

DRAFT — UNOFFICIAL — NOT FOR OPERATIONAL USE

DATA LITERACY

ADRP-SL



DATA LITERACY FOR SENIOR LEADERS

Data Literacy

HEADQUARTERS
UNITED STATES ARMY EUROPE AND AFRICA
(USAREUR-AF)
Wiesbaden, Germany

DRAFT — NOT FOR OFFICIAL USE. FOR TRAINING PLANNING PURPOSES ONLY.

26 MARCH 2026

DRAFT — UNOFFICIAL — NOT FOR OPERATIONAL USE

DATA LITERACY FOR SENIOR LEADERS

HEADQUARTERS UNITED STATES ARMY EUROPE AND AFRICA Unit 29351 APO AE 09014
Wiesbaden, Germany

2026

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies and their contractors only. Other requests must be referred to Headquarters, USAREUR-AF, C2DAO, Wiesbaden, Germany.

PROPONENT: Headquarters, United States Army Europe and Africa (USAREUR-AF), C2DAO

NOTE

This publication is the senior leader companion to Data Literacy Technical Reference. It presents foundational principles and command responsibilities without procedural detail. Senior leaders read this publication; those requiring technical depth consult Data Literacy Technical Reference.

DATA LITERACY FOR SENIOR LEADERS

COMMANDING GENERAL'S NOTE

[To be inserted upon receipt of signed CG guidance — to be provided by C2DAO prior to publication.]

PREFACE

This publication establishes data literacy principles and command responsibilities for USAREUR-AF. Audience: O-5 and above, CSM, SGM, and senior Civilian equivalents.

USAREUR-AF is the ASCC to USEUCOM and USAFRICOM, responsible for theater land operations across the European and African AOR. Subordinate commands include III Corps, V Corps (Forward), 21st Theater Sustainment Command (21 TSC), 7th Army Training Command (7ATC), 10th AAMDC, 56th MDC-E, and SETAF-AF. USAREUR-AF supports NATO Article 5 and operates in a coalition environment

requiring data interoperability with Allied nations. Adversary forces actively exploit data gaps and analytical failures. Data literacy is therefore more operationally consequential here than in any peacetime garrison environment.

This publication implements ADP 3-13, Information. It tells senior leaders what they are responsible for and why it matters. Technical guidance belongs in Data Literacy Technical Reference.

CHAPTER 1 — WHY DATA LITERACY MATTERS FOR SENIOR LEADERS

BLUF: Data-literate commands win. Data-illiterate commands are surprised. The commander sets the standard.

1-1. Bottom Line Up Front

Every modern military operation generates and depends on data. Logistics status, personnel readiness, threat assessments, route conditions, and sensor feeds are all data products. Commanders who understand what data tells them — and what it does not — make better decisions under pressure. Commanders who cannot read, question, or direct data products cede decision advantage to the enemy, to their own biases, and to whatever their staff decides to show them.

Data literacy for senior leaders is a combat multiplier.

1-2. The Operational Reality

USAREUR-AF and NATO ground forces are already integrating allied sensors, data, and AI-powered analytical tools into real-time decision-making. This is not a projected capability — it is operational today. Formations whose leaders cannot direct, evaluate, and integrate data products are already behind.

Commanders already depend on data whether they recognize it or not. Every COP update, readiness report, and intelligence summary is a data product. The question is not whether commanders use data — they do. The question is whether they use it deliberately, critically, and effectively.

In USAREUR-AF's operational environment, data volume has increased faster than formations' capacity to use it. Without data-literate leaders directing the analytical effort, formations either drown in data or ignore it entirely. Both outcomes degrade decision quality.

NOTE

Data-literate leaders at every echelon are required to sustain and extend USAREUR-AF's operational data advantage.

1-2a. The ODT Model — What Senior Leaders Need to Know

Operational Data Teams (ODTs) are multifunctional teams of product managers, designers, software engineers, data engineers, and data scientists that solve operational problems with data at the speed of need. XVIII Airborne Corps was among the first to pilot the concept beginning in 2022 and published their experience in *Military Review* (February 2026). The MCCoE has since codified ODT employment in the Decision Optimization CONOPS. The XVIII ABC model is one corps' pilot approach — USAREUR-AF and other commands are adapting the concept to their own echelon, mission, and manning realities. Notably, LTG Donahue directed the original Data Warfare Company activation at XVIII ABC and now commands USAREUR-AF, providing continuity of vision. The principles below are drawn from XVIII ABC's experience — senior leaders should understand them as reference points from one corps' pilot, not rigid prescriptions.

