SUMMER/FALL 2024 | VOLUME 37 ISSUE 2

SPECIAL WARFARE

THE OFFICIAL PROFESSIONAL JOURNAL OF U.S. ARMY SPECIAL OPERATIONS FORCES

SOF-SPACE-CYBER TRIAD
USASOC COMMANDING GENERAL TALKS TRIAD, DIVES INTO ARSOF STRATEGY

SOF-SPACE-CYBER TRIAD IN ACTION:
RECLAIMING THE INITIATIVE IN UKRAINE

MEET 11TH CYBER BATTALION:
ARMY CYBER'S WORKHORSE FOR THE TRIAD

HOW ARSOF FIGHTS
FUTURE INTEGRATION OF THE SOF-SPACE-CYBER TRIAD

From the COMMANDING GENERAL

Since the 1920s, interwar periods have been rife with innovation. Professional writing fueled new and imaginative approaches to military problems. Dialogue and debate strengthened our profession of arms. Following World War I, mechanical, radio, and radar innovations led to combined arms maneuvers during World War II. The character of war changed from unimaginative attrition to movement, surprise and initiative. Warfare combined the land, maritime, and air domains. Professional dialogue about who to fight, where to fight, how to fight, and what to fight with ignited innovation at tactical, operational, and strategic levels.

Following the wars in Afghanistan and Iraq, the current period stokes innovation in information, deep sensing, long-range fires, robotics, unmanned systems, and other technologies. Warfare expanded to space and cyberspace domains. New capabilities are employed in imaginative ways by combatants in the Russo-Ukrainian War. Data analytics, machine learning, and artificial intelligence promise to further accelerate technological innovation at a rate never seen in human history. The character of war is changing. Professional writing, dialogue, and debate have never been more important than today—the objective is to outpace and gain an advantage over our adversaries.

This issue of *Special Warfare* focuses on the 'SOF-Space-Cyber Triad.' The Triad is a forward-thinking multi-domain framework to drive new and imaginative approaches to tactical, operational, and strategic military problems. The articles in this issue offer some experiences, insights, and ideas for operationalizing the Triad to enable the U.S. Army and joint force to achieve objectives and defeat enemy capabilities across multiple domains during large-scale combat operations.

– Veritas et Libertas –

JASON C. SLIDER
MAJOR GENERAL, U.S. ARMY
COMMANDING GENERAL

"This issue of *Special Warfare* focuses on the SOF-Space-Cyber Triad. The character of war is changing. Professional writing, dialogue, and debate have never been more important than today—the objective is to outpace and gain an advantage over our adversaries."

— Maj. Gen. Jason C. Slider

SPECIAL WARFARE

U.S. ARMY JOHN F. KENNEDY
SPECIAL WARFARE CENTER AND SCHOOL
The Special Operations Center of Excellence

MISSION To produce world - class quality ARSOF Soldiers, is our non-negotiable contract with the U.S. Army, the Nation, and the American people. There is no second place in the Profession of Arms, and anything less than exceptional is unacceptable.

GUIDING PRINCIPLES Always strive for Excellence in all we do! Our Profession and our Nation demands it. Everything we do should be planned, organized and executed effectively and efficiently. Every success and every mistake is an opportunity to learn and improve. Serving our country carries the responsibility for unwavering Courage. Courage to do what is right and put the mission before self. This requires Trust…the Trust I have in you and your Trust in me. Trust and integrity is foundational to personal accountability and critical self-assessment. As Leaders, I expect you to empower subordinates, build Trust, build Teams, and Do What's Right – Always!

EDITOR NOTE Acronyms USAJFKSWCS and SWCS are used interchangeably. Partners of the Triad, Cyber, Space, and SOF, are used interchangeably.

SUBMISSIONS

ARTICLE SUBMISSIONS

Special Warfare aims to inform, educate, and bring awareness to the talented, highly effective, and instrumental skill sets of Special Operations Forces.

We welcome submissions of academic work from students, professors, and cadre of the U.S. Army John F. Kennedy Special Warfare Center and School, scholarly, independent research from members of the armed forces, security policy-makers and -shapers, defense analysts, academic specialists, and civilians from the U.S. and abroad.

Manuscripts should be 500 to 3,000 words in length. Include a cover letter with the following: Full name, rank, job title, e-mail address, phone number, intended audience (1-3 sentences), abstract/brief summary (1-3 paragraphs), and key words.

Manuscripts should be submitted in plain text, double-spaced, and in a digital file. Endnotes should accompany works in lieu of embedded footnotes. Please consult *The Associated Press Stylebook*.

Artificial intelligence (AI) is useful for ideation, however, no publishable article in *Special Warfare* can be written exclusively or in part by AI.

Articles that require security clearance should be cleared by the author's security manager and public affairs office prior to submission. A memo of the security clearance should be forwarded with the article. If the article talks about a specific theater special operations command (TSOC), the article will be forwarded to the TSOC for clearance.

PHOTO AND GRAPHIC SUBMISSIONS

Special Warfare welcomes photo submissions featuring Civil Affairs, Psychological Operations, Special Forces, and all other ARSOF Soldiers and enablers. Ensure that all photographs are reviewed and released by the unit public affairs officer prior to submission.

Special Warfare accepts high-resolution (200< dpi or 2MB file size) digital photos, in the format of .jpg, .png, .tif, .pdf, and .eps. Be sure to include a caption and photographer's credit. **Do not** send photos within PowerPoint slides or Word documents.

Photos, graphics, tables and charts that accompany articles should be submitted in separate files from the manuscript (no embedded graphics).

SUBMISSION REVIEW AND PUBLICATION

Authors will receive a confirmation email of receipt typically within one week of submission. If your content is selected for publishing, additional correspondence will occur until the editorial process is complete.

Please note that submitted content is not guaranteed to be published in *Special Warfare*. There are several factors that determine what content is ultimately published including time and space availability, the approved editorial outline and theme, as well as relevance to the *Special Warfare* target audience and mission. *Special Warfare* will not republish articles that are concurrently under review elsewhere or have already been published. Exceptions may be granted for professional work that is core to concepts discussed in a journal issue.

Special Warfare reserves the right to edit all contributions. *Special Warfare* will attempt to afford authors an opportunity to review the final edited version; requests for changes must be received by the given deadline.

No payment or honorarium is authorized for publication of articles or photographs. Material appearing in *Special Warfare* is considered to be in the public domain and is not protected by copyright unless it is accompanied by the author's copyright notice. Published works may be reprinted, except where copyrighted, provided credit is given to *Special Warfare* and the authors.

SUBMIT ARTICLES FOR CONSIDERATION TO:

E-mail: SpecialWarfare@socom.mil

FOR ADDITIONAL INFORMATION,
CONTACT THE SPECIAL WARFARE TEAM AT:

Commercial: (910) 432-5703 or (910) 396-9494

E-mail: SpecialWarfare@socom.mil

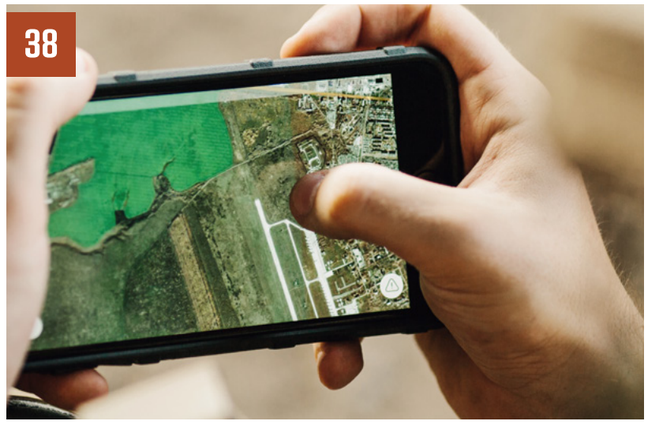
Special Warfare is an authorized, official publication of the United States Army John F. Kennedy Special Warfare Center and School, Fort Liberty, N.C. Its mission is to promote the professional development of special operations forces by providing a forum for the examination of established doctrine and new ideas.

CONTENTS

ARTICLES

ON THE COVER

Illustration of the future ARSOF operator in a Triad battle front. (Adobe Stock)



Letter from the EDITOR

We are thrilled to share that the U.S. Army John F. Kennedy Special Warfare Center and School, the Special Operations Center of Excellence, welcomed two Harding Project fellows as part of the Army Chief of Staff Gen. Randy George's Harding Project initiative.

The Harding Project initiative aims to renew the systems of professional writing and journals across the Department of Army, and the *Special Warfare Journal* is a part of it.

Lt. Col. Zachary Griffiths and Sgt. 1st Class Leyton Summerlin, the Army Chief of Staff's Harding Project leaders spearheading the initiative, outlined the four components about the program on the Harding Project website that explains it best:

- MODERNIZE: Longtime readers of Infantry or Engineer will see them modernized to a web-first, mobile-friendly format that reaches the scrolling Soldier. This website is under development and will launch this fall.
- ARCHIVES: We're also making archives more accessible. Armor dates to 1888. Infantry to 1930. Through partnership with the Defense Technical Information Center, the Army will soon make about 120,000 articles searchable on Google and other search platforms.
- STEWARDSHIP: After decades of cuts, the Army will right-size journal staffing. The uniformed staff will ensure journals remain relevant in content and format, while the civilians bring editorial expertise and continuity. Look for a new Broadening Opportunity that competitively selects, develops through graduate education, and employs uniformed editors this fall.
- EDUCATION: The Army is also looking at low-cost changes to professional military education curriculum. For example, adding requirements to cite military journals will familiarize the force with them, but not add burdensome new requirements.

Because of the initiative, the Special Warfare gained two talented editors in chief – the Harding Project fellows.

The Special Operations Center of Excellence is excited to introduce Maj. Emily Lopez, our Harding fellow officer and a Civil Affairs Soldier, and Sgt. 1st Class Benjamin L., our Harding fellow noncommissioned officer and a Special Forces Soldier.

Maj. Lopez, Sgt. 1st Class Benjamin L., and the Special Warfare team will work together to forge the new direction of the journal as the U.S. Army's professional publication for special operations.

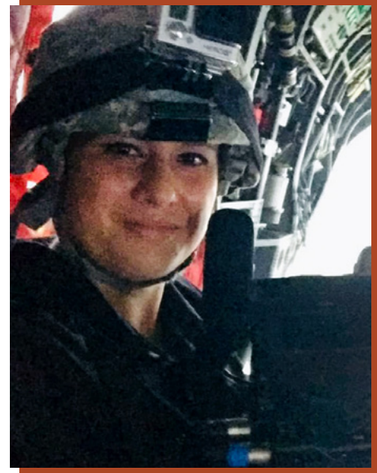
While I won't be far and will continue to contribute to the journal, the Harding fellows will keep you updated on *Special Warfare* through the editor's letter and other ways through the Harding Project program and Army University Press.

Don't miss a beat. Stay tuned at www.armyupress.army.mil/Journals/Branch-Journals.

Until then, we hope you find this edition of the "SOF-Space-Cyber" Triad informative and encourages conversation.

Happy reading!

ELVIA KELLY
EDITOR, SPECIAL WARFARE MAGAZINE
U.S. ARMY JOHN F. KENNEDY SPECIAL WARFARE CENTER AND SCHOOL



Elvia Kelly, the Special Warfare editor and SWCS Public Affairs officer, captures video footage from a Chinook on Fort Liberty, North Carolina.

STAY CONNECTED TO A SPECIAL COMMUNITY

Follow us online for all things ARSOF

SCAN ME

WEBSITE

FACEBOOK

YOUTUBE

INSTAGRAM

Check out the Pineland Underground Podcast episode featuring the Fellows of the Harding Project, click the Pineland image to listen.

JFKSWCS PINELAND UNDERGROUND PODCAST

Welcome HARDING FELLOWS

We are honored to assume the role of Harding Fellows for *Special Warfare*. As we step into this responsibility, we look forward to fostering thought-provoking discussions and advancing the critical conversations that shape the future of Army special operations forces (ARSOF). Our mission is to continue building on the rich legacy of *Special Warfare* as ARSOF's professional journal and serve as a platform for the voices within our community. We are committed to driving forward the exchange of ideas, innovations, and experiences that will prepare our formations for the future operating environment.

Since 2022, the SOF-Space-Cyber Triad has charted a promising course toward a more integrated joint force as the Army adopts multidomain operations as its guiding concept. Two and a half years into the initiative, the ARSOF community faces a pivotal moment. Some contributors in this issue argue the Triad is losing relevance due to unclear foundational principles. In contrast, others see its early application as an opportunity to refine and strengthen it for future use.

Regardless of stance, the articles in this issue challenge ARSOF professionals to rethink how our formations will fight, influence, and partner in shaping the operational environment's physical, informational, and human dimensions. The rapid pace of technological change is driving the Army to evolve. Success will depend on how quickly and effectively we sense, adapt, and respond to threats from state and non-state actors. Concepts like the Triad and multidomain operations represent the shifts needed for future formations to grasp modern warfare's tangible and intangible aspects in a digitized battlespace.

Special Warfare continues to foster this vital dialogue by featuring the perspectives of diverse authors, including experts from private industry, U.S. Space and Missile Defense Command, and U.S. Army Cyber Command, among others. Their intellectual dedication and courage in sharing these insights are greatly appreciated.

Emily B. Lopez

MAJ. EMILY LOPEZ
CIVIL AFFAIRS, HARDING FELLOW
USAJFKSWCS

SGT. 1ST CLASS BENJAMIN L.
SPECIAL FORCES, HARDING FELLOW
USAJFKSWCS

SOF-SPACE-CYBER TRIAD

USASOC COMMANDING GENERAL TALKS TRIAD, DIVES INTO ARSOF STRATEGY

SPECIAL WARFARE JOURNAL - What is the SOF-Space-Cyber Triad? Why is this concept important to "How ARSOF Fights?" As one of Lt. Gen. Jonathan Braga's USASOC 2030 priorities, the Triad offers a solution:

"We are building a concept referred to as the SOF-Space-Cyber Triad. This is a convergence of trans-regional, multi-domain, and joint capabilities to exponentially increase the holistic strategic effects of each capability across the spectrum of conflict now and in the future. Our increasingly complex strategic landscape requires innovative approaches that fuse and integrate all our expertise to maximize our collective impact." [01]

It may be helpful to open with what has already been articulated about the Triad by Lt. Gen. Braga and in some publicly available documents from the United States Army Special Operations Command (USASOC).

These extracted dialogues and excerpts serve as a primer to help orient readers to the original intent and the underlying thinking that supports the SOF-Space-Cyber Triad concept. When wrestling with what the Triad means for the future of U.S. Army Special Operations, and the Joint Force, it is helpful to trace the concept's origins, where it is going, and how it is evolving.

One of Lt. Gen. Braga's first official articulations of what the Triad is and why it is important emerged in a statement he gave to the Senate Armed Services Committee in 2022.

The following year, USASOC began to build on the Triad concept by including it in the ARSOF Strategy 2030 document, integrating the Triad into other ARSOF initiatives. A few months later, Lt. Gen. Braga offered more detail in on the Irregular Warfare Podcast, addressing how the concept does and does not relate to the nuclear triad and a reaffirmation of how the concept continues to be a guiding organizational idea as ARSOF navigates an increasingly complex operating environment.

