

The Army Intelligence Data Platform is the large-scale, enterprise data cloud solution that fuses strategic and operational intelligence, while the Tactical Intelligence Targeting Access Node is the tactical, AI-enabled edge device that directly processes actionable sensor data for frontline units and long-range precision fires. Together, they bridge the gap between global intelligence data and localized, real-time battlefield operations. (U.S. Army photos)



FROM DATA DELUGE TO DECISION DOMINANCE: FORGING THE INTELLIGENCE DATA TEAM

BY COLONEL JAMES LEIDENBERG AND CAPTAIN JENA M. TYSON

Today's Intelligence Data Platforms—Weapon Systems Without a Crew

The modern operational environment, as demonstrated in recent exercises like Warfighter Exercise (WFX) 25-04 and 26-03, is characterized by a data deluge that has overwhelmed traditional intelligence processes. Analysts are bogged down by time-consuming manual tasks. They spend most of their shifts managing data with endless updates to PowerPoint slides and Excel spreadsheets, rather than performing the analysis that drives decision making. This isn't just inefficient—it's dangerous. Stale data, over-reported numbers, and a fragmented common intelligence picture (CIP) paralyze a commander's ability to see the battlefield and act decisively.

Under Army Transformation Initiative 2.0, data is no longer a byproduct of operations; it is a weapon system. However, a weapon system is only effective if it has a trained and ready crew. While the Army is fielding advanced platforms like the Army Intelligence Data Platform (AIDP) and the Tactical Intelligence Targeting Access Node (TITAN), WFX 25-04 proved to the III Armored Corps that the gap is not in hardware; it is in human capital and methodology. To win in large-scale combat operations, the Army must formally establish intelligence data teams (IDTs) at all echelons.

This article reflects how the III Armored Corps G-2 established its IDT program and outlines specific requirements for building these teams. It finds that success requires a specialized "human weapon system" crew led by officers possessing a hybrid blend of military tradecraft and civilian data education. We propose a phased training pipeline—from foundational data literacy to technical mastery—integrated into an Agile project management framework (e.g., Scrum).

These recommendations are designed to nest directly with emerging training guidance. IDTs are uniquely designed to close the gap between advanced platforms and the human capital required to operate them.

A Drought of Insight in a Deluge of Data

The friction points identified in recent exercises are not theoretical. They are tangible obstacles with direct operational consequences.

The Battle Damage Assessment (BDA) Quagmire. The BDA process is a case study in inefficiency. Analysts manually aggregate "kill chats" and unstructured reports, which leads to significant over-reporting of enemy losses and a distorted view of enemy combat effectiveness. During recent Warfighter exercises, the III Armored Corps IDT observed analysts spending several hours each shift manually updating PowerPoint slides. This bean-counting procedure produces stale data and disrupts the decide, detect, deliver, and assess (D3A) targeting methodology.

The Digital RSOI Failure.¹ Recent intelligence and electronic warfare battalion (IEW BN)-Next experimentation revealed a critical requirement for all formations: units must arrive "digitally ready." Without completing this requirement before arriving in theater, units may not be fully capable of maximizing the potential capabilities of the enterprise for several days or longer due to lengthy "digital RSOI" phase requirements. These requirements will consume personnel with basic tasks like account validation, software familiarization, initial setup and provisioning, and data source integration. Units can no longer show up to the fight and expect to be effective; digital readiness must be planned, rehearsed, and validated long before deployment.

The Multinational Bottleneck. The III Armored Corps' recent WFX 25-04 multinational exercise highlighted how current and future operating environments require teams that can rapidly enable multinational data sharing. Recent advances in multinational sharing, including initiatives such as the U.S. Army Intelligence and Security Command Cloud Initiative for the Mission Partner Environment (MPE), as well as sharing digital CIPs through AIDP and Maven Smart System (MSS), are promising. However, the growth of sensors and the data generated by proliferation of artificial intelligence and machine learning (AI/ML) on the battlefield demand more robust and reliable, real-time data exchanges. Sharing must enable coalition forces operating from different intelligence pictures to synchronize targeting and deny the adversary any advantage.

The III Armored Corps Intelligence Data Team Model

To move from passive data consumption to active “data warfare,” the III Armored Corps G-2 established a pilot IDT built on three pillars. This model provides a blueprint for the specialized crew required to operate our data weapon systems.

Hybrid Leadership. The most critical lesson is that the IDT lead cannot be a traditional intelligence officer. The role requires a “hybrid lead”: a company grade officer or warrant officer possessing both operational experience in targeting or collection *and* a civilian degree or certification in Data Analytics, Data Science, or Information Systems Management. Current professional military education does not include courses in Python scripting, Structured Query Language (SQL) database management, or complex Application Programming Interface (API) integrations. The lead must have a background with the Army Strategic Planning System, collection management, or targeting to understand *why* the data matters because, ultimately, the IDT lead must be able to translate the commander's intent into discrete technical tasks for the team.