What a senior leader must understand about ODTs:

Principle	Implication for Commanders
ODTs solve problems, not requests	Staff elements articulate a problem — not a desired solution. The ODT determines the best technical approach. Directing a specific solution ("build me a dashboard that shows X") bypasses the scoping process and often produces less effective outcomes.
Capacity is finite	A single ODT executes 2 tasks per sprint: 1 development, 1 scoping. Starting work on a new problem requires the ODT to stop work on another. There will always be more data-centric problems than time to solve them.
Governance prevents overextension	XVIII ABC learned this the hard way: without a CG-signed governance policy, too many customers requested ODT resources simultaneously, and efforts became overextended on unrealistic timelines. The governance process is a command responsibility.
MVP timeline: at least 5 months	Scoping (2 wk) → Discovery (4 wk) → Framing (4 wk) → Development (8 wk) → Handoff (2 wk). This is the fastest responsible timeline. Pressure to deliver faster degrades quality.
Exercise integration is deliberate	During exercises, MVP products receive only bug fixes and minor adjustments. Products in early phases get user research, not development. This is by design — exercises are for validation, not feature development.

The XVIII ABC proof point: Their ODT delivered a BDA visualization capability — prototype in 3 months, MVP in 6, handoff to an Army program of record in 9. The commander defined the problem ("visualize attrition of the enemy integrated fires complex in real-time"), the ODT built the solution, and it has since been adopted across four divisions and is being absorbed by Army enterprise programs. That is what a properly resourced, governed, and trained ODT delivers.

NOTE

The MSS training curriculum (TM-10 through TM-50) is the pipeline that produces the personnel who staff ODTs. Senior leaders who resource MSS training are building the workforce that enables the ODT model at echelon.

Source: Forney, Herrmann, and Steele, "Fighting with Live Data," *Military Review Online Exclusive*, February 2026.

1-2b. Automated Fighting Products — What Your Staff Is Building

One useful framing for the evolution of staff products comes from Adkins ("Achieving Decision Dominance," *Military Review*, January-February 2025), a thought piece proposing terminology for data-enabled operations:

Generation	Format	Example	Limitation
Analog	Hand-written	OPORD shell filled out in the field	Slow, no data connection, single copy
Digital	Excel / PowerPoint / SharePoint	Staff running estimate in a shared drive	Manual data entry, no live feed, version control problems
Automated (AFP)	Visualization tool connected to live data	MSS dashboard auto-refreshing from GCSS-A pipeline	Requires trained builders, governance, and platform access

MSS applications are AFPs. Every dashboard your staff uses, every readiness tracker, every SITREP generator — these are Automated Fighting Products connected to live, authoritative data sources. Adkins names the Maven Smart System as an ASCC-level COP platform for this capability.

What senior leaders must understand about AFPs: - AFPs reduce the time required to produce staff running estimates — freeing cognitive bandwidth for analysis and planning - AFPs must be built, tested, and validated **before** they are needed in combat — Adkins calculates that a division has as little as 2:22 to deploy new tools while in contact - Untrained personnel cannot build or maintain AFPs — the MSS training program (TM-20 through TM-50) is the pipeline that produces AFP builders - AFPs are not "nice-to-have IT projects" — they are operational capabilities on the same plane as any other weapon system that requires trained operators

NOTE

Adkins argues that without a programmatic approach to decision dominance, tactical commanders will default to ad hoc methods that do not scale under LSCO conditions. The MSS training program addresses this concern by building a systematic training pipeline. (*Adkins is one officer's proposal — the Forney "Fighting with Live Data" article in Section 1-2a above documents the most relevant pilot experience for how ODTs operationalize these concepts.*)

Source: Adkins, "Achieving Decision Dominance," *Military Review* 105, no. 1 (January-February 2025).

1-3. What Data Literacy Means for a Senior Leader

Data literacy for a senior leader is NOT the ability to write code, build databases, or design analytical pipelines. A data-literate senior leader does the following:

Competency	Description
Direct	Specify what data is needed and why, linked to CCIR
Question	Ask the right questions about a data product before accepting its conclusions
Evaluate	Identify red flags — gaps, inconsistencies, unsupported claims
Integrate	Connect data products to decisions without over-relying on any single source
Resource	Allocate people, time, and tools to data tasks as deliberate capability investment
Protect	Enforce classification and access control discipline as a command responsibility

1-4. The VAULTIS-A Standard — What Makes Data Trusted

Before acting on a data product, commanders must assess it against eight quality dimensions. The current authoritative standard is **VAULTIS-A** (DDOF Playbook v2.2, T2COM C2DAO, December 2025), which extends the DoD Data Strategy's 7-dimension VAULTIS framework by adding Auditable.

