

The background is a dark, abstract composition. It features numerous silhouettes of laptops arranged in a grid-like pattern, receding into the distance. Overlaid on this are vibrant green digital elements: thin, jagged lines resembling data paths or fiber optics, and vertical columns of small, light-green dashes that look like binary code or data streams. The overall effect is one of high-tech connectivity and digital infrastructure.

THE INTEROPERABILITY WINDOW: BRIDGING THE NATO—U.S. INTELLIGENCE GAP

BY CHIEF WARRANT OFFICER 3 PAUL A. CRAWFORD

Introduction

Over the past five years, intelligence advisors from the 4th Security Force Assistance Brigade have identified operationally significant lessons that improve interoperability between NATO and U.S. Army headquarters. These findings derive from multiple force package rotations, episodic missions, and multinational exercises with advisors, all focused on achieving interoperability across the “human, procedural, and technical domains,” as defined in Army Regulation 34-1, *Interoperability*.¹ The findings reveal that NATO allies and partners face many of the same integration challenges as the U.S. Army, especially when scaling operations across digital and analog environments. Common issues include poor intelligence, surveillance, and reconnaissance (ISR) asset management, ineffective use of digital systems, and a lack of standard operating procedures. Both the U.S. Army and NATO units employ similar operational frameworks and processes. Still, there is a disparity in command decision making, in the variety of ISR assets, in the capabilities of digital systems, and in the requirements for transitioning from digital to analog processes and systems. This conclusion stems from the inherent difficulty of sustaining interoperability continuously throughout a conflict: much as maintaining uninterrupted communications is the objective, the enemy gets a vote. These issues, specific to U.S. Army and NATO units, indicate that the method to achieve interoperability is inaccurate. These lessons demonstrate how the *interoperability window*—a finite opportunity to synchronize human, procedural, and technical domains—can be widened through tailored intelligence formations and by standardizing both digital and analog procedures and transitions.

The interoperability window is a defined period during which two or more headquarters can exchange digital or analog information and make decisions synchronized with critical operational events. For instance, during a forward or rear passage of lines, NATO and U.S. Army elements must maintain continuous, reliable communication regardless of enemy actions or friendly constraints. This communication prevents fratricide, ensures unity of effort, and denies the enemy opportunities to exploit gaps. Without an established interoperability window, units may experience communication breakdowns or asynchronous decision making, leading to operational fragmentation and potential mission failure. In multinational operations, the interoperability window is not just helpful—it is essential.

A Difference in Intelligence Processes

To maximize the effectiveness of small intelligence formations, NATO must employ intelligence resources, ISR assets, and digital systems more efficiently throughout the intelligence process. However, the wide disparity in intelligence capabilities among NATO nations results in uneven detection depth compared to adjacent units at the same echelon. When some units struggle to process information or maintain detection depth, they create situational awareness gaps—such as blind spots in collection or in the ability to process collected intelligence in a timely manner—that the enemy can exploit. The core challenge is to execute an efficient intelligence process using available resources, assets, and digital tools.

Intelligence formations must align with the information flow—whether high or low—in proportion to ISR volume, collection and analysis capability, and digital system integration. This method’s center of gravity is data, which drives the intelligence process and enables commanders to make decisions. Depending on the information environment, the requirements to make these decisions differ.

Digitally advanced nations traditionally operate in a high-information environment capable of processing large quantities of data and making decisions rapidly. In less digitally advanced nations, high information flow may be overwhelming, leading to overload and analysis paralysis. On the other hand, nations that depend on high volumes of information but lack sufficient bandwidth, digital system access, or ISR assets risk missing critical intelligence and failing to meet the commander’s decision-making threshold. The key is that both NATO and the U.S. Army need to scale intelligence resources regardless of the volume of information, while enabling their commanders to make decisions.

NATO and U.S. Army organizations both execute the intelligence process, but with different levels of detail and depth. With its advanced ISR assets, analysis tools, and digital systems, the U.S. Army enables decision making by managing high volumes of information across multiple echelons to provide greater detail. NATO, with fewer personnel and more limited tools, cannot achieve the same depth. While NATO commanders can and do make decisions with less information, they lack the flexibility to adapt plans. In contrast, U.S. commanders require high levels of detail—and when that detail is missing, they often delay decisions. This disparity in decision-making thresholds creates vulnerabilities that adversaries can exploit.

“When some units struggle to process information or maintain detection depth, they create situational awareness gaps ... that the enemy can exploit.”

Structural Differences in Intelligence Formations

NATO and U.S. Army intelligence formations differ structurally as well. Unlike the U.S. Army, NATO typically separates analysis and collection into separate disciplines: NATO analysis formations confirm enemy courses of action and support targeting, while their collection formations determine how to satisfy intelligence requirements. ISR regiments and intelligence, surveillance, target acquisition, and reconnaissance, or ISTAR, battalions handle collection, while the analysis function remains within unit headquarters. This clear separation simplifies operational tasks. Many NATO intelligence officers and soldiers come from reconnaissance backgrounds, giving them a strong understanding of combat operations and collection planning.