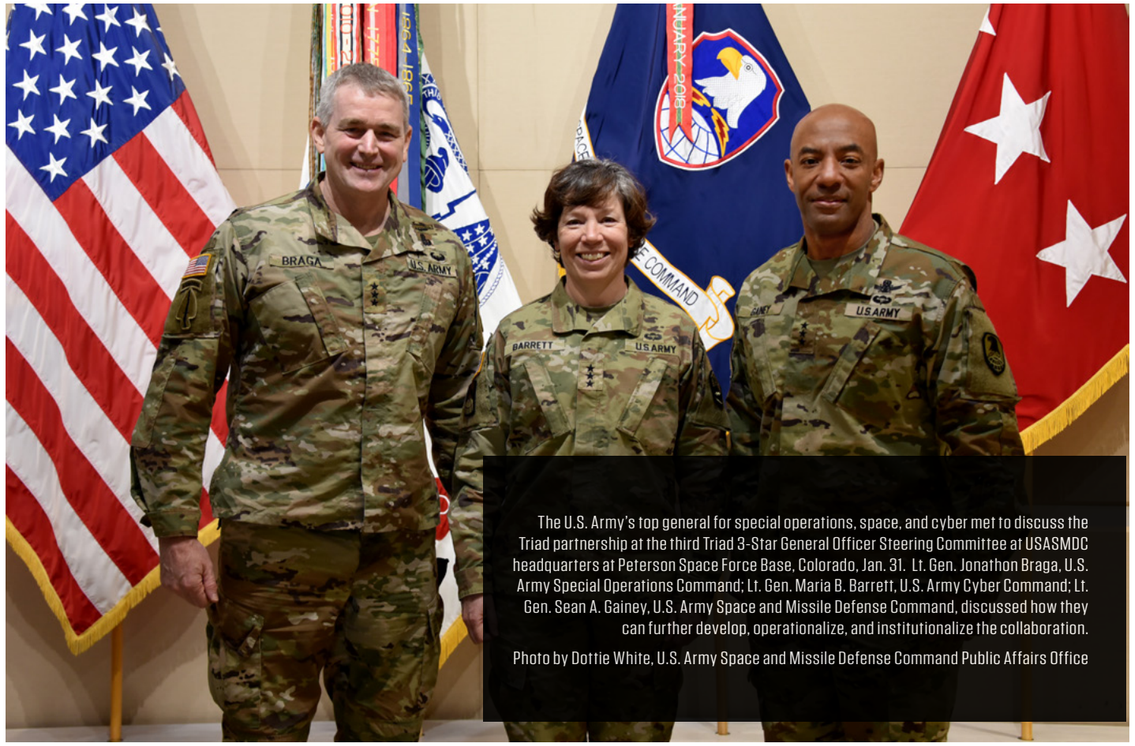
> "We are building a concept referred to as the SOF-Space-Cyber Triad. This is a convergence of trans-regional, multi-domain, and joint capabilities to exponentially increase the holistic strategic effects of each capability across the spectrum of conflict now and in the future. Our increasingly complex strategic landscape requires innovative approaches that fuse and integrate all our expertise to maximize our collective impact." [01]
>
> Lt. Gen. Jonathan Braga
> Letter to The Senate Armed Services Committee: April 27, 2022

HOW DOES THE SOF-SPACE-CYBER TRIAD INTEGRATE WITH OTHER USASOC INITIATIVES? WHY IS THERE SO LITTLE PUBLICLY AVAILABLE INFORMATION ABOUT THE TRIAD? HOW IS THE TRIAD BEING IMPLEMENTED ACROSS THE ARSOF ENTERPRISE?

Lt. Gen. Braga's testimony to The U.S. Senate Committee on Armed Services, Wednesday, April 27, 2022, on efforts to sustain special operations force readiness and transform the force for future security challenges.

"The seven modernization priorities for USASOC are: Irregular Warfare, Information Advantage, Multi-Domain Operations Interoperability, Next Generation Precision Effects, Unmanned Systems-Robotics-Artificial Intelligence, Next Generation Mobility, and Enhanced ARSOF Soldiers. We synchronize within these priorities while remaining a bottom-up driven organization. We have men and women on the ground identifying problems and providing requirements. Whether we lead or support, USASOC serves as a catalyst for innovation through our continued experimentation and operational use. We are deliberate with our selective disclosure, knowing our initiatives drive adversary decision cycles.

Last month, 44 organizations participated in a USASOC exercise focused on the intersection of SOF-Space-Cyber Triad capabilities leading to a series of upcoming experiments. Lessons learned allow us to test our assumptions and solutions in Service (Army Project Convergence 2022) and Joint Force exercises (Unified Pacific 2022). Hardware solutions are important, but people remain our primary focus." [02]



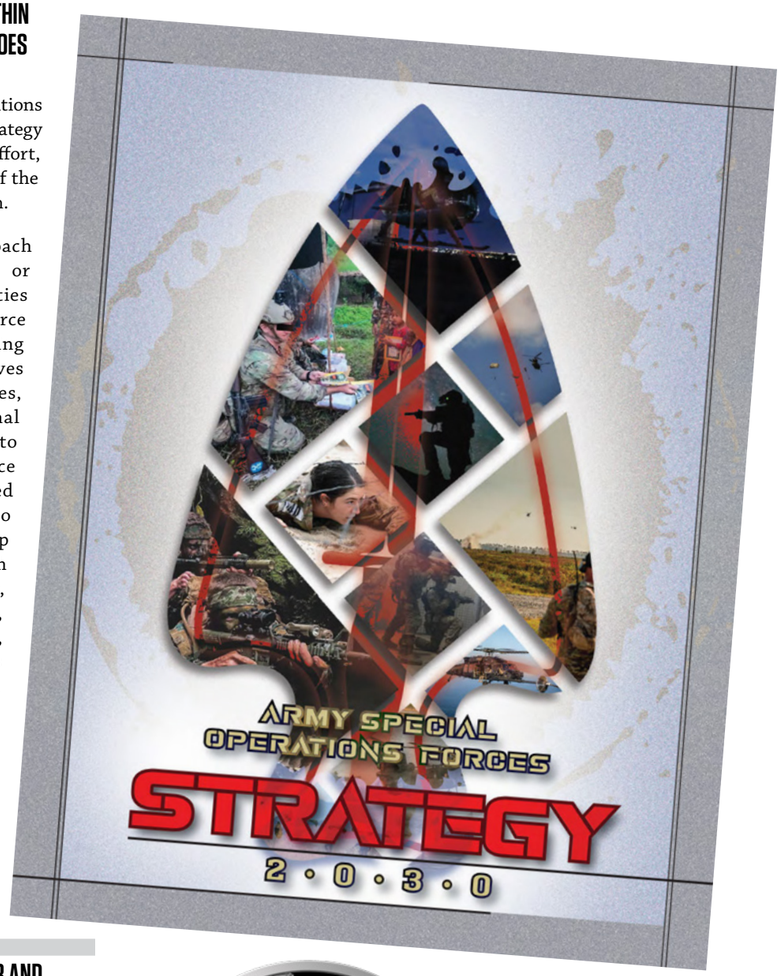
The U.S. Army's top general for special operations, space, and cyber met to discuss the Triad partnership at the third Triad 3-Star General Officer Steering Committee at USASMDC headquarters at Peterson Space Force Base, Colorado, Jan. 31. Lt. Gen. Jonathon Braga, U.S. Army Special Operations Command; Lt. Gen. Maria B. Barrett, U.S. Army Cyber Command; Lt. Gen. Sean A. Gainey, U.S. Army Space and Missile Defense Command, discussed how they can further develop, operationalize, and institutionalize the collaboration.

Photo by Dottie White, U.S. Army Space and Missile Defense Command Public Affairs Office

WHERE DOES THE SOF-SPACE-CYBER TRIAD EXIST WITHIN USASOC'S STRATEGIC LINES OF EFFORT (LOE)? HOW DOES THE TRIAD SUPPORT THE WIDER JOINT FORCE?

The United Stated Army Special Operations Command's Army Special Operations Forces Strategy 2030, released April 6, 2023, describes the lines of effort, capabilites and resources, and roles and missions of the organzation as it looks to modernize and transform.

LINE OF EFFORT 1. *Transform ARSOF*–This approach allows USASOC to recognize new, or existing, problems that current capabilities cannot adequately address. USASOC's force modernization efforts are mutually supporting the Army, and the Joint Force's objectives in the employment of new technologies, operational methods, and organizational approaches. USASOC will contribute to and at times lead Army and Joint Force experimentation events. Activities associated with this effort include actions designed to identify future requirements and develop solutions to future challenges through concepts, doctrine, organization, training, materiel, leadership, personnel, facilities, and policy. Our triad partnership (SOF, Space, and Cyber) will break down barriers to operating across these new and contested domains to deliver unique options. Development of the triad conceptually, as well as experimentation, nests under this LOE, as do our modernization efforts in next-generation precision strike, unmanned systems-robotics-AI, counter unmanned aerial systems, and contested communications. [03]



HOW DO THE COMPONENTS RELATE TO ONE ANOTHER AND WHY IS THEIR RELATIONSHIP IMPORTANT TO THE CURRENT STRATEGIC ENVIRONMENT?

In the 2030 Strategy, released April 6, 2023, it describes the another line of effort of the organzation as it looks to modernize and transform.

The Space-Cyber-SOF Triad describes an interdependent and mutually supporting relationship between cyberspace, space, and SOF. Special operations often rely upon the information advantage provided by cyberspace and space capabilities to see, sense, and stimulate to influence relevant populations or strike deep into the physical nodes of an adversary's system and assess the results. Cyberspace operations may rely on SOF's physical access and placement to deliver effects. Cyberspace, space, and SOF are unique in their global reach, persistence, endurance, and responsiveness. The cross-domain convergence of capabilities enables effects at all levels and can be seamlessly integrated into irregular warfare campaigns. [04]

Army Special Operations Forces Strategy 2030 vision and strategy describes how USASOC will generate, posture, and transform our forces to realize this vision alongside our generational partners and allies.

Images provided by USASOC.

HOW IS THE SOF-SPACE-CYBER TRIAD OPERATIONALIZED AND WHERE DOES IT FIT WITHIN POLICYMAKER RESPONSE OPTIONS TO STRATEGIC PROBLEM SETS? HOW DOES THIS TRIAD COMPARE TO THE TRADITIONAL NUCLEAR TRIAD?

Irregular Warfare Podcast: May 2, 2023 Interview, hosted by Ben Jebb and Kyle Altwell, Modern Warfare Institute at West Point as part of the Irregular Warfare Initiative.

BRAGA: "…everything in space or in cyber all has some type of terrestrial conduit that, in a sense, is networked and, in a sense, is a vulnerability point for both friend and foe and is an opportunity. So, SOF can absolutely be mutually supporting to our cyber and our space partners out there, but I think combined [sic], that's why I talk about the combined SOF-Space-Cyber Triad. It's absolutely critical that we develop this and bring capability both for high-end conflict but, I would argue, steady-state competition as well. This is a modern-day triad; it doesn't replace nuclear triad. It doesn't replace strategic deterrence. But it's absolutely complimentary because it is used throughout the spectrum of conflict, and it provides policymakers flexible deterrence and response options that are below the level of armed conflict."

HOST: "So, something of note that I found especially interesting in the ARSOF strategy was this term that you just used, the Space-Cyber-SOF Triad. I think most people's images of SOF conjures decked out operators, kicking in doors, conducting raids, things like that. But the Space-Cyber-SOF Triad talks a lot more about the interplay being mutually supportive in the space domain, offering cyber capabilities, and it seems like SOF might be well situated to address that. So, can you kind of flesh that concept out a little bit and talk about how you define this concept and explain why SOF is particularly well suited to leverage and, I guess, leverage and enhance cyber and space capabilities? Question for both of you, but I'll direct that one to Jon first."

BRAGA: "Sure, and I'll start with the word 'concept'. I think it's important when we coalesced around that term triad, it did have connotations. You know, back in the day if you were my age or older and you took any international relations degree, you knew about George Kennan and Thomas Schelling. And the word 'triad' meant everything from the word capabilities from subs, silos, and bombers to deterrence theory and game theory to international relations to the Cuban missile crisis to tactical nuclear weapons to artillery delivered nuclear weapons, I mean it meant everything. From TTPs up to strategy up to policy. There wasn't an international relations degree-producing university that didn't cover it.

I think that much thought needs to go into this modern-day triad, the SOF-Space-Cyber Triad there, because it is the newest tools out there that can have strategic effect, or it can be a much lower effect depending on what is decided and what is employed there. So, it' important that there is a robust investment, in my opinion, from the academic community to the policy community to the military community of, 'what is the best way to employ these capabilities and techniques,' again, from strategy, theory, policy down to things and widgets and capabilities and equipment. Ultimately, some of our tasks are the same. Whether it is employing the SOF-Space-Cyber Triad or other elements. It's to help our force, the joint force, see further, strike faster, and hopefully inhibit the adversary to do the same and blind the adversary there a little bit and hopefully impose doubt, cost, and belief [sic] on different ways there."

CONCLUSION:

The SOF-Space-Cyber Triad is a concept that integrates trans-regional, multi-domain, and joint capabilities to achieve strategic effects. This approach advocates for dismantling the artificial barriers between military domains in response to the increasingly complex geopolitical landscape, evolving threats, and advancing technologies. Such innovation is critical to developing capabilities to support military campaigns in competition and conflict. It is important to note that the SOF-Space-Cyber Triad is neither intended to replace nor replicate the historically established U.S. nuclear triad. Drawing from Lt. Gen. Braga's forward-looking perspective, this triad is an evolving model that addresses emerging challenges. It aims to inspire similarly deep strategic thought and complement all US war-making and deterrence methods by introducing pioneering strategies that leverage modern information technology—from the ground to orbital planes. Doing so provides the joint force with enhanced tools and offers policymakers greater flexibility.

01 Jonathan Braga. "Statement of Lieutenant General Jonathan Braga Commanding General United States Army Special Operations Command (USASOC) Before the Senate Armed Services Committee Emerging Threats and Capabilities Sub-Committee." 27 April 2022. pg. 1-2. (Accessed on 8 August 2024 https://www.armed-services.senate.gov/imo/media/doc/2022%20USASOC%20Posture%20-%20LTG%20Braga%20-%20SASC-ETC%20(27%20April)%20(Final).pdf)

02 Jonathan Braga. "Statement of Lieutenant General Jonathan Braga Commanding General United States Army Special Operations Command (USASOC) Before the Senate Armed Services Committee Emerging Threats and Capabilities Sub-Committee." 27 April 2022. pg. 4. (Accessed on 8 August 2024 https://www.armed-services.senate.gov/imo/media/doc/2022%20USASOC%20Posture%20-%20LTG%20Braga%20-%20SASC-ETC%20(27%20April)%20(Final).pdf)

03 USASOC. "Army Special Operations Forces Strategy 2030." 6 April 2023. Pg. 12. (Accessed on 8 August 2024 at https://www.soc.mil/temp-pages/strategy/ARSOF_STRATEGY_2030.pdf.)

04 USASOC. "Army Special Operations Forces Strategy 2030." 6 April 2023. Pg. 15. (Accessed on 8 August 2024 at https://www.soc.mil/temp-pages/strategy/ARSOF_STRATEGY_2030.pdf.)

LEVERAGING PROXIMITY:

WHY SPECIAL OPERATIONS FORCES' PHYSICAL PRESENCE IS THE MOST UNDERAPPRECIATED COMPONENT OF THE CYBER-SPACE-SOF TRIAD

By Maj. Dalton Fuss, 18A NATO Special Operations-A

Space and cyber are two of the three elements of the triad that draw the most attention, but the critical role of the last element—special operations forces' (SOF) physical proximity—is commonly overlooked.

An example demonstrating the vital role of physical proximity is reflected in a Russian case study. An exposed intelligence operation conducted by the Russian-speaking espionage organization, Turla Group, provides us with an unclassified example of how SOF can utilize space-based assets to enhance the operational security of cyber operations. This case study demonstrates that a small group of highly-trained personnel can leverage their physical location within a satellite's coverage area to exploit space-based assets. By taking advantage of unencrypted downlinks, Russian operatives were able to translate physical proximity into operational anonymity for a separate intelligence operation that was conducted in cyberspace. We should examine this case study closely to build upon these techniques and maximize the primary value proposition of SOF—the access and placement of perpetually deployed elements.

Photos provided by Adobe Stock

HOW DID THE OPERATION WORK?

