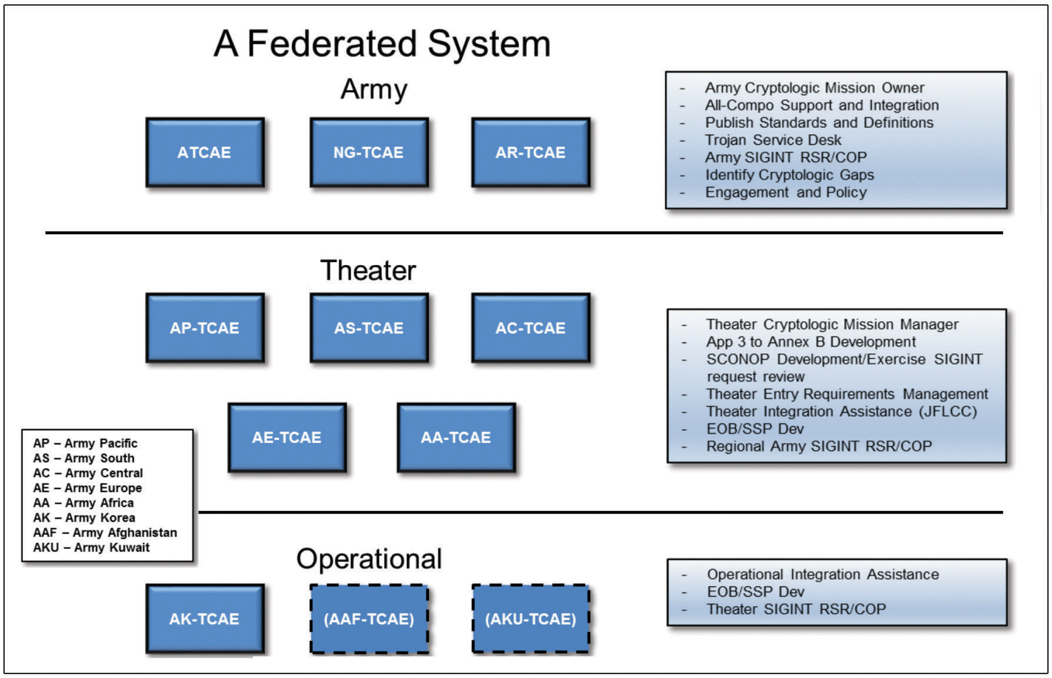
Certain regions or operations will also establish operational TCAEs (OTCAEs). These OTCAEs are responsible for and enable cryptologic forces aligned to or involved in their operation. The first OTCAE has been established as part of the 501st MIB–T. The OTCAE will synchronize efforts with the Army Pacific TCAE, passing authorities and responsibilities for Army cryptologic forces as they transition from theater into the specific operation. As shown in Figure 3 (on the next page), the Army National Guard and Army Reserves are also establishing TCAEs to enable cryptologic operations within their respective components. The Army National Guard-TCAE and the Army Reserve-TCAE will work closely and be collocated with the ATCAE to synchronize and enable Army cryptologic operations holistically.[11]

TCAE Core Functions

TCAEs at every echelon enable compliant and effective execution of Army cryptologic operations.[12] To provide the maximum level of support to a commander's priorities, SIGINT requires integration of collection, storage, and analysis across echelons, from tactical to national, as part of the U.S. SIGINT system. To accomplish this, TCAEs task organize into three lines of effort:

- ✦ Exercise technical control.
- ✦ Generate technical production.
- ✦ Enable operational readiness.[13]

These lines of effort ensure Army cryptologic forces have access to the U.S. SIGINT system, knowledge of the signals environment and threat, and the tradecraft necessary to execute their mission.[14]


A Federated System
Army
ATCAE
NG-TCAE
AR-TCAE
- Army Cryptologic Mission Owner
- All-Compo Support and Integration
- Publish Standards and Definitions
- Trojan Service Desk
- Army SIGINT RSR/COP
- Identify Cryptologic Gaps
- Engagement and Policy
Theater
AP-TCAE
AS-TCAE
AC-TCAE
AE-TCAE
AA-TCAE
- Theater Cryptologic Mission Manager
- App 3 to Annex B Development
- SCONOP Development/Exercise SIGINT request review
- Theater Entry Requirements Management
- Theater Integration Assistance (JFLCC)
- EOB/SSP Dev
- Regional Army SIGINT RSR/COP
AP – Army Pacific
AS – Army South
AC – Army Central
AE – Army Europe
AA – Army Africa
AK – Army Korea
AAF – Army Afghanistan
AKU – Army Kuwait
Operational
AK-TCAE
(AAF-TCAE)
(AKU-TCAE)
- Operational Integration Assistance
- EOB/SSP Dev
- Theater SIGINT RSR/COP