In contrast, U.S. Army military intelligence companies and brigades employ more complex formations that blend analysis and collection capabilities. During exercises or deployments, these units attach to the intelligence staff (S-2) section of a unit headquarters, which also manages analysis and some collection. This structure breeds confusion in command relationships: commanders own the units, but senior intelligence officers control intelligence operations. Despite this complexity, U.S. formations benefit from high-end ISR assets and powerful digital tools that allow even small units to process large volumes of national-level intelligence data—an advantage NATO lacks.

Intelligence, Surveillance, and Reconnaissance Asset Disparities

NATO nations maintain limited ISR capabilities. Most have limited ground reconnaissance units and a narrower range of unmanned aerial vehicles than the U.S. Army. These modest assets align with NATO’s structure, where brigades are often the largest maneuver formations. Many NATO countries are creating division-level headquarters; however, they are not increasing ISR capabilities. This expansion increases information

flow, but analytical and digital capacities lag. Many NATO countries also lack effective coordination between their air forces and armies, limiting their ability to conduct joint operations.

The U.S. Army, while better integrated, still faces its own challenges with the overwhelming volume and variety of ISR data. To manage those challenges, it scales assets by echelon to allow higher headquarters to detect targets and support subordinate units, employing everything from ground reconnaissance to national technical means. Managing this breadth of data is challenging, especially as different theaters and missions require distinct command and control setups. Commanders often expect near-perfect intelligence, and if ISR collection falters, decision making halts until intelligence formations restore the expected level of detail.

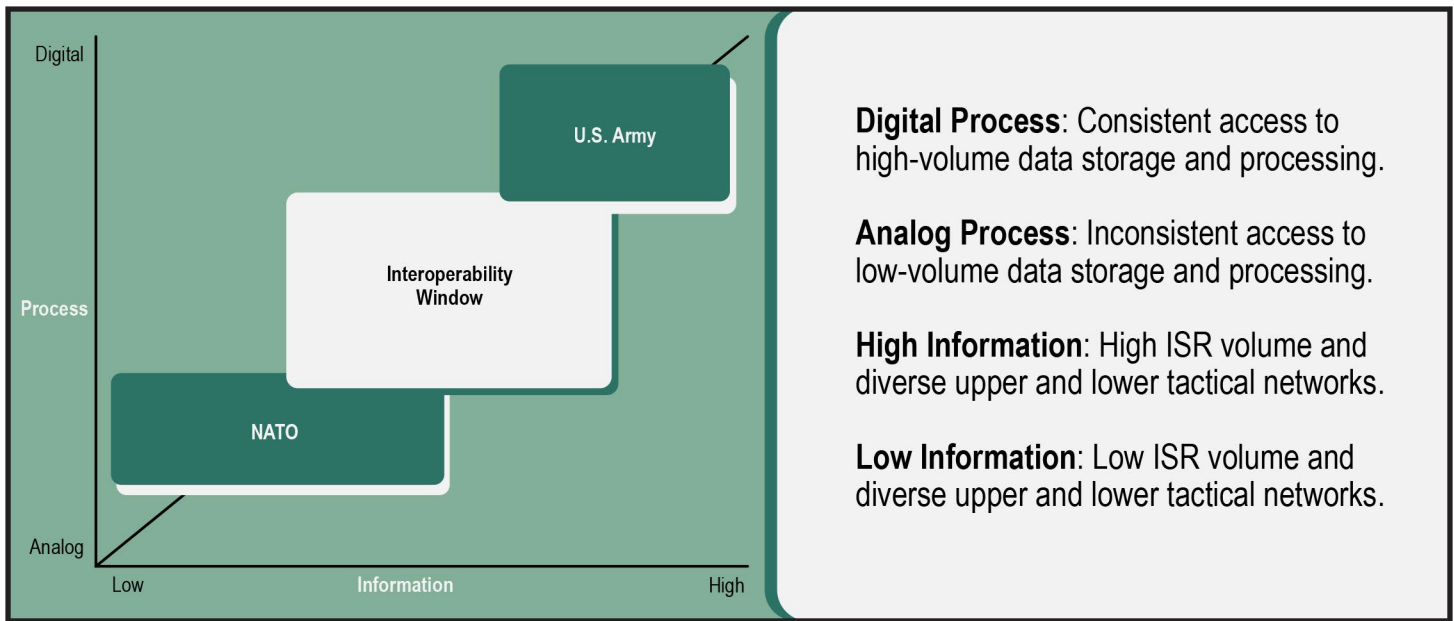
Digital Systems and the Problem with Transition

NATO’s biggest interoperability issue lies in its digital systems. Each nation uses its own systems to build a common operational picture, but these systems rarely interconnect. Vendor differences and unique network requirements cause fragmentation. While NATO does provide digital systems for alliance formations, these are not widely available. Cyber and electronic warfare threats further complicate matters, forcing NATO units to train on both analog and digital processes—without effectively practicing transitions between them.