Starting in 2007, cyber operatives from Turla Group began exploiting unencrypted downlinks from satellites.[01] The Russian-speaking attackers were operating within the coverage area of a satellite that was providing internet to ground-based computers through an unencrypted downlink. The coverage area, or "footprint," refers to the area on the Earth's surface that a satellite's signal covers.[02] By "listening" to downstream satellite traffic with a rudimentary antenna from within this footprint, the attackers collected metadata on the computers involved.[03] This action provided the attackers with the active IP addresses of those computers relying on the satellite. The attackers reconfigured their own server to mimic these IP addresses and trick the satellite into accepting the hacker's computer as the legitimate user. This process is known as "satlink hijacking."[04]

Critically, the attackers did not access the legitimate user's computer. Instead, they reconfigured their server so that the satellite would perceive it as the legitimate computer, thereby creating a clone that also received the information sent to the legitimate user. When the satellite sent data packets to the legitimate user's IP address, the attackers would also receive that information. After uncovering these active IP addresses within the satellite's footprint, Turla Group then configured their malware to transfer stolen data to these new IP addresses.[05]

To spread this modified malware more efficiently, the Russians employed the worm called Agent.BTZ that has historically been used to infect American and European government computers.[06] In previous attacks, the worm quickly propagated across entire networks and exfiltrated information to a separate network, a malicious code known as spyware. Agent.BTZ was "not optimized for stealing data" with precision.[07] The spyware lacked the sophistication required to determine high-value information. To compensate for this shortfall, the malware exfiltrated mass amounts of information for later processing.

This malicious code was designed to clandestinely export data from the target network and then routed through satellites to IP addresses that were employing unencrypted downlinks for internet access—a Wi-Fi café in the Central African Republic, for example.[08] Agent.BTZ commanded the infected computer to send the files to a seldom-used or unopened port on the receiving end, which ensured that the legitimate user's computer did not notify the user of the inbound traffic.[09]

Russian operatives that were in the satellite's footprint, cloned the legitimate user's IP address, so they, too, would receive the stolen data without being detected.[10] To further hide their trail, they often used satellite internet connection providers located in countries like Afghanistan, Lebanon, Libya, Niger, Somalia, and Zambia, which helped hide the location of their command-and-control servers and avoid attribution.[11]

The Russian-speaking espionage organization hoped that no one would discover the malware. But, if the code were uncovered, forensic analysts attempting to reveal the perpetrator would only be able to track it to legitimate users employing satellite-based internet, not the Russian-speaking operatives.

After the operation, investigators obtained a sample of Agent.BTZ from a government computer. Digital forensic analysts at the Moscow-based Kaspersky Labs dissected this malware through dynamic analysis in an isolated environment. Fortunately, because the operatives employed poor tradecraft and reused the same techniques and procedures from previous operations, Kaspersky Labs concluded that Turla Group was responsible for this attack. Analysts recognized programming patterns that were consistent with Turla Group's previous attacks. Even with this information, investigators were unable to identify the exact location of the attacker's servers. All they knew for sure was that the attackers were operating somewhere within the satellite's footprint.

HOW THE ATTACKS WORKED:

Attackers operate within the coverage area of a satellite that provides internet to ground-based computers through an unencrypted downlink.

The coverage area, or **"footprint,"** refers to the area on the Earth's surface that a satellite's signal covers.[02]

By **"listening"** to downstream satellite traffic with a rudimentary antenna from within this footprint, the attackers collected metadata on the computers involved.[03]

This action provided the attackers with the active IP addresses of those computers relying on the satellite. The attackers reconfigured their own server to mimic these IP addresses and trick the satellite into accepting the hacker's computer as the legitimate user. This process is known as **"satlink hijacking."** [04]

EXPLOITING THE ADVERSARY: WHAT CAN WE STEAL FROM THE RUSSIANS?

Detailed lessons from this operation need to be discussed through classified channels. However, at the unclassified level, it is possible to identify ways to leverage physical proximity to create options for decision-makers and generate dilemmas for adversaries.

EMPHASIZE HOW PHYSICAL PROXIMITY CAN ENHANCE SOF'S ROLE IN THE TRIAD IN COURSES LIKE THE ARMY'S SPACE CADRE BASIC COURSE.

Classified case studies in this course should demonstrate how space assets can support SOF in semi-permissive or denied environments. For example, multidomain operations require SOF to operate in areas where the electromagnetic spectrum is contested and vulnerable. In this environment, space assets can obfuscate the exact location of the SOF element in the same way that the Turla attackers could remain hidden anywhere within a satellite's footprint. In the same way, a SOF unit could receive unencrypted messages from anywhere within a satellite's footprint.

WITHIN ARMY SPECIAL OPERATIONS FORCES, INCREASE THE NUMBER OF BILLETS FOR THE ARMY SPACE CADRE ADDITIONAL SKILL IDENTIFIER.

The Turla Group only has a small number of qualified attackers with the technical skills needed to conduct the attacks described above. SOF must ensure that it has enough qualified personnel to perform these tasks. At a minimum, the special operations community should cultivate proficiency in space operations. Even a rudimentary understanding of orbital mechanics, GPS constellations, and electromagnetic spectrum fundamentals will make SOF personnel more effective by encouraging a more integrated approach to responding to threats. Courses like the Army's Space Cadre Basic Course provide overviews of these technical competencies. Commanders can institutionalize the technical knowledge of space operations within their formations by coding these SOF personnel billets as Space Cadre. This additional skill identifier can be designated at the O-6 (colonel) level in coordination with the Army's Space and Missile Defense Command. While this is a small step to building the required skillset within SOF, this credential will encourage service members to attend the schools needed to perform their assigned roles.

SEND A SPECIAL OPERATIONS EXPERT TO LECTURE AT SPACE AND CYBER PROFESSIONAL MILITARY EDUCATION COURSES TO OUTLINE HOW SOF CONTRIBUTES TO THE TRIAD OPERATIONALLY.

Discussions about the triad frequently center on technical solutions and specialized devices that drive operational outcomes without adequately emphasizing the human dimension. The United States Special Operations Command (USSOCOM) should send lecturers to space and cyber professional military education courses to address this gap. This program would allow SOF personnel to articulate their roles and responsibilities within the triad explicitly. Enhanced comprehension regarding SOF's role in irregular warfare, especially among space and cyber experts, could significantly clarify how their contributions support SOF units in the field.

CONCLUSION

The Russian Turla group leveraged unencrypted satellite communications to obfuscate their location and intercept critical data. This provides a clear example of how physical proximity within a satellite's footprint can be transformed into a tool for anonymity and operational security. This Russian operation also demonstrates the potential for SOF to conduct similar operations with only basic equipment. SOF should replicate this capability of hijacking satellite downlinks with equipment that reduces their digital signature, such as a locally sourced laptop, a portable antenna, and necessary cables. Adopting this approach would necessitate a shift towards greater autonomy and reliance on mission command principles, allowing SOF units to operate independently without direct oversight or constant communication. This strategy would transform geographical location and satellite proximity into operational assets, enhancing the effectiveness of the SOF-Space-Cyber Triad in national security efforts. The strategy would suggest a leaner, more agile operational model that maximizes stealth and minimizes detection risk.

---

01 Lucian Constantin. "Turla Cyberespionage Group Exploits Satellite Internet Links for Anonymity: The group routes traffic to their command-and-control servers through hijacked DVB-S Internet connections." PC World. 9 September 2015. (Accessed on 9 February 2024 at https://www.pcworld.com/article/423504/turla-cyberespionage-group- exploits-satellite-internet-links-for-anonymity.html).

02 Marcin Frackiewicz. "What is the Footprint? Glossary of Satellite Terms." TechnoSpace2. 4 September 2023. (Accessed on 9 February 2024 at https://ts2.com.pl/en/what-is-the-footprint-glossary-of-satellite-terms/).

03 Mike Lennon. "Russian-Speaking Turla Attackers Hijacking Satellite Internet Links." Security Week: Cybersecurity News, Insights & Analysis. 9 September 2015. (Accessed on 3 February 2024 at

https://www.securityweek.com/russian-speaking-turla-attackers-hijacking-satellite-internet-links/).

04 Oleg Gorobets. "Satellite Turla: Still Alive and Hiding in the Sky." Kaspersky Daily. 9 September 2015. (Accessed on 3 February 2024 at https://www.kaspersky.com/blog/satellite-turla/15098/).

05 Kaspersky Labs. "How Turla and "Worst Breach of U.S. Military Computers in History" are Connected ." Kaspersky. 12 March 2014. (Accessed on 12 February 2024 at https://usa.kaspersky.com/about/press-releases/2014_how- turla-and--worst-breach-of-u-s-military-computers-in-history-are-connected).

06 Mike Lennon. "Russian-Speaking Turla Attackers Hijacking Satellite Internet Links." Security Week: Cybersecurity News, Insights & Analysis. 9 September 2015. (Accessed on 3 February 2024 at https://www.securityweek.com/russian-speaking-turla-attackers-hijacking-satellite-internet-links/). Kim Zetter. "The Return of the Worm That Ate the Pentagon." Wired. 9 December 2011. (Accessed on 12 February 2024 at https://www.wired.com/2011/12/worm-pentagon/).

07 Jim Finkle. "Agent.BTZ Spyware Hit Europe Hard After U.S. Military Attack: Security Firm." Reuters. 12 March 2014. (Accessed on 12 February 2024 at https://www.reuters.com/article/us-russia-cyberespionage/agent-btz-spyware-hit-europe-hard-after-u-s-military-attack-security-firm-idUSBREA2B25R20140312/).

08 John Leyden. "State Cyberspies Wriggle Into Satellites For Super-Duper Sneaky Ops." The Register. 9 September 2015. (Accessed on 3 February 2024 at

https://www.theregister.com/2015/09/09/turla_apt_satellite_stealth/#:~:text=A%20Russian-speaking%20cyber- espionage%20group%20which%20exploits%20the%20Turla,global%20satellite%20networks%20as%20part%20of% 20its%20tradecraft).

09 Stefan Tanase. "Satellite Turla: APT Command and Control in the Sky." SecureList (By Kaspersky). 9 September 2015. (Accessed on 9 February at https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/).

10 Kim Zetter. "Russian Spy Gang Hijacks Satellite Links to Steal Data." Wired. 9 September 2015. (Accessed on 3 September 2024 at https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections- to-steal-data/).

11 Kaspersky Lab. "Turla Hiding in the Sky: Russian Speaking Cyberespionage Group Exploits Satellites to Reach the Ultimate Level of Anonymity." Kaspersky Lab. 9 September 2015. (Accessed on 3 February 2024 at https://media.kaspersky.com/pdf/Kaspersky_Lab_press_release_Satturla_eng_final.pdf).Ullaboritium aborera eperum resciuntius doloreprae et labore peliquia quis quide sus es res es et autemodi alicipiet eturem. Cient.

MEET 11TH CYBER BATTALION

ARMY CYBER'S WORKHORSE FOR THE TRIAD

SCHOFIELD BARRACKS, Hawaii – Sgt. James Hyman, Expeditionary CEMA operator for the 11th Cyber Battalion's Expeditionary Cyber-Electromagnetic Activities Team-01, collects information from two sensors – on an unmanned aerial system and a robotic dog named Spot – to conduct cyber effects operations, during an Operational Readiness Assessment for the battalion, March 30, 2023.

Photo by Steven Stover, 780th Military Intelligence Brigade (Cyber)

By Joshua Good, U.S. Army Cyber Command

As Staff Sgt. Chandler Harkins was about to brief his team on the day's mission, his battalion commander called the tent to attention.

In walked Lt. Gen. Maria Barrett, commander of U.S. Army Cyber Command (ARCYBER).

"As you were," Barrett said.

Harkins went right into his briefing, not missing a beat. The electromagnetic warfare specialist walked his team through the convoy route and pointed out the objective location on a sand table and explained how his team would collect electromagnetic warfare data at a training range on Fort Eisenhower, Georgia. His Soldiers took notes and repeated key details, such as the grid coordinates of checkpoints and the objective.

Harkins is a leader in the 11th Cyber Battalion, the workhorse of ARCYBER's contribution to the new triad—a combination of space, cyber, and special operations capabilities. After Harkins' sand table rehearsal, Barrett spoke with his team members.

"The things you are doing here are super important," she told them. "We can't do everything from a computer in garrison. We are looking to expand access. You are giving commanders options to degrade our adversary's capabilities."

The Soldiers of 11th Cyber Battalion showed Barrett the tools they will use to support the triad, including drones, a handheld radio spectrum analyzer, and offensive cyber operations equipment.

"Everything can be applied to the triad," said Lt. Col. Lou Etienne, 11th Cyber Battalion's commander.

Etienne's job is to build 12 expeditionary cyberspace electromagnetic activities teams. His marching orders are to quickly develop cyberspace electromagnetic capabilities and train the expeditionary teams to address the Army's multidomain operations capability gaps related to cyber and electromagnetic warfare.

"The focus for preparing for near-peer conflicts is learning how to overcome access denial capabilities of America's adversaries," Etienne said. "We have to understand how to defeat that."

"Etienne's team members met with Navy and Marine researchers to learn from their electromagnetic warfare experience," said Etienne's former Executive Officer, Maj. Eric Haupt Jr., who now works as the aide de camp for Barrett.

"Why reinvent the wheel when someone already has an incredible wheel?" Haupt said.

The 11th Cyber Battalion has cyber, as well as software developers. It has the backing of ARCYBER's cyber lab, the Technical Warfare Center, and the Cyber Center of Excellence, the Army school for cyber on Fort Eisenhower, Georgia.

Former Cyber School Commandant, Brig. Gen. Brian Vile, is an advocate for getting electromagnetic warfare right and sees 11th Cyber Battalion's work as aiding maneuver commanders.

"After you break your squelch on your radio, you are going to learn two things eight minutes later," Vile said at an Army Maneuver Center's conference last year. "Number one, how good was your emissions control, your EMCON (electromagnetic emission control). And, number two, how good are the enemy's EW (electromagnetic warfare) Soldiers. Because eight minutes is the doctrinal time it is going to take the adversary's EW guys to knock out your grid coordinate, send it back to fires, the king of battle, and have them launch effects on your targets. And, if your EMCON wasn't good and the adversary's EW Soldiers were, you are going to get incoming."

Advanced military forces use radio frequency triangulation to locate enemy troops and use that information to engage with indirect fires, such as rockets and artillery.

Etienne and his Soldiers have taken Vile's eight-minute drill to heart and learn similar lessons as they study electromagnetic warfare lessons from the war in Ukraine and the Middle East.

"Our enemies are very good at figuring out things to do that are below the threshold of nuclear war that still have strategic implications," Etienne said. "Our adversaries are fighting in a gray zone. There is no better pairing of cyber, space, and special operations forces to be a strategic advantage for the Department of Defense and for the Army."

SCHOFIELD BARRACKS, Hawaii – Staff Sgt. Ryan Hedgcoth, Expeditionary Cyber-Electromagnetic Activities (CEMA) operator with Expeditionary CEMA Team-01, 11th Cyber Battalion, inspects a Tactical RF Applications Chassis, a platform that enables mission-tailored CEMA capabilities, during an Operational Readiness Assessment for the battalion, March 29, 2023.
Photo by Steven Stover,
780th Military Intelligence Brigade (Cyber)

Etienne's battalion also has the backing of the ARCYBER G39 Information Advantage Division, which is nested under ARCYBER's G3, the staff directorate of a general-officer staff section in charge of planning and issuing orders. Aaron Pearce is the ARCYBER G39 director and in charge of making recommendations about 11th Cyber Battalion's future.

"Where we would like to go in the future is to serve as a specialized cyber and electromagnetic warfare force," Pearce said.

Pearce sees 11th Cyber Battalion supporting land component units at the theater Army, corps, and division levels.

Most of 11th Cyber Battalion's missions have been training exercises, such as Combat Training Center rotations at the National Training Center at Fort Irwin, California, and the Joint Readiness Training Center at Fort Johnson, Louisiana, formerly Fort Polk.

Those training centers are large enough to support a brigade-plus size unit.