AR	Army Reserves	NG	National Guard
ATCAE	Army TCAE	RSR/COP	resource status report/common operational picture
EOB/SSP	electronic order of battle/SIGINT support package	SCONOP	security concept of operations
JFLCC	Joint Force Land Component Commander	SIGINT	signals intelligence

Figure 3. TCAEs as Part of a Federated System

Technical Control

In order to access the U.S. SIGINT system, cryptologic forces must comply with laws, regulations, and executive orders that drive National Security Agency policy. The ATCAE serves as the cryptologic mission owner for access to national databases. In this role, the ATCAE exercises technical control of all Army units operating under the SIGINT operational tasking authority.[15] The multi-domain operating concept identifies the need for Army units to conduct detailed tactical and operational intelligence preparation of the battlefield, including cryptologic operations, during periods of competition.[16] The Army units, as part of a joint, interagency, and multinational team, must be enabled with the necessary authorities to operate in the electromagnetic spectrum and cyberspace.[17] The ATCAE's technical control section bears the responsibility to ensure that Army units are postured to execute their respective SIGINT missions compliantly.[18] They secure the Army's necessary SIGINT authorities and entitlements to support Army cryptologic forces through all phases of an operation (Figure 4).

TTCAEs and OTCAEs serve as anchor points for all Army cryptologic operations within their theater or operation. Army cryptologic forces coordinate access to the U.S. SIGINT system and mission authorizations with their respective TTCAE/OTCAE. Units submit all required documents and certifications to secure the SIGINT authorities necessary to satisfy their commander's priority intelligence requirements. TTCAEs assist with the documents and certifications and then exercise technical control of the cryptologic missions. The technical control encompasses both the mission management (administrative requirements) and data flow management (technical connectivity requirements). TTCAEs also work closely with the Army Service component commands to articulate cryptologic requirements clearly within theater entry requirements. This ensures that Army forces arrive in theater ready and able to execute their cryptologic mission.

The ATCAE's technical control section supports the federated system of TCAEs with two 24-hour watch desks that monitor network access and adjust cryptologic missions in support of command requirements. They also manage a SIGINT common operational picture, network access support, and resource status reports.[19] The TTCAEs and OTCAEs feed their own common operational pictures and resource status reports to the ATCAE for inclusion in the global Army common operational picture and resource status reports. This information provides situational awareness and understanding of capabilities and capacity, critical to leaders and decision makers at every echelon.

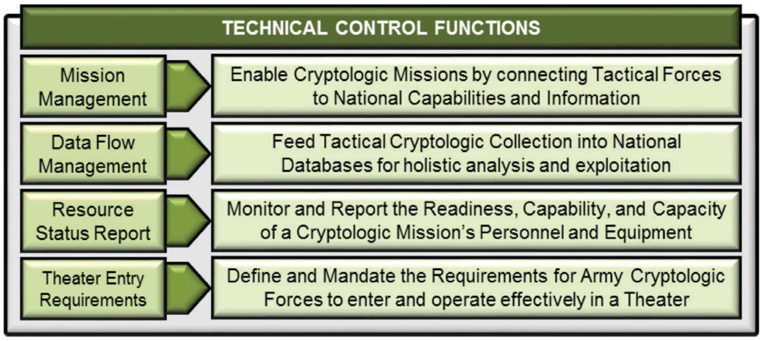

TECHNICAL CONTROL FUNCTIONS
Mission Management
Enable Cryptologic Missions by connecting Tactical Forces to National Capabilities and Information
Data Flow Management
Feed Tactical Cryptologic Collection into National Databases for holistic analysis and exploitation
Resource Status Report
Monitor and Report the Readiness, Capability, and Capacity of a Cryptologic Mission's Personnel and Equipment
Theater Entry Requirements
Define and Mandate the Requirements for Army Cryptologic Forces to enter and operate effectively in a Theater

Figure 4. Technical Control Functions

Technical Production

While technical control enables Army cryptologic forces with the technical access and authorities necessary for their mission, technical production focuses on technical intelligence and tradecraft development.[20] Technical production requirements derive from Army Service component command priorities, as well as operational and contingency plans. These requirements focus technical production on how best to enable cryptologic forces. At the theater level, technical production centers around—

- SIGINT support packages describing the signals environment in a specified region.
- Electronic order of battle focused on the threat's communications and emanations within the electromagnetic spectrum.
- Working aids that enable Army cryptologic forces to more effectively execute their mission.

