Beyond SATCOM: How Tactical Radios and Cyber Defense Forge Coalition Resilience

Author: LTC Vernon V. Logan
CALL Analyst: Willis D. Heck III

No. 26-1142
April 2026

Introduction

To maintain decision advantage in contested environments, commanders must build a resilient communications architecture layered with tactical radios and integrated cyber defense. While commercial SATCOM provides reach, its vulnerabilities to jamming, spoofing, and cyber intrusion demand a robust PACE plan. The U.S. Army Southern European Task Force, Africa (SETAF-AF) G6 actively advances this capability by improving multinational interoperability through research, targeted training, and operational collaboration. Lessons from exercises like Justified Accord demonstrate that interoperable radios and shared cyber readiness build the trust and cohesion essential for effective mission command. SETAF-AF is codifying these insights into new defensive cyber operations (DCO) curriculum for the Kenya Defence Forces (KDF) and other regional partners, creating a framework that strengthens theater security cooperation, enhances partner readiness, and ensures resilient mission command at the tactical edge.

Limitations of Commercial SATCOM

Commercial SATCOM supports long-distance communication but present constraints that will drive adaptation for allies, partners, as well as adversaries. These include:

- Susceptibility to jamming, spoofing, and cyber intrusion
- Creation of single points of failure when over-relied upon
- Latency issues affect time-sensitive missions
- Limited interoperability with partner forces due to proprietary architectures
- Logistical constraints in austere environments

These conditions demand and demonstrate why radios, and terrestrial networks remain essential, but complimentary, components of a resilient communications architecture.[1,2] The benefits of SATCOM are critical when properly integrated. To make risk-informed decisions, commanders must have the right information to weigh the advantages of SATCOM against its vulnerabilities.

Defensive Cyber Operations Training

Defensive Cyber Operations (DCO) training provides the essential foundation for identifying, mitigating, and defeating cyber threats targeting tactical networks, radios, and mission-command systems. For U.S., KDF, and Tanzanian forces, this training strengthens operational resilience and builds shared defensive capacity.

---

[1] Kari A. Bingen and Todd Harrison, Space Threat Assessment 2023 (Washington, D.C.: Center for Strategic and International Studies, April 2023), 15-18.
[2] Raphael Satter, "U.S. says Russia was behind cyberattack against Viasat in Ukraine," Reuters, May 10, 2022, https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10/.

During multinational activities cyber teams detected suspicious network activity, responded to scenario-driven cyber injects, and synchronized defensive actions across tactical radio and mission command networks. Their collaboration reinforces a common understanding of cyber threats and builds confidence across the force. These partners now inform us how they design future exercises to lower the learning curve for all participants.

This partnership reflects an African principle: “The part of the fence a good neighbor protects is a part you don’t have to worry about.” Cyber defenders embody this principle by securing their sections of the digital and electromagnetic environment. This shared protection reduces coalition vulnerabilities, strengthens trust, and enhances overall mission assurance. Through repeated collaboration, these forces are developing into informed and agile defenders capable of sustaining mission-critical systems under contested conditions. Forces put the principles of this shared defensive model into practice and emphasize that cyber defense is not just a cyber function, but a command responsibility enabled by teams.

Insights, Observations and Outlook

The Justified Accord exercise highlights four key takeaways from its focus on communications experimentation, interoperability validation, and cyber readiness development:

1. Multinational radio interoperability is achievable.
During Justified Accord 26, SETAF-AF will use Harris CPA software to generate and distribute Type 3 AES-256 encryption keys. This demonstrates U.S. and Kenyan elements’ ability to establish a shared tactical radio network—an important step toward achieving multinational technical interoperability.

2. Shared technical training reduces integration time.
Partner engagements in 2024 and 2025—such as military-to-military engagements, workshops and knowledge exchanges validated that early training in encryption, waveform alignment, and radio network configuration significantly reduces time-to-integration during operations.

3. Cyber disruptions directly affect tactical radios.
Cyber injects reveal that abnormal network behavior, spoofed signals, and electromagnetic interference can degrade radio and command and control performance. Cross-training radio and cyber personnel improves troubleshooting and reduces operational risk.

4. Common waveforms enhance coalition situational awareness.
Partners who employ compatible waveforms achieved faster network convergence, improved shared understanding, and more effective mission synchronization.

Key Observations on Tactical C2 in Contested Environments

Synthesizing insights from multiple SETAF-AF engagements, the following five observations are critical for success in modern operations:

Observation 1: Layered Communications Are Essential for Survivability
Radios remain the most reliable method of sustaining C2 in degraded environments. They must anchor all contingency pathways.

Recommendation 1: Mandate Dynamic PACE Planning and Rehearsals
To ensure continuity of mission command, all elements must treat PACE (Primary, Alternate, Contingency, Emergency) not as a static planning construct, but as an actively exercised capability. This requires integrating mandatory PACE execution into all training and joint exercises, deliberately simulating the loss of primary satellite communications and requiring units to transition to tactical radios as the primary contingency layer. Commanders should enforce dedicated "radio-only" communication periods to deliberately stress interoperability, discipline operators, and refine tactics under degraded conditions. Assess PACE effectiveness explicitly in after-action reviews, with observations and lessons learned shared across components and mission partners to drive continuous, collective improvement.[3]

Observation 2: Interoperability Requires Early, Intentional Planning
Multinational operations fail when waveforms, crypto, or equipment differences go unaddressed. Effective integration requires joint planning and preliminary network testing[4].