Dimension	Target	Commander's Question
V — Visible	100%	Can we find this data when we need it?
A — Accessible	99%	Do the right people have access within SLA?
U — Understandable	100%	Does the staff know what this actually measures? Is metadata complete?
L — Linked	100%	Can we trace this data from source to decision product?
T — Trusted	95%	Do we have confidence in the source, method, and sponsor sign-off?

Dimension	Target	Commander's Question
I — Interoperable	90%	Can we exchange this with joint and Allied partners on approved platforms?
S — Secure	100%	Are classification markings correct and access controls enforced?
A — Auditable	100%	Can we prove who accessed this data and every transformation it underwent?

Quality Gate: 85% minimum weighted average across all eight dimensions to pass DDOF Phase 3. Products below threshold are returned for remediation.

A data product that fails any VAULTIS-A dimension introduces risk into the decision it supports. Commanders must require explicit VAULTIS-A evaluation for significant decisions.

NOTE

The earlier 5-dimension VAULTI standard (AR 25-1, 2019) has been superseded. The three new dimensions — Linked, Secure, Auditable — address gaps in traceability, security compliance, and provenance that are critical in the USEUCOM theater environment.

In the USEUCOM AOR, interoperability carries additional weight. Data products shared with NATO Allies must meet both U.S. standards and applicable NATO data exchange standards. Interoperability is Allied nations' foremost concern, and the root cause is trust — trust that is solvable through disciplined data standards and rigorous security protocols. Data standards, disciplined handling, and rigorous security protocols build that trust at the working level.

1-5. Decision Dominance

Decision dominance is the operational objective of superior data and analytical capability: to make better decisions than the adversary, faster, and at higher confidence. It is not a technological state — it is a command state achieved through disciplined data collection, rigorous analysis, and effective integration of information into command decisions.

In the USAREUR-AF AOR, where adversary forces invest heavily in deception, EW, and IO designed to degrade Allied situational awareness, decision dominance is a competitive requirement. Senior leaders are responsible for building and maintaining their formation's capacity for decision dominance. This means investing in data capability as a readiness priority.

1-6. The Cost of Data Illiteracy — Three Vignettes

Vignette 1 — The Invisible Readiness Gap. A brigade commander reviewed weekly readiness reports and consistently saw green across all subordinate units. Three days before a V Corps exercise at Grafenwöhr, the brigade discovered that one battalion had been manually entering estimated values for

deadline equipment rather than pulling live data from the maintenance system. The exercise launched with a 22 percent vehicle shortfall no brigade-level leader had known about. The commander had never asked how the data was collected or validated.

Vignette 2 — The Confident Wrong Answer. A staff officer presented a route analysis showing three viable MSRs into an assembly area near the Suwałki Gap, supported by a detailed chart with color coding and statistics. The commander approved the plan. During execution, the lead element encountered an impassable bridge — documented in an engineer survey from the previous week that had not been integrated into the analysis. The data product had looked authoritative. The commander had not asked what data sources it drew from or how current they were.

Vignette 3 — The Culture That Punished Honesty. A battalion intelligence section consistently reported high-confidence threat assessments. Pressure from senior leaders for clear, actionable products had led analysts to remove uncertainty language from their reports. The battalion operated for weeks with misplaced confidence in threat assessments that had significant gaps. When contact occurred in an unexpected location along a Baltic flank corridor, the commander was surprised. The staff had known about the gaps. They had learned not to report them.

1-7. The Commander's Role in Building a Data-Literate Formation

Culture is set by command. If the commander does not ask data-driven questions, subordinates will not prepare data-driven answers. If the commander accepts charts without questioning their sources, staff will produce charts without validating their sources. The standard the commander walks past is the standard the formation adopts.

Building a data-literate formation requires three things: demand honest data products including uncertainty; resource the capability to produce them; model data-critical behavior in every briefing, planning session, and AAR.

1-8. Doctrinal Foundation — ADP 3-13 and Information Advantage

SIDEBAR: ADP 3-13 — Data Is the Raw Material of Combat Power

ADP 3-13, *Information* (2023), establishes that information is combat power. It defines *information advantage* as the operational condition achieved when a force generates, protects, and exploits information more effectively than the adversary.

Data literacy is the prerequisite for that advantage.

