JSOU PRESS
JOINT SPECIAL OPERATIONS UNIVERSITY

QUICKlook
BRIEF OVERVIEWS | COMPLEX TOPICS

Fading into the Background: From Risk Awareness to Technological Intuition

MARCH 2026

ANNA M. GIELAS, PhD

JSOU REPORT 26-5

Technological intuition is not an adjunct skill but increasingly a baseline capability—one that underwrites survivability and effectiveness wherever operations unfold inside increasingly technologized terrain. (Photo generated with Microsoft Copilot).

Summary

Emerging technologies are increasingly adept at detecting Special Operations Forces (SOF) in denied or contested environments. By developing a mental model of how these environments sense, process, and retain data on operator activity—from multiple directions and across different timescales—personnel can sharpen their risk awareness. Furthermore, cultivating two specific types of technological intuition through training enables operators to manage their signatures and exposure more effectively.

Introduction

During missions, SOF teams have traditionally focused on visible, kinetic dangers, but emerging technologies complicate this threat picture. Some new systems integrate sensing, identification, and targeting so tightly that they significantly narrow opportunities for human judgment and mitigation. Other systems gather, fuse, and analyze data for prospective exploitation and future analytic value, making operations and personnel more detectable in the moment and over time. In short, emerging technologies compress the timeline

Scan here to see the digital version.

from exposure to consequence while also extending risk beyond the immediate moment—increasing short-term vulnerability and long-term detectability.

Exposure can unfold from multiple directions—ahead of, behind, above, below, or near the operator—and across different timescales. Viewing risk through this lens makes emerging technological threats easier to recognize and avoid. To add another layer of protection, sharpening technological intuition can help operators anticipate how their actions generate data and trigger downstream effects. Together, risk awareness and technological intuition enhance personnel safety and operational effectiveness.

> *Sharpening technological intuition can help operators anticipate how their actions generate data and trigger downstream effects.*

Ahead: Automated Perception and Classification

Emerging risk increasingly comes from automated sensing systems such as smart perimeter technologies that do more than record. These systems can identify, categorize, and report specific behaviors.[1] In surveilled environments with established patterns of movement, normal activity thus becomes predictable, and deviations stand out. In such settings, an operator may draw attention simply by behaving differently from what is typical. Ask, "What about me—including my movement, posture, or dwell time—could be perceived as unusual in this environment?"

Behind: Data Persistence and Retrospective Attribution

The modern tail can include data persistence. Being "behind you" not only means physical pursuit—it can also consist of distributed sensors, logs, and records that capture fragments of one's presence.[2] An operator can now be linked to a specific place or event after the fact, when data is broadly fused and reviewed. This can happen through state intelligence and law enforcement networks but also through commercial data brokers, across time and space. To reduce risk, ask, "What traces do my movements, communications, and associations leave behind that could later be fused into attribution?"

Above: Vertical Sensing and Overhead Observation

Vertical advantage once depended on high-end assets like manned aircraft. Today, elevation can be cheap, temporary, and expendable. Proliferating small drones, low-cost sensors, and improved stabilization now enable both state and non-state actors to generate dense, localized aerial sensing.[3] From above, heat signatures, shadows, movement cadence, and group behavior may be sufficient for an adversary to detect and track a team over time. As a result, overhead sensing can reduce the effectiveness of some camouflage and concealment measures. Ask, "What of my actions or equipment could be detected from above—and what would that enable an adversary to do next?"

Below: Ground-Coupled Sensing and Subsurface Detection

Silence—when defined only acoustically—can be misleading, because the absence of sound does not mean the absence of other physical signals. Even when quiet to the ear, movement still couples into surfaces through vibration, repetition, and timing. The ground

and subsurface can register activity through technologies such as seismic sensors, buried fiber-optic lines, and infrastructure-mounted vibration sensors.[4] Advances in signal processing and machine learning allow these systems to increasingly separate human activity from background noise and to strengthen detection by correlating weak signals over a short period of time, even when individual events seem insignificant. Ask, "What vibrations, timing patterns, or repeated routes am I imprinting into the ground or built environment?" and "Does our equipment introduce periodic signals that are easier or faster to classify than our footsteps?"

Nearby: Ambient Sensing and Co-Presence Analytics

Crowds and everyday consumer technologies can turn nearby space into a sensor-saturated environment. People carry devices that record, emit, and receive data, while buildings and public venues add their own layers of technological infrastructure, including visual surveillance systems. None of these technologies need to be directed at anyone specifically to capture their presence. As people move, pause, and cluster, their devices collectively create a dense, overlapping picture of activity in the immediate area—potentially linking them to locations, vehicles, or other individuals through co-presence and timing. Ask, "What data do I generate simply by being near other people?" and "Would someone else's elevated risk status indirectly raise mine through proximity?"