In the U.S. Army, the issue lies more in the transition than in the variety of systems. U.S. Army digital systems handle large data volumes well but struggle in contested environments. When connectivity drops, units can no longer process information using analog methods because they depend on high volumes of data to make decisions. During transitions from digital to analog, units often lose access to critical data, leading to gaps in situational awareness. Without digital systems, the U.S. Army loses ISR collection depth and detail—and with that, the commander’s ability to make timely, informed decisions.

Feature	U.S. Army Formations	NATO Formations
Information Flow	High volume requirements	Low to medium volume
System Reliance	Complex digital dependencies	Limited digital dependency
ISR Integration	Vast, integrated capabilities	Limited ISR asset availability
Analog Transition	Challenging; volume dependent	High; purpose-built for analog
Operational Depth	High detail/situational awareness	Reduced depth and situational detail

Decision Making and Interoperability Comparison (figure adapted from author’s original)



Decision Information Framework (figure adapted from author's original)

A Framework for Interoperability

To resolve these issues, NATO and U.S. Army formations need a flexible, scalable intelligence architecture. The ideal formation must operate effectively in both high- and low-information environments while transitioning between digital and analog processes. Headquarters elements should house analysis functions, while separate formations conduct collection. This clear division in the intelligence process supports scalable training and clarifies command relationships. During conflict or exercises, collection formations should operate in direct support of the unit's S-2 section. Even with limited command and control, the S-2 should have access to nearly all collection data if digital infrastructure allows it.

Interoperability between a NATO headquarters and a U.S. Army headquarters begins with both headquarters' ability to transition seamlessly between digital and analog systems and processes without disrupting commanders' decision making. As a first step, each headquarters should complete a staff running estimate that defines—

- ◆ Available ISR assets.
- ◆ Digital system capabilities.
- ◆ Data pathways from sensors to systems.
- ◆ Information throughput capacity.
- ◆ Detection depth.
- ◆ Criteria for transitioning between digital and analog modes.

Once these estimates are complete, both headquarters can assess for any misalignment in detection depth or information flow. If detection depth is insufficient, this must be communicated to higher headquarters to allocate additional ISR support. If there is a mismatch in information flow, both headquarters must coordinate to ensure decision making

occurs at a synchronized pace, preventing operational seams that an adversary can exploit. Higher headquarters must also direct subordinate NATO and U.S. Army elements to report when transitioning between digital and analog processes. This reporting is critical: uncoordinated transitions can degrade higher-level situational awareness and slow operational momentum. Once these foundational steps are in place, interoperability must be reinforced across human, procedural, and technical domains.

Interoperability is complete once human, procedural, and technical linkages are established and tested between multinational units. Human linkages are established through liaison officers. Procedural linkages are established through operational processes like targeting and planning. And technical linkages are established by ensuring that networks are federated and that cross domain solutions exist between higher- and lower-classification networks—for example, between U.S. Secret networks and U.S. sensitive but unclassified networks. All these steps enable the unit to create the conditions for the interoperability window.

Conclusion

NATO and U.S. Army units must build adaptable intelligence formations capable of operating in both high- and low-information settings. This sets flexible conditions enabling the human, procedural, and technical foundations of interoperability. It also strengthens commander decision making and eliminates vulnerabilities during transitions between digital and analog systems. A modular, scalable structure for analysis and collection teams within military intelligence formations ensures interoperability, even before factoring in cyber and electronic warfare threats. Only through this approach can military intelligence define a reliable baseline and quantify the impact of enemy actions. In an era defined by artificial

intelligence, long-range precision fires, and advanced ISR, military intelligence must move at the speed of decision dominance—delivering depth and detail while denying the enemy any opportunity to exploit a seam. ✨

Endnote

1. Department of the Army, Army Regulation 34-1, *Interoperability* (Government Publishing Office, 2020), 1-2. Interoperability is the ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives.

CW3 Paul Crawford is currently the officer in charge of the 4th Infantry Division G-2 Intelligence Reach Operations Center, providing target system analysis support to the U.S. Indo-Pacific Command focused on electronic warfare. Previously, he served in the 4th Security Force Assistance Brigade (SFAB), supporting multiple U.S. Army Europe and Africa and NATO exercises at the division and corps levels, supporting multiple military-to-military engagements in Europe to enhance partner and ally intelligence capabilities, and, in 2022, deploying as part of the 4th SFAB's first brigade-level deployment supporting the Russo-Ukraine Conflict. CW3 Crawford has served in the 7th Special Forces Group (Airborne), the 82nd Airborne Division, the 1st Infantry Division, the 4th Infantry Division, the 173rd Airborne Brigade, and the 4th SFAB. He has three combat tours to Afghanistan and one non-combat tour to Poland.