Information advantage begins with data. Without disciplined data collection, rigorous data quality, and leaders who can direct and evaluate data products, no formation can generate the analytical outputs that information advantage requires. A formation with excellent data practices is more resistant to adversary

deception, better able to maintain situational awareness under pressure, and faster to recognize and act on opportunity.

For USAREUR-AF, operating within a coalition theater where adversaries actively contest the information environment, this connection is operationally urgent. Building data literacy is not separate from information operations — it is its foundation.

This publication implements ADP 3-13 by establishing the data literacy foundation required for information advantage in the USAREUR-AF AOR. Data literacy is not separate from information operations — it is its prerequisite. A commander who cannot direct and evaluate data products cannot generate the quality analytical outputs that information advantage requires.

1-9. NATO and EUCOM AOR Context

USAREUR-AF data operations must comply with NATO Architecture Framework version 4 (NAFv4) and support interoperability with Allied Joint Publications (AJP-01, AJP-3, AJP-5). Data systems, data products, and sharing practices must be designed for coalition use. Commanders must ensure data products shared with Allied or partner nation forces are marked under both U.S. and NATO classification standards and that systems can exchange information with Allied equivalents.

Europe serves as the premier battle laboratory for building the lethal, data-driven force required to meet any adversary. The real-time C2 system established in USAREUR-AF must now be scaled globally. Commanders and formations that master data-driven operations here are building the template the Army will export worldwide.

CHAPTER 2 — CORE PRINCIPLES OF DATA-DRIVEN COMMAND

BLUF: Eight principles define how commanders should think about and use data. These apply regardless of operation type, tool, or echelon.

2-1. Principle 1 — Data Is Ammunition

Data is a tactical and operational resource. Like ammunition, it must be collected deliberately, protected from the adversary, and expended at the right time for the right purpose. Commanders must treat data requirements with the same rigor they apply to logistics planning.

2-2. Principle 2 — Quality Over Quantity

One trustworthy data product is worth more than ten unreliable ones. Formations under time pressure default to the most available data, even if poor quality. Commanders must establish and enforce data quality standards before operations, not during them. When quality is uncertain, demand explicit uncertainty statements rather than false precision.

2-3. Principle 3 — Context Converts Data Into Intelligence and Decisions

Raw data has no value without context. A number means nothing without knowing what it measures, when it was collected, how it was collected, and what it is being compared to. Commanders must demand that data products include source, collection method, time, and known limitations — not just findings. Analysis without context is assertion.

2-4. Principle 4 — Commanders Must Ask the Right Questions

Analytical effort follows commander guidance. Establishing PIR and FFIR is the mechanism by which commanders direct analytical effort. A vague CCIR produces vague data products. A precise requirement produces focused, actionable analysis.

2-5. Principle 5 — Automation Enables Scale; Judgment Enables Decisions

Automated systems can process data at volumes and speeds no human can match. They cannot exercise judgment. Commanders must understand what their automated systems are and are not doing. Commanders who treat automated outputs as decisions — rather than inputs — have surrendered their judgment to their tools.

2-6. Principle 6 — Data Lineage Enables Trust and Accountability

Data lineage is the documented trail of where data came from, who handled it, what transformations were applied, and when. Without lineage, a commander cannot assess whether a data product is trustworthy. Commanders must require that data products used for significant decisions include a clear lineage statement.

2-7. Principle 7 — Security Is Not Optional

Data classification and access control are command responsibilities. Data aggregation — combining multiple unclassified elements — can produce a classified product. Commanders must enforce classification discipline and ensure data sharing practices comply with applicable security requirements. A data breach caused by poor access discipline is a command failure.

2-8. Principle 8 — Culture Is Set by Command

If the commander does not use data, neither will the formation. If the commander punishes uncertainty — by reacting negatively to "we don't know" answers — the formation will stop reporting uncertainty and start producing false confidence. The commander's daily behavior in briefings, planning sessions, and AARs defines the formation's data culture. No training program compensates for a command climate that does not value honest, rigorous data use.

CHAPTER 3 — COMMANDER'S DATA RESPONSIBILITIES

BLUF: Commanders have seven core data responsibilities. These are not delegated tasks — they are command functions. The C2DAO is the commander's primary advisor and enforcer across all of them.

3-1. The Command Chief Data and Analytics Officer (C2DAO)

The C2DAO is the commander's primary advisor on data governance, data quality, platform use, and compliance with Army enterprise data policy. The C2DAO implements and enforces policy established at HQDA — it does not create that policy.