Though an expeditionary cyberspace electromagnetic activities team is a division or higher-level unit asset, the team could support a brigade if a division commander decided that supported brigade was the main effort.

"That would be up to the corps and division commanders," Pearce said.

During a recent three-star general officer steering committee meeting, all three commanders said they want to move from training to operationalizing the Cyber-Space-SOF Triad. "I'm excited for the next 20 years," said Lt. Gen. Jonathan Braga, commander of the U.S. Army Special Operations Command. "You will be looking back at this as the black and white, the dark ages. We are going to help the Army."

Harkins, 11th Cyber Battalion's staff sergeant, epitomizes the Soldiers Etienne and his team recruit for the unit. Harkins was formerly a military police branch Soldier and worked for 7th Special Forces Group before he reclassed to electromagnetic warfare. Etienne also has Soldiers, who have been coders since middle school.

The battalion is a mix of technical and tactical—just what the Army needs to build the triad.

Staff Sgt. Chandler Harkins is an electromagnetic warfare specialist and leader in the 11th Cyber Battalion, stationed at Fort Eisenhower, Georgia. Harkins used to work for 7th Special Forces Group and was a Military Police Soldier before he reclassed to EW.

Photo by Steven Stover,
780th Military Intelligence
Brigade (Cyber)

ARMY SOF-SPACE-CYBER TRIAD:
MULTIDOMAIN COGNIZANCE

By Col. Pete Atkinson, Division Chief, U.S. Army Headquarters

The Army SOF-Space-Cyber Triad is a collaboration effort involving the United States Army Special Operations Command (USASOC), United States Army Space and Missile Defense Command (USASMDC), and United States Army Cyber Command (ARCYBER).

Over a decade ago, the Triad concept was a feature of the USASOC Silent Quest exercise, which focuses on emerging threats in complex operational environments. Silent Quest is a series of exercises and events, nested with the Army's Unified Quest and United States Special Operations Command (USSOCOM) Shadow Warrior Project, that tests Army Special Operations concepts.

With recent attention at the 2022 Space and Missile Defense Symposium in Huntsville, Alabama, and the 2023 Association of the United States Army (AUSA) Annual Conference in Washington D.C., the senior leaders from the three commands took a keen interest in the "modern" or "new" Triad. Both events featured Triad-specific panels supported by Army senior leaders from the respective proponents. Using "Integrated Deterrence," a key concept from the 2022 National Defense Strategy as the common denominator, there is a conscious effort to differentiate the SOF-Space-Cyber Triad from the U.S. nuclear triad. Historically, the nuclear triad involves the U.S. Air Force and the U.S. Navy delivery of nuclear warheads by land, air, and sea as a means of strategic deterrence from nuclear attack. While the nuclear and SOF-Space-Cyber triads are a vital component to national security, the distinct purpose of each is what separates the two.

The SOF-Space-Cyber partnership is not a new concept. Throughout the past two decades of conflict during the Global War on Terrorism, special operations, space and cyber forces have been working together. The SOF-Space-Cyber collaboration gained notoriety due to the rapidly evolving threats pertaining to great power competition and the Army's shift from counterinsurgency operations to large-scale combat operations. At the same time, the Army changed its doctrine from AirLand Battle to multidomain operations to account for the space domain and information environment increasingly extending the modern battlefield. AirLand Battle doctrine takes a nonlinear view of battle, and enlarges the battlefield area, stressing unified air and ground operations throughout the theater. The "extended battlefield" and the associated concept of AirLand Battle helped visualize the battlefield of the time, which now extends into the maritime, space, and cyberspace domains.

The Triad is not the main effort. The convergence of effects needs to coalesce around ground maneuver forces that are purpose-built to seize and hold terrain at scale. While not the only consideration, recent conflicts in Ukraine and Gaza demonstrate that 21st-century warfare still boils down to armies fighting to control terrain. The rapid proliferation and democratization of space capabilities, aerial systems, and cyberspace tools act as an equalizer among disadvantaged states. On the other hand, such systems prove to be an asymmetric advantage for the most powerful states. Technology continues to change the character of warfare, yet the nature of war remains constant. Trench warfare in Ukraine and underground tunnel clearing in Gaza persist with precision drone munition strikes and access to space-based intelligence, surveillance, and reconnaissance by all.

The Triad collaboration serves to shoot, move, communicate, and survive on a 21st-century battlefield more effectively. Through exercises, wargames and experiments like Project Convergence and Silent Quest, Triad efforts accelerate continuous transformation and warfighting. These lessons are positively influencing Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy solutions. Examples include advancements in Army space operations peculiar uncrewed aerial systems and high-altitude platforms. Most importantly, the SOF-Space-Cyber partnership is spurring a new way of thinking, a multidomain way of thinking. Over the years, this is the most beneficial outcome of the SOF-Space-Cyber partnership.

When SOF, Space, and Cyber forces work together there is also a transfer of knowledge among highly specialized career fields. Space forces learn irregular warfare tenets, cyber forces understand how space can expand access to networks, and SOF gains a better understanding of the electromagnetic spectrum across multiple domains. This is why Triad collaboration is more than a formation or capability.

LONDON, ALABAMA, UNITED STATES – Project Convergence 2022, a joint force experimenting with speed, range, and decision dominance to achieve overmatch and inform the Joint Warfighting Concept and Joint All Domain Command and Control – C Company of the 2nd Battalion, the Yorkshire Regiment – the 'Experimental Company' took the opportunity to take part in more experiments using a number of recourses. On the ground, soldiers from C Company are working alongside the Infantry Trials and Development Unit (ITDU) utilized equipment such as the SkyDIO unmanned aerial vehicle (UAV) and variants of the Remote Piloted Vehicles (RPV).

Photo provided by Army Futures Command and Extraction from 2 Yorks – British Army Website.

The Triad collaboration helps us better understand multidomain operations, as well as electromagnetic spectrum familiarization more broadly. As the Army pivots to great power competition and large-scale combat operations, familiarity with the electromagnetic spectrum must be standard across the Army. The 21st-century warfare demands a more thorough understanding of electromagnetic spectrum signatures, emissions control, and who is emitting what and where. Electromagnetic spectrum mastery is becoming increasingly more integral to understanding friendly and adversarial kill chains, as well as the find, fix, finish, exploit, analyze, and disseminate cycle. There are a lot of positive features regarding the Triad collaboration, but there are also some negative aspects. Next, we will explore the downsides of the Triad partnership.

The "Triad" re-branding effort created confusion throughout the Army and across the Department of Defense. The overuse of Triad branding makes the collaboration seem exclusive to USASOC, USASMDC, and ARCYBER. While these three commands represent the genesis of the SOF-Space-Cyber partnership, the initiative must expand beyond these commands. Separate from the Triad moniker and branding efforts, another downside involves Army core competencies. The SOF-Space-Cyber forces need to strike a balance between specialization and generalization. As highly specialized Soldiers cross-train, it dilutes their core competency skills. Specialized skills are often perishable and require constant training to remain proficient. At some point, there is a diminishing return when cross-training and highly specialized Soldiers must build external dependencies, such as leveraging space operations officers' expertise. The Triad cannot jeopardize Army core competencies to gain general knowledge. For example, Army space professionals would find it difficult to remain proficient in space capability certifications while adding SOF training requirements like language proficiency and survival, evasion, resistance, and escape training.

The purpose of the Triad collaboration must culminate with enabling the Army to seize and hold terrain. Warfighting at scale matters, and the Triad collaboration needs to extend beyond USASOC, USASMDC, and ARCYBER. With niche organizations and exquisite capabilities, there is a tendency to focus internally. For example, there needs to be a focus on how Triad-related exercises, wargames, and experiments can support infantry and armor divisions. Further, can Triad lessons scale across the Army? The disadvantages should not discourage the SOF, Space and Cyber collaboration from persisting. Such criticisms can strengthen the initiative and generate broad appeal.

The Triad must extend into day-to-day operations. This means USASOC, USASMDC, and ARCYBER need to work more closely together and alongside other Army service component commands. This will expand the scope and scale of experiments, exercises, and wargames. Next, the Triad collaboration should double down on how the initiative directly supports ground maneuver forces to seize and retain terrain at scale. I recommend pivoting from integrated deterrence and moving toward multidomain operations as the underlying principle that unites SOF-Space-Cyber forces. It is never too late to re-brand. I recommend avoiding the use of buzzwords and conflating terminology and focusing on long-term strategic goals. The higher purpose of the Triad must always be to enable the Army to close with and destroy the enemy. As lessons learned from Ukraine showcase, 21st century wars remain incredibly violent and bloody.

Soldiers assigned to 1st Battalion, 7th Calvary Regiment, conduct combat maneuvers containing an Advanced Targeting and Lethality Aided System (ATLAS) at Fort Irwin, California, on Nov. 5, 2022. During Project Convergence 2022, many systems were tested to determine how future command and control capabilities can be integrated with all-service multi-national partners.

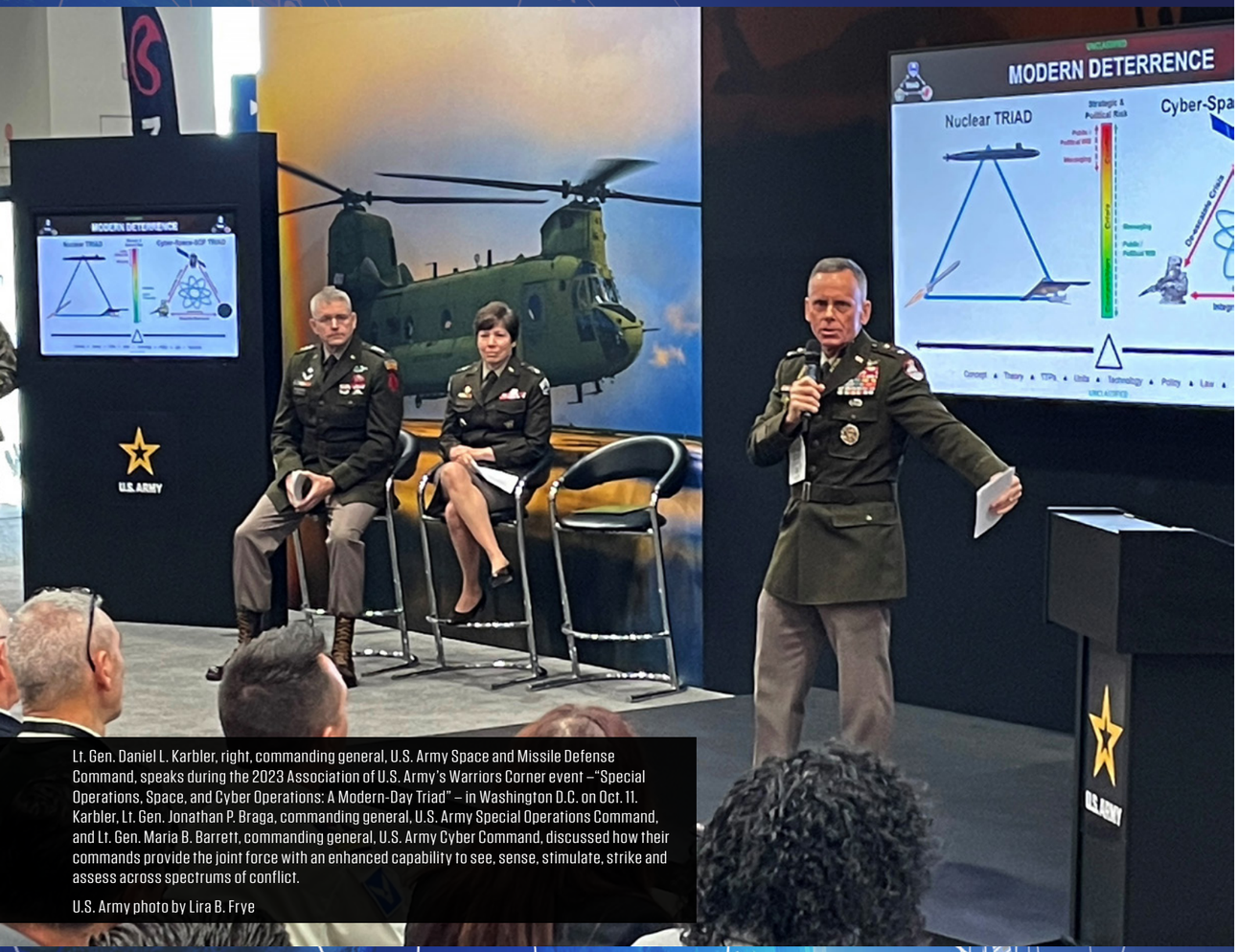
U.S. Army photo by Spc. Gabriella Bruce-Larkin.

Finally, the Triad collaboration should produce holistic, Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy changes to shape future operating concepts and doctrine. When appropriate, scale Triad lessons learned across Army formations, especially multi-domain task forces. The Triad should inform the Planning, Programming, Budgeting, and Execution System and forums like the Total Army Analysis, Strategic Portfolio Reviews, Program Decision Memorandum studies, and Program Objective Memorandum. As a result, the SOF-Space-Cyber partnership will spur large-scale organizational change. When drawing parallels to multidomain operations, the Triad partnership allows the Army to rethink traditional mission areas. As the Army better understands space and cyberspace threats, this will change Army warfighting. The SOF-Space-Cyber collaboration could serve as the Army vanguard that develops the next generation of creative problem solvers who embody a new way of thinking.

FROM TRIANGLES TO CIRCLES

RESHAPING CYBER-SPACE-SOF TRIAD FOR MAXIMUM OPERATIONAL IMPACT

By Lt. Lloyd Forrest Hansen, U.S. Navy



Lt. Gen. Daniel L. Karbler, right, commanding general, U.S. Army Space and Missile Defense Command, speaks during the 2023 Association of U.S. Army's Warriors Corner event –"Special Operations, Space, and Cyber Operations: A Modern-Day Triad" – in Washington D.C. on Oct. 11. Karbler, Lt. Gen. Jonathan P. Braga, commanding general, U.S. Army Special Operations Command, and Lt. Gen. Maria B. Barrett, commanding general, U.S. Army Cyber Command, discussed how their commands provide the joint force with an enhanced capability to see, sense, stimulate, strike and assess across spectrums of conflict.

U.S. Army photo by Lira B. Frye

INTRODUCTION

Mastering the art of strategy is crucial. Clear models and concise acronyms enable swift, effective decisions, whether on the battlefield or in the boardroom. Renowned concepts like the observe, orient, decide, act loop and mutually assured destruction are staples in military jargon because their framing is intuitive and simple.

In contrast, military concepts like a Fabian strategy, C5ISRT, and campaigning are only likely to be understood in the realms of professional military education and, perhaps, by general officers. While these concepts may be important, they demand considerable mental effort to translate from abstract ideas into concrete actions. One such contemporary concept with suboptimal framing that directly impacts the special operations forces (SOF) community is the Cyber-Space-SOF Triad.

A triad framework is not new in military discourse. The most notable triad is the nuclear triad consisting of land-based intercontinental ballistic missiles, strategic bombers, and ballistic missile submarines. This represents a three-pronged approach to nuclear weapons, specifically to deter a first strike and represents the potential to leverage combinations of capabilities across multiple military domains to create synergized battlefield effects.

In 2022, Lt. Gen. Jonathan Braga, commanding general of the U.S. Army Special Operations Command, noted that the intent "is to really increase the holistic strategic effect of each of the multidomain capabilities across the spectrum of conflict both now and in the future." [01] With this intent, it becomes clear that the Cyber-Space-SOF Triad needs to be reframed and reshaped.

PROBLEMS

The Cyber-Space-SOF Triad, often likened to the nuclear triad, is mischaracterized as a "modern deterrence triad." [02] This framing of the Cyber-Space-SOF Triad is like forcing a square peg into a round hole.