Recommendation 2: Fuse Cyber and Radio Defenses
To establish a coherent defense across the electromagnetic spectrum, organizations must move beyond functional stovepipes and permanently integrate DCO and signal forces at the point of execution. This integration begins with the formation of combined communications–cyber defense teams embedded in operational planning, training, and response—not as adjuncts, but as core mission enablers. Build these teams through deliberate cross-training that equips signal soldiers to recognize and report cyber threats, while enabling DCO personnel to understand and operate within tactical radio network architectures. Once formed, these integrated teams must routinely rehearse combined response drills that reflect the reality of modern conflict, including simultaneous cyber intrusion, electronic warfare jamming, and command-and-control degradation. The objective is not organizational alignment, but operational adaptability—units that can sense disruption early, respond decisively, and continue to fight through contact.

---

[3] Richard W. Skowyra, Samuel A. Mergendahl and Roger Khazan, "Holding the High Ground: Defending Satellites from Cyber Attack", Signal Magazine, March 2023.
[4] U.S. Army Futures Command, The U.S. Army Modernization Strategy 2023 (Austin, TX: Army Futures Command, 2023), 22.

Observation 3: Cyber–EW Threats Are Persistent and Affect All Echelons
Cyber and radio teams consistently observed jamming, denial-of-service attempts, and anomalous network behavior. Cyber and radio teams' habitual integration versus episodic cooperation will demonstrate success faster at a smaller cost in the long run[5].

Recommendation 3: Field Redundant "Go-Kits" for Expeditionary Command Posts
Equip expeditionary command posts with pre-configured, layered communications packages designed for contested environments. This will allow them to establish mission command on arrival, rather than assembling packages ad hoc after making contact. The G6 should field lightweight communications "go-kits" that integrate multi-band tactical radios (HF/VHF/UHF), low-bandwidth SATCOM, and resilient cellular pathways as a single, expeditionary capability. Maintain these kits in a ready state, pre-configure them for rapid, plug-and-play employment, continuously patch them, and align them for interoperability with key partners before deployment. To prevent obsolescence and stay ahead of emerging threats, the force should adopt a disciplined three-year technical refresh cycle and train dedicated teams to rapidly emplace, operate, and troubleshoot these systems forward. This approach replaces improvised, bespoke solutions with a standardized, repeatable capability that improves interoperability, accelerates deployment timelines, and enables mission command to persist through disruption.

Observation 4: Expeditionary CPs Demand Lightweight, Redundant Solutions
When SATCOM access degrades, radios fill critical gaps. CPs need portable, energy-efficient systems that sustain C2 under austere conditions.

Recommendation 4: Execute "Break the Network" Hybrid Exercises
To identify and mitigate vulnerabilities before an adversary can exploit them, organizations must routinely subject their combined radio, SATCOM, and terrestrial networks to adversarial testing. This requires establishing a dedicated opposing force (OPFOR) Red Team empowered to actively jam, intercept, and attempt to exploit hybrid networks during major training and exercise events. Institutionalize biannual "network stress tests", which require units to sustain mission command while the Red Team executes coordinated electromagnetic warfare and cyber-attacks against command-and-control nodes. Units must formally capture, and track all identified challenges, and then develop, implement, and re-test mitigation measures in follow-on exercises. Red Team findings are not punitive, but developmental. These results should directly inform refinements to network architecture, training priorities, and future procurement decisions, ensuring the force adapts faster than the threat.

Observation 5: Training Under Stress Enhances Readiness
Units that train in low bandwidth, contested, or disrupted environments consistently outperform those that rely on ideal network conditions.

---

[5] Headquarters, Department of the Army, ADP 6-0, Mission Command: Command and Control of Army Forces (Washington, D.C.: U.S. Government Publishing Office, July 2019), 1-14.

Recommendation 5: Operationalize Partner Interoperability Through Focused Engagements

To advance from conceptual alignment to operational interoperability, units should increase both the frequency and technical depth of hands-on communications training with African and European partners. Commands can achieve this by hosting semiannual "coalition waveform and network alignment" workshops that enable partner technicians to collaboratively load, configure, test, and troubleshoot secure radio and data networks. In parallel, commands should expand bilateral and multilateral signal-focused exercises that emphasize clearly defined mission-essential tasks, such as:

- transmitting secure digital traffic
- executing radio-based medical evacuation requests
- sustaining command and control under degraded conditions

To reinforce these efforts and ensure continuity, integrate partner-nation signal planners and cyber specialists early into exercise design and operational planning cells. This helps interoperability mature as a habitual capability rather than a one-time activity.

Conclusion

While commercial SATCOM remains indispensable, it cannot alone guarantee mission assurance in a contested environment. We achieve true resilience through layered, integrated communications architectures anchored by hardened tactical radios and disciplined PACE execution. By strengthening radio and cyber interoperability with partners across Africa and Europe, SETAF-AF reinforces distributed mission command and improves coalition survivability in environments defined by scale, diversity, and constant friction. Africa's vast geography and the presence of more than fifty distinct military, political, and operational contexts make ad hoc or bespoke integration impractical; interoperability must instead be habitual, exercised, and built into how forces plan, train, and operate together.

Achieving this requires fusing technology, tactics, and partnerships—equipping expeditionary command posts with redundant communications, rigorously testing hybrid networks against thinking adversaries, and embedding defensive cyber expertise throughout communications planning and execution. By implementing these recommendations, U.S. and its partners build more than just interoperability; they forge the trust, cohesion, and shared capacity necessary to win. This integrated approach empowers coalition forces to maintain decision advantage and operational effectiveness, even when an adversary actively contests the electromagnetic spectrum. Ultimately, communications interoperability is not a technical achievement, it is a combat multiplier that enables coalition forces to think, decide, and act faster than any adversary seeking to disrupt them.