Additionally, if an Army unit identifies tradecraft gaps or the need for tailored SIGINT training or tradecraft, the TTCAE can reach out to the ATCAE's technical production section. The ATCAE technical production section is able to leverage organizations and entities from across the U.S. SIGINT system and intelligence community to develop needed tradecraft solutions. They then export it to the force through mobile training teams, digital training venues, and whatever means best support the forward cryptologic elements.[21]

Operational Readiness

Technical control and technical production feed operational readiness. Together, they enable TCAEs to ensure that Army cryptologic forces around the globe possess the authorities, accesses, and knowledge necessary to execute their respective SIGINT missions. The TTCAEs ensure that theaters are set for rotational units, regionally aligned forces, time-phased force deployment data units, and any other cryptologic forces. Close collaboration between the theater and Army TCAEs ensures that Army cryptologic forces are operationally ready, both from a technical control perspective and from a situational understanding and tradecraft perspective. The federated system creates a mutually supportive relationship—vertically from strategic to theater to operational, and horizontally across cryptologic forces aligned against a mission or operation. The federated TCAE system establishes the foundations for the SIGINT discipline of the intelligence warfighting function to fight and win, regardless of threat, across domains, in an environment where all domains are contested.

Additional Resources

The ATCAE offers additional resources, including a series of ATCAE publications available on milSuite.
Access https://login.milsuite.mil/ and enter "ATCAE" in the Search field (common access card login required).

Endnotes

[1] Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, n.d., 2, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[2] Ibid.

[3] Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet (Pam) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), v.

[4] Ibid., xi.

[5] Ibid., 17.

[6] Department of the Army, Army Technical Control and Analysis Element (ATCAE) Publication (Pub) 1-0, *ATCAE Charter* (Fort George G. Meade, MD: May 2018), 2 (common access card [CAC] login required).

[7] Department of the Army, Army Techniques Publication 2-22.6*, Signals Intelligence Volume II: Reference Guide* (Washington, DC: U.S. Government Publishing Office, 20 Jun 2017), 2-6 (CAC login required).

[8] Ibid.

[9] Department of the Army, *The United States Army Signals Intelligence (SIGINT) Strategy*, 25 June 2018.

[10] Department of the Army, ATCAE Pam 1-0, *The TCAE* (Fort George G. Meade, MD: November 2018), 4 (CAC login required).

[11] Ibid.

[12] Ibid., 4.

[13] Department of the Army, ATCAE Pub 1-0, *ATCAE Charter,* 16.

[14] Department of the Army, ATCAE Pam 1-0, *The TCAE,* 3.

[15] Department of the Army, ATCAE Pub 1-0, *ATCAE Charter,* 16.

[16] Department of the Army, TRADOC Pam 525-3-1, *The U.S. in Multi-Domain Operations,* 27.

[17] Ibid., 28.

[18] Department of the Army, ATCAE Pub 1-0, *ATCAE Charter,* 21.

[19] Ibid., 21–22.

[20] Ibid., 29.

[21] Ibid., 30.

CPT Thomas Mahoney serves as the officer in charge of technical production within the Army technical control and analysis element, 704th Military Intelligence Brigade. Past assignments of note include command of Headquarters and Service Company, Eighth Army; command of C Company, 304th Military Intelligence Battalion; and two deployments to Iraq.