Behind the Wall: Through-Wall Sensing and Inference

Barriers such as walls stop people much more easily than they stop signals. Some modern sensing relies on measuring how ambient radio frequency, cellular, or other electromagnetic signals propagate and change as people move within a structure.5 Walls now act less like shields and more like filters with known loss rates—reducing signal strength but rarely eliminating it entirely. Individually, these signals may be weak or ambiguous, but together they may allow machine-based inference of an individual's presence and activity. Ask, "Which signals pass through the walls around me, and how does my body change them?"

Technological Intuition: Types and Training

The preceding section describes how exposure occurs from above, below, behind, and nearby. Recognizing that risk now surrounds operators from multiple directions and persists across time is the first step toward managing exposure. But awareness alone is insufficient. The second crucial step is moving from understanding threats to actively shaping one's interaction with them. Doing so requires a deeper internalization of how technology works in practice—an internalization best described as developing *technological intuition*. Here, intuition does not mean instinct or guesswork, but judgment shaped by training, repeated exposure, feedback, and deliberate reflection. For SOF, technological intuition falls into at least two distinct types.

Modern sensing systems exploit how different signals propagate through terrain, structures, and infrastructure—and how those signals can be fused and interpreted. Therefore, one type of technological intuition is characterized by signal

> ***In denied and complex environments, technological intuition is a form of readiness.***

literacy and inference awareness. *Signal literacy* is the ability to see an environment as a dynamic field of signals and to understand how those signals are generated, leaked, distorted, amplified, and blocked. *Inference awareness* is the ability to anticipate what an adversary can conclude when those signals are combined and evaluated against expected baseline patterns. The goal is to use technological intuition to manage exposure proactively: remaining within expected baselines so that sensing systems and human analysts have no statistical or behavioral reason to escalate scrutiny.

Because this tech intuition is anchored to invariants, it remains durable despite technological change: cameras get smaller, sensors get cheaper, and software changes—but signals such as light, sound, and motion remain fundamental. This is why technological intuition shifts attention away from identifying individual pieces of sensing hardware toward a broader understanding of exposure—and may be especially relevant for SOF teams primarily focused on direct action and other time-compressed, kinetic activities.

This intuition can be sharpened during routine movement, rehearsals, and urban exercises by deliberately identifying natural signal traps, likely sensing paths, and areas where exposure to technical systems either rises or falls. Operators can practice noting where their presence would be easiest to detect and where it would blend into background activity. Beyond specific training, operators can routinely ask how light, heat, sound, vibration, and radio frequency are shaped within a specific space, how those signals move, and where they are likely to concentrate or escape.

Training should also expand the core questions operators ask. Instead of focusing only on "Is there a camera?" or "Are there sensors?", the questions may shift to "What signals could be captured in this space?" and "What signals am I generating right now that a system could exploit?" This reframing reflects how contemporary systems increasingly work: They often detect deviation, correlation, or persistence rather than a single, obvious signature. In practice, this technological intuition sounds like: this surface leaks; this route accumulates memory; this space punishes deviation.

The second type of technological intuition is characterized—somewhat paradoxically—by an in-depth understanding of the human element embedded in new capabilities. This intuition recognizes that every technological system reflects the people behind it. It therefore does not focus primarily on signals and physics—but on people and their behavior. Organizational and individual strengths, limitations, habits, and incentives shape how emerging systems are designed, funded, deployed, and operated. Training levels, maintenance practices, and local workarounds are further factors that define how technology is ultimately used in the field.

This technological intuition may be more relevant to SOF personnel operating through relationship- and partnership-based missions, including within the context of irregular or unconventional warfare. Over time, this intuition can provide advantages by allowing operators to anticipate patterns of technology use, misuse, and failure. Experience with how specific institutions or groups behave around new systems may help SOF teams predict where technologies will be overtrusted, underused, misconfigured, and only intermittently or

> *"In denied and complex environments, technological intuition is a form of readiness."*

selectively available.

This form of technological intuition is developed through close, sustained exposure to how people and institutions actually use technology, not how it is described in manuals or capability briefs. SOF personnel can train it by observing how partners and adversaries configure systems, maintain equipment, enforce rules, and work around limitations under real operational pressure. Finding out informal details—who has access, when systems are powered on, which alerts are ignored, and what routine shortcuts look like—often reveals more about true capability than technical specifications.

Training should deliberately include reflection on organizational and individual behavior. After engagements, site visits, or partnered operations, teams can ask how organizational priorities influenced system use, what incentives shaped collective and individual behavior around systems, and when basic human characteristics—such as acting out of convenience—overrode both institutional priorities and policies. Comparing documented procedures with observed practice helps expand technological intuition.

Over time, this intuition is strengthened by feedback and correction. Teams refine their judgments by noting which assumptions about human behavior and institutional reliability proved accurate and which did not. This continuous calibration helps operators better anticipate how technology will be employed, ignored, or misused in future environments.

Final Remarks

In denied and complex environments, technological intuition is a form of readiness. It prepares teams not by cataloging specific devices but by sharpening their judgment about the practical implications of emerging technologies across different missions. This readiness enables operators to manage exposure rather than chase invisibility and to anticipate second- and third-order consequences before they materialize. In that sense,

> *Over time, this intuition can provide advantages by allowing operators to anticipate patterns of technology use, misuse, and failure.*

technological intuition is not an adjunct skill but increasingly a baseline capability—one that underwrites survivability and effectiveness wherever operations unfold inside increasingly technologized terrain.

