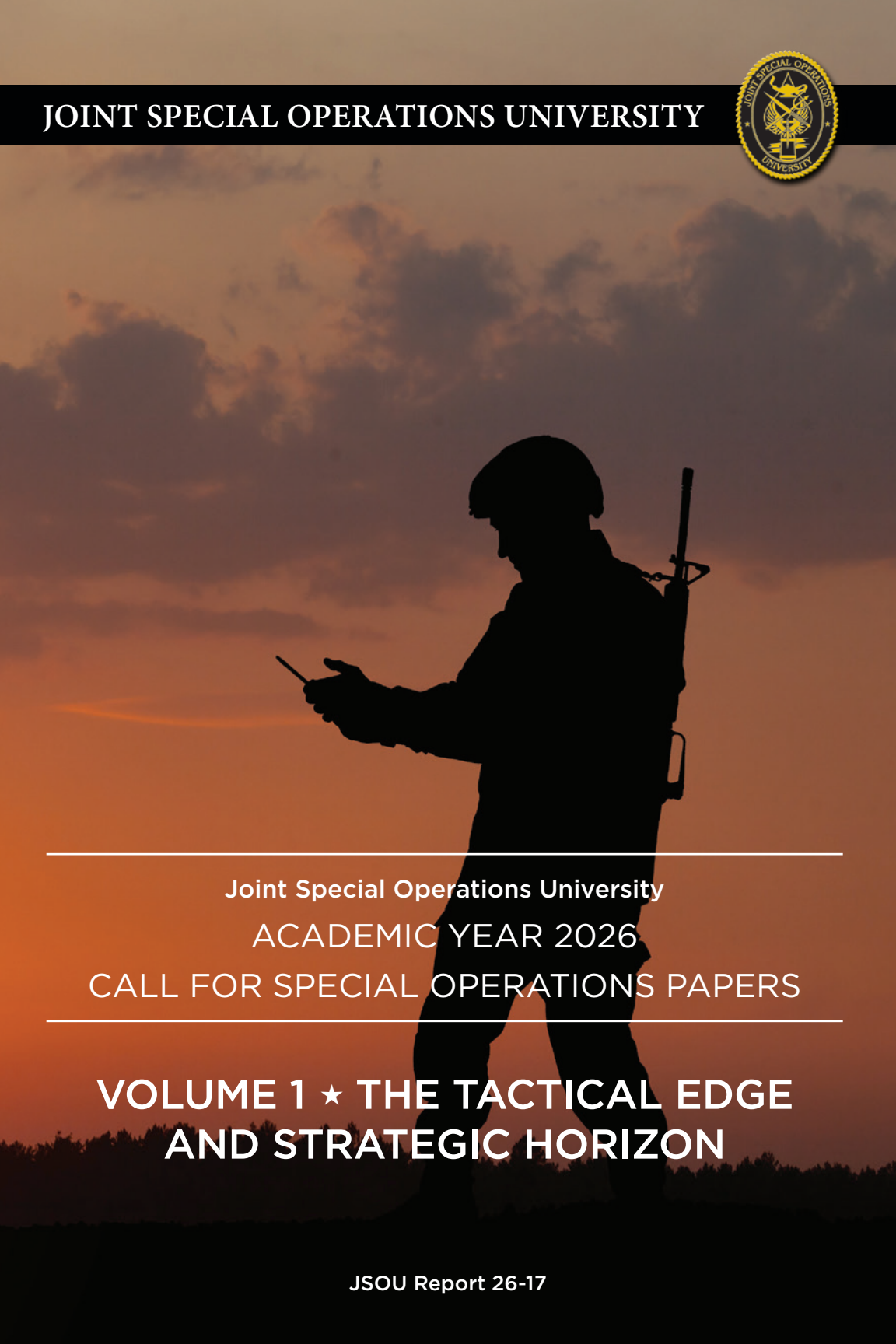
JOINT SPECIAL OPERATIONS UNIVERSITY



Joint Special Operations University

ACADEMIC YEAR 2026

CALL FOR SPECIAL OPERATIONS PAPERS

VOLUME 1 ★ THE TACTICAL EDGE AND STRATEGIC HORIZON

JSOU Report 26-17

JSOU PRESS
JOINT SPECIAL OPERATIONS UNIVERSITY

Joint Special Operations University

ACADEMIC YEAR 2026
CALL FOR SPECIAL OPERATIONS PAPERS

Volume 1 ★ The Tactical Edge and Strategic Horizon

JOINT SPECIAL OPERATIONS UNIVERSITY
MacDill Air Force Base, Florida | November 2026

JSOU Report 26-17

On the cover: A silhouette of a soldier using a drone and laptop computer for scouting during a military operation. Source: hamara/ Adobe Stock

The views expressed in this work are entirely those of the author and do not necessarily reflect the views, policy, or position of the U.S. Government, Department of War, United States Special Operations Command, or the Joint Special Operations University.