Echelon	Role
HQDA MADOs (Major Army Data Owners)	Establish enterprise data standards and policy
Data Stewards	Own and enforce standards for designated data domains
Functional Data Managers	Manage data within functional areas
C2DAO (Command Level)	Advise commander; integrate governance; enforce compliance

The C2DAO is effective only to the extent the commander empowers the role. A C2DAO without resourcing, access to leadership, and command backing cannot enforce standards across a formation. Commanders are responsible for resourcing and empowering their C2DAO.

Use the C2DAO for: - Assessing the formation's data governance posture - Evaluating readiness of data systems before major operations or exercises - Reviewing compliance with Army CIO guidance (2024) and UDRA v1.1 (2025) - Advising on data sharing arrangements with NATO Allies and partner nations - Escalating data quality or security issues crossing functional boundaries

3-2. Establishing Data Requirements

Data requirements must be linked to decisions. Every CCIR implies a data requirement. Commanders must be able to answer: what data will tell me whether this requirement has been satisfied? Vague CCIRs produce vague collection and analysis.

Question	Purpose
What decision does this data support?	Ensures data serves a decision, not a briefing
What does "satisfied" look like?	Creates a clear threshold for action
When do I need it?	Sets collection and reporting timeline
What is the acceptable confidence level?	Defines quality standard up front
What happens if I don't get it?	Forces assessment of decision risk

3-3. Appointing and Supporting Data Stewards

Every formation managing significant data needs a data steward — the individual responsible for accuracy, completeness, and appropriate handling of a specific dataset or system. Commanders must formally appoint data stewards and define responsibilities in writing. Appointment without authority is ineffective. Data stewards are not administrators — they are quality owners.

3-4. Demanding Data Quality Standards

Commanders define quality by what they accept. Minimum standards when receiving data products in any formal setting:

- Source and collection method are identified
- Data currency (age) is stated
- Known gaps or limitations are disclosed
- Confidence levels are expressed, not implied
- Derived figures (calculations, estimates) are distinguished from raw collected data

Apply these standards consistently, not just in high-stakes briefings. Inconsistent standards produce inconsistent quality.

3-5. Data in the MDMP

MDMP Step	Commander's Data Role
Receipt of Mission	Identify initial information gaps; issue initial CCIR

MDMP Step	Commander's Data Role
Mission Analysis	Validate data requirements against mission variables; assign collection tasks
COA Development	Specify what data each COA assumes; flag untested assumptions
COA Analysis (Wargame)	Test COAs against data uncertainty — what if the data is wrong?
COA Comparison	Require explicit data basis for each comparative factor
Orders Production	Ensure data requirements and reporting triggers are in the OPORD
Execution and Assessment	Monitor CCIR status; adjust collection effort as situation develops

3-6. Resourcing Data Capability

Data capability requires people with skills, tools that work, time to do the analysis, and a command climate that rewards doing it well. Assess three factors:

People. Do staff sections have personnel with sufficient skill? Are they employed on data tasks or diverted? Is there a training path that develops data skills over time?

Tools. Do the tools meet the formation's data needs? Are they operational, licensed, and maintained? Do personnel know how to use them effectively?

Time. Is analytical effort protected from administrative tasks? Is there time in the battle rhythm for analysis — not just reporting? Are deadlines realistic given available capacity?

Underfunding data capability while demanding data products is a command contradiction.

3-7. Enforcing Data Security and Classification Discipline

Commanders are responsible for the classification and access control practices of their formation. Commanders must ensure:

- Data products are classified at the appropriate level based on content, including aggregation effects
- Access to sensitive data systems is granted on a need-to-know basis, not convenience
- Personnel transfers and departures are accompanied by prompt access revocation
- Data sharing with partner nations, joint forces, or external agencies follows applicable security agreements
- Data breaches or suspected unauthorized access are reported immediately through proper channels

In the USEUCOM AOR, coalition data sharing carries additional complexity. Data products shared with NATO Allies must comply with both U.S. classification standards and applicable NATO handling requirements. Classification discipline is not the S-6's problem — it is a command problem.

CHAPTER 4 — EVALUATING DATA PRODUCTS

BLUF: Commanders must be active consumers of data products — not passive recipients. Every briefing is an opportunity to enforce standards, identify gaps, and direct analytical effort.

4-1. Questions Every Commander Should Ask

Question	What It Uncovers
What is the source?	Origin and potential bias of the data
How was this collected?	Method limitations, sampling gaps, reporting errors
How current is this data?	Whether conditions may have changed
What is not included here?	Gaps the product may not advertise
What is the confidence level?	Distinguishes findings from estimates
What assumption is this built on?	Untested premises that may invalidate the product
What would change this conclusion?	Robustness of the finding
Who produced this and do they have conflicts of interest?	Organizational or analytical bias

4-2. Red Flags in Data Products

Red Flag 1 — No Uncertainty Stated. Products presenting findings without confidence levels, margins, or acknowledged limitations are incomplete. Real analysis always has uncertainty.