Agile Management. IDTs cannot operate on a traditional military decision-making process timeline; data development is continuous and iterative. The III Armored Corps IDT adopted the Agile approach to project management using the Scrum framework,² organizing work into one-week “sprints” focused on delivering specific products such as a targeting dashboard or a BDA normalization script. This allows the team to pivot rapidly as battlefield requirements change, ensuring they deliver relevant capabilities at the speed of need. Short, 15-minute meetings identify “blockers” and synchronize efforts between developers and analysts. The Project Manager generates weekly summaries for the Senior Intelligence Officer (a colonel) and Officer in Charge (a captain), focusing on “deliverables” (capabilities built) rather than “activities” (meetings held).

Specialized Personnel Archetypes. Finally, a successful IDT requires a crew with distinct, complementary skills. Trained

personnel from various intelligence military occupational specialties (MOS) can fill these roles:

- ◆ **The Data Steward (the data literacy champion).** Responsible for ensuring data quality, governance, and data entry at the lowest level meet the strict standards required for automated ingestion.
- ◆ **The Data Developer (the builder).** A Soldier trained in the AIDP developer initiative who builds the dashboards and workflows that bypass data bottlenecks.
- ◆ **The Data Scientist (the algorithm master).** Focuses on advanced modeling and AI/ML development to predict adversary actions and automate analysis.

Training and Developing an Intelligence Data Team

The structural integration of IDTs does not require a complete force redesign but rather a specialized alignment within emerging Army structures. At the corps- and division-level, the G-2 IDT is envisioned as the central node for data architecture and governance. It should be collocated with the intelligence and electronic warfare (IEW) systems integration element, expanding its mission beyond managing hardware connectivity to overseeing data-layer management. The team's key mission is to direct the intelligence architecture by managing data pipelines from systems like TITAN, AIDP, and subordinate IEW BNs.

Within the IEW BN, which serves as the tactical engine for intelligence collection, IDTs are embedded at two levels:

- ◆ **The Analysis and Exploitation Company IDT.** Located in the division's technical control and analysis center, it focuses on data normalization, ensuring reports from signals intelligence, geospatial intelligence, and open-source intelligence are correctly formatted for ingestion into the CIP.
- ◆ **The Multi-Domain Military Intelligence Detachment IDT.** This team supports deep sensing and cross-domain targeting by focusing on data analytics, automating sensor data correlation to accelerate the kill chain. The team's role is directly tied to supporting the collection integration and analysis team's integration of intelligence and non-intelligence sensors across the division.

Creating this “human weapon system” requires a deliberate, phased training approach that moves an analyst from basic literacy to technical mastery.

Phase 1—Foundational Data Literacy (Crawl). This phase is for all intelligence professionals. Every analyst must understand that data entry is intelligence production. Courses like the III Armored Corps G-2's “Data Literacy for Intelligence Personnel” establish this baseline, teaching the difference between structured and unstructured data and the impact of “dirty data” on targeting.

Phase 2—Technical Competence (Walk). This phase provides hands-on training for the “builders.” It includes courses such as the Military Data Strategy Course on data governance and the AIDP Foundry/Compass courses on platform-specific development skills.

Phase 3—Collective Readiness (Run). This phase validates the team’s ability to perform under stress. It involves two key events: the Data Communications Exercise, a technical rehearsal to test data flows, and the Digital Command Post Exercise, an exercise to ensure the intelligence architecture is resilient in a denied, degraded, intermittent, and limited environment.

Lessons from Developing Intelligence Data Teams

Analysis of WFX 25-04, WFX 26-03, and associated command post exercises highlighted critical lessons across the DOTMLPF-P spectrum,³ revealing gaps in digital readiness, personnel development, technology, and doctrine that must be addressed to enable data-centric operations.

Doctrine and Organization

- ◆ **Ambiguous technical ownership.** There is ambiguity between the IDT, which is responsible for data flow, and the IEW systems maintainers (MOs 35T/353T), who are responsible for the physical architecture. This creates confusion over who owns the “data fabric.”
- ◆ **Modified table of organization and equipment (MTOE) shortfalls.** Current manning for specialized teams, particularly the multidiscipline analysis team—targeting and the collection integration and analysis team, is insufficient to support sustained 24/7 operations needed to counter a peer threat.

Training and Personnel

- ◆ **Specialized skills gap.** A human capital gap emerged. Success requires a “human weapon system” crew led by hybrid leaders—officers and warrant officers who possess both operational experience and civilian data education in fields like Data Science and Information Systems.
- ◆ **Lack of a formal training pipeline.** There is no institutionalized training pathway to develop data professionals. Bridging this gap will require a structured pipeline with courses in data literacy, Python, SQL, and Agile project management, culminating in the Military Data Strategy Course.

Materiel and Technology

- ◆ **Cross-domain inefficiency.** The lack of organic, mobile cross-domain solutions forces analysts into inefficient “swivel-chair” workflows to manually move data between security enclaves, such as the Secure Internet

Protocol Router Network (SIPRNet) and MPE, resulting in delays.