JSOU PRESS

Melanie Casey, Editor in Chief
Beth DeGeorge, Editor
Alina Alvarez Perez, Editor
Arianna Czesler, Designer
Rebecca Kurk, Designer

This work was cleared for public release; distribution is unlimited.

Published November 2026

ISBN 978-1-941715-89-5

jsou.edu/press

From Signature Reduction to Digital Force Protection: Operationalizing Counteroffensive Irregular Warfare in the Digital Domain

By Christopher Moede

Introduction

Congress, in the National Defense Authorization Act from Fiscal Year 2026, defined digital force protection as the "policies, tools, and practices used to protect military personnel, operations, and critical assets from adversarial exploitation of the commercial digital surveillance economy, associated commercial data, and digital footprints."[1] This definition was positioned not as an ancillary concern but rather a critical enabler of special operations forces (SOF) mission success.[2] Policymakers have rightly grasped the unmitigated risks to mission and force from the commercial digital surveillance economy and the digital footprints SOF leave behind—characterized by conditions of ubiquitous technical surveillance (UTS). This necessitates an adequate doctrinal response.[3] Digital force protection for SOF is not a defensive security discipline but rather the operational manifestation of signature reduction doctrine in the digital domain, enabling counteroffensive irregular warfare maneuver, survivability, and freedom of action for SOF in the UTS environment.

The Operational Condition: Ubiquitous Technical Surveillance

The commercial digital surveillance economy is now a direct and persistent threat to SOF, not just in theaters of conflict but across operational and personal aspects of mission preparation as well. AI-enabled targeting,[4] commercial surveillance ecosystems,[5] open-source intelligence,[6] and data brokers have dramatically reduced the barriers adversaries face when tracking previously undetected force movements. This allows them to conduct extensive digital surveillance and compromise operations before they ever depart home station.[7] This persistent and offensive problem extends across domains to wherever digital devices are in use, not just in theaters of conflict. Digital exhaust from units in forward operating

Where digital systems are used routinely, omnipresent information is produced, routinely collected, and exploited across time and space.

locations can be used for effects at home station, impacting service members' families in disturbing ways and vice versa. This generates difficult-to-measure effects and erodes operational effectiveness while increasing risk.[8] Where digital systems are used routinely, omnipresent information is produced, routinely collected, and exploited across time and space.

These conditions characterize a UTS environment in which observability itself becomes a form of vulnerability that can be weaponized by adversaries with the aid of other technologies.[9] This vulnerability extends across what is now known as gray zone warfare. In such an environment, force protection cannot be limited to a series of defensive security measures in forward operating locations alone, augmented by operational security (OPSEC) measures at home.[10] It must be grounded in an adequate counteroffensive doctrine that reclaims decision advantage and freedom under such prohibitive conditions before SOF depart to the operational area.

Signature Reduction as Counteroffensive Doctrine

Warfare has progressed into an unrestricted format in which irregularity and asymmetry dominate.[11] This gray zone warfare significantly challenges legacy systems and structures which struggle to adapt and keep pace as risk profiles increasingly span time and space with the help of digital technology, the phenomenon of UTS. This risk is both acute and generalized.[12]

Accordingly, maneuver suffers as the offensive technology-derived risks to mission and force growth. UTS poses such an existential threat because it collapses the boundaries of war and non-war, reaching from service members' personal devices to the closed-circuit television cameras which might physically place them in the operational area conducting sensitive activities.

This leads to the discovery of signature reduction—the doctrinal counteroffensive corollary to unrestricted warfare in the gray zone. Signature reduction offers a holistic and ordered logic that promotes freedom of action under conditions of UTS. Its value proposition is not necessarily anonymity or invisibility for SOF in digital spaces, but rather adequate obfuscation, deception, and denial of adversary visibility. Properly understood, signature reduction is maneuver under surveillance, and thus operational survivability for the post-digital age. Within this doctrinal foundation, digital force protection, the operational form in the digital domain, is discovered.