First, Cyber, Space, and SOF are meant to be mutually supporting capabilities and a force multiplier. During a U.S.-U.K. panel discussing the new triad, Commodore Adam Bone of U.K. Space Command Director of Operations, Plans and Training said, "…by synchronizing effects, the layered output adds up to be greater than the sum of their parts—that's what makes the triad concept so valuable." The nuclear triad's capabilities are independent. Each leg of the nuclear triad is meant to serve as a means of ensuring weapons delivery even if one leg is compromised while the Cyber-Space-SOF triad is meant to work collaboratively. Therefore, in terms of mutual support to maximize effects, the nuclear triad is nothing like the Cyber-Space-SOF Triad.

Second, using the triad structure (the layout of three lines connecting three points to create a triangle) undermines the concept of mutual support for maximum effect. When visualized, the triangle gives no indication of how a combination of capabilities maximize effects. Even with directional arrows connecting each capability, the design only indicates that each capability assists the other. Additionally, the center of the triangle remains conspicuously empty and does not project a sense of effects maximization (or even of real conceptual substance). If trying to conceptualize a combination of efforts to maximize effects, a hollow triangle is not the proper way to portray this information.

Third, calling the Cyber-Space-SOF Triad a deterrent triad is misleading. In the age of integrated deterrence, initiatives are often forced to fit this mold. However, this can convey a message to the joint force that contradicts the initiative's inherent intent. [03] Unlike the nuclear triad, the Cyber-Space-SOF Triad gives commanders usable options that are less likely to escalate into armed conflict. [04] According to Lt. Gen. Daniel L. Karbler, "The combined use of space, cyber and special operations force capabilities provides other options to commanders that are less likely to cause escalation." [05] While the nuclear triad provides deterrence, the Cyber-Space-SOF Triad provides offense, defense, stability, and deterrence options. Framing the Cyber-Space-SOF Triad as a modern deterrent undervalues it as a tool that provides commanders multiple options throughout the conflict continuum.

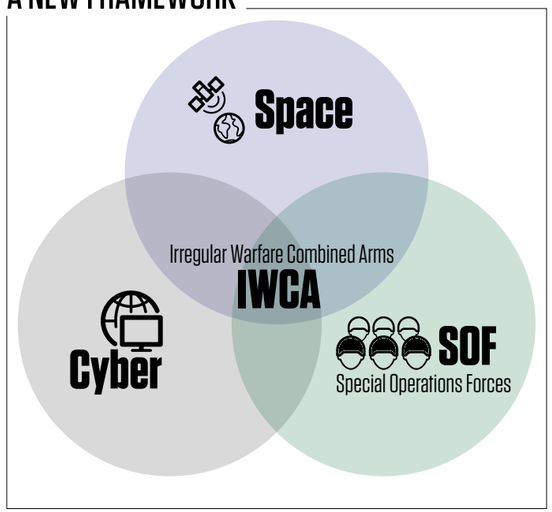
> Noted that the intent "is to really increase the holistic strategic effect of each of the multidomain capabilities across the spectrum of conflict both now and in the future." [01]
>
> *Lt. Gen. Jonathan Braga*
> *Commanding General*
> *U.S. Army Special Operations Command*

Braga stated that the Cyber-Space-SOF Triad provides non-attributable options to the joint force. [06] Non-attributable options are not good deterrent mechanisms because it is hard to deter an adversary without presenting a credible threat. Consider the destruction of the Nord Stream pipeline. Without attribution, holding a critical asset like the Nord Stream pipeline at risk does not work as a deterrent. [07] If the triad provides non-attributable options then messaging it as a modern deterrent triad is misleading.

To articulate the strategic value of the Cyber-Space-SOF Triad more effectively, it is important to recast it not as a reactionary tool, but as proactive options to be used across the competition continuum. Rather than a "break glass in case of emergency" tool, like the nuclear triad, the Cyber-Space-SOF Triad is a "break glass now to avert a future crisis" tool.

A NEW FRAMEWORK

An enhanced conceptual framework that highlights the combined strength and offensive capabilities of the Cyber-Space-SOF Triad would better serve U.S strategic objectives. Consider the proposition of the irregular warfare combined arms framework. In this Venn diagram exists the three components of Cyber, Space, and SOF each in their own set. The intersection of each of these sets represents irregular warfare combined arms.



Firgure provided by Lt. Lloyd Forrest Hansen

This framework provides a more intuitive understanding of the relationship between each element. Combined they offer a unique capability that otherwise would not be possible.

Additionally, there are options that can involve two of the three capabilities to increase effect. This visualization of the irregular warfare combined arms framework presents a more accurate understanding of the interplay between these capabilities and the combined arms title gives the whole framework an intuitive understanding across the joint force.

APPLICATION AND RECOMMENDATION

Beyond an academic debate between triangles and circles, the application of this concept is what ultimately matters. Great concepts are meaningless if they do not lead to action.

One way this new framework is better suited for joint force adoption is the relatable vocabulary it brings. Concepts like enabling maneuver, force multipliers, mutual support, and battlefield integration can be applied to irregular warfare combined arms. Using this joint language helps this concept spread throughout the joint force in a manner that takes the elusive and misunderstood space-and-cyber domains along with SOF capability and make them digestible. Irregular warfare combined arms are mutually supporting force multipliers that enable battlefield maneuver to generate impacts across the continuum. This is the language of the joint force.

Another benefit of using this combined arms construct is that it gives a blueprint on how to combine these arms. Looking at conventional combined arms, elements can be established that encourage integrated planning and coordination. For example, combined arms battalions and brigade combat teams in the Army are cross-functional forces that were developed to facilitate planning and integration of their capabilities. According to Army doctrine on combined arms battalions, "The CAB combines the efforts of its armor and mechanized infantry companies to execute tactical missions."[08] Furthermore, the Army has developed the multidomain task force specifically to counter adversary anti-access, area denial technologies. In recognition of the challenges and demands of the modern battlespace, this task force synergizes capabilities from various domains to achieve its objectives effectively. Organizations like these, with a focus on combining conventional or domain-based arms, provide blueprints for combining the irregular warfare capabilities of cyber, space, and SOF.

By reimagining the traditional combined arms model, commanders can forge innovative irregular warfare combined arms elements tailored to their unique operational demands. Envision an irregular warfare combined arms platoon composed of a Navy SEAL platoon or Psychological Operations team merged with maritime space officers and cryptologic warfare technicians integrated directly within the theater special operations commands. These units would be strategically positioned to coordinate their efforts, providing theater special operations commands and combatant commanders with versatile options to sculpt the battlespace and engage with adversaries with minimal risk of escalation.

CONCLUSION

The irregular warfare combined arms framework is a more effective way to understand the important intent behind the Cyber-Space-SOF Triad. Rather than framing the trinity concept as a modern deterrent with parallels to the three nuclear weapons delivery modalities, the triad should be reshaped into a combined arms framework that builds upon the understanding of conventional combined arms. This framework is easier to conceptualize, and it emphasizes the purpose behind the triad model—that the combination of cyber, space, and SOF capabilities can provide leaders with synchronized and scalable options across the spectrum of conflict. Leaders who reconceptualize the triangular structure of the triad to the intersecting sets of the irregular warfare combined arms are not just reshaping frameworks; they are reshaping the battlespace.

01 AUSA Warfighter Summit and Exposition – USASOC - SOF, CYBER AND SPACE TRIAD, 2022, https://www.youtube.com/watch?v=I1AUbX7daJQ. (12:05)

02 AUSA Warfighter Summit and Exposition – USASOC - SOF, CYBER AND SPACE TRIAD.

03 "Biden-Harris-Administrations-National-Security-Strategy-10.2022.Pdf," accessed January 31, 2024, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

04 AUSA Warfighter Summit and Exposition – USASOC - SOF, CYBER AND SPACE TRIAD.

05 "Leaders Give Update on 'Modern Triad,'" www.army.mil, accessed January 22, 2024, https://www.army.mil/article/268971/leaders_give_update_on_modern_triad.

06 AUSA 2023 Warriors Corner: The Special Operations Forces, Space and Cyber Triad , 2023, https://www.youtube.com/watch?v=bgQYCGmoiBw.

07 Sergey Vakulenko, "Shock and Awe: Who Attacked the Nord Stream Pipelines?," Carnegie Endowment for International Peace, accessed January 28, 2024, https://carnegieendowment.org/politika/88062.

08 "ARN32974-ATP_3-90.5-000-WEB-1.Pdf," accessed January 30, 2024, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN32974-ATP_3-90.5-000-WEB-1.pdf.

SOF-SPACE-CYBER TRIAD IN ACTION:

RECLAIMING THE INITIATIVE IN UKRAINE

By Dr. Spencer Meredith, Professor of National Security Strategy, National Defense University

Ukraine's recent incursion into the Kursk region of Russia has temporarily rekindled Western interest in the war. Yet, despite reclaiming the strategic initiative, the circumstances of Ukraine's survival remain dire. Frozen battle lines along a vast front have depleted Ukrainian morale as much as manpower, and the potential for Russian advances will continue to threaten them for the foreseeable future. Ukraine can only survive by winning an increasingly desperate fight, but victory is constrained by the nature of its partnership in war. Sustaining munitions remains paramount and, while long-range artillery and logistics dominate the policy debates, Special Operations partnerships have also been essential to Ukraine's survival.

Ukraine needs to maneuver to win, as evidenced in the first year of the war and the recent cross-border advances. Unfortunately, its armed forces lack the necessary staff officers to sustain those efforts with a military culture still wedded to Soviet-style mass attacks. The effect has been to relegate special operations forces (SOF) to "elite infantry" roles supporting conventional units. Yet special operations include a range of irregular warfare capabilities to menace enemy positions and mobilize civil resistance behind the lines. The exploitation of breakouts and harrying attacks inside of Russia are well within the realm of special operations capabilities. They are also some of the only Ukrainian units enabling concentrated fire on Russian vulnerabilities while drawing attention away from their own defenses. However, from the early victories around Kyiv through the ongoing battles in the marshes above Crimea, Ukrainian special operations forces (UKRSOF) are sustaining Ukraine's war effort in ways that do not receive widespread attention.

Making matters more difficult, the West has yet to arrive at a consensus on what Ukraine is as a partner, let alone where it should go after current hostilities end. Ukraine is not a proxy against Russian aggression nor is it a novice in the struggle against Moscow's predations. Ukraine is a partner fighting a centuries-old battle to remain free. As a result, the lack of Western consensus cedes the strategic initiative to Russia and creates confusion as to how to fight and win the war. This has led to critical missed opportunities on the battlefield, opportunities Ukraine will run out of if fundamental changes are not made.

The most time-sensitive goal is to prioritize special operations as a force multiplier and operational "connective tissue" across Ukraine's military. As a pillar in the *SOF-Cyber-Space Triad*, special operations provide decision makers with diverse, multidomain, and transregional networks to operationalize innovation across partnerships. This enables SOF to produce discrete options that impose costs on adversaries while building partner capacity to do the same.

Note: Yellow and blue text denote hyperlinks.

Ukrainian solider holding Ukraine flag in front of bombed bulding.

Photo provided by Adobe Stock

The Combined Joint Special Operations Task Force (CJSOTF) model applies lessons learned fighting non-state actors to campaigning against peer adversaries. It also sharpens the skills needed to help partner forces defeat a global adversary. The small-unit, network approach to special operations enables them to adapt to changing battlefield conditions more quickly than larger units. Innovations in drones grab the headlines; equally important have been SOF innovations in communications, logistics, and battlefield medicine keeping Ukrainians alive and in the fight. So far, UKRSOF partnerships across the Triad have contributed to the destruction of more than $1 billion of Russian combat power and a generation of Russian military leadership.

As masters of human networks, SOF connect diverse communities of expertise – from intergovernmental and interagency to commercial and academic – in order to develop solutions to critical problems. Ukraine needs the full breadth of those partnerships because it cannot survive a conventional war without special operations playing a more central role. Saying so goes against the tide of cuts to U.S. special operations forces personnel. It also challenges the dominant argument that big conventional movements matter more than surgical strikes that SOF enable. The misconception stems from a larger problem of ignorance of the partner and partner war, one which special operations forces are ideally capable of correcting.

UNTIMELY IGNORANCE

When the war began more than two years ago, the assessments of Russian strategy and capabilities were almost as wrong as those about Ukraine. Ignorance of "maskirovka," – camouflage and surprise, and "lazha," lying with half-truths, led most to assume uncontested Russian superiority. Equally, ignorance of Ukrainian resilience missed the longstanding resistance inherent to its culture and historical experience over centuries. Thus, while the reemergence of Russia in U.S. strategic priorities might have begun in 2014, it followed more than 20 years of marginalization in academic and intelligence communities. The periphery of the historic Russian empire remained even more under examined with episodic attention on color revolutions or flaring military conflicts, yet subject matter expertise cannot be created after a crisis. The lack of deep, contextual knowledge has meant that U.S. approaches to Ukraine follow a similar pattern in U.S.-led partner wars – functional experts and theorists set the analytical framework and recommendations rather than those who know the partner and adversary deeply.

The communal assessment in February 2022 accepted Russia's self-proclaimed military superiority and planned for Ukraine's rapid defeat. In contrast, the relatively few Ukrainian experts and small U.S. special operations forces contingent in Ukraine understood better, as seen in recommendations to the U.S. joint task force preparing for Ukraine's resistance. However, even though their minority report was quickly proven correct, the lessons of collective ignorance have not led to changes in the approaches to the war in Ukraine.

The consequences of this analytical asymmetry have been all too familiar – oversimplified explanations that produce unsustainable solutions. Theory-based assertions that the U.S. and NATO caused Russia to react defensively show as much intellectual laziness as ignorance of the offensive nature of the Russian Empire. The recommendation to cede nearly a quarter of Ukraine's legal territory may offer a short-term solution to the fighting, but it ignores the Kremlin's existential need to reclaim all of Russia's lost empire. Putin carries the weight of history in stamping out a sovereign Ukraine, just as his successors will for the whole of "Russkiy Mir."

Equally so, claiming Ukraine can win a war of attrition because defense has the advantage along the front ignores Russia's long-term opportunistic theory of victory. With China's expanding financial backing, Russia is able to sustain and increase offensive operations at a higher pace than previously in the war. Neither can Ukraine defend the extent of the front lines over the long-term given mounting battle fatigue and high casualty rates. Even more damaging are losses to the country's industrial base, energy production, and agricultural capacity. Any resulting Ukrainian defeats imply its unsustainability to undecided international partners. To some, the fall of Avdiivka became a harbinger of worse things to come.

The current U.S. and NATO force posture outside of Ukraine means the tyranny of distance hinders some aspects of support. Reintroducing U.S. and NATO forces into Ukraine would benefit the "advise and assist" mission and could provide a strategic trip wire to deter Russian escalation in Ukraine, including the use of tactical nuclear weapons. However, it can also undermine Kyiv's critical role in deciding how to escalate to deescalate. Even more so, it alleviates some of the pressure currently on Ukraine's leadership to confront hard adaptations necessary to succeed against Russia.

Fighting and winning a partner war requires understanding the partner, but also how partnerships differ from proxy wars. Proxies enable comparatively safer escalation against peer adversaries because they are indirect relationships; partners must manage escalation together.

Proxies also necessitate multiple control mechanisms through asymmetries in intelligence, resourcing, training, and operational planning. Dependence means unequal decision-making, which weakens the legitimacy of a proxy as a governing agent. The quick collapse of Afghanistan's government owes much to the proxy relationship that denigrated Afghan leaders to a subservient role in their own country. By contrast, successful U.S.-led partner war involves self-constraint at times. This requires deep contextual knowledge to know when and where to push the partner, and when to support the partner's leadership. U.S. and NATO partners have decades of integration enabling interoperability and symmetric decision making. Partnership with Ukraine is comparatively new and must first recognize that Ukraine is not a proxy for U.S. escalation against Russia nor is its government unsuited for equal decision making in defending the country's sovereignty.