NOTES

1. Tuan-Hung Vu et al., "Anomaly Detection in Surveillance Videos by Future Appearance-Motion Prediction," in Proceedings of the 15th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2020), vol. 5: VISAPP, 484–490. https://doi.org/10.5220/0009146704840490; Diane Simpson et al., *Strategic Roadmap for Interoperable Public Safety Video Analytics*, NIST Special Publication 1500–1515 (National Institute of Standards and Technology, 2020); University of Houston, "Multi-tiered Video Analytics for Abnormality Detection and Alerting," created September 28, 2017, updated December 30, 2022, https://www.nist.gov/ctl/pscr/multi-tiered-video-analytics-abnormality-detection-and-alerting.
2. Electronic Frontier Foundation, "Automated License Plate Readers," updated October 1, 2023, https://sls.eff.org/technologies/automated-license-plate-readers-alprs (accessed February 7, 2026); Anna M. Gielas, "Networked Sensors, Pervasive Surveillance, and AI-Powered Analytics: Urban Warfare in the Age of Smart Cities," Modern War Institute, July 31, 2025, https://mwi.westpoint.edu/networked-sensors-pervasive-surveillance-and-ai-powered-analytics-urban-warfare-in-the-age-of-smart-cities/ (accessed February 7, 2026; Anna M. Gielas, "The Hidden National Security Risk in Smart Cities," The Cipher Brief, https://www.thecipherbrief.com/cybersecurity-smart-cities (accessed February 7, 2026).
3. Knut Torbjørn Moe, "Small Drones: From Cheap Toys to Terrorist Tools—Detection and Disruption Challenges," *Journal of the Joint Air Power Competence Centre* 21 (2015); Federico Borsari and Gordon B. "Skip" Davis Jr., An Urgent Matter of Drones (Center for European Policy Analysis, 2023); Don Rassler and Yannick Veilleux-Lepage, "On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism," *CTC Sentinel* 18, no. 3 (March 2025).
4. Priyankar Choudhary et al., "A Survey on Seismic Sensor-Based Target Detection, Localization, Identification, and Activity Recognition," *ACM Computing Surveys* 55, no. 11 (2023): Article 223. https://doi.org/10.1145/3568671; Zhaoqiang Peng et al., "Identifications and Classifications of Human Locomotion Using Rayleigh-Enhanced Distributed Fiber Acoustic Sensors with Deep Neural Networks," *Scientific Reports* 10 (2020): 21014. https://doi.org/10.1038/s41598-020-77147-2; Slah Drira et al., "Using Footstep-Induced Vibrations for Occupant Detection and Recognition in Buildings," *Advanced Engineering Informatics* 49 (2021): 101289.
5. Fadel Adib et al., "3D Tracking via Body Radio Reflections," 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI '14). April 2–4, 2014, Seattle, WA, https://www.usenix.org/system/files/conference/nsdi14/nsdi14-paper-adib.pdf; N. Patwari and J. Wilson, "RF Sensor Networks for Device-Free Localization: Measurements, Models, and Algorithms," *Proceedings of the IEEE* 98, no. 11 (2010): 1961–1973; Qiuye He et al., "A Survey on Human Profile Information Inference via Wireless Signals," *IEEE Communications Surveys & Tutorials* 26, no. 4 (2024): 2577–2610.

ABOUT THE AUTHOR

Anna M. Gielas, PhD

Anna M. Gielas holds a PhD in the history of science from the University of St. Andrews (United Kingdom). After earning fellowships at Harvard University and, most recently, the University of Cambridge, she is currently pursuing a second PhD focusing on SOF and emerging technologies.

United States Special Operations Command
ATTN: **JSOU Press**
7701 Tampa Point Blvd.
MacDill AFB, FL 33621-5323
jsou.edu/press

JOINT SPECIAL OPERATIONS UNIVERSITY PROVIDES RELEVANT JOINT SPECIAL OPERATIONS-PECULIAR EDUCATION PROGRAMS THAT EDUCATE JOINT SOF LEADERS, ENABLE ACADEMIC ACTIVITIES, ENHANCE THE SOF EDUCATION ECOSYSTEM, AND STRENGTHEN THE SOF ENTERPRISE'S IMPACT ON THE JOINT FORCE AND THE NATION.

The JSOU Press is the scholarly publishing arm of U.S. Special Operations Command (USSOCOM). Through unclassified, open-access materials and SOF-relevant thought leadership, the press supports both the university and USSOCOM in advancing the SOF warrior mind. SOFspecific publications and research, enterprise-wide engagement, and an annual Academic Call for Special Operations Papers facilitate creative, innovative solutions in alignment with command priorities.

JSOU PRESS
JOINT SPECIAL OPERATIONS UNIVERSITY