Red Flag 2 — Precision Without Basis. "Enemy force is 847 personnel" based on observer reports warrants scrutiny. False precision signals numbers were manipulated to appear more authoritative than the underlying data supports.

Red Flag 3 — Conclusions That Confirm Existing Assumptions. If every product confirms what the commander and staff already believe, the analytical process may be producing advocacy rather than analysis. Honest data frequently surprises.

Red Flag 4 — Missing Data Described as Zero. "No reports of enemy activity in sector" is not "no enemy activity in sector." Missing data must be disclosed as missing, not treated as evidence of absence.

Red Flag 5 — No Audit Trail. If the analyst cannot explain where the data came from, what transformations were applied, and who reviewed it, the product does not meet minimum standards.

Red Flag 6 — Single-Source Products for High-Stakes Decisions. One source is insufficient for decisions with significant operational consequences. Require corroboration.

4-3. Understanding Uncertainty and Confidence Levels

Uncertainty is not weakness — it is honesty. Commanders who demand certainty will receive false certainty. A high-confidence assessment based on poor data is not trustworthy. A low-confidence assessment based on strong data may be more reliable than it appears. Commanders must understand both factors.

The appropriate response to uncertainty is risk management: identify what you know, what you do not know, and what you need to find out before the decision point. Assign collection tasks to close critical gaps and make decisions with explicit acknowledgment of residual uncertainty.

NOTE

Intelligence products use defined confidence level terminology (high, moderate, low). When working with non-intelligence data products — logistics, personnel, engineering — require equivalent language. "We think" and "the data suggests" are not confidence statements. "Based on three independent sources with collection from the last 48 hours, we assess with moderate confidence" is.

4-4. Distinguishing Correlation from Causation

Correlation means two things move together. Causation means one thing causes another. These are not the same. Confusing them leads to actions that do not produce expected results.

Example: Incidents increase on days when a particular patrol route is used along a contested corridor in the eastern AOR. That is correlation. The cause may be the route — or both the route use and the incidents may be driven by elevated threat conditions. Acting on correlation as if it were causation (stopping the route) may not reduce incidents if the route was not the cause.

Commanders should require analysts to explicitly state whether a relationship is correlational or causal and to explain the basis for that claim.

4-5. Directing the Analytical Effort

Commanders direct analytical effort through requirements, not by telling analysts what conclusions to reach. Directing conclusions corrupts analytical integrity.

Commanders specify: - What question needs to be answered - What decision the answer will inform - When the answer is needed - What level of confidence is acceptable given the stakes

Commanders do NOT specify: - What answer is expected - What data sources to prioritize in ways that bias the outcome - That uncertainty should be removed from products before briefing

Analysts directed toward conclusions rather than questions will eventually produce the conclusions the commander wants — regardless of what the data says. That is how formations end up surprised.

CHAPTER 5 — BUILDING A DATA-MITERATE FORMATION

BLUF: Data literacy is a trained and developed competency, not a natural talent. Commanders build it through deliberate training, integration into collective events, and consistent command climate.

5-1. Training Requirements and the Data Literacy Continuum

Data literacy exists on a continuum. Not every Soldier needs the same level of proficiency. The USAREUR-AF data literacy training framework consists of five tiers organized as Technical Manuals (TMs).

Tier	Target Audience	Core Competency
TM-10 (Operator)	All personnel	Navigate and consume data products on MSS; observe data security and accuracy standards
TM-20 (Builder)	All personnel	Build basic Workshop applications; run light transforms; manipulate and share data products
TM-30 (Advanced Builder)	Data-adjacent personnel (17/25-series, S6/G6/G2)	Design pipelines and Ontology objects; build complex dashboards; apply governed data patterns
TM-40 Series (Specialist)	Designated specialist roles	Role-specific mastery: WFF tracks (A–F) and technical tracks (G–O)
TM-50 Series (Advanced Specialist)	TM-40 graduates in senior/lead roles	Research-grade capability; leads and mentors others in specialist track

Senior leaders sit at the TM-10 level for technical skills and at a distinct "Commander" level for direction, evaluation, and command responsibilities.

NOTE

Gaps in training coverage are a readiness issue, not an administrative issue. A formation with no personnel trained to TM-20 on a critical data system is as vulnerable as a formation with no personnel qualified on a critical weapons system.