Echelons Corps and Below Technical Control and Analysis Cell Concept

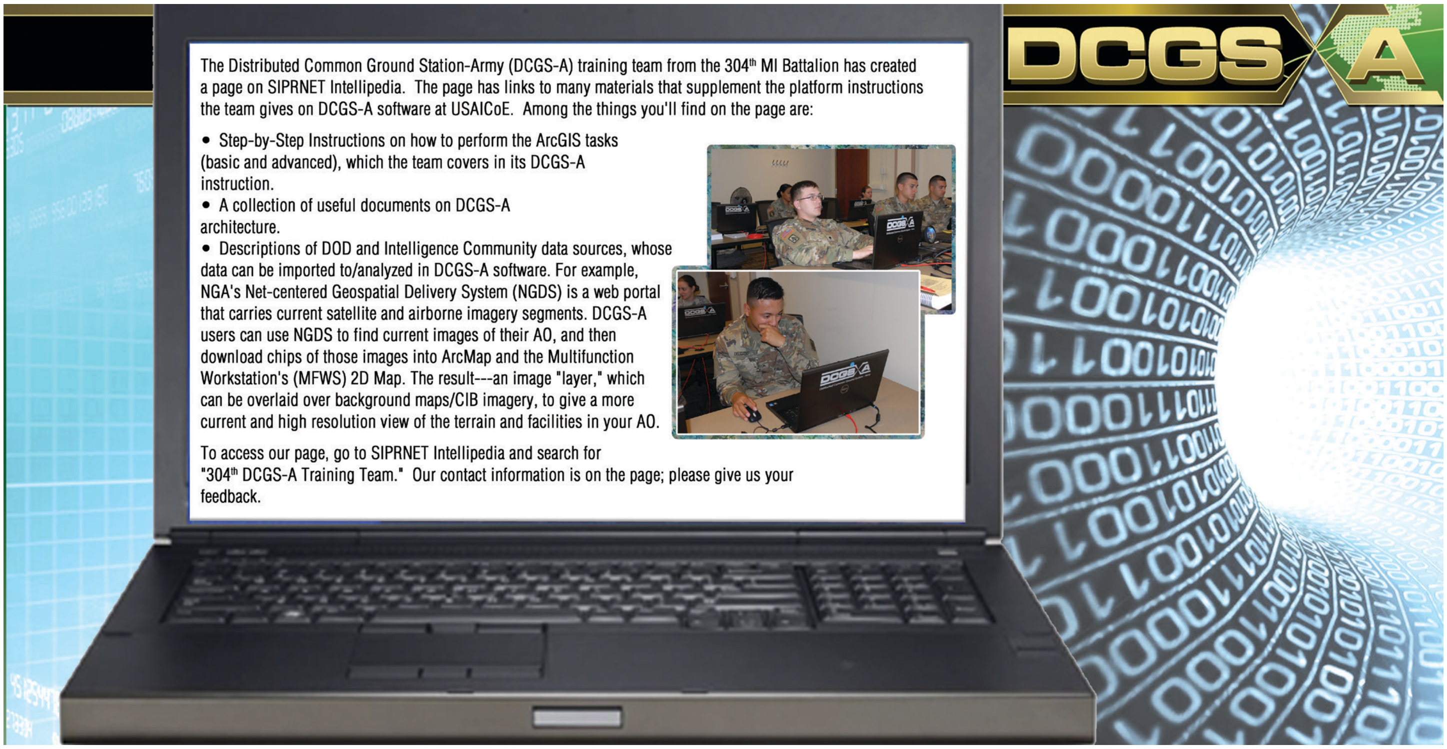
Signals intelligence (SIGINT) elements at the corps, division, brigade combat team, and expeditionary-military intelligence brigade (E–MIB) could form technical control and analysis cells (TCACs). These TCACs would perform administrative functions that ensure subordinate units' adherence to cryptologic access requirements, as well as staff functions that ensure SIGINT integration into operations.

The TCAC will provide technical control, in-depth analysis, integration, and synchronization of SIGINT operations in a distributed environment to de-conflict ongoing national-to-tactical SIGINT operations and to maximize support to the commander through access to the SIGINT enterprise. These actions involve coordination with other intelligence organizations and agencies, both in theater and through intelligence reach, to ensure their SIGINT operations do not conflict with other organizations'/agencies' planned SIGINT operations. The TCAC also creates target packages for SIGINT collection missions and recommends targets for action to the commander. The TCAC conducts detailed analysis to provide actionable intelligence for the commander.

Subordinate to the TCAC are the SIGINT collection teams. These teams provide SIGINT collection, exploitation, and limited analysis to generate actionable intelligence. They detect, track, and locate targets and provide SIGINT support to electronic warfare and cyberspace operations in support of missions within assigned areas of the corps and division area of operations.

At both the corps and the division, the TCAC will be located within intelligence and electronic warfare battalion (corps)/(division) multi-domain military intelligence (MI) detachments of the E–MIB. These detachments conduct multi-discipline intelligence analysis, targeting, and battle damage assessment; SIGINT collection support to electronic warfare and cyberspace operations; and expeditionary processing, exploitation, and dissemination.

At the brigade combat team, the TCAC will be an element of the MI company's intelligence collection platoon.



The Distributed Common Ground Station-Army (DCGS-A) training team from the 304th MI Battalion has created a page on SIPRNET Intellipedia. The page has links to many materials that supplement the platform instructions the team gives on DCGS-A software at USAICoE. Among the things you'll find on the page are:

- Step-by-Step Instructions on how to perform the ArcGIS tasks (basic and advanced), which the team covers in its DCGS-A instruction.
- A collection of useful documents on DCGS-A architecture.
- Descriptions of DOD and Intelligence Community data sources, whose data can be imported to/analyzed in DCGS-A software. For example, NGA's Net-centered Geospatial Delivery System (NGDS) is a web portal that carries current satellite and airborne imagery segments. DCGS-A users can use NGDS to find current images of their AO, and then download chips of those images into ArcMap and the Multifunction Workstation's (MFWS) 2D Map. The result---an image "layer," which can be overlaid over background maps/CIB imagery, to give a more current and high resolution view of the terrain and facilities in your AO.

To access our page, go to SIPRNET Intellipedia and search for "304th DCGS-A Training Team." Our contact information is on the page; please give us your feedback.