UKRAINE AS A VIABLE PARTNER IN WAR

Even with the de facto loss of territory since 2014, the past three decades represent one of the longest periods of Ukrainian sovereignty over such a large extent of territory. Despite the hardships and grim prospects for the future, the national identity of Ukraine is holding because the country maintains legitimacy as an independent state. The potential to mobilize the population relies on historic legacies of the Zaporozhe Cossacks and the anti-Bolshevik Poltava Uprising a century ago. These inspire continued resistance to Ukraine's "eternal foe" in Russia. Government measures to lower the draft age and rebuild depleted forces along the forward lines mean Kyiv still has social capital to expend. In addition, battlefield innovations have expanded well-developed military research and development, broadening the scope of defense partnerships across the country and internationally. Despite losses to largescale farmlands and agricultural equipment, Ukrainians still have access to self-sustaining food supplies through familial or communal connections to village farming. This, too, bodes well for resilience over time.

Secretary of Defense Lloyd J. Austin III and Ukrainian President Volodymyr Zelenskyy address the media at the 24th meeting of the Ukraine Defense Contact Group at Ramstein Air Base, Germany, Sept. 9, 2024.

DoD photo by Chad J. McNeeley

However, even with renewed U.S. funding, the country can afford very few failures before serious problems will arise. Given the prevalence of historic corruption and weak federal governance, how long the Ukrainian populace will remain active participants in the fight remains to be seen. There are simply too many living memories of political apathy available to undermine political efficacy. How then to bolster what is still strong, reinforce what is weakening, and restore what has been lost?

Ukraine faces two core challenges from which other problems arise. The first is convincing the West that Ukraine is worthy of sacrifice for the foreseeable future. Strategic balancing adds weight to the argument, but competing alternatives to constrain Russia could sacrifice Ukraine instead. The alarm of further Russian aggression also lost some of its comparative resonance since war erupted in the Middle East and looms larger in the Pacific. Thus, while President Volodymyr Zelenskyy, President of Ukraine, remains a visible figure internationally, his "hat in hand" message wears thin on strained Western economies and divided Western electorates.

The second challenge requires Ukrainian decision makers to make fundamental changes to how they approach the war. Foremost is discarding Soviet-era doctrine with its top-heavy decision making and siloed operational planning that has often appeared as "one-size-fits-all." The current battle lines are not uniform with significant variations in population centers, avenues of attack, and topography. Movement from the northern region of Sumy into neighboring Kursk makes sense as ongoing, low-level Russian attacks have hardened rather than weaken local resistance. Equally importantly, flat terrain favors maneuver.

Lands east of the Dnieper also tend to be flat compared to the western Carpathian Mountains, even as the river delta north of Crimea presents distinct operational challenges for combatants attempting to advance. It also presents opportunities to maneuver around marshland islands and assault Russian positions. In contrast, Russian fortifications across former farmlands, as well as around urban centers, make offensive operations there vastly more challenging. The lack of sufficient artillery to weaken those fortifications compounds the difficulties.

Yet despite important variations in the operational landscape, Ukrainian armed forces largely rely on homogenous operational approaches. Overreliance on mass artillery has meant munitions shortages do more than give Russian forces time and space to consolidate gains. It also cedes the operational initiative to an increasingly well-armed enemy. The failure of the previous **counter-offensives** and persistent **sluggishness** of Ukrainian operations also stem from broader leadership problems. One of the core tenets of the SOF-Cyber-Space Triad is that smaller units lead the race to innovate capabilities. Due in large part to SOF partnerships, they are also reshaping Ukraine's tactics, techniques, and procedures. Yet much of that forward-thinking does not reach senior level commanders.

Even with successes in Kursk, Ukraine's ability to sustain effective combined arms maneuver is low, threatening to cut short gains from initially successful advances. The primary reason is a lack of trained staff officers capable of integrating units across multiple domains and areas of operation. The Soviet model of highly concentrated decision-making at higher echelons remains a constant even among new recruits, who quickly gain the most operational experience. Even when not attacking, senior leaders rely on previous Soviet military training, as seen in the decade of defensive **joint force operations** around the Donbas region. That phase of the conflict began and remained an artillery duel along relatively fixed position. In contrast, the first year of the war was characterized by maneuver on multiple fronts. Early victories owed as much to the weakness of Russian forces, as to the shock that Ukrainians could and did maneuver to destroy them. With nearly a decade of partnership, the first generation of **U.S. and NATO trained special operators** galvanized the country's defense in many of those victories against superior Russian forces.

Special operations forces are ideally positioned for asymmetric advantage because they are assessed, selected, and trained based on three core skills: critical problem solving, the ability to build and operate across networks, and leadership. The "team of teams" model highlights modular abilities that can adapt across operational environments as much as between diverse relationships. The ability to engage and harmonize efforts with disparate organizational priorities and cultures requires specific a priori personality traits, as much as advanced training as interlocutors. Despite criticisms of "hammers seeking new nails," the true nature of Special operations forces is more akin to a "Swiss Army Hammer" replete with a range of hard and soft power tools.

Special operations have adapted from a short-lived dominant role in the Global War on Terrorism to include broader support functions in strategic competition. Initially relegated to countering non-state threats, initiatives by the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD SO-LIC) and U.S. Special Operations Command (USSOCOM) have reinforced the SOF role across competition, crisis, and conflict. In particular, the relevance of strategic sensors and high value targeting increases as threats proliferate. However, despite recent reviews by defense analysts, much of the discussion about SOF remains superficial. Escalating geostrategic threats require a more detailed case of special operations successfully fulfilling the unique SOF role campaigning in a partner war against a peer adversary. The current Combined Joint Special Operations Task Force – 10 **(CJSOTF-10)** offers such a model.

THE SPECIAL ROLE OF SPECIAL OPERATIONS IN UKRAINE

U.S. and NATO special operations have entered the third phase of partnership with Ukraine. The first phase of "boots on the ground" from 2015 until early 2022 focused on developing and maturing Ukrainian professional soldiers. Heavily resourced by Western partners, Ukrainian special operations forces balanced training away from the frozen front in the east with operational execution along and behind Russian-backed lines. The proof of UKRSOF abilities came in the initial days of the war through their defense of **Hostomel** Airport and the northern route around **Chernihiv**. Both saved Kyiv, buying time for Ukrainian Armed Forces to maneuver against shocked Russian troops.

The second phase saw the gradual depletion of UKRSOF through attrition in the first year of the war. Their leading role in the initial Ukrainian counteroffensive, followed by close fighting along the front reduced their operational capacity by estimates of 90 percent. Despite the catastrophic **losses**, the net effect helped to save much of Ukraine from Russian occupation. The Western partnership during this phase was limited due to the withdrawal of U.S. and NATO forces from Ukraine. However, the U.S. European Command and subordinate U.S. Security Assistance and Special Operations commands rebuilt and expanded resupply networks from afar. The CJSOTF-10 facilitated those relationships through a vast network of liaisons that maintained the relationship with Ukrainian forces.

The current third phase of partnership works to broaden partnerships and strengthen Ukrainian capabilities to counter increasing Russian threats. CJSOTF-10 engages "up and out" relationships with US government and international partners in support of UKRSOF. Being embedded with Conventional units gives CJSOTF-10 farther reach into procurement and distribution along the front lines. Day-to-day activities reside with the subordinate Special Operations Task Force 10.1 (SOTF 10.1) overseeing training, equipping, advising, and assistance to Ukrainian Special Operations.

The SOTF 10.1 relies on three aspects of U.S. Special Operations to work within policy constraints preventing in-country engagement with Ukrainian forces. First, SOF doctrine prioritizes identifying centers of gravity capable of mobilizing larger groups. This gives SOF operators a force multiplying role through Irregular Warfare emphasis on populations. Second, SOF training enables teams to identify and quickly take advantage of opportunities to gain asymmetric advantage against adversaries through special reconnaissance and high value targeting. Third, the SOF network extends globally across government and commercial sectors, a hallmark of the SOF-Cyber-Space Triad in action. The combination has enabled SOTF 10.1 to reposition Ukrainian Special Operations Forces for a pivotal role once again.

The SOTF 10.1 oversees a "Remote, Advise, and Assist" (RAA) team that serves as a call center, library, and laboratory. While remote engagement does not permit shared risk, it does enable Ukrainian advances by 1) facilitating communications between units, 2) enhancing Ukrainian adaptation of existing capabilities, and 3) broadening partnerships with Western groups innovating battlefield technology across the Triad. Over the past year, the team has developed persistent communications with UKRSOF units all along the front lines. Using a range of systems, they help troubleshoot immediate tactical problems to improve operational effectiveness. Additionally, while shortages at the front are a constant reminder of Ukraine's precarious position, SOTF 10.1 creates links for any unit – SOF or Conventional – to share resources, as well as resupply technical components from civilian sources.

Networks across governments and commercial entities also enable the RAA team to help Ukrainian messaging efforts beyond the front. Using a web of connections supported by the broader SOF community, Ukraine has improved the quality and quantity of messaging through multiple media outlets. Begun in earnest after 2014 to bolster domestic resilience and counter Russian **cyber capabilities**, current efforts focus heavily on external audiences to keep Western attention on Ukraine's viability as a partner. The leading effort has been to increase online **English content** beyond **Kyiv Post** and **Ukrinform** as mainstays of information operations, thereby helping Ukraine compete in a crowded field of influence marketing.

Supporting this has been the inclusion of civilian foreign language translators during training exercises. Many are former public school **teachers** serving on short-term rotations. Cycling civilians through training bolsters domestic awareness of Ukraine's military effectiveness. Doing so outside of Ukraine also enables SOTF 10.1 to rely on NATO partner expertise in vitals skills including trench warfare, demolitions, sniper skills, and riverine maritime operations.

Regular adaptations to the programs of instruction incorporate emerging battlefield conditions. In particular, the RAA team facilitates adaptation and innovation in electronic warfare as it evolves in the war. Ukraine's early efforts to bolster cyber defense have expanded to include a range of capabilities targeting enemy information nodes. Bridging civilian and Triad networks, SOF liaisons assist the development of rapid coding evolutions to identify gaps and exploit short-term vulnerabilities through the Special Operations "**find, fix, finish**" methodology.

In addition, much has been written about the growing ubiquity of unmanned aerial systems as essential elements for both sides. Yet while Russia's initial performance was lower than expected, recent improvements in electronic warfare have meant increased risks to Ukrainian drones. The lack of abundant intelligence, surveillance, and reconnaissance resources means each drone matters greatly to Ukraine's success. **Crowd-source** funding has proliferated the number of drones, but it takes time to procure the necessary funds; even $200 racing drones take weeks to source, to say nothing of actually producing and testing them. One-way-attack-drones have proven their worth taking out main battle tanks, electronic warfare platforms, command posts, and communication nodes, but they are not limitless. Russian jamming extends broader and deeper on both sides of the lines, leading to losses as well. Both sides actively capture and repurpose enemy drones, but Russia can afford the losses more readily than Ukraine.

The SOTF 10.1 oversees a Remote, Advise, and Assist (RAA) team that serves as a call center, library, and laboratory. While remote engagement does not permit shared risk, it does enable Ukrainian advances by:

1. Facilitating communications between units

2. Enhancing Ukrainian adaptation of existing capabilities

3. Broadening partnerships with Western groups innovating battlefield technology across the Triad.

Over the past year, the team has developed persistent communications with UKRSOF units all along the front lines.

Therefore, the RAA team assists Ukrainian forces to find safe routes by passing along mission reports from other units along the line. As a central hub with real-time awareness, this supports Ukrainian mission success with accurate information of enemy capabilities. Increased battlefield awareness helps UKRSOF to find, fix, and finish targets, while also sharing lessons across the broader Conventional Armed Forces. Many of those lessons include technical advances in drone carrying capacity and flight time to increase range and lethality. Emerging research areas include munitions and **trauma care resupplies**, as well as expanding kinetic strikes against hardened targets.

While the drone arms race accelerates, SOTF 10.1 expands its partnerships with U.S. and European drone companies to help keep Ukraine at the cutting edge. As part of the SOF network

approach, the team relies on civilians with expertise in several key areas. Foremost are Ukrainian and Russian language experts. The former becomes more important as the country "de-Russifies" its common language; Ukrainian callers have already begun switching to **Ukrainian for communications** with the RAA call center. The second key area is commercial experience. A recent SOTF 10.1 team was a National Guard unit. Members included technology business owners, senior engineers, and computer scientists. Showcasing the critical importance of SOF-Cyber-Space integration, their expertise greatly facilitated accelerated advances in Ukrainian hardware and software capabilities. Deployments of U.S. Reservist subject matter experts would help to advance those efforts as well.

The combined effect of civilian involvement has led to greater trust of Western partners by Ukrainian units. SOTF 10.1 prioritizes feedback loops between advising, assisting and training that build on partner trust to improve the critical area of **mission command**. Mission command means more than knowing how to plan operations. It requires using a range of **information sources** to exploit adversary weaknesses, and critically, enable follow-on missions by partnered forces. The decentralized leadership paradigm of special operations means UKRSOF pursue objectives rather than specific pathways to achieve them. Creative and critical thinking also enables units to assess results beyond battle damage, specifically identifying broader effects that support other types of operations. These can include psychological operations to increase Russian defections, strikes beyond the front lines, and increased testing of advanced weaponry. Recent efforts to improve long-range fires show the centrality of special operations as a network of specialists capable of resolving the most critical problems facing Ukraine.

POSITIONING THE PARTNER TO WIN

High Mobility Artillery Rocket Systems (HIMARS) and GPS-guided bombs have dominated the story of Ukraine's war for independence. Their utility was witnessed throughout the war, destroying much of Russia's initial combat power in the first year alone. They became more central to the partner war as U.S. stocks ran low and political will to resupply Ukraine even lower. While Congress debated financial support, Russian electronic warfare and surface-to-air missile systems were not idle. Improvements in equipment and deployment effectively negated the utility of GPS-guided bombs given the risks to Ukraine's precious few aircraft. The HIMARS are also a costly weapon system compared to alternatives. Priced at over $4.5 million each platform, and with lengthy manufacturing timelines, Ukraine cannot risk using, let alone losing a HIMARS system as happened earlier in 2024 nor have HIMARS always hit their targets, at times missing due to operator error, and at others from inaccurate coordinates for fire missions.

The SOTF 10.1 training has helped UKRSOF units increase precision writ large, but at a time of diminished stocks when senior Ukrainian commanders have been unwilling to use what they have left. Even standard 155mm artillery rounds have been rationed, with numerous fire missions going unheeded by higher headquarters. Combined with a predisposition for massed artillery as the sine qua non for offensive maneuvers, it is no wonder Ukrainian operations stalled for so long. As a result, prior to the Kursk incursion, calls for attrition warfare made sense when viewed through the fixed paradigm of Soviet doctrine. However, SOTF 10.1 has begun to develop alternatives to work around those limitations through operational innovation from below.

As Russian defenses and electronic warfare signals penetrate deeper into "no-man's land," Ukraine **loses opportunities** to use existing drones for strikes. In response SOTF 10.1 has adapted training to enable UKRSOF to reach out farther from the front lines. This has included utilizing alternative munitions systems for longer range targets. Repurposing spent artillery shells and cluster munitions for multiple targets has added to Ukraine's weapons stocks, but the real challenge has been overcoming line of sight targeting that exposes fire teams to Russian defenses. For example, Javelin missiles have comparable capacity to a single HIMARS rocket, and at a fraction of the cost compared to the overall system needed to fire the rocket.

Yet, with an effective range of only a few kilometers, Javelins have been limited to **intercepting advancing Russian armored units**. They are much less successful forcing the Russians to move from fortified positions since Ukrainian teams cannot approach close enough to their targets and survive long enough to advance in force.

Technical solutions do exist though, as seen in the Israel-Hamas war. The Israeli **Spike** missile system incorporates a range of optics and **over the horizon targeting** to provide both mobility and stand-off options. Ukraine's existing reconnaissance systems do not automatically match partner weapons platform though. However, as a clear example of the Triad in action, SOTF 10.1 is able to support Ukrainian problem solving to identify requirements, integrate systems, and develop prototypes for battle lab testing. Current operations have highlighted those evolutions.