- ◆ **API and network latency.** In multinational settings, IDTs must understand API settings and data transport quality to move data to the MPE, preventing fragmented intelligence pictures and slowing the sensor-to-shooter cycle to an operationally unacceptable pace.

Digital Readiness and Processes

- ◆ **Unstructured data overload.** The reliance on manual, unstructured data formats such as PowerPoint, Excel, and chat for critical processes like BDA is a major friction point. It leads to stale data, cognitive overload for analysts, and significant over-reporting of combat losses.
- ◆ **Ingestible data not provided.** The full capability of the IDT was hampered because the Mission Command Training Program did not provide the start of exercise data covering units, equipment, and locations in a machine-readable format for ingestion into platforms like AIDP and MSS until after the exercise began.

Recommendations for the Force

By grounding these innovations in the doctrine of the current and developing Training Circular (TC) 2-19 series, the Army will ensure that Army Transformation Initiative 2.0 delivers not just new platforms, but a force capable of wielding data as a decisive weapon. Three concrete steps will transform the IDT from a promising pilot program into a force-wide capability:

- ◆ **Formalize the IDT MTOE.** Modify IEW BN and division G-2 structures to formally code positions for data stewards, developers, and scientists. This will move data expertise from an inefficient, ad hoc additional duty to a dedicated, recognized capability essential to the warfighter.
- ◆ **Institutionalize the hybrid IDT lead profile.** Prioritize company-grade officers and warrant officers with civilian data education for IDT leadership roles. This ensures leaders can bridge the gap between tactical requirements and technical execution, a skill set not currently produced by standard professional military education.
- ◆ **Adopt the Data-Communications Exercise as a training requirement.** Mandate architecture-focused rehearsals as part of the collective training cycle for the IEW BNs and division G-2s in the TC 2-19 series. We must treat intelligence architecture as a warfighting system that, like any other, must be tested, stressed, and validated before the first shots are fired.

Building IDTs is not a futuristic goal; it is an immediate requirement for winning in large-scale combat operations. The military intelligence community must act now.

Conclusion

The lessons from WFX 25-04 and 26-03 are clear: possessing advanced data platforms is not enough. Victory in the next conflict will belong to the force that can turn the deluge of data into decision dominance. By investing in human capital to create trained, agile intelligence data teams with effective leadership, the Army ensures it is building not just new platforms, but a force capable of wielding data as a decisive weapon. ✨

Endnotes

1. Digital RSOI is an updated readiness model that expands on the traditional military process of Reception, Staging, Onward Movement, and Integration (RSOI) to include the technical preparations necessary for modern, data-centric warfare. Its purpose is to ensure that units are “digitally green” and mission-capable on day one of an exercise or deployment, preventing the delays that occur when foundational digital tasks are left until arrival in the field. Key activities of Digital RSOI include: Reception—validating user accounts and network access; Staging—powering on all systems, validating data feeds and API endpoints, and pulling necessary datasets; Onward Movement—familiarizing soldiers with the specific tools, systems, dashboards, and workflows they will use during the mission; and Integration—connecting to the tactical network and confirming data can be exchanged with adjacent units through a digital handshake. This process should begin 30 to 60 days before deployment, if possible, and a Digital Data Execution Checklist often formalizes it to ensure all technical prerequisites are met.

2. Claire Drumond, “What is Scrum? Breaking Down the Agile Framework,” Atlassian, accessed May 27, 2026, <https://www.atlassian.com/agile/scrum>.

3. Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities—Policy.

COL James Leidenberg is the G-2 for III Armored Corps at Fort Hood, TX. He previously served as the 1st Cavalry Division G-2; the 501st Military Intelligence (MI) Brigade Planner; the 504th Expeditionary MI Brigade S-3; 163rd MI Battalion executive officer, 532nd MI Battalion S-2; 1st Brigade Combat Team, 101st Airborne Division S-2; MI Company Commander; and 1st Squadron, 32nd Cavalry Regiment S-2. His previous assignments include joint staff, Army staff, two deployments to Afghanistan, two deployments to Iraq, and 2 years assigned to Korea. COL Leidenberg is a 2004 graduate of the U.S. Military Academy. He holds a master's degree in policy management from Georgetown University and a master's degree in national security and resource strategy with a data and disruptive technologies concentration from Eisenhower School, National Defense University.

CPT Jena Tyson is the Special Security Officer and Officer in Charge of the Intelligence Data Team for III Armored Corps G-2 at Fort Hood, TX. She previously served as a company executive officer, brigade collection manager, battalion S-2, and intelligence collection platoon leader for the 82nd Brigade Engineer Battalion, 1st Infantry Division. Her previous experience includes a deployment to the U.S. Army European Command area of responsibility, two rotations to the National Training Center, and eight years in corporate operations management. CPT Tyson is a 2015 graduate of California State University, Fresno. She holds a master of business administration in data analytics and management from Texas A&M University. Her academic foundation is strengthened by a practical background in coding and data architecture, enabling her to design computational solutions and translate complex data science principles into actionable military intelligence.