Digital Force Protection: Navigating the Digital Terrain

In gray zone warfare, digital terrain is not merely an OPSEC consideration prior to deployment but rather a critical battlespace that holds the key to positional and decision advantage in forward deployed locations. The conditions of UTS transform observability in digital terrain into vulnerability that spans time and space. Since digital technology makes SOF observable at home and during mission preparation, they now require digital safeguards in the operational area and prior to their arrival. We are vulnerable at home and in our daily lives simply by virtue of using digital devices and the commercial surveillance ecosystem which exploits them.[13] Simply not having a digital presence is neither practical nor helpful, as the absence of a digital signature also becomes its own signature. Yet,

> *We are vulnerable at home and in our daily lives simply by virtue of using digital devices and the commercial surveillance ecosystem which exploits them.*

by correlating digital device data using vehicles in the commercial surveillance economy, adversaries can target specific individuals at-scale.[14] This identity persistence amounts to risks to mission and force, especially for sensitive operational activity. Digital force protection, then, becomes maneuver in the digital terrain that mitigates or otherwise manages digital risk through policies, tools, and practices for SOF.

Digital force protection does not necessarily seek anonymity or invisibility in the digital terrain. Rather, it enables navigating this terrain through signature management or controlling visibility. Digital force protection is not merely "security through obscurity," but rather is a counteroffensive capability that holds power to shape digital observability, and thus, actively minimizes vulnerability and risk under conditions of UTS. The objective is to intentionally shape what an adversary may be able to observe. Adversary targeting depends not solely on collection but on attributing observability to an identity in time and space for some desired effect. Digital force protection disrupts this logic by degrading the adversary's ability to correlate and attribute with certainty. It is, in some sense, "hiding in the noise." Through digital force protection, freedom for action is preserved and survivability is extended—not because there is no digital footprint or signature, but because the digital footprint has been intentionally and systematically managed to control visibility according to desired operational outcomes.

As the digital terrain continues to grow, digital force protection is necessary to shape the battlespace and retain freedom for action often before physical movement occurs. This is to say, agility and decisiveness for SOF in digital terrain is shaped prior to their deployment. The commercial digital surveillance economy extends from the operational area to home station. Digital force protection reduces risk before SOF physically enter the operational area. These are not mere defensive force protection measures, or cybersecurity best practices, but functions of maneuver that shape operations.

Mapping Digital Force Protection to Ubiquitous Technical Surveillance Threat Vectors

UTS poses a multi-vector threat to freedom for action, seeking to correlate and attribute identity across time and space persistently. UTS operates across online, electronic, financial, visual–physical, and travel vectors to disrupt SOF activities.[15] Digital force protection is not specific to any of these vectors but functions across them and offers proactive multi-domain signature management that shapes identity correlation and reduces attribution risk. It directly enables operational flexibility under conditions of persistent observability. Understanding these vectors is not merely academic; it informs the operational steps that shape SOF digital signatures before deployment.

Through digital force protection, freedom for action is preserved and survivability is extended.

Operationalizing digital force protection begins with individuals and their devices as the locus where key digital terrain is won or lost. When the battlefield is everywhere, everyone must respond to efforts to collect, correlate, and disrupt their activity; this

should begin in the personal setting and continue to apply in an operational one. This requires coordinated planning, decision-making, and risk shaping from individuals to organizations before SOF deploy forward. Digital force protection is an operational effort that proactively shapes the digital terrain and denies the adversary observability. This begins in the pre-deployment environment where understanding and shaping activities are being conducted. Understanding adversary collection and correlation capabilities across UTS vectors is critical, and recognizing where SOF are exposed across UTS vectors uncovers hidden attribution risk for force movements. Implementing training and education programs to address this risk shapes the digital terrain prior to physical arrival.[16] Coordinating team device usage to reduce attribution risk while forward deployed becomes standard operating procedure. By shaping individual digital signatures prior to deployment, digital force protection preserves operational initiative, reduces adversary targeting certainty, and extends SOF survivability under UTS.

Toward Counteroffensive Freedom for Action

Digital force protection is the operational form of a counteroffensive signature reduction doctrine. It proactively reduces attribution risk in the UTS environment and extends survivability and optionality in gray zone warfare, where digital terrain demands shrewd navigation. It begins with individuals and their devices and has operational impacts well before reaching the physical battlespace. Digital force protection does not seek invisibility but a managed signature, or reduced adversary observability and correlation of SOF prior to operational activity. A controlled digital footprint in the digital terrain is the key to navigating gray zone warfare, providing a doctrinal lens for planning, training, and decision-making in UTS environments.

Digital force protection does not seek invisibility but a managed signature.