5-2. Key Training Outcomes by Tier

TM-10 — Operator: Navigate MSS; understand data vs. information distinction; know responsibilities for accurate data entry; recognize and report data quality problems; observe classification requirements.

TM-20 — Builder: Build basic Workshop applications and simple pipelines; apply data quality standards; identify and escalate data integrity issues; produce basic analytical products.

TM-30 — Advanced Builder: Design Foundry pipelines and Ontology objects; build governed data products for formation-wide use; perform analytical validation and data profiling; support the data requirements process; mentor TM-10/20 users.

TM-40 Series — Specialist: Role-specific mastery within a defined track; produce command-level data products independently; apply advanced analytical, engineering, or operational methods.

TM-50 Series — Advanced Specialist: Lead and mentor within the specialist track; conduct research-grade analysis; design new frameworks, tools, and capability; develop and update training materials.

5-3. Integrating Data Tasks Into Collective Training

Data literacy is best developed in context — during the tasks it supports.

STX. Include data entry, reporting, and quality check tasks in STX lane design. Train Soldiers and NCOs to enter accurate data under time pressure and flag discrepancies.

FTX. Operate formation data systems in field conditions. Require data products — readiness reports, logistics status, assessment products — to meet quality standards throughout. Use AARs to identify and correct data discipline failures.

CPX. Exercise the full data product chain from collection requirement to command-level brief. Require staff to source their briefing products and disclose uncertainty. Practice the commander's questioning routine on every data product presented.

NOTE

If data quality standards are relaxed during training because of time pressure or administrative convenience, the formation will relax them during operations for the same reasons. Train the standard you intend to enforce.

5-4. Creating Conditions for a Data-Driven Culture

Recognition. Identify and recognize personnel who catch data errors, produce high-quality analytical products, or improve data practices in their section.

Expectation. Set explicit standards for data products in all formal briefings and planning events. Publish those standards. Apply them consistently.

Resourcing. Fund training time, protect analytical personnel from unrelated taskings, and acquire tools that enable the standard. A command that requires excellent data products but does not provide time, tools, or training has made an unfunded mandate.

Senior NCO leadership is critical. CSMs and SGMs who enforce data discipline in unit administration, training management, and NCO development reinforce the command climate the commander sets at the top.

5-5. Key Indicators of a Data-Literate Formation

Indicator	What It Signals
Staff volunteers uncertainty in briefings without being asked	Formation trusts that honesty is safe
Data products include source, currency, and confidence by default	Quality standards are internalized, not enforced by exception
Data errors are reported up, not hidden	Command climate rewards accuracy over appearance
CCIRs drive collection planning, not reporting formats	Data requirements are linked to decisions
Data stewards are empowered to reject non-compliant products	Authority matches responsibility
Collective training uses live data systems under realistic conditions	Training replicates operational conditions
AARs identify and correct data failures, not just tactical failures	Data is treated as an operational domain

KEY TERMS

AAR — After-Action Review. Structured review of events to identify what happened and why.

Analytical Pipeline — Sequence of steps that transform raw data into an analytical product.

Audit Trail — Documentation of data origin, handling, and transformations.

C2DAO — Command Chief Data and Analytics Officer. Commander's primary advisor on data governance, quality, platform use, and Army enterprise data policy compliance. Implements and enforces enterprise policy established by HQDA MADOs.

CCIR — Commander's Critical Information Requirements. Information the commander requires to make timely decisions; includes PIR and FFIR.

Confidence Level — Expressed degree of certainty in an analytical assessment.

COP — Common Operating Picture. Shared display of relevant operational information.

Correlation — Statistical association between two variables; does not imply causation.

Causation — One variable directly produces change in another.

Data Currency — How recent the data is; the age of a data product.

Data Lineage — Documented chain of a dataset's origin, handling, and transformation.

Data Literacy — Ability to read, evaluate, direct, and act on data products at a level appropriate to one's role.

Data Quality — Degree to which data is accurate, complete, consistent, and timely.

Data Steward — Individual responsible for accuracy and appropriate handling of a dataset.

Decision Dominance — The operational state in which a force makes better decisions than the adversary, faster, and at higher confidence — achieved through superior data collection, analytical rigor, and effective command use of information products.

FFIR — Friendly Force Information Requirements. Information the commander needs about friendly forces.

HQDA MADOs — Major Army Data Owners. HQDA organizations with enterprise authority over designated Army data domains. They establish standards and policy that Data Stewards, Functional Data Managers, and C2DAOs implement at command level.