Even with technical solutions though, Ukrainian military culture requires a fundamental change for the innovations to work and endure over time. During a previous engagement with SOTF 10.1, I spoke at length with UKRSOF group commanders about their requirements to win the war. Without hesitation, the consensus was "World War One artillery barrages followed by infantry charges from the trenches." The collective ignorance of the failures inherent to the "cult of the offensive" was shocking. Even more so was the assertion that such tactics actually won the First World War.

Instead, Ukraine must adopt a "**Defense in Depth**" approach like the allies more than a century ago. Faints, harassing fire, and tactical withdrawals restore maneuver to the battlefield when combined with out-of-area assaults like Kursk. The aggregate uncertainty taxes Russia's already insufficient command and control capabilities, to say nothing of straining the Kremlin's **triumphalist propaganda** necessary for popular support of the war.

Yet despite the initial tactical gains in Kursk, the larger operational outcome hinges on Ukrainian combined arms maneuver. In that regard the earlier failure at Avdiivka was not tactical. Ukrainian soldiers fought against impossible odds, as UKRSOF units held positions until evacuation routes and casualty collection centers could be established behind their lines. The **barrage of artillery** – one Ukrainian round per 1200 Russian rounds – and human waves of Russian cannon fodder did not break the Ukrainians as they withdrew in good order, despite horrific casualties. The failure was operational because other Ukrainian Armed Forces did not exploit their own breaches

Ukrainian soldier near Mariupol, Ukraine.
Photo provided by Adobe Stock

in the south, or place "stay behind" units to harass Russian advances while Avdiivka was being assaulted. U.S. and NATO SOF taught UKRSOF those skills, but the operational learning had not filtered upward.

Even with renewed U.S. funding for the war effort, Ukraine still needs to train a cadre of joint force staff officers capable of seeing the battlefield holistically and coordinating combined arms maneuver across the front. To meet the need, U.S. professional military education institutions should prioritize "**mobile education teams**" to teach mid-grade officers how to plan and execute large-scale, multi-domain operations. Previous discussions with UKRSOF company commanders have shown their willingness to adapt their operational paradigm if units could gain time away from the front and senior leaders buy into the approach.

Guided by ASD SO-LIC country prioritization and relying on various funding authorities, **mobile education teams** currently engage with NATO and other regional partners. Expanding those efforts to include a three-week "operational art" training module would meet the planning need, while allowing Ukrainian forces to maintain their "dwell time" ratios away from the front. Based on discussions with SOTF 10.1 and its instructional unit, Task Group Ukraine, an example course would include two weeks for mid-grade staff officers, followed by three days for senior commanders, concluding with a two-day Tabletop Exercise showing the integration of learning and practice. The National Defense University and Service Staff Colleges are replete with existing course materials, much of which can be augmented by the Joint Special Operations University and U.S. Army John F. Kennedy Special Warfare Center and School to include SOF-specific material. This will enable Ukrainian armed forces to mature operationally in empirically grounded theory and doctrine of combined arms maneuver.

The SOTF 10.1 and Task Group Ukraine have already established programs of instruction that implement adaptive curriculum and "**train the trainers**" through iterations of courses. As part of the overarching SOF-Cyber-Space Triad approach, ongoing training events focus on integrating conventional and special operations, joint force coordination, electronic warfare, and drone utilization. A staff-level operational design course would enable tactical learning from below to filter upwards.

Education requires knowing what is needed to learn as much as time to learn it. Western assistance should prioritize SOF relationships that know the partner's needs and can buy time beyond the immediate effects of the current Kursk offensive. Building staff capacity to plan, execute, and sustain combined arms maneuver should rely on UKRSOF to gain tactical mobility with over-the-horizon targeting as part of a larger Defense in Depth strategy. Doing so will help relieve immediate pressures on the frontlines by augmenting **anticipated resourcing of artillery munitions**. More importantly, it would stress Russian capabilities to manage the complexities of mobile warfare, something they have proven inept at accomplishing throughout the war.

With U.S. and NATO expertise supporting them across the operational spectrum, Ukrainian special operations forces are essential to implementing both the battlefield push and training pause to build a more capable force. Only then Ukraine can show the West the value of partnering over the long-term and, in so doing, help the country achieve lasting victory.

The views expressed by this article are those of the author and do not reflect the official policy or position of the National Defense University, Department of Defense, or U.S. Government.

Note: Dr. Spencer Meredith is a Professor of National Security Strategy, National Defense University, specializing in Russia and Ukraine. He serves as Strategic Advisor at the Joint Special Operations Command and for the Combined Joint Special Operations Task Force – 10 (Ukraine).

THE IMPORTANCE OF COLLABORATION FOR
BUILDING SUPERIOR MISSION CAPABILITIES

By Clyde Seepersad, Senior Vice President, General Manager, Education, Linux Foundation

Photo provided by Adobe Stock

Recently, I had a conversation with a Marine working on air-gapped, edge cloud solutions in the field. He pointed out that the military is focused on building IT workflows and tools that save time because, on the battlefield, time equals lives.

Since the *Art of War* was penned more than 2,500 years ago, militaries have sought the means to establish battlefield superiority to save lives and conquer the enemy. Today, the battlefield is less a plane and more of a sphere. We continue to have traditional boots-on-the-ground battlefields, but now every electronic device in every business, piece of infrastructure, and home around the world represents a potential virtual combat zone. Add space as a theatre of operations to this virtual combat zone and the volatilities, complexities, and ambiguities increase exponentially.

It's not uncommon to read comparisons of today's global geopolitical situation to those that led to World War II. The need for battlefield superiority in that war united a team of scientists to harness the power of fission in The Manhattan Project. Achieving superiority today will require uniting the whole of the United States civilian and military defense structure to build a sphere of technology that leverages the vast array of software, global networks, and massive data sets to deliver critical insights in real time to command leadership, as well as the boots on the ground. The biggest difference this time around is that much of the software powering these capabilities is collaboratively developed under open-source licenses, which has significant implications for the path of getting from an innovative idea to high-quality, mission-ready digital products that help the U.S. achieve its military objectives.

Unlike The Manhattan Project's clear end goal, realizing information advantage across this expanded "battlesphere" at echelon and across all domains require constant innovation just to keep pace with evolving technology. Constant innovation is not something the U.S. Army or the U.S. Department of Defense can achieve on their own. Success will require unified collaboration across the civilian and uniformed U.S. military, its foreign partners, and their technology industry partners. Among industry partners, the open-source community's systems operate at a global scale to collaboratively build and improve secure, efficient, and innovative software technologies that are easy to access and use.

CULTURE FIRST

While technology itself can do much of the heavy lifting, the effort must begin with an honest assessment of the culture. If organizational culture doesn't support an operational structure and strategic objectives, the effort to leverage rapid and persistent innovation is bound to fall significantly short of its goals if not outright fail. All civilian and military members of the armed forces must be seen as integral technology infrastructure of the organization. Their habits and behaviors will directly affect the security and capability of government information technology systems, but that extends beyond the official government networks and devices. Every person has their own personal devices — phones, watches, gaming consoles, and so on — that create both risk and opportunity. How users introduce and utilize personal or issued devices in military technology ecosystems can have a diverse, often unintuitive, cascade of operational or even strategic consequences.

Above, U.S. Army Capt. Jonathan J. Springer, fire support officer for 1st Battalion, 327th Infantry Regiment, 1st Brigade Combat Team, 101st Airborne Division, tests his new smart phone application in eastern Afghanistan's Pech River Valley Jan. 9, 2011. Capt. Springer, a Fort Wayne, Ind., native, invented the navigational application to find an inexpensive yet reliable tool for soldiers to use while at home or in a deployed environment.

Left, Capt. Springer tests his new smart phone application in eastern Afghanistan's Pech River Valley Jan. 17, 2011.

Photos by: U.S. Army Sgt. 1st Class Paul Shoemaker

There are two examples of this from the post-9/11 conflict in Afghanistan that articulate the risks and benefits of personal devices and individual user initiative. In early 2018, it was made evident that not seeing everyone's digital footprint — and not accounting for all of their devices — as part of the military's tech infrastructure exposed a significant vulnerability. The event revealed that watches with GPS tracking were revealing highly sensitive information about the locations and activities of service members at U.S. military installations overseas. Conversely, a U.S. Army field artillery officer built the app *TacticalNav* from the ground up to create a low-cost, highly accurate mobile navigation platform specifically for military service members. That self-financed effort shows the opportunity that untapped talent within the organization presents and reinforces the promising benefits of technological innovation driven from the bottom-up, as well as the top-down.

OPEN-SOURCE AND THE COMING TECH LEAP

Any leader who looks back at the ever-increasing rate of technological innovation and feels confident they are prepared for what is coming needs to shift their focus from the last 20 years toward an accelerating future. The coming confluence of quantum computing, generative artificial intelligence, ultra-high bandwidth, satellite proliferation, and edge computing will redefine our expectations of the rate of technological transformation. In the process, it will transform every aspect of warfare including how tools and armaments are deployed, where the so-called front of the battlefield is, and the roles humans will play.

What is the key to integrating these technologies to generate advantage and build mission superiority? Software, specifically open-source software, is the answer. For example, listed below are several opensource technology projects that currently impact this new spherical theater of cyberspace, space, and the rest of the battlefield:

QIR ALLIANCE enables a community-driven effort to develop a forward-looking, fully interoperable specification for quantum computing programs.

PYTORCH and **LLAMA** for AI were both originally developed by Meta and are now open-source projects supporting the development of generative AI platforms and products.

ONAP is an open-source platform for orchestration, management, and automation of network and edge computing services for network operators, cloud providers and enterprises along with **FDO** (FIDO device onboard). Both open-source platforms are considered essential for effective cloud and edge management and security.

EDGEX FOUNDRY is an open-source platform that facilitates interoperability between devices and applications at the internet of things' (IoT) edge while **AKRAINO** is an open set of application and infrastructure blueprints for the Edge.

The advantages of select open-source or commercial off-the-shelf technologies are significant, especially when it comes to opportunities to build on innovation, as well as capitalize on battlefield superiority. Firstly, because open-source is built by a community of interested organizations and IT developers, it attracts the best and most experienced technology professionals. Secondly, because the most useful open-source software is constantly being used ("consumed" in open-source parlance), it is being continuously vetted for security, resulting in some of the most secure technology solutions available.

OPEN-SOURCE CAN BE PUBLIC? PRIVATE? PERMISSIONED? ALL OF THE ABOVE?

Perhaps the biggest and least understood advantage of open-source is that it easily enables confidential solutions that stay confidential. Open-source usually sits at the core of a technology or software solution enabling developers and engineers to start with a fully built framework. This saves time and resources, allowing IT professionals to focus on building the more intricate customized tools and solutions needed. Importantly, those solutions, once developed, can remain highly confidential, subject to all the typical security considerations. Any organization or individual that uses open-source software has the option to share ("contribute" in open-source parlance) anything they create, but they are under no obligation to do so.

There are many well-known examples in the commercial sector, such as public cloud service providers Amazon AWS, Microsoft Azure, and IBM Bluemix, which are all built on the open-source operating system Linux and use Kubernetes. Similarly, public and private network operators including AT&T, Verizon, Nokia, Ericsson, and T-Mobile all rely on open-source versions of ONAP and FIDO to keep their network operations consistent, efficient, and secure.

A particularly excellent example for the military comes from the U.S. Joint Office of Energy and Transportation, which has just adopted the EVerest open-source framework for developing the nation's electric vehicle (EV) charging infrastructure. The EVerest open-source technology project develops and maintains a software stack for energy communications across charging stations, vehicles, generation resources, batteries, adjacent chargers, power grids, backend payment systems, user interfaces, and mobile devices. The project will enable the nation to overcome the incompatibilities of proprietary systems as it builds out its EV infrastructure.

The true power of open-source lies in the massive opportunities it creates for decentralized innovation. It is built through a culture of community that has proven, strong structures and tools to facilitate that innovation. That culture attracts passion and creativity that encourages the kind of interdisciplinary collaboration needed to solve complex problems. For example, to successfully thwart enemy missile attacks, a team of co-operators will need to intercept and interpret intelligence, infiltrate launch software, distort GPS data to affect its course, or use quantum-powered AI to intercept it in flight if all else fails. All of these capabilities require leaders who are willing to invest in building the right culture, providing outcome-focused training and conducting structured experiments that deliver repeatable results.

How do you build and nurture a collaborative community mindset across all our military domains to ensure technologically superior mission capabilities? The old-fashioned way, by following the principles of mission command to build trust and esprit de corps that facilitates and encourages decentralized collaboration. The first step? Recognize that everyone—all Soldiers, all leaders, all people—are technologists. With the right training and skills, everyone has data and ideas to contribute to the community. Ideas that, when parsed by the community, will result in time and lives saved.

Author bio: Clyde Seepersad is responsible for the education arm of the Linux Foundation. Over the past decade, Clyde held senior leadership positions in the education space.

Prior to his involvement in education, Clyde was a Principal at the Boston Consulting Group. He started his career in the public sector, working within the Ministry of Finance in Trinidad and Tobago. He holds a master's in business administration and a master's in economics from Oxford University, where he was a Rhodes Scholar.

THE SIX EVENTS
OF THE ARMY CYBER FITNESS TEST

By Allison Moore, Data Scientist, Defense Threat Reduction Agency

To combat hostile cyber actors, military leaders at all echelons must understand the attack vectors used by cyber threat actors. The best way to truly understand these vectors is to become familiar with the tools a hostile actor uses when executing an offensive or reconnaissance cyber mission.

Despite the gravity of a very real threat to our network infrastructure, there are currently no standards for service members to follow to ensure they are "cyber conscious." As a result, we propose six cyber functions to serve as foundational areas to transform the military's cyber culture and enhance "unit cyber fitness," a readiness achieved by mastering levels of performance and standards, such as the Army Cyber Fitness Test (ACFT).

The six events of the Cyber Army Combat Fitness Test are Securing a Machine, Securing Data, Securing Network Traffic, Concealing Network Traffic, Understanding Social Engineering, and Managing Location Data. They include a baseline minimum standard—which is defensive by nature—and an advanced maximum standard that goes beyond simple cybersecurity and ventures into the realm of understanding actions taken by malicious actors in cyberspace. It is important to note unauthorized access to a network is illegal, and several of the tasks required to max the Cyber ACFT will require users to provide or establish their own target and/or attacking device.

EVENT 1: SECURING A MACHINE

MINIMUM - APPLY STRONG COMPUTER PHYSICAL SECURITY MEASURES.

We all know you should never leave your computer unattended in a public space, but there are additional measures you can take to secure access to your computer. This includes using separate administrator and user accounts, establishing strong passwords, and enabling good screen-lock settings. Although creating unique and complex passwords for all your accounts may seem inconvenient and challenging, a strong password manager can drastically reduce the annoyance while simultaneously increasing security.

MAXIMUM - EMPLOY A VIRTUAL MACHINE.

A virtual machine is essentially a computer within a computer. It uses a segregated portion of your computer's hardware to sandbox the virtual machine from your operating system. This allows users to run any operating system (i.e., Windows, Mac, Linux, etc.) in a manner that minimizes the likelihood of spillage of information from the virtual machine to the user's original operating system, and vice versa. Cybersecurity professionals and ethical hackers often use a virtual machine to test scripts and to create a target and/or attacking device for practice. If you find yourself wanting to practice some of the maxing events later but have another device to target legally, a virtual machine is probably a good solution.

Photo provided by Adobe Stock

EVENT 2: SECURING DATA

MINIMUM - ENCRYPT DATA.

Text encryption or other types of data inside an image file is known as steganography. There are many known vulnerabilities associated with basic password protection for files. File encryption may require a subscription or third-party software and regular maintenance. Using steganography adds an additional layer of protection for free. You can encrypt your data with a number of open-source software tools.

MAXIMUM - CRACK INTO A PASSWORD PROTECTED FILE.