By integrating digital force protection into planning, training, and pre-deployment preparation, SOF translate signature reduction doctrine into real operational advantage, anticipating adversary collection and disrupting correlation attempts. This shapes their digital footprints in advance, creating freedom for action before deployment. This freedom for action translates to operational maneuver in the physical battlespace. Digital force protection thus degrades adversary targeting and attribution, transforming observability from a vulnerability into an opportunity for decisive action.

About the Author

Christopher Moede is the director of the Institute for Signature Reduction, an independent 501(c)(3) nonprofit charitable organization dedicated to advancing the disciplines of signature reduction, digital force protection, and cyber privacy in support of national defense and public institutions. Moede develops instruction for SOF units on emerging technology-based threat vectors and the operational risks of digital exposure, and explores how signature reduction can serve as a doctrinal foundation for modern irregular warfare. He also previously served as a mission commander in a selectively manned unit.

Notes

1. U.S. Congress, House, Committee on Armed Services, *Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026*, 119th Cong., 1st sess., H. Rep.119-231, H.R. 3838, sec. 1083, https://www.congress.gov/bill/119th-congress/house-bill/3838?s=1&r=5.

2. U.S. Congress, Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026, 1033.

3. Christopher Moede, "Counteroffensive Irregular Warfare: A Doctrine of Signature Reduction for Strategic Competition," *Small Wars Journal*, December 22, 2025, https://smallwarsjournal.com/2025/12/22/counteroffensive-irregular-warfare/.

4. Harry Davies and Yuval Abraham, "Revealed: Israeli Military Creating ChatGPT-Like Tool Using Vast Collection of Palestinian Surveillance Data," *The Guardian*, March 6, 2025, https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance.

5. U.S. Congress, Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026, 1037.

6. "Iran Monitor | Real-Time Open-Source Intelligence Dashboard for Iran," Iran Monitor, accessed March 2026, https://www.iranmonitor.org/.

7. U.S. Congress, Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026, 1035.

8. An uncorroborated operational vignette came to us from Ukraine, where a U.S. SOF member was discovered by foreign intelligence and security services to be using a particular location-based mobile application for various personal purposes during their deployment. While the individual was still deployed, a pair of ethnic representatives posing as salespersons arrived at their home address in the U.S. and asked the service member's spouse if they could speak with him. In a moment of surprise, the spouse let slip that their husband was unavailable as he was currently deployed. The salespersons' chilling response reportedly was: "We know." While clearly an attempt at intimidation and harassment, this vignette highlights the collapse between war and non-war, where omnipresent information—in this case made available to hostile security services through mobile application data—became a personalized instance of actualized risk. The emotional, psychological, and otherwise personal effects now compound even if the apparent operational effects seem limited.

9. *2024 Annual Threat Assessment: Testimony Before the Armed Services Subcommittee on Intelligence and Special Operations*, U.S. Congress, House (April 11, 2024) (statement of U.S. Air Force Lieutenant General Jeffrey Kruse, Director of Defense Intelligence Agency), https://docs.house.gov/meetings/AS/AS26/20240411/117088/HHRG-118-AS26-Wstate-KruseJ-20240411.pdf.

10. Joe Littell, Maggie Smith, and Nick Starck, "The Devil Is in the Data: Publicly Available Information and the Risks to Force Protection and Readiness," *Modern War Institute*, September 20, 2022, https://mwi.westpoint.edu/the-devil-is-in-the-data-publicly-available-information-and-the-risks-to-force-protection-and-readiness/.

11. Christopher Moede, "Ubiquitous Technical Surveillance and the Renewal of Irregular Warfare," *Small Wars Journal*, February 13, 2026, https://smallwarsjournal.com/2026/02/13/ubiquitous-technical-surveillance/.

12. 2024 *Annual Threat Assessment*, 33.