MDMP — Military Decision-Making Process. Army's deliberate planning process; seven steps from receipt of mission through orders production.

PIR — Priority Intelligence Requirements. Intelligence the commander needs to understand the threat and environment.

Red Flag — Characteristic of a data product warranting additional scrutiny before use.

UDRA — Unified Data Reference Architecture. Army enterprise data architecture standard. UDRA v1.1 (2025) is the current version.

Uncertainty — Acknowledged limits of confidence in data or analytical conclusions.

VAUTI — Original 5-dimension data quality framework (AR 25-1, 2019). **Superseded** by VAULTIS/VAULTIS-A. See VAULTIS-A.

VAULTIS-A — Current 8-dimension data quality standard (DDOF Playbook v2.2, December 2025): Visible, Accessible, Understandable, Linked, Trusted, Interoperable, Secure, Auditable. 85% minimum weighted average required to pass DDOF Phase 3 quality gate. Supersedes VAUTI and extends DoD VAULTIS.

ADP 3-13 — Army Doctrine Publication 3-13, Information. Establishes information as combat power and defines information advantage as a key operational objective.

Information Advantage — Per ADP 3-13: the operational condition achieved when a force generates, protects, and exploits information more effectively than the adversary.

JADC2 — Joint All-Domain Command and Control. DoD concept connecting sensors, shooters, and decision-makers across all domains.

NAFv4 — NATO Architecture Framework version 4. NATO standard for data and system architecture.

USEUCOM — United States European Command. One of two Combatant Commands to which USAREUR-AF serves as ASCC (the other being USAFRICOM).

REFERENCES AND RELATED PUBLICATIONS

ADP 3-13, Information — Establishes information as combat power and the foundation for information advantage. This publication implements ADP 3-13 at the senior leader level.

ADP 5-0, The Operations Process — Defines the MDMP and the role of information in planning and execution.

Data Literacy Technical Reference, Data Literacy — Technical companion to this publication. Contains procedural guidance, analytical methods, data lifecycle doctrine, and the USAREUR-AF 5-Layer Data Stack architecture.

AR 25-1, Army Information Technology (Jul 2019) — Statutory framework for Army data governance and IT management policy. Established the original VAUTI (5-dimension) data quality standard, now superseded by VAULTIS-A.

DoD Data Strategy (2020) — Establishes the VAULTIS framework (7 dimensions) as the DoD standard for enterprise data quality. Supersedes VAUTI.

DDOF Playbook v2.2 (December 2025) — T2COM C2DAO implementing document. Extends VAULTIS to VAULTIS-A (8 dimensions, adds Auditable). Establishes the 6-phase data product lifecycle and 85% minimum quality gate. Current authoritative standard for MSS data products.

Army CIO Guidance (2024) and UDRA v1.1 (2025) — Current governance and architecture codified in Army CIO guidance (2024) and UDRA v1.1 (2025). The C2DAO ensures USAREUR-AF compliance.

CALL 25-10, Commander and Staff Guide to Data Literacy (April 2025) — Center for Army Lessons Learned handbook providing an accessible introduction to data literacy tailored for commanders and staff. Covers data interpretation, analysis, and application within military contexts including intelligence analysis and operational planning. Progresses from foundational concepts to real-world applications. Directly complements this publication.

NATO Architecture Framework version 4 (NAFv4) — NATO standard for data and system architecture. USAREUR-AF data operations must align to NAFv4 for coalition interoperability.

Allied Joint Publications (AJP-01, AJP-3, AJP-5) — NATO joint doctrine governing operations, conduct, and planning.

C2DAO — Authoritative source for technical architecture guidance, ontology standards, NATO NAFv4 alignment resources, and the USAREUR-AF 5-Layer Data Stack implementation documentation.

DoD Data, Analytics & AI Adoption Strategy (November 2023) — Establishes the AI Hierarchy of Needs and the DoD framework for scaling data, analytics, and AI adoption across the enterprise.

Brito, Gary M. "Data Literacy: How We Prepare for the Future." *Military Review Online Exclusive*, January 2025. — TRADOC Commanding General's statement on Army-wide data literacy as a readiness imperative. Establishes senior leader intent for data-literate formations at every echelon.

DATA LITERACY FOR SENIOR LEADERS HEADQUARTERS, UNITED STATES ARMY EUROPE AND AFRICA (USAREUR-AF) Wiesbaden, Germany 2026

By order of the Commanding General, United States Army Europe and Africa.

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies and their contractors only. Other requests must be referred to Headquarters, USAREUR-AF, C2DAO, Wiesbaden, Germany.