A password-protected file is only as good as the password. To demonstrate the importance of selecting strong passwords and to develop an understanding of why certain criteria creates stronger passwords, you can create and hack into your own password-protected files.

Passwords usually are not stored as plaintext. They are stored as a hash, a unique combination of characters generated by a one-way function.[01] When you enter a password, the system checks if the hash of your entered text matches the stored hash of the true password. Salting involves adding characters to a password prior to hashing it, such that two identical passwords will have different salted hash values — thus, making them appear to be two different passwords. To crack passwords, hackers use a number of tools such as rainbow tables[02], dictionaries[03], and social engineering.


Photo provided by Adobe Stock

EVENT 3: SECURING NETWORK TRAFFIC

MINIMUM - ESTABLISH STRONG ROUTER SETTINGS.

The United States Special Operations Command (USSOCOM) provides a plethora of cybersecurity recommendations in Identity Management Smartcards.[04] After following USSOCOM Wi-Fi recommendations, you should also configure a firewall. Learn more about firewalls from InfoSec Institute.[05]

MAXIMUM - IDENTIFY/TRACE ABNORMAL NETWORK TRAFFIC.

When you go on the internet, your computer sends and receives network packets, small segments of data that form the totality of the information shared.[06] You can view all these packets using a packet sniffer—or protocol analyzer—that can help identify abnormal or suspicious network traffic Open-source packet analysis tools are well documented and offers useful tutorials.[07] They offer a user interface that provides an intuitive design to reduce the learning curve.


Photo provided by Adobe Stock

EVENT 4: CONCEALING NETWORK TRAFFIC

MINIMUM - EMPLOY A VIRTUAL PRIVATE NETWORK (VPN).

Survey data from NordVPN demonstrates an increasing trend in VPN use within the United States following the COVID-19 pandemic, with approximately one third of Americans choosing to use a personal VPN.[08] If you are in the subset of Americans who does not know what a VPN is, you can get more information about them from cyber security and tech news and research websites, such as cybernews.com.[09] A VPN essentially masks your IP address as you navigate the web and is one of the simplest tools you can employ to increase your security online.

MAXIMUM - ESTABLISH A CUSTOM PROXY CHAIN.

A proxy chain is a chain of proxy servers used to achieve the similar goal of masking the originating IP address. These are much more advanced than simply hitting 'connect' and are generally easiest to implement by using proxy chain tools.[10] Understanding the tools required to create a proxy chain will introduce users to some of the foundational knowledge hackers have.

Photo provided by Adobe Stock

EVENT 5: UNDERSTANDING SOCIAL ENGINEERING

MINIMUM - IDENTIFY SOCIAL ENGINEERING ATTEMPTS.

Social engineering involves manipulating people and exploiting their weaknesses. Social engineering aids bad actors during their attempts to gain access to systems or to gain information about their target. It can be done in any domain and is not limited to cyberspace. All basic users should be familiar with elicitation, shoulder surfing, baiting, tailgating, and phishing (and its variants).

MAXIMUM - ESTABLISH A REVERSE TCP CONNECTION.

A reverse TCP attack navigates around a firewall by socially engineering a target user into initiating a TCP connection (rather than the attacker initiating the connection). Once a user initiates the connection, an attacker can employ several malicious cyber activities. Kali Linux Metasploit is a common tool used to accomplish this task. Executing a reverse TCP connection without the knowledge and authorization of the target user is illegal. Maxing Event 5 will require you to establish a target and Linux attacker machine on your private network.

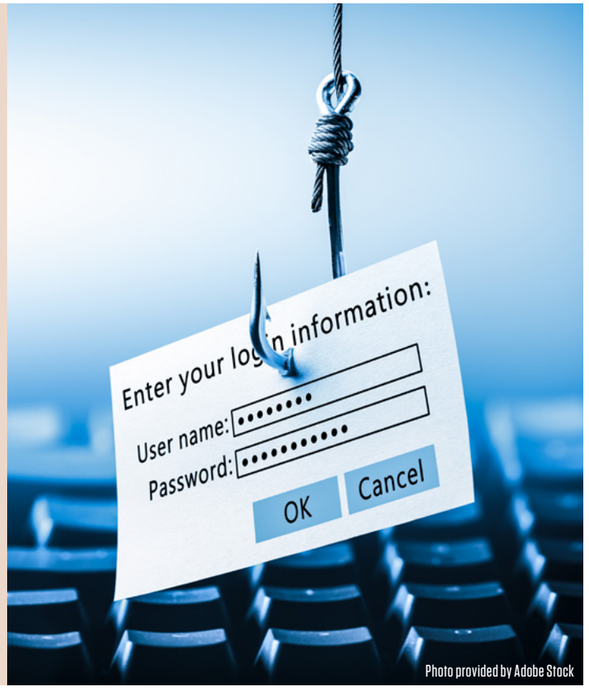


Photo provided by Adobe Stock

EVENT 6: MANAGING LOCATION DATA

MINIMUM - TURN OFF GEOTAGGING AND LOCATION SHARING.

Geotagging is the process applied to digital media that results in location and other data being applied as metadata to the media. You can turn off photo geotagging and location sharing settings on your devices by following the USSOCOM Identity Management Smartcards for your types of devices found under "Phones and Hardware." Check out the "Smartphone EXIF Removal" smartcard for more information on geotagging.[11]

MAXIMUM - GEOLOCATE A SPECIFIC DEVICE.

Although geolocating a specific device is no simple feat, you can make yourself an exceptionally hard target by minimizing your digital exposure and familiarizing yourself with the tools needed to track a device in time and space. It may be easiest to hack the password for a user's 'Find My Phone' functionality (check your device's Find Me function to see how well you locked down your location sharing). However, you can obtain geospatial information for a specific device using secured ingress platforms and some high-quality social engineering. Learn how from Loi Liang Yang.[12]


Photo provided by Adobe Stock

CONCLUSION

The minimum standards for the Cyber ACFT represent measures that are absolutely mission essential in protecting the joint force from hostile cyber actors. Although the minimum standards are not the only cyber events to be aware of, they provide a baseline for establishing a cyber-conscious foundation. As you progress through the events, you will find maxing the Cyber ACFT is quite difficult, as it demands a deeper understanding of networks and the tools available to malicious actors.

01 Ghosh, Riku, "Want to Know What is Hashing inCybersecurity? The Ultimate Guide," https://www.emeritus.org/blog/cybersecurity-what-is-hashing-in-cybersecurity/.

02 GeeksforGeeks, "Understanding Rainbow Table Attack," 10 February 2023, https://www.geeksforgeeks.org/understanding-rainbow-table-attack/.

03 GeeksforGeeks, "What isa Dictionary Attack," 4 July 2022, https://www.geeksforgeeks.org/what-is-a-dictionary-attack/.

04 United States Special Operations Command, "USASOC Identity Management," 14 November 2023, https: /www.soc.mil/IdM/publications/IdMpubs.html.

05 Gonzalez, Bianca, "Howto Configure a Network Firewall: Walkthrough," 13 March 2023, https://resources.infosecinstitute.com/topics/network-security-101/configure-network-firewall/.

06 Cloudflare, "What isa Packet?" https://www.cloudflare.com/learning/network-layer/what-is-a-packet/.

07 WireShark, "Wireshark Training," https: /www.wireshark.org/docs/.

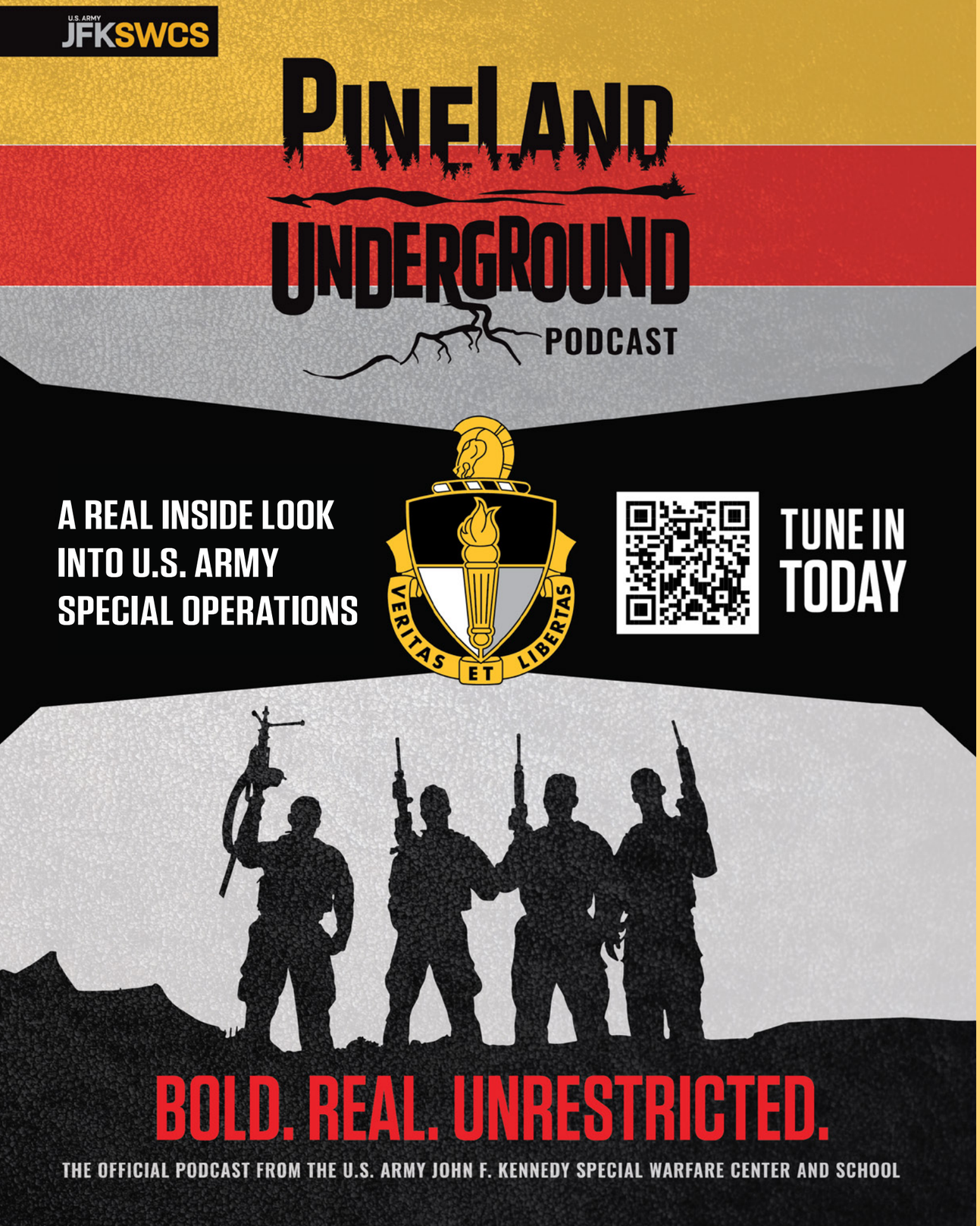
08 Globytė, Ema, "NordVPNSurvey Shows: AThird of Americans Use a VPN," 28June 2023, https://nordvpn.com/blog/nordvpn-usage-surveyus/#:~:text=Two%20in%20three%20people%20(66.8,25%20and%2044%20years%20old.

09 Jankevičiūtė, Dovilė, "HowTo Set Up a VPN," 15 November 2023, https://cybernews.com/what-is-vpn/how-to-set-up-a-vpn/.

10 Kali Linux, "Proxychains-Ng: Packages and Binaries," https://www.kali.org/tools/proxychains-ng/.

11 United States Special Operations Command, "USASOC Identity Management," 14 November 2023, https://www.soc.mil/IdM/publications/IdMpubs.html.

12 Yang, Loi Liang, "Geolocation Tracking Via HTML5 and JavaScript. Track APhone's Location Over the Internet." https://www.youtube.com/watch?v=0kbvwUf5FLo&ab_channel=LoiLiangYang.



VOICES OF ARSOF

"HOW DO YOU SEE THE ARMY OPERATIONALIZING SOF•SPACE•CYBER TRIAD IN 10 YEARS?"

This edition of Special Warfare Journal focuses on the SOF-Space-Cyber Triad. As part of the overall theme for 2024 "How ARSOF Fights," we asked members from the academic and DoD communities where they see the Triad going in the next 10 years, and these are their responses:

"The Army's approach to ensuring Electromagnetic Spectrum (EMS) superiority on future battlefields require prioritizing the integration of low-tech tactical "soft sciences" with the high-tech "hard sciences" of space and cyber. Operationalizing the Triad requires the Army to enhance interoperability between advanced technologies and capabilities to achieve strategic flexibility while maintaining global partnerships. SOF's culture of decentralized combat operations can be enhanced by integrating space and cyber capabilities at the tactical edge. Supporting tactical and operational elements with improved communications, enhanced ISR, early warning systems, and EW capabilities will ensure the Army can operate in complex environments and counter any emerging threat while maintaining strategic advantage."

Chief Warrant Officer 4 Balwinder 'Bobby' Singh, Electromagnetic Warfare Branch Chief, USASOC

"The future of Army space comprises a plethora of small, highly mobile, and capable units operating in contested environments. Convergence of space, cyber, and SOF capabilities will provide scalable, economical, and feasible options for our combatant commanders and policy makers. Operating in the corps deep and extended deep, future triad assets will continue to enable freedom of movement and maneuver across multi-domain and full spectrum operations by interdicting adversary use of space-based capabilities. The Army of 2030 and beyond employs the unique interoperability of all three components across complex battlefield geometry in order to ensure success."

Capt. Paulina R. Montgomery, Strategic Initiatives Chief, 1st Space Brigade

"I believe that the Triad will replace COIN, CT, and FID as the main focus of SOCOM in the next 10 years. As a former SOF officer, now an Orbital Warfare Space Force officer, I see our adversaries engaging in unconventional warfare on-orbit by utilizing the Triad to their advantage. We are being targeted via space, cyber and electromagnetic warfare capabilities daily. The Triad's importance will grow in the future because our enemies value unique operations to achieve their goals rather than committing a conventional force. I also believe that the cyber element will encompass all CEMA activities, including EW, spectrum defense, and non-kinetic weapons. SOF is in a position to lead the Triad due to their ability to provide access, operational oversight, and force multiplying operations. SOCOM proves the SOF truth "that humans are more important than hardware" by using space and CEMA as tools in SOF missions. Bottom line, the Triad is the future."

Lt. Col. Mark D. "Nix" Natale, Director of the Joint Commercial Space Operations Center, U.S. Space Force

"I see the Army operationalizing the Triad in three parts: First, SOF needs internal capacity for cyber and space operations by increasing the number of Soldiers trained for Brighton-level cyber tasks and who understand basic space capabilities through the Space Cadre Course. Second, persistent relationships between SOF, Space, and Cyber commanders need to foster integrated training strategies, operational initiatives, and CONUS and OCONUS collaboration. Finally, the Triad enterprise needs to issue the types of survey equipment, remote access devices, or space-enabling kits needed for SOF formations to support space and cyber operations. In the end, the key to effective Triad operations is using SOF's global access and placement to enable tactical space and cyber capabilities, augmenting Army sensing and targeting of enemy vulnerabilities across all domains."

Maj. Philip Ficken, USASOC

"In the next 10 years, I see the Army operationalizing the Triad by creating billets for cyber and space experts within the special operations team (SOT) A/B structure. The SOT A/Bs are currently manned by signals intelligence specialists, and the addition of cyber and space personnel is a natural set of skillsets that enhance the full-spectrum, multi-domain operational capabilities of SOF. Furthermore, this integration will allow SOT A/Bs to leverage advanced cyber techniques, employ electronic warfare tools, and exploit real-time satellite data to enable SOF teams' execution of their operational priorities. Ultimately, the more robust SOT A/B construct will help ensure SOF successes in austere, complex, and contested environments."

Capt. Kurt Wilson, U.S. Army Cyber Center of Excellence