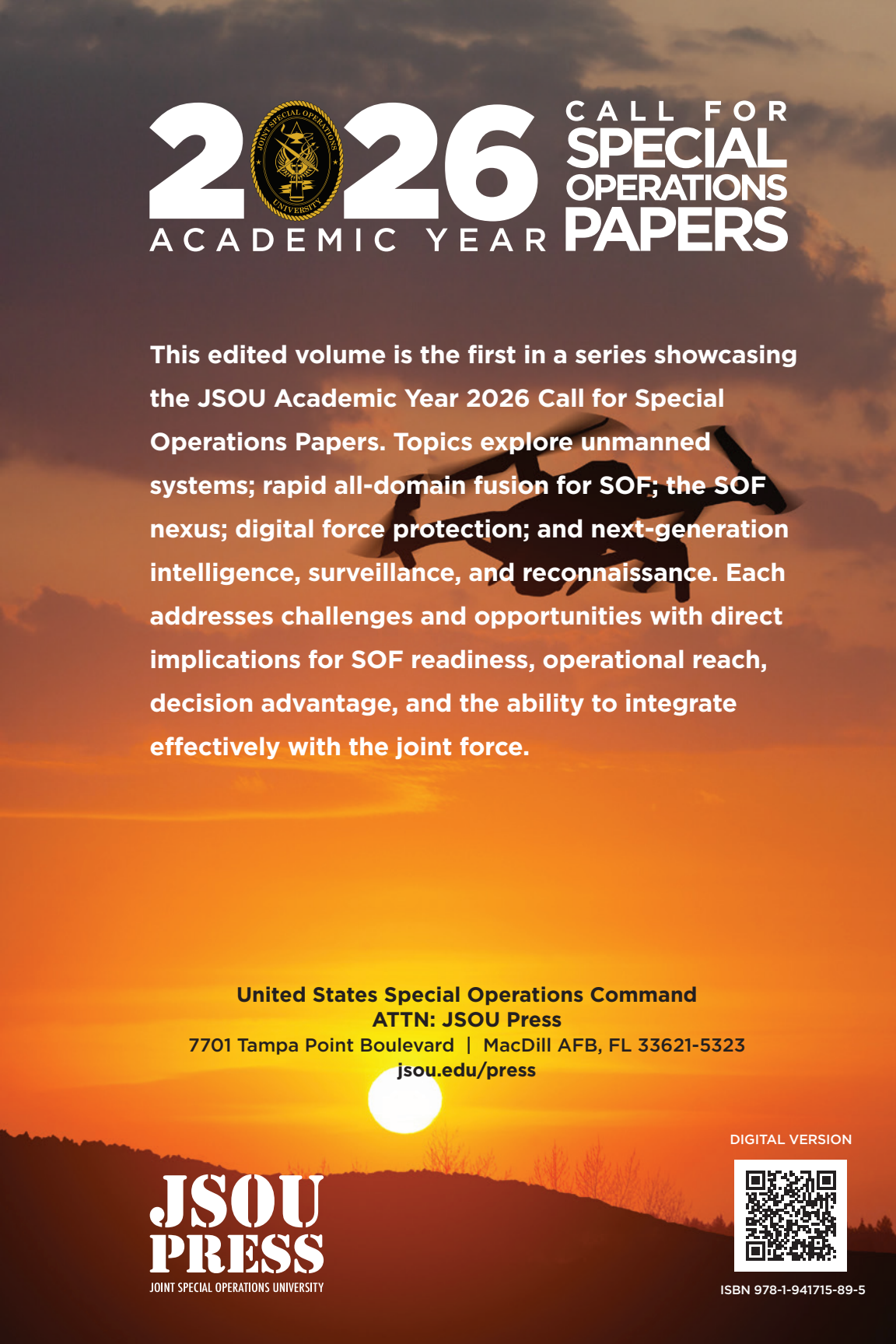
13. Alexander Master et al., *Tracking the Trackers: Commercial Surveillance Occurring on U.S. Army Networks*, Army Cyber Institute Technical Report (The Army Cyber Institute at Westpoint Military Academy, 2025), February 12, 2026, https://arxiv.org/pdf/2602.12388.pdf.

14. U.S. Government Accountability Office, Information Environment: DoD Faces Risks with Publicly Available Data, GAO-26-108771 (Government Accountability Office, 2025), https://files.gao.gov/reports/GAO-26-108771/index.html.

15. Ma'Ceo Bell, "Data Security Concerns Rise as Surveillance Becomes Ubiquitous," *U.S. Army*, August 12, 2025, https://www.army.mil/article/287760/data_security_concerns_rise_as_surveillance_becomes_ubiquitous.

16. Moede, "Counteroffensive Irregular Warfare."

2026 ACADEMIC YEAR CALL FOR SPECIAL OPERATIONS PAPERS



This edited volume is the first in a series showcasing the JSOU Academic Year 2026 Call for Special Operations Papers. Topics explore unmanned systems; rapid all-domain fusion for SOF; the SOF nexus; digital force protection; and next-generation intelligence, surveillance, and reconnaissance. Each addresses challenges and opportunities with direct implications for SOF readiness, operational reach, decision advantage, and the ability to integrate effectively with the joint force.

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

JSOU PRESS
JOINT SPECIAL OPERATIONS UNIVERSITY

DIGITAL VERSION

ISBN 978-1